UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escuela Técnica Superior de Ingeniería Informática
Universitat Politècnica de València

PLAN DE AUDITORÍA DEL DESARROLLO DE APLICACIONES EN UNA EMPRESA INFORMÁTICA

Proyecto Final de Carrera

INGENIERÍA TÉCNICA DE INFORMÁTICA DE GESTIÓN

Autor: Mª AMPARO AGUILAR ESCOBÍ

Director: JOSÉ MARÍA TORRALBA MARTÍNEZ

Valencia, Junio 2012

Tabla de contenidos

1. Introducción

1.1 Ámbito de desarrollo del Proyecto

En los últimos tiempos el ejercicio en las actividades de auditoría y control en tecnologías informáticas, ha auspiciado un desarrollo más que acelerado de todas las demás actividades inmersas en la economía de un país. Esto da pie a pensar que las tareas realizadas por ellas han de ser igualmente auditadas. El propósito a alcanzar por una organización que contrata la auditoría de cualquier parte de sus SI es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura. En la actualidad, los temas relativos a la auditoría informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas, representando su principal ventaja estratégica, por lo que estas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles. La gerencia, debe establecer un sistema de control interno adecuado, y tal sistema debe soportar debidamente los procesos del negocio. El proceso de la auditoría requiere una gran recopilación de datos, realización de pruebas y comprobación de requisitos de control.

En los próximos capítulos pretendemos, primero mostrar una visión global de la auditoría para posteriormente centrarnos en la auditoría que nos interesa en este proyecto, la auditoría de los Sistemas de Información, concretamente en el desarrollo de aplicaciones informáticas, explicaremos las características que tiene la organización a la que le vamos a realizar el plan de auditoría junto con el propio plan que desarrollaremos para que el auditor puede desempeñar su función correctamente y detectar así las posibles anomalías, errores que pueda estar realizando en el departamento en cuestión, de este modo el auditor puede ayudar a la mejora de la organización en sí. Pasamos pues a hacer una pequeña introducción de a la auditoría en las organizaciones.

2. La Auditoría de las Tecnologías de la Información y la Comunicación (TIC) y los Sistemas de Información (SI)

2.1 Introducción a la Auditoría en las organizaciones

2.1.1 Breve reseña de la Historia de la Auditoría

Si profundizamos a lo largo de los primeros antecedentes de la auditoría son casi tan antiguos como la propia historia de la humanidad, ya que la profesión auditora, en cuanto actividad de control de la actividad económico financiera, surge en el momento en que la propiedad de los recursos financieros o fuentes de financiación y la responsabilidad de la asignación de los mismos a usos productivos no se encuentran en manos de la misma persona, es decir cuando se produce un deslinde entre la propiedad y la gestión. Sin embargo la auditoría, como se conoce hoy en día, no tiene su origen hasta la revolución industrial del siglo XVIII en Inglaterra, o al menos es en este país donde se encuentran los primeros antecedentes, con la aparición de las primeras sociedades anónimas, donde los accionistas, exigen la garantía de que sus fondos han sido gestionados de manera adecuada, y de que las cuentas que les presentan los administradores son ciertas y fidedignas.
Posteriormente la profesión auditora ha continuado extendiéndose a otros países como Estados Unidos, que se configura como la nación más avanzada en el desarrollo de la profesión, mientras que en países como España, no fue oficialmente reconocida hasta la promulgación de la Ley de Auditoría del año 1988.

Podemos distinguir tres etapas o fases en las que se ha ido desarrollando la auditoría:

- “Edad Antigua”
- “Edad Media-Moderna”

- “Edad Contemporánea”

Pasamos a explicarlas:

- Edad Antigua

En los pueblos primitivos al no existir una actividad comercial intensa no fue preciso un sistema de información complejo, de forma que se aplicaba el recuento como un sistema de control válido y efectivo. Es en el estamento político donde se afirma que aparece el término auditor, persona que efectuaba los controles de los gastos e ingresos que se producían en el Estado, dichos controles se realizaban única y exclusivamente escuchando (ya que auditor procede del término “audire” oír) las relaciones de las cuentas que las personas encargadas del manejo de estas comentaban de viva voz.

Posteriormente se encuentran vestigios también de la función auditora, como actividad de supervisión, en las culturas griega y romana.

- Edad Media-Moderna

A consecuencia del auge del comercio italiano con los países de Oriente y Occidente nacen las sociedades mercantiles colectivas y de participación, dando lugar a la necesidad de contar con un sistema de registro e información de las operaciones contables. Así el desarrollo de la contabilidad originó que fuese Italia el país en el que nace la figura del revisor contable, de forma que en Venecia se pagaban los servicios al revisor en función del número e importancia de los errores y fraudes descubiertos. De manera que en los comienzos de la labor de auditora su función fue principalmente la de descubrir fraudes, sobre todo en la gestión de los fondos públicos y en el comercio.

En el año 1310 ya se realizaban funciones de auditoría en Inglaterra a través de los “Consejos Londinenses”. Más tarde, en 1581, se funda en Italia la asociación de revisores contables “Il colegio dei Raxonati”. En París en 1640 aparece el “Tribunal de Cuentas”, y en 1658 se crea en Milán y Bolonia la “Academia dei Ragioneri”. Ya en el siglo XVIII, en el año 1739, se constituye en Milán el segundo “Colegio de Revisores Contables”, cuyo propósito primordial es detectar errores e irregularidades en la llevanza de la contabilidad.

- Edad Contemporánea

La auditoría no nace como profesión, como actualmente se conoce, hasta el período de la revolución industrial y la aparición de las sociedades anónimas en las que se desliga la propiedad del capital de los gerentes de las mismas, y se encarga a un profesional independiente la revisión de la labor encomendada a los administradores. De estos técnicos especializados en la revisión de la contabilidad surge la profesión de auditor o accountant, que se potencia en 1854 con la creación del “Institute of Chartered Accountants of Scotland”.

La profesión auditora es reconocida, en Gran Bretaña, por la Ley de Sociedades de 1862, posteriormente, en 1879, a través de la “Companies Act” se obliga a las entidades bancarias a someter sus cuentas a auditoría, y a las sociedades mercantiles a la llevanza de una contabilidad ordenada. En 1880, la reina Victoria les confiere a los auditores de Inglaterra y Gales el derecho a llamarse “Chartered Accountants” y ese mismo año nace el “Institute of Chartered Accountants of England and Wales” que continua en la actualidad.

A partir de comienzos del siglo XX se intensifica la constitución de las empresas industriales y comerciales como sociedades anónimas, y esa transformación lleva aparejada que la auditoría se convierta en obligatoria, con el fin de garantizar la transparencia del tráfico mercantil de los países. Debido a la influencia inglesa se va a desarrollar y consolidar la auditoría en Estados Unidos, surgiendo en el año 1887 la primera asociación americana de auditores la “American Association of Public Accountants (AAPA)”.

Posteriormente en 1896, en el Estado de Nueva York, aparece la primera ley que regula la profesión del auditor o contador público, tal y como se conoce al auditor en América, mediante la “Act to regulate the Profesión of Public Accountants” que otorga el título de “Certified Public Accountant” a las personas que logran superar una prueba de aptitud.

En 1916, la AAPA pasa a denominarse “Institute of Public Accountants (IPA)” constando de 1.150 miembros. Un año más tarde se cambia el nombre por el de “American Institute of Accountants (AIA)” y, a solicitud de la Comisión Federal de Comercio de Estados Unidos (Federal Trade Commission), elabora

un documento, el “Uniform Accounting”, que constituye el primer conjunto de estándares sobre procedimientos de auditoría de balances, que fueron publicados bajo el título de “Aproved Methods for the Preparation of Balance Sheet Statements”. Para corregir sus deficiencias, en 1922, el AIA lo revisó y publicó bajo el título de “Verification of Financial Statements”.

No obstante, lo que supuso un giro radical en la elaboración de la información financiera fue la crisis económica de 1929, momento a partir del cual se trabaja para paliar la falta de transparencia y de armonización de los principios contables, gracias a la iniciativa de la AIA y la Bolsa de Nueva York, y se acuña la expresión de “generally accepted accounting principles (GAAP)”, principios de contabilidad generalmente aceptados.

Cuatro años más tarde, en 1933, la Comisión Federal del Congreso Norteamericano crea la “Securities and Exchange Commission (SEC)”, órgano regulador y controlador de la bolsa a cuyo cargo corre el reconocimiento de los principios y normas de auditoría a aplicar, y se produce la publicación de dos leyes, las “Securities Acts” de 1933 y 1934; en las que se exigía que todas las sociedades que cotizaban en bolsa debían acompañar sus estados financieros de un informe de auditoría.

En 1939, el AIA crea el “Committee on Auditing Procedure (CAP)” que a su vez se subdivide en tres comisiones:

- La “Accounting Research Division” (ARS) dedicada al estudio e investigación de la contabilidad.
- El “Accounting Principles Board” (APB) dedicado a la emisión de principios de contabilidad.
- El “Accounting Research Bulletin” (ARB) para la publicación de las investigaciones en materia de contabilidad.

La AIA pasa en el año 1957 a denominarse “American Institute of Certified Public Accountants (AICPA)” y este nuevo organismo se encarga de la emisión de los “Statements on Auditing Procedure” (SAP), conjunto de procedimientos de auditoría que desarrollan y profundizan en la profesión auditora. En 1972, se

realizan los “Statements on Auditing Standards” (SAS) que recogen normas y procedimientos de auditoría y un año después nace el “Financial Accounting Standard Board” (FASB) órgano encargado de la elaboración y emisión de principios de contabilidad, siendo en la actualidad la principal fuente normativa contable en los Estados Unidos de Norteamérica.

Más adelante, a partir de los años 40 y 50 el objetivo de la auditoría ya no es la detección de errores y fraudes mediante la revisión de la totalidad de los registros contables, sino que el trabajo de auditoría sufre cambios sustanciales, reforzándose los siguientes cometidos:

- Se pone un mayor énfasis en la revisión y evaluación de los sistemas de control interno.
- Se centran los esfuerzos en las partidas que componen la Cuenta de Resultados.
- Se reduce el tiempo empleado en el trabajo de auditoría.
- Se extrapola parte del trabajo realizado en momentos anteriores al cierre del ejercicio contable, apareciendo así los conceptos de “auditoría preliminar” y “auditoría final”.

El auditor ya no certifica sobre la información revisada sino que emite una opinión profesional sobre la representatividad de una información financiera o contable.

La Auditoría en España

Hasta fechas muy cercanas la auditoría en nuestro país no ha tenido un gran desarrollo ni a nivel legislativo ni en la práctica en la gestión de los negocios.

Podemos decir que la auditoría empezó a practicarse más reiteradamente en las empresas privadas a partir de 1970, hasta este momento la auditoría era únicamente conocida en las empresas que tenían participación de capital extranjero. Los países de origen de estas inversiones eran países como Estado Unido, Canadá, Inglaterra… donde la legislación les exige que tanto las empresas que tienen dentro del país como de las inversiones que realizan en el extranjero estén auditadas por auditores reconocidos en estos países que estamos haciendo mención.

Como decíamos anteriormente es a partir de 1970 cuando las empresas españolas empiezan a contratar, de forma esporádica, los servicios de auditoría, que en la mayoría de los casos eran impuestos con motivo de negociaciones de compra venta de sociedades, concesiones de créditos bancarios, exigencias de accionistas disidentes…
Más adelante con la integración de España en la Unión Europea cobra mucha más importancia la transparencia informativa económica contable, por lo que se promueve más el desarrollo de la auditoría en España teniendo un mejor conocimiento de situación económica, patrimonial y financiera de las empresas.

2.1.2 La necesidad de la Auditoría

Las auditorías nacen para (Apuntes de la Asignatura: Auditoría de los Sistemas de Información (ASI), 2009-10, Tema 2: Introducción a la Auditoria, transparencia 6):

- Ofrecer la seguridad a los propietarios de las empresas de la fiabilidad de los estados financieros.
- Ofrecer la seguridad a otros posibles usuarios: acreedores, Hacienda...
- Cuando se realiza una venta o cambio de titularidad
- Por obligación legal

2.1.3 Definiciones

Definición de Auditoría: “la investigación, consulta, revisión, verificación, comprobación y obtención de evidencia, desde una posición de independencia, sobre la documentación e información de una organización, realizadas por un profesional -el auditor- designado para desempeñar tales funciones” (Apuntes de ASI Curso: 2009-10).

NORMA AFNOR (Asociación Francesa de Normalización) X50-109:

“Examen metódico de una situación relativa a un producto, proceso, organización, en materia de calidad, realizado en cooperación con los

interesados, a fin de verificar la concordancia de la realidad con lo preestablecido, y la adecuación al objetivo buscado.”

Normas españolas

1) **LEY 19/1988 DE AUDITORÍA DE CUENTAS, de España:**

"... la actividad que, mediante la utilización de determinadas técnicas de revisión, tiene por objeto la emisión de un informe acerca de la fiabilidad de los documentos contables auditados; delimitándose, pues, a la mera comprobación de que los saldos que figuran en sus anotaciones contables concuerdan con los ofrecidos en el balance y en la cuenta de resultados,...".

2) **REAL DECRETO 1636/1990**

"1.- Se entenderá por auditoría de cuentas la actividad, realizada por una persona cualificada e independiente, consistente en analizar, mediante la utilización de las técnicas de revisión y verificación idóneas, la información económico-financiera deducida de los documentos contables examinados, y que tiene por objeto la emisión de un informe dirigido a poner de manifiesto su opinión responsable sobre la fiabilidad de la citada información, a fin de que se pueda conocer y valorar dicha información por terceros".

2.1.3.1 Puntos en común de las definiciones

Los puntos en común de las definiciones comentadas anteriormente son:

- La realización de un examen ordenado y planificado.
- La comprobación de la calidad de lo examinado.
- La verificación de la fiabilidad de lo examinado en cuanto a los hechos reales que refleja.
- La obligación de informar a terceros con una opinión fundada.

2.1.4 Los objetivos de la Auditoría

Los objetivos de la Auditoría son (Apuntes de ASI, 2009-10, Tema 2: Introducción a la Auditoria, transparencia 7):

- Informar sobre la fidelidad y razonabilidad de la situación de la empresa.
- Reflejar la imagen de la empresa.
- Descubrir fraudes o situaciones anómalas (errores).
- La responsabilidad de la gestión corresponde a la empresa.
- El auditor no es responsable de la preparación de la documentación revisada.
- El auditor podrá realizar sugerencias constructivas.

2.1.5 Diferentes clases y tipos de Auditoría

2.1.5.1 Diferentes tipos de Auditoría

- Auditoría Contable.
- Auditoría Financiera.
- Auditoría de Gestión (que comprende las dos anteriores)
- Auditoría de los Sistemas de Información.

2.1.5.2 Diferentes clases de Auditoría

Criterio 1.- Según el **sujeto** que la efectúa puede ser (Apuntes de ASI, 2009-10, Tema 2: Introducción a la Auditoria, transparencia 14):

- Auditoría Interna:

La Auditoría Interna es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de la

misma. Estos informes son de circulación interna y no tienen trascendencia a terceros.
Las Auditorías Internas son hechas por personal de la empresa. Un auditor interno tiene a su cargo la evaluación permanente del control de las transacciones y operaciones y se preocupa de sugerir el mejoramiento de los métodos y procedimientos de control interno que redunden en una operación más eficiente y eficaz.
Cuando la Auditoría está dirigida por Auditores Públicos profesionales independientes, la opinión de un experto desinteresado e imparcial constituye una ventaja definida para la empresa y una garantía de protección para los intereses de los accionistas, los acreedores y el Público.

La imparcialidad e independencia absolutas no son posibles en el caso del auditor interno, puesto que no puede divorciarse completamente de la influencia de la alta administración, y aunque mantenga una actitud independiente, como debe ser, esta puede ser cuestionada ante los ojos de terceros. Por esto se puede afirmar que el Auditor no solamente debe ser independiente, sino parecerlo para así obtener la confianza del Público.

La Auditoría Interna es un servicio que reporta al más alto nivel de la dirección de la organización y tiene características de función asesora de control, por tanto no puede ni debe tener autoridad de línea sobre ningún empleado de la empresa, a excepción de los que forman parte de la oficina de Auditoría Interna, ni debe en modo alguno involucrarse o comprometerse con las operaciones de los sistemas de la empresa, pues su función es evaluar y opinar sobre los mismos, para que la alta dirección toma las medidas necesarias para su mejor funcionamiento.
La Auditoría Interna solo interviene en las operaciones y decisiones propias de su oficina, pero nunca en las operaciones y decisiones de la organización a la cual presta sus servicios, pues como se dijo es una función asesora.

- Auditoría Externa:

Aplicando el concepto general, se puede decir que la Auditoría Externa es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Auditor Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

El dictamen u opinión independiente tiene trascendencia a terceros, pues da plena validez a la información generada por el sistema ya que se produce bajo la figura de la Fe Pública, que obliga a los mismos a tener plena credibilidad en la información examinada.

La Auditoría Externa examina y evalúa cualquiera de los sistemas de información de una organización y emite una opinión independiente sobre los mismos, pero las empresas generalmente requieren de la evaluación de su sistema de información financiero en forma independiente para otorgarle validez ante los usuarios del producto de este, por lo cual tradicionalmente se ha asociado el término Auditoría Externa a Auditoría de Estados Financieros, lo cual como se observa no es totalmente equivalente, pues puede existir Auditoría Externa del Sistema de Información Tributario, Auditoría Externa del Sistema de Información Administrativo, Auditoría Externa del Sistema de Información Automático, etc.

La Auditoría Externa o Independiente tiene por objeto averiguar la razonabilidad, integridad y autenticidad de los estados, expedientes y documentos y toda aquella información producida por los sistemas de la organización.

Una Auditoría Externa se lleva a cabo cuando se tiene la intención de publicar el producto del sistema de información examinado con el fin de acompañar al mismo una opinión independiente que le dé autenticidad y permita a los usuarios de dicha información tomar decisiones confiando en las declaraciones del Auditor.

Una Auditoría debe hacerla una persona o firma independiente de capacidad profesional reconocida. Esta persona o firma debe ser capaz de ofrecer una opinión imparcial y profesionalmente experta acerca de los resultados de Auditoría, basándose en el hecho de que su opinión ha de acompañar el informe presentado al término del examen y concediendo que pueda expresarse una opinión basada en la veracidad de los documentos y de los estados financieros y en que no se imponga restricciones al auditor en su trabajo de investigación.

Bajo cualquier circunstancia, un Auditor profesional acertado se distingue por una combinación de un conocimiento completo de los principios y procedimientos contables, juicio certero, estudios profesionales adecuados y una receptividad mental imparcial y razonable.

Diferencias entre Auditoría Interna y Auditoría Externa

- Según (Apuntes de ASI, 2009-10, Tema 2: Introducción a la Auditoria, transparencia 40) Las diferencias entre la auditoría interna y la auditoría externa aparecen en el cuadro 2.1.5.2:

AUDITORIA INTERNA	AUDITORIA EXTERNA
- El sujeto que realiza la auditoría pertenece a la organización auditada. - Independencia limitada. - Responsabilidad del sujeto que realiza la auditoría es de tipo laboral. - El objetivo de la auditoría es el examen de la gestión. - El informe emitido es un informe con recomendaciones para la gerencia. - El uso del informe está restringido al ámbito de la propia empresa.	- El sujeto que realiza la auditoría es un profesional independiente de la organización auditada. - Independencia total. - Responsabilidad del sujeto que realiza la auditoría es de tipo profesional, que puede llegar a ser penal. - El objetivo es el examen de las cuentas anuales para determinar su fiabilidad y calidad. - El informe emitido además de ir dirigido a la gerencia, está dirigido también a terceros. - El uso de informe trasciende de la propia empresa.

2.1.5.2 Cuadro resumen de las diferencias entre auditoría interna y auditoría externa.

Criterio 2.- Dependiendo de su **contenido** y **fines**:

- De gestión
- Organizativa
- Operativa
- Financiera/ Contable
- **Informática / Sistemas de Información**

Criterio 3.- Por su **amplitud**:

- Total: Se realiza a toda la organización
- Parcial: Se realiza a aquellos departamentos específicos que solicite la organización

Criterio 4.- Por su **frecuencia**:

- Permanente: La organización tiene auditorías de una forma seguida y continuada durante toda su vida como tal.
- Ocasional: La organización solicita de forma esporádica la realización de una auditoría.

2.1.6 Beneficiarios de la Auditoría

En la Auditoría Interna, es la propia empresa y todos los órganos de gobierno y ejecutivos.

En la Auditoría externa, son accionistas o socios, consejeros y ejecutivos. También pueden ser proveedores, acreedores y otros inversores. Así como la Banca, la Bolsa o Hacienda Pública. Del mismo modo puede ser beneficiosa para los propios empleados de la empresa y/o otros organismos públicos e instituciones.

Una vez explicada a grandes rasgos la auditoría en sí, contexto histórico, definiciones, tipos de auditoría pasamos a explicar el tipo de auditoría que

vamos a desarrollar más profundamente a lo largo del trabajo, Auditoría de los Sistemas de Información.

2.2 Auditoría de los Sistemas de Información

2.2.1 Introducción

La Auditoría de los Sistemas de Información ha adquirido entidad propia dentro de la Auditoría Empresarial, en la misma forma que los Sistemas de Información, han adquirido una posición fundamental dentro de la estrategia y operatividad de la empresa.

Este tipo de auditoría mantiene los conceptos básicos y las normas y reglas generales de la auditoría tradicional, pero ha desarrollado procedimientos y pruebas de cumplimiento adecuados a los entornos operativos específicos y complejos en los que se aplica. Por tanto, las técnicas y herramientas que debe utilizar el Auditor Informático son bastante más abundantes y especializadas.

Por otra parte, las innovaciones técnicas incorporadas en la Auditoría de los Sistemas de Información se han trasladado, en parte, a la auditoría tradicional, hasta el punto de que debemos distinguir entre:

- Auditoría de los Sistemas de Información, como la auditoría aplicada al examen de los Sistemas de Información, y
- Auditoría por medio del ordenador, como la auditoría tradicional que hace uso de los recursos informáticos para alcanzar sus objetivos.

Podemos concluir con esta introducción apuntando que la auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoría en informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que

además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

2.2.2 Perspectiva histórica

Pasamos a analizar la evolución que ha tenido la auditoría de los Sistemas de Información:

- Auditoría alrededor del ordenador: El auditor se limitaba a verificar la corrección de los datos de salida frente a los datos de entrada, ignorando la lógica y funcionamiento interno de las máquinas de proceso de datos.
- Auditoría del ordenador: Consiste fundamentalmente en la adaptación de los criterios para la evaluación del control interno, en los sistemas organizativos, financieros y contables, al centro de proceso de datos y, concretamente, a la sala del ordenador.
- Auditoría a través del ordenador: En este enfoque se estudia también el tratamiento lógico de la información a través de los programas y las aplicaciones que los integran.

2.2.3 Características de los sistemas mecanizados

Antes de centrarnos en la Auditoría de los Sistemas de Información nos gustaría especificar a qué nos referimos cuando hablamos de los sistemas mecanizados, informatizados…

En las organizaciones con el paso del tiempo han ido evolucionando y con ello introduciendo los sistemas de información por ello pasamos a explicar brevemente y de forma concisa cuales son los elementos fundamentales de un sistema de Proceso Electrónico de Datos para que quede claro a que nos referimos cuando hablamos de un sistema informatizado:

Un sistema informático dispone de un conjunto de recursos:

Técnicos: máquinas de proceso de datos, instalaciones de aporte de energía, consumibles, instalaciones de acondicionamiento climático, etc.

Personales: personal empleado interno o externo, organización y gestión de personal y recursos, etc.

Financieros: presupuesto para el funcionamiento del sistema, presupuesto para los salarios del personal, amortizaciones, impuestos, etc.

Materiales: bienes inmuebles, material de oficina, vehículos de transporte, etc.

2.2.4 Definiciones de Auditoría de los Sistemas de Información

Norma ANSI N45.2.10.1973:

“Actividad para determinar por medio de la investigación, la adecuación de y la adhesión a, los procedimientos establecidos, instrucciones, especificaciones, códigos y estándares, u otros requisitos aplicables contractuales o de licencia, así como la eficacia de su implantación.”

P. van der Ghinst - CEGOS.

“Conjunto de técnicas y actividades destinadas a analizar, evaluar, verificar y recomendar sobre el control, la planificación, la adecuación, eficacia y seguridad de la función informática de la Empresa.”

“Examen discontinuo de un sistema informático, o del servicio informático, a petición de su dirección para mejorar la calidad, la seguridad y la eficacia.”

Acha Iturmendi J.J. Auditoría Informática en la Empresa:

“Conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa, y para conseguir la eficiencia exigida en el marco de la organización correspondiente.”

Alonso Rivas G. Auditoría Informática:

“Es un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema que resultan auditados.

Weber R.“EDP Auditing. Conceptual Foundations and Practice”:

“Es el proceso de reunir y evaluar evidencia para determinar si un sistema informático protege su patrimonio, mantiene la integridad de los datos, alcanza los objetivos de la organización con efectividad, y consume los recursos con eficiencia.”

2.2.4.1 Los puntos en común de las definiciones

- Examen metódico: obtención de información, investigación y análisis planificados de acuerdo con los objetivos marcados de antemano.

- Verificación de Calidad del servicio informático o sistema informático: comprobación de que las actividades desarrolladas de ejecutan con eficiencia y que los recursos se utilizan en la forma adecuada, tal y como marcan las normas de calidad informática y organizativa generalmente aceptadas. También verificación de que se mantiene la integridad de la información.

- Verificación de Seguridad de la función informática: comprobación de que se aplican todas las normativas y procedimientos para mantener un nivel de seguridad adecuado del sistema o servicio en todos los aspectos.

- Obtención de evidencia: los resultados de las pruebas de cumplimiento y sustantivas que efectúa el Auditor le deben proporcionar la suficiente y necesaria evidencia para que pueda emitir una opinión fundada.

- La Auditoría de los Sistemas de Información ha adquirido entidad propia dentro de la Auditoría Empresarial, en la misma forma que los Sistemas de Información, han adquirido una posición fundamental dentro de la estrategia y operatividad de la empresa.

2.2.5 Objetivos de la Auditoría de los Sistemas de Información

FIABILIDAD + OPERATIVIDAD

Los **objetivos fundamentales** de las Auditorías de los Sistemas de Información son los siguientes:

- Objetivos de Protección del Patrimonio o Activos y Recursos: el patrimonio de una instalación informática incluye el conjunto de recursos materiales (máquinas, mobiliario, etc.), inmateriales (software, datos, etc.), inmuebles y recursos personales (empleados y organización). Debe existir un sistema de control interno que proteja este patrimonio de todas las posibles amenazas y riesgos.
- Objetivos de Integridad de los Datos: La integridad de los datos es el conjunto de condiciones que deben cumplir los datos: completitud,

robustez, pureza, y veracidad; para que puedan reflejar con fidelidad la situación económico-financiera y general y otros hechos relacionados con la empresa. El sistema de control interno debe tener mecanismos que vigilen constantemente el mantenimiento de esta integridad.

- Objetivos de Efectividad del Sistema: Un sistema de proceso de datos efectivo alcanza sus objetivos. En la evaluación de la efectividad hay que conocer las características y necesidades del usuario y los canales y procedimientos de decisión. La auditoría de la efectividad se puede realizar durante la fase de diseño del sistema, o cuando el sistema está en funcionamiento normal después de cierto tiempo.
- Objetivos de Eficiencia del Sistema: Un sistema de proceso de datos eficiente utiliza el mínimo de recursos para producir las salidas requeridas. Los recursos suelen ser escasos y caros en su operación, y además, deben estar compartidos entre diferentes procesos de datos. La eficiencia no debe medirse de forma aislada sino considerando el conjunto de procesos y el conjunto de recursos disponibles.

En definitiva el objetivo que se pretende alcanzar realizando auditorias consiste en apoyar a los miembros de la empresa en el desempeño de sus actividades, informar sobre la fidelidad y razonabilidad de la situación de la empresa y reflejar la imagen de la empresa. Para ello la Auditoría proporciona a la empresa: análisis, evaluaciones, recomendaciones, asesoría e información concerniente a las actividades revisadas.

Se plantean también como objetivos secundarios:

- Descubrir fraudes o situaciones anómalas (errores).
- La responsabilidad de la gestión corresponde a la empresa.
- El auditor no es responsable de la preparación de la documentación revisada.

2.2.6 Finalidad

Los fines de la auditoria son los aspectos bajo los cuales su objeto es observado. Podemos escribir los siguientes:

- Indagaciones y determinaciones sobre el estado patrimonial.
- Indagaciones y determinaciones sobre los estados financieros.

- Indagaciones y determinaciones sobre el estado reditual.
- Descubrir errores y fraudes.
- Prevenir los errores y fraudes.

Estudios generales sobre casos especiales, tales como:

- Exámenes de aspectos fiscales y legales.
- Examen para compra de una empresa (cesión patrimonial).
- Examen para la determinación de bases de criterios de prorrateo, entre otros.
- Los variadísimos fines de la Auditoría muestran, por si solos, la utilidad de esta técnica.

2.3 Resumen

En este capítulo lo que pretendemos es explicar de una forma clara y concisa lo que es la Auditoría en general, su evolución, sus pros y sus contras, los beneficiarios, los diferentes tipos de auditoría…para poder entender posteriores capítulos.

Por otro lado explicamos que es la Auditoría de los Sistemas de Información, variante que ha nacido posteriormente a causa de la evolución que han sufrido las organizaciones. Las organizaciones han ido evolucionando y con ello han ido informatizándose, mecanizándose por ello nació la necesidad no solo de controlar los periféricos en sí, sino también de cómo viaja la información a través de este, ya que la información es el elemento clave de toda organización. Este tipo de Auditoria será el caso de estudio de este proyecto, donde en capítulos posteriores realizaremos un Plan de Auditoria de una organización, donde analizaremos si la organización en cuestión controla, maneja de forma adecuada todos sus activos.

2.4 Bibliografía del capítulo 2

Asignatura: Auditoría de los Sistemas de Información, ETS de Ingeniería Informática de la UPV, Plan de Estudios de ITIG, Curso 2009-2010, http://www.inf.upv.es/webei/webETSIA/la_escuela/titulaciones/ITIG01/lista_optativas_con_info.php#ausi (Fecha de consulta: 06/06/2011)

http://www.monografias.com (Fecha de consulta: 26/05/2011)

http://www.eumed.net/cursecon/libreria/rgl-genaud/1i.htm (Fecha de consulta: 26/05/2011)

http://www.wikilearning.com/monografia/fundamentos_teoricos_de_la_auditoria_vinculados_a_la_calidad-antecedentes_historicos_de_la_auditoria/12675-1 (Fecha de consulta: 06/06/2011)

http://www.monografias.com/trabajos16/auditoria-de-informacion/auditoria-de-informacion.shtml (Fecha de consulta: 06/06/2011)

http://www.eumed.net/libros/2006a/jcmn/1c.htm (Fecha de consulta: 08/08/2011)

3. Organismos, certificaciones y normativas

Pasamos a hablar en este capítulo de los organismos, certificaciones y normativas que regulan las auditorías.

Con el paso del tiempo todo ha ido evolucionando y como no las auditorías también, lo que en un principio se realizaba para controlar el fraude sobre las cuentas de los más poderosos, ahora es requisito indispensable para que cualquier organización funcione correctamente. Debido al papel tan importante que juegan las auditorías en las organizaciones ha provocado la necesidad de que estas sean reguladas, y por ello se han formado organizaciones que proporcionan estudios, desarrollos y normativas, de la misma manera que dichas organizaciones son las encargadas de otorgar certificaciones para acreditar a los profesionales del sector.

Pasamos pues, a explicar algunos de estos organismos, certificaciones y normativas.

3.1 Organismos

3.1.1 ISACA (Information Systems Audit and Control Association)

ISACA nació en 1967, cuando un grupo reducido de personas, con trabajos muy similares relacionados con los controles en los sistemas de información, vieron la necesidad de construir una fuente donde estuviera centralizada toda la información necesaria y orientación en el campo, finalmente fue en 1969 cuando se formalizó.

Actualmente, en julio del 2011 los miembros que forman la ISACA son más de 95.000, se caracterizan por su gran diversidad. Dichos miembros viven y trabajan en más de 160 países y cubren una grandísima variedad de profesionales del sector de las TI (Tecnologías de Información).

Las actividades que realiza la ISACA son:

- Desarrollo y administración de cuatro certificados líderes en la industria:
    - Certified Information Systems Auditor (CISA)
    - Certified Information Security Manager (CISM)
    - Certified in the Governance of Enterprise IT (CGEIT)
    - Certified in Risk and Information System Control (CRISC)
- Patrocinadores técnicos y de gestión de conferencias en los cinco continentes, dichas conferencias se realizan cada año para garantizar que los profesionales tienen la educación necesaria para su buena formación, dichas conferencias son:
    - Congreso Mundial, celebrado cada año en una región geográfica.
    - Conferencias del equipo de Auditoría, Control y Seguridad (CACS), celebradas en los cinco continentes.
    - Semanas de entrenamiento, que se celebran en varios lugares.
    - Conferencia de las TI de Gestión de Riesgos y Cumplimiento (GRC IT).
    - Conferencia de la Gestión de Seguridad y Riesgo (ISRM), que se celebran en América del Norte, Europa y América Latina.
    - Formación COBIT (Control Objectives for Information and related Technology).
    - Revisión de Certificación del Curso.
    - E-Learning, incluyendo la publicación mensual de ISACA y Simposio y eventos.
- Desarrollo y actualizaciones seguidamente:
    - COBIT
    - ValIT (IT Value Delivery)
    - Garantía de IT Framework (ITAF)
    - Modelo de negocio de Seguridad de Información (BMIS).

A continuación mostramos el logotipo de este organismo en la figura 3.1:

3.1 Logotipo de Information Systems Audit and Control Association

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

3.1.2 ISACA-CV (Information Systems Audit and Control Association-Comunidad Valenciana)

ISACA-CV es el capítulo 182 de la ISACA, cuenta con 203 profesionales asociados, entre los cuales 117 son CISA, 34 CISM, 14 CGEIT y 6 CRISC. Dicho capítulo se constituyó en marzo del 2003. La mayoría de los asociados son auditores de sistemas de información, pero cuenta también con consultores, académicos, profesionales de la seguridad TIC, miembros de la Administración Pública y auditores internos. Entre ellos están representados tanto profesionales independientes como directivos y responsables de los Sistemas de Información de grandes empresas, representantes de cajas de ahorros y bancos, académicos de las principales universidades, y representantes de la administración pública.

El capítulo está abierto a todos los profesionales de la auditoría, la seguridad y la gestión de las TIC. Los objetivos de la asociación están fijados en sus estatutos.
www.**isaca**-**cv**.org/(Fecha de la consulta: 22/07/2011)

3.1.3 ITGI (IT Governance Institute)

ITGI se estableció en 1998 a causa del peligro cada vez más notable en las TI para conseguir el éxito de la empresa, ya que en muchas empresas su éxito depende de la capacidad de TI para permitir el logro de los objetivos de negocio establecidos. Moviéndonos en tal ambiente, en la gobernanza de la TI es tan importante un consejo y la disciplina de gestión como en el gobierno corporativo o de gobierno de la empresa. El gobierno de TI ayuda a asegurar

que TI soporta los objetivos de negocio, maximizar la inversión empresarial en TI, y gestiona adecuadamente los riesgos relacionados y oportunidades.
ITGI conduce la investigación sobre las prácticas mundiales y las percepciones de la gobernanza de la TI para la comunidad empresarial. ITGI tiene como objetivo ayudar a los líderes empresariales a entender cómo el gobierno eficaz puede que sea un éxito en el apoyo a la misión de la empresa y sus objetivos.

El IT Governance Institute (ITGI) existe para ayudar a los líderes de la organización en su responsabilidad de garantizar que TI esté alineada con el negocio y ofrecer valor, que sus recursos están debidamente asignados y mitigar en los riesgos que le pueden afectar a su organización.

A continuación mostramos el logotipo del organismo IT Governance Institute en la figura 3.2:

3.2 Logotipo del Instituto de Gobierno de las Tecnologías de Información

www.**itgi**.org (Fecha de la consulta: 23/07/2011)

3.1.4 IIA (The Institute of Internal Auditors)

El instituto de Auditores internos fue fundado en 1941, es una asociación profesional internacional con sede central en Altamonte Springs, Florida, EE.UU.
El IIA es la voz global de la profesión de auditoría interna, reconocido como el líder, principal impulsor y principal educador. Los miembros del instituto trabajan en la auditoría interna, gestión de riesgos, gestión, control interno, auditoría de tecnología de la información, educación y seguridad.

La misión del Instituto de Auditores Internos es proporcionar un liderazgo dinámico de la profesión global de auditoría interna.

Los profesionales que forman parte del instituto proporcionan los recursos para los recién llegados a la profesión de auditoría interna, así como para profesionales con experiencia que quieren promover la profesión y su papel en el éxito de una organización.

La Profesión del IIA proporciona una variedad de herramientas y consejos para la construcción de una amplia sabiduría acerca de la auditoría interna, tanto a nivel interno dentro de su organización y externamente a las partes interesadas.

A continuación mostramos el logotipo que utiliza este organismo en la figura 3.3:

3.3 Logotipo del instututo de auditores internos

http://www.theiia.org/ (Fecha de la consulta: 24/07/2011)

3.1.5 ISO (Organización Internacional de Normalización)

ISO es en el mundo el mayor desarrollador y editor de las normas internacionales.

ISO es una red de los institutos de normas nacionales de 162 países, un miembro por país, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema.

ISO es una organización no gubernamental que forma un puente entre los sectores público y privado. Por un lado, muchos de los institutos de sus miembros forman parte de la estructura gubernamental de sus países, o están obligados por su gobierno. Por otra parte, otros miembros tienen sus raíces únicamente en el sector privado, habiendo sido creada por las asociaciones nacionales de las asociaciones de la industria.

Por lo tanto, la norma ISO permite un consenso para llegar a soluciones que satisfagan tanto las necesidades de negocio y las necesidades más amplias de la sociedad.

A continuación mostramos el logotipo utilizado por este organismo en la figura 3.4:

3.4 Logotipo de la Organización Internacional de Normalización

http://www.iso.org/ (Fecha de la consulta: 26/07/2011)

3.1.6 Instituto de Auditores Internos de España

Una Asociación profesional sin ánimo de lucro, formalmente constituida en nuestro país al amparo de la Ley de Asociaciones, cuyo objetivo fundamental es el desarrollo de la Auditoría Interna y la profesión de auditor interno en España. El Instituto es miembro de TheInstitute of InternalAuditors, es una organización nacida en Estados Unidos en 1941 y que hoy agrupa a más de 160.000 profesionales en más de 120 países.

Asimismo pertenece a la EuropeanConfederation of Institutes of InternalAuditing (ECIIA) en la que se integran todos los institutos y asociaciones de auditoría interna de Europa e Israel. El IAI desarrolla sus actividades en España desde 1983.

A continuación mostramos el logotipo que utiliza este organismo en la figura 3.5:

3.5 Logotipo del Instituto de Auditores Internos de España

http://www.iai.es/ (Fecha de la consulta: 27/07/2011)

3.2 Certificaciones

3.2.1 CISA (CertifiedInformationSystem Auditor)

CISA es una certificación para auditores respaldada por la Asociación ISACA, como hemos mencionado anteriormente. Los candidatos deben cumplir con los requisitos establecidos por la ISACA.

La certificación CISA fue establecida en 1978 debido a las siguientes razones:

- Desarrollar y mantener una herramienta que pueda ser utilizada para evaluar las competencias de los individuos al realizar auditorías de sistemas.
- Proveer una herramienta motivacional para los auditores de sistemas de información para mantener sus habilidades, y monitorizar la efectividad de los programas de mantenimiento.
- Proveer criterios de ayuda y gestión en la selección de personal y desarrolladores.

El primer examen se llevó a cabo en 1981, y los registros han crecido cada año. En la actualidad, el examen es ofrecido en 11 idiomas y más de 200 lugares de todo el mundo. En 2005, la Asociación de Control y Auditoría de Sistemas de Información (InformationSystemsAudit and Control Association, ISACA), anunció que el examen será ofrecido en junio y diciembre, empezando en 2005. Anteriormente, el examen sólo había sido administrado anualmente, en junio. Más de 50000 candidatos han conseguido el certificado CISA.

Los candidatos a la certificación CISA deben pasar un examen de acuerdo al Código Profesional de Ética de ISACA, además de comprobar 5 años de experiencia en auditoría de sistemas, control interno y seguridad informática y tener un programa de educación continua.

En caso de no cumplir con estos requisitos existen algunas equivalencias definidas en la página de ISACA, las cuales son las siguientes:

- Un máximo de un año de experiencia en sistemas de información o un año de experiencia en auditorías operacionales, pueden ser sustituidos

por un año de experiencia auditoría de sistemas, control interno y seguridad informática.

- 60 a 120 horas de estudios profesionales pueden ser sustituidos por uno o dos años de experiencia respectivamente de auditoría de sistemas, control interno y seguridad informática.
- 2 años de instructor a tiempo completo en Universidad en campos relacionados (ejemplo: ciencias computacionales, contabilidad, auditoría de sistemas de información), pueden ser sustituidos por un año de experiencia de auditoría de sistemas de información, control interno y seguridad de informática.

A continuación mostremos el logotipo de este certificado en la figura 3.6:

3.6 Logotipo del Certified Information System Auditor

http://es.wikipedia.org/wiki/CISA (Fecha de la consulta: 24/07/2011)

3.2.2 CIA (Certificado de Auditor Interno)

Certificado de auditor interno, es la única certificación globalmente aceptada para los auditores internos y sigue siendo el estándar por el cual las personas demuestran su competencia y profesionalidad en el campo de la auditoría interna. Los candidatos abordan el programa enriquecido con la experiencia educativa, información y herramientas de negocio que se pueden aplicar de inmediato en cualquier organización o entorno empresarial.

A continuación mostramos el logotipo de esta certificación en la figura 3.7:

3.7 Logotipo del Certificado de Auditor Interno

http://www.theiia.org/certification/certified-internal-auditor/ (Fecha de la consulta: 27/07/2011)

3.2.3 CISM (Certified Information Security Manager)

CISM , una designación innovadora para los líderes que manejan la seguridad de una organización de la información. Más de 14.000 han obtenido la designación CISM desde que se estableció en 2002.

A continuación observamos el logotipo de dicho certificado en la figura 3.8:

3.8 Logotio del Certified Information Security Manager

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

3.2.4 CGEIT (Certified in the Governance of Enterprise IT)

CGEIT , este certificado es para los profesionales que manejan, proporcionan asesoramiento y / o servicios de auditoría, y / o que de alguna manera apoyan la gestión de una empresa de TI. Más de 4.500 profesionales han obtenido la designación CGEIT desde que se estableció en 2007.

A continuación mostramos el logotipo de esta certificación en la figura 3.9:

3.9 Logotipo del Certified in the Governance of Enterprise IT

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

3.2.5 CRISC (Certified in Risk and information System Control)

CRISC , certificado para los profesionales que tienen experiencia con la identificación de riesgos, la evaluación de respuesta al riesgo y la vigilancia de riesgos. Es el diseño de control y ejecución, y es seguimiento, control y mantenimiento. Más de 1.000 profesionales han sido certificados desde su creación en 2010.

A continuación mostramos el logotipo de la certificación en la figura 3.10:

3.10 Logotipo del Certified in Risk and information System Control

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

3.3 Normativas

3.3.1 Cobit (Control Objectives for Information and related Technology)

El estándar Cobit ofrece un conjunto de “mejores prácticas” para la gestión de los Sistemas de Información de las organizaciones.

El objetivo principal de Cobit consiste en proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos con tal de:

- Asegurar el buen gobierno, protegiendo los intereses de los clientes, accionistas, empleados…
- Garantizar el cumplimiento normativo del sector al que pertenezca la organización
- Mejorar la eficacia y eficiencia de los procesos y actividades de la organización

- Garantizar la confidencialidad, integridad y disponibilidad de la información

La definición abarca desde aspectos organizativos por ejemplo, flujo para pedir autorización a determinada información, procedimiento para reportar incidencias, selección de proveedores… hasta aspectos más tecnológicos y automáticos como por ejemplo el control de acceso a los sistemas, monitorización de los sistemas mediante herramientas automatizadas…

Por otra parte, todo control tiene por naturaleza un objetivo. Es decir, un objetivo de control es un propósito o resultado deseable como por ejemplo: garantizar la continuidad de las operaciones ante situaciones de contingencias.

En consecuencia, para cada objetivo de control de nuestra organización podremos implementar uno o varios controles por ejemplo la ejecución de copias de seguridad periódicas, traslado de copias de seguridad a otras instalaciones… que nos garanticen la obtención del resultado deseable como por ejemplo la continuidad de las operaciones en caso de contingencias.

Cobit clasifica los procesos de negocio relacionados con las TIen 4 dominios:

- Planificación y Organización
- Adquisición e Implementación
- Entrega y Soporte
- Supervisión y Evaluación.

En definitiva, cada dominio contiene procesos de negocio (desglosables en actividades) para los cuales se pueden establecer objetivos de control e implementar controles organizativos o automatizados.

http://www.marblestation.com/?p=645 (Fecha de la consulta: 18/09/2011)

3.3.2 ISO

ISO/IEC 17799 (denominada también como ISO 27002) es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la International OrganizationforStandardization y por la Comisión Electrotécnica Internacional en el año 2000, con el título de Informationtechnology - Security techniques - Code of practiceforinformationsecuritymanagement. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en el British Standard BS 7799-1 que fue publicado por primera vez en 1995.

-Publicación de la norma en España:

En España existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada Código de buenas prácticas para la Gestión de la Seguridad de la Información, que es una copia idéntica y traducida del inglés de la Norma Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 está disponible desde 2006.

El estándar ISO/IEC 17799 tiene equivalentes directos en muchos otros países. La traducción y publicación local suele demorar varios meses hasta que el principal estándar ISO/IEC es revisado y liberado, pero el estándar nacional logra así asegurar que el contenido haya sido precisamente traducido y refleje completa y fehacientemente el estándar ISO/IEC 17799.

www.**iso**.ch/(Fecha de la consulta: 26/07/2011)

3.3.3 ITIL (*Information Technology Infrastructure Library*)

ITIL es el enfoque más ampliamente adoptado para la Gestión de Servicios TI en el mundo. Proporciona un enfoque práctico para identificar, planificar, ejecutar y apoyar los servicios de TI con el negocio.

Visión general y beneficios:

ITIL remarca que los servicios de TI deben estar alineados con las necesidades del negocio y sustentar los procesos de negocio. Se ofrece orientación a las organizaciones sobre la manera de utilizar las TI como una herramienta para facilitar el cambio de negocios, la transformación y el crecimiento.

Las mejores prácticas ITIL están detalladas dentro de las cinco principales publicaciones que proporcionan un enfoque sistemático y profesional para la gestión de servicios de TI, permitiendo a las organizaciones ofrecer servicios adecuados y asegurarse de que continuamente están cumpliendo los objetivos de negocio y distribuir los beneficios.

Las cinco guías básicas de todo el ciclo de vida de ITIL Service, comenzando con la identificación de las necesidades de los clientes y los que se encargan de obtener los requisitos de TI, a través del diseño e implementación de los servicios en funcionamiento y, por último, a la fase de seguimiento y mejora del servicio.

La adopción de ITIL puede ofrecer a los usuarios una amplia gama de beneficios que incluyen:

- mejora de los servicios de TI
- reducción de costes
- atención al cliente mejorando la satisfacción a través de un enfoque más profesional a la prestación de servicios
- mejora de la productividad
- un mejor uso de las habilidades y la experiencia
- mejora de la prestación de servicios de terceros.

http://www.itil-officialsite.com/ (Fecha de la consulta: 26/07/2011)

3.4 Resumen

Como podemos observar en este capítulo existe una gran variedad de organismos, certificados y normativas para todo este mundo de la auditoría, la que cada vez juega un papel más importante en todas las organizaciones ya sean privadas o estatales, todo directivo, empresa externa… quiere tener conocimiento de en qué estado esta su organización, la organización a auditar… para poder así implantar la mejoras que sean necesarias si es que lo son, detectar posibles fraudes, conseguir que la organización en cuestión se encamine por el trayecto más apropiado… todos estos aspectos se consiguen mucho mejor con la ayuda que tiene el auditor con los conocimientos adquiridos gracias a los certificados y normativas que regulan los organismos en cuestión. A continuación en la figura 3.11 mostramos una tabla que nos hace un resumen de los organismos certificaciones y normativas que acabamos de explicar a la largo de esta capitulo.

Es el próximo capítulo pasaremos a hablar más en detalle del camino que sigue el auditor a la hora de analizar a una organización, cuales son las pautas que debe seguir, es decir, la metodología concreta que el auditor utiliza para realizar su trabajo de forma objetiva y concisa sin que su análisis final tenga lugar a la objeción.

ORGANISMOS	CETIFICACIONES	NORMATIVAS
ISACA (Information Systems Audit and Control Association)	**CISA** (Certified Information System Auditor)	**COBIT** (Control Objectives for Information and related Technology) **ISO** **ITIL** (Information Technology Infrastructure Library)
	CISM (Certified Information Security Manager)	
	CGEIT (Certified in the Governance of Enterprise IT)	
	CRISC (Certified in Risk and information System Control)	
ITGI(IT Governance Institute)		
IIA (The Institute of Internal Auditors)	**CIA**(Certificado de Auditor Interno)	
ISO(Organización Internacional de Normalización)		
IAI-E(Instituto de Auditores Internos de España)		

Fuente: Elaboración propia basada en la información aportada en el capítulo 3

3.11 Tabla Resumen de Organismos, Certificaciones y normativas.

4. Metodología de la Auditoría

A continuación pasamos a explicar la metodología que deben seguir todos los auditores a la hora de realizar el análisis de las organizaciones, es como una guía con las pautas que se deben seguir a la hora de realizar el análisis, de esta forma nos aseguramos de realizar todos las tareas necesarias para detectar cualquier anomalía en las organizaciones si es que tiene.

Para realizar el trabajo de auditoría, el auditor necesita establecer una serie de guías, procedimientos, **métodos**... Es decir, necesita seguir una **metodología**, la cual podemos definir como un conjunto de procedimientos documentados de auditoría diseñados para alcanzar los objetivos de auditoría planeados, así mismo pretende esclarecer el alcance, los objetivos y los programas de auditoría. El auditor debe evaluar los riegos y desarrollar un programa en el que se encuentren los objetivos de control y los procedimientos que serán revisados, además debe recopilar evidencias y en función de los hallazgos evaluar las debilidades y fortalezas de los partes auditadas. Para finalizar el auditor deberá realizar un informe de auditoría, el cual presentará a la organización auditada, dicho informe debe ser los más objetivo posible.

Por otra parte todos aquellos planes, actividades, pruebas, hallazgos e incidentes que sucedan durante la realización de la auditoría deben ser documentados en los papeles de trabajo. Los objetivos principales de los papeles de trabajo son:

- Facilitar la realización de las pruebas y la preparación del informe.
- Comprobar y explicar en detalle las opiniones resumidas en el informe.
- Coordinar y organizar todas las fases del trabajo.
- Proveer un registro histórico permanente de la información examinada y los procedimientos de auditoría aplicados.
- Servir de guía en revisiones posteriores.
- Cumplir con las disposiciones legales.

A continuación vamos a explicar cuáles son las fases comunes que debe seguir cuando se realiza cualquier tipo de auditoría.

4.1 Toma de contacto

Cuando una organización solicita la realización de una auditoría el primer paso que se debe realizar es llevar a cabo una toma de contacto con la organización que se va a auditar. En esta fase es donde el auditor debe obtener toda la información relevante de la organización, entendiendo la arquitectura de información y de la dirección tecnológica sobre el Sistema de Información que utiliza la organización auditada. La información relevante que el auditor debe conocer y entender después de realizar esta primera toma de contacto (**Autores:** Bernal Montañés, Rafael y Coltell Simón, Oscar (1996). **Título:** Auditoría de los sistemas de información. Universidad Politécnica de Valencia, Servicio de Publicaciones. **Año:** 2008. **Fecha de la consulta:** 27/09/2011):

- Saber a qué se dedica la organización a auditar.
- Saber en qué contexto legal se encuentra la organización, para conocer cuáles son las leyes a las que se somete su Sistema de Información, así como la actividad que realiza.
- Conocer la distribución geográfica de las instalaciones que posee la organización, el presupuesto anual, el número de empleados.
- Entender la estructura organizativa y responsabilidades de cada uno de los elementos que componen la organización, así como las relaciones entre dichos elementos.
- También debe entender de cada departamento cuales son la funciones que debe realizar, centrándonos en el caso de estudio en aquellos que utilizan el Sistema de Información.
- El auditor debe conocer cuál es el flujo de la información dentro de la organización.
- Además es preciso saber el organigrama informático de las relaciones que existen entre los diferentes departamentos y el seguimiento de la información interna.
- Entendimiento global de la estructura de red.
- Volumen del área informática.

- Número de empleados, distribución de personal por áreas de explotación, mantenimiento, desarrollo e investigación…

4.2 Planeación de la Auditoría

Un vez realizado el primer paso que es la toma de contacto con la organización a auditar, el siguiente paso es realizar la planificación de la auditoría, en la que se debe desarrollar un plan que tenga en cuenta los objetivos relevantes de la organización a auditar, el cumplimiento de las leyes aplicables y los estándares de auditoría profesionales.

También es conveniente en esta fase que el auditor realice un análisis del riesgo, entendiendo por riesgo, la probabilidad de que una amenaza determinada provoque que las vulnerabilidades de un activo o grupo de activos tengan lugar ocasionando pérdida o daño de los activos. El impacto del riesgo es proporcional al valor para el negocio de la pérdida o daño y a la frecuencia estimada de la amenaza.

Cuando el auditor realiza un análisis de riesgo, lo primero es identificar los activos para así poder asociarlos a una potencial vulnerabilidad o amenaza, posteriormente debe identificar los posibles controles implantados para mitigar los riesgos identificados, dichos controles pretenden reducir los riegos a niveles que sean aceptables para la dirección. Además durante todo el proceso de auditoría no nos podemos olvidar de los niveles que poseen dichos riesgos, sino que deben tener un seguimiento continuo, el cual nos ayudará a iterar el proceso de análisis de riesgo en caso de que no se llegara a un nivel aceptable de mitigación de riesgo. Como conclusión del análisis de riesgo podemos decir que el auditor debe realizar estos pasos:

- Identificar los riesgos potenciales.
- Evaluar y priorizar riesgos potenciales.
- Identificar controles para mitigar los riegos encontrados.
- Seguimiento de los niveles de desempeño de los riesgos identificados.

Para este análisis de los posibles riesgos que puede darse en la organización el auditor puede ayudarse de la metodología MAGERIT versión 2, publicada por el Ministerio de Hacienda y Administraciones Públicas, este metodología es un método formal que sirve para investigar los riegos que pueden afectar a los Sistemas de Información, proponiendo medidas adecuadas que la organización en cuestión debería realizar para controlar los riegos. Los objetivos que persigue esta metodología son:

- Hacer ver a los responsables de los Sistemas de Información de la existencia de riegos y las necesidades de atajarlos a tiempo.
- Proporcionar un método para analizar estos riegos.
- Ayudar a planificar las medidas oportunas para mantener los riegos bajo control.

Cuando hablamos de investigar los riegos nos referimos a que MAGERIT propone una evaluación del impacto que una violación de la seguridad tiene en la organización, muestra los riegos existentes, marcando cuales son las amenazas que afectan al Sistema de Información además de determinar las vulnerabilidades del sistema de prevención de estas amenazas, obteniendo unos resultados. Estos resultados le permiten al auditor saber cuáles serán las medidas adecuadas que deberían realizarse para conocer, prevenir, impedir, reducir o controlar los riegos que hemos identificado, y así poder reducir su potencialidad y sus posibles perjuicios.

Además de realizar el análisis del riesgo el auditor también debe entender que aspectos de privacidad y requerimientos regulatorios pueden afectar el enfoque general de la auditoría. Es decir, el auditor de SI debiera desarrollar y documentar el plan de auditoría detallando la naturaleza, los objetivos, el tiempo, el alcance y los recursos requeridos.

Un factor muy importante en la planificación es conseguir la correspondencia entre los recursos de auditoría disponibles y las tareas definidas en el plan de auditoría. Cuando se realiza el plan se deben considerar los requerimientos del proyecto, los recursos del personal, y el tiempo que se va a emplear para

hacer una asignación correcta de los recursos, cosa que posteriormente pasaremos a explicar más detalladamente.

Finalmente, en la planificación, se desarrollará un programa de auditoría donde se establezcan los procedimientos que el auditor debe seguir a la hora de recopilar los datos.

4.3 Procedimientos de Auditoría y pasos para la recopilación de datos

El siguiente paso de la auditoría sería realizar los procedimientos de auditoría necesarios para obtener las evidencias confiables y que permitan al auditor formarse un juicio sobre el estado de la adecuación del Sistema de Información.

Es en esta fase donde el auditor debe conseguir toda la información necesaria con el fin de reunir una variedad de evidencias suficientes, confiables y relevantes. Una vez halladas dichas evidencias se deben documentar para apoyar la opinión final del auditor.

El auditor utiliza una serie de determinantes que ahora nombraremos para evaluar si las evidencias son fidedignas:

- Independencia del proveedor de la evidencia: las evidencias obtenidas por fuentes externas son más confiables que las obtenidas por la propia organización auditada.
- El auditor debe considerar los conocimientos de las personas que suministran la información independientemente de si estas personas son externas o internas a la organización.
- La evidencia si es objetiva es más confiable que si requiere de una opinión o interpretación.
- El auditor debe tener en cuenta el tiempo que perdura la información.

Pasamos a explicar ahora cuales son los procedimientos que el auditor seguirá para la recolección de evidencias**,** pueden variar en función de Sistema de Información del auditado:

- Revisar la estructura organizativa del Sistema de Información y determinar el nivel de control que posee.
- Se debe entender cuáles son los estándares vigentes dentro de la organización, así como comprobar si existen políticas y procedimientos adecuados, y su cumplimiento por parte de los empleados.
- El auditor debe recopilar toda la documentación vigente existente de los Sistemas de Información.
- El auditor debe realizar una serie de entrevistas con el personal de la organización, con el fin de obtener evidencias, para ello el auditor debe apoyarse en cuestionarios y *checklists*.
- Se deben observar los procesos así como los empleados en el desarrollo de sus funciones, para detectar posibles anomalías, las cuales serán mostradas como evidencias.
- Utilización de técnicas de auditoría asistidas por computador.
-

Todas estas técnicas de recolección de evidencias forman parte de la auditoría, pero la auditoría también incluye un examen de comprobación de los controles así como de las propias evidencias que obtenemos. El documento principal que emplearemos para anotar el resultado de las pruebas son los papeles de trabajo.

4.4 Procedimientos para evaluar la prueba o revisar los resultados

Una vez obtenida toda la información que el auditor necesita, el siguiente paso es evaluar la información recopilada, a partir de dicha información el auditor tendrá los conocimientos necesarios para fundamentar una opinión de auditoría. Es muy importante que el auditor conozca cuales son las debilidades y fortalezas de la organización a auditar para poder así alcanzar los objetivos establecidos previamente en la planificación.

Por otra parte a la hora de revisar los procedimientos de control, es probable que algunos controles suplan carencias que otros controles tienen, a estos controles los llamamos *controles compensatorios* Podría poner en cursiva los términos que desee resaltar. Es interesante que el auditor conozca la existencia de dichos controles allí donde existan controles que no provean el suficiente grado de seguridad, confidencialidad o integridad. Algunos ejemplos pueden ser las pistas de auditoría, informe de incidencias, revisiones de supervisión…

Además cuando el auditor está revisando los resultados obtenidos también debe tener en cuenta la **materialidad** de los hallazgos para saber cuál de ellos deberá incluirse en el informe de auditoría. Para ello el auditor deberá ser consciente de lo significativo que sea el hallazgo.

Otro factor que se debe tener en cuenta a la hora de realizar los procedimientos para evaluar la prueba o revisar los resultados es que durante esos intervalos de tiempos es probable que se den interrupciones tanto por parte del auditor como de la organización a auditar, las posibles interrupciones pueden ser por parte del auditor, como, necesidad de apoyo de otros auditores, conflictos con calendarios con otros proyectos…o por parte de la organización a auditar como falta de disponibilidad de empleados, falta de documentación adecuada…

4.5 Elaboración del Informe de Auditoría

El informe de auditoría es el resultado final de trabajo realizado, donde el auditor expone su opinión a partir de las evidencias obtenidas y su previa experiencia.

El informe deberá contener:

- Identificar la organización, los destinatarios y cualquier restricción sobre su publicación.

- Definir el alcance, los objetivos, el periodo cubierto y la naturaleza, tiempo y extensión del trabajo de auditoría realizado.
- Evidencias objetivas obtenidas por el auditor para la determinación de las evidencias.
- Establecer los hallazgos, conclusiones y recomendaciones, así como cualquier restricción sucedida durante el proceso.
- Mostrar evidencias para respaldar la opinión del auditor.
- Medidas correctoras necesarias para solventar las deficiencias halladas.
- El propio informe debe estar firmado, fechado y se debe distribuir conforme el contrato establecido.

4.6 Seguimiento

Una vez entregado el informe de auditoría y halladas todo tipo de vulnerabilidades a las que la organización se enfrentaba, es conveniente que la organización auditada tenga un seguimiento, y con más razón si la opinión emitida por el auditor no ha sido del todo favorable, dicho seguimiento no es necesario que lo realice el auditor, ya que si pertenece a una empresa externa, la cual ha sido contratada por la organización a auditar, no sería necesario a no ser que la empresa solicitara dicho servicio.

Es también interesante realizar dicho seguimiento para asegurarse de que se toman las medidas correctivas para subsanar las debilidades halladas en la auditoría, además también es de interés realizar dicho seguimiento si la empresa auditada realiza cambios.

4.7 Resumen

Acabamos en este capítulo de explicar cuál es la metodología, es decir los pasos, que es conveniente que cualquier auditor a la hora de hacer un análisis profundo de una organización tenga en cuenta. Gracias a estas pautas conseguiremos unas conclusiones lo mas exactas posibles de la organización auditada, ya que lo que queremos conseguir es tener una visión lo más exacta posible de la información y quien, cuando y como la maneja.

En el posterior capítulo pasamos a hablar del primer punto que comentamos en este capítulo, no exactamente de la toma de contacto que debe tener el auditor cuando va a auditar a una empresa, sino a explicar cómo está formada la empresa a auditar, que departamentos la componen, cuales son las personas que componen esos departamento, y cuáles son sus funciones, para así posteriormente realizar un plan de auditoría coherente con la organización en cuestión.

4.8 Bibliografía del capítulo 4

4.8.1 Libros Apuntes y Artículos

Autor: David Lorente Guzmán. **Asignatura:** Auditoría de los Sistemas de Información, ETS de Ingeniería Informática de la UPV, Plan de Estudios de ITIG, Curso 2009-2010, **Fecha de consulta:** 25/09/2011. **Dirección:** http://www.inf.upv.es/webei/webETSIA/la_escuela/titulaciones/ITIG01/lista_optativas_con_info.php#ausi

Autores: Bernal Montañés, Rafael y Coltell Simón, Oscar (1996). **Título:** Auditoría de los sistemas de información. Universidad Politécnica de Valencia, Servicio de Publicaciones. **Año:** 2008. **Fecha de la consulta:** 27/09/2011

4.8.2 Webs

Autor: Ángela Jiménez. **Fecha de la consulta:** 25/09/2011. **Dirección:** http://www.uclm.es/area/aef_TO/pdf//publicaciones/AngelaJimenez_Tema5.pdf

Autor: Eduardo Horacio Quinn. **Título:** Auditoría Informática dentro de las etapas de análisis. **Fecha de la consulta:** 25/09/2011. **Dirección:** http://www.monografias.com/trabajos5/audi/audi.shtml

Institución: Ministerio de Hacienda y Administraciones Públicas, D.G. de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. **Título:** MAGERIT, versión 2. **Año:** 2010. **Fecha de la consulta:** 07/01/2012. **Dirección:** http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

5. Descripción de la Organización en la que se va a implantar el plan de auditoría

El tipo de empresa al que se hace referencia en este proyecto, es una empresa imaginaria que utilizaremos como base para hacer el plan de auditoría donde intentaremos dar las guías para analizar el departamento de desarrollo de aplicaciones, este tipo de empresa está englobada en aquellas con una **organización lineal** y compuesta por los departamentos característicos que la integran.

Este empresa se encarga básicamente del desarrollo y mantenimiento de aplicaciones, web tanto para clientes externos a la empresa como para el personal de la propia empresa, que lo ayuda de estas herramientas puede mejorar la manera de tratar, administrar… las propia empresa, pero no solo está formada por este departamento, aunque el producto final que llega a los clientes san aplicaciones, tenemos diferentes departamentos en la empresa como puede ser en de ventas, de recursos humanos… pero el que a nosotros nos interesa para el departamento de desarrollo de aplicaciones informáticas.

5.1 El Tipo de Estructura Organizativa: Organización lineal

Estos tipos de organizaciones tienen su origen en los antiguos ejércitos y en la organización eclesiástica de los tiempos medievales, se constituyen de la forma estructural más simple y es el tipo de organización más antiguo. Cuando decimos que una organización es lineal lo que significa es que entre el directivo superior de la empresa y los empleados que no son directivos (puesto de base) hay impuestas unas líneas directas y únicas de autoridad y responsabilidad.

Este tipo de estructuras son de conformación piramidal y bastante simple, donde cada jefe recibe y transmite lo que pasa en su área. En estas

organizaciones existe una autoridad lineal o única donde la principal característica de la organización lineal es la autoridad única y absoluta del superior sobre sus subordinados. Son las características típicas de las organizaciones militares.

Además este tipo de organizaciones utilizan líneas formales de comunicación, donde la relaciones entre los órganos o cargos que existen en la organización se dan únicamente a través de las líneas que existen en el organigrama de la empresa en cuestión. Todo órgano o cargo perteneciente a la organización tiene dos terminales de comunicación, uno está orientado al cargo superior, y el otro a sus subordinados única y exclusivamente.

Por otra parte encontramos una fuerte **centralización de las decisiones** donde es la autoridad, el jefe, quien controla toda la organización centralizando los canales de comunicación y asumiendo la responsabilidad de toda decisión tomada dentro del organigrama de la empresa.

Otra característica que encontramos en este tipo de Organizaciones, es que a medida que ascendemos en la escala jerárquica disminuye el número de cargos. Como resultado observamos que a medida que ascendemos el nivel de jerarquía, aumenta la generalización, centralización y visión global de la organización, conforme descendemos la escala jerárquica aumenta la especialización, la delimitación de las responsabilidades y la visión específica del cargo o función que cada individuo desempeña dentro de la organización. (Dirección Web: http://www.mitecnologico.com/Main/OrganizacionLineal y fecha de consulta: 10/04/2012)

5.1.1 Ventajas de la organización lineal

Según (dirección Web: http://www.mitecnologico.com/Main/OrganizacionLineal y fecha de consulta: 10/04/2012), las ventajas son las siguientes:

- Es sencilla y clara.
- No hay conflicto de autoridad ni fugas de responsabilidad.
- Se facilita la rapidez de acción.

- Se crea una firme disciplina, cada jefe adquiere toda la autoridad ya que para sus subordinados es el único que la posee.
- Es útil en la pequeña empresa, por lo que para la empresa imaginaría que estamos utilizando nos sirve, ya que esta empresa no tendría más de 30 o 40 empleados.
- La autoridad lineal recibe el asesoramiento y servicio técnico de un cuerpo especialista.

5.1.2 Desventajas de la organización lineal

Según (dirección Web: http://www.mitecnologico.com/Main/OrganizacionLineal y fecha de consulta: 10/04/2012), las desventajas son las siguientes:

- Se carece de especialización.
- No hay flexibilidad para futuras expansiones.
- Es muy difícil capacitar a un jefe en todos los aspectos que debe coordinar.
- Se propicia la arbitrariedad de que el jefe observe toda la responsabilidad de la autoridad.
- La comunicación, por obedecer a la escala jerárquica, se vuelve indirecta, lenta y está sujeta a intermediarios y distorsiones.

5.1.3 Campos de aplicación

La organización lineal es aplicable específicamente en los siguientes casos: (Dirección Web: http://www.buenastareas.com/ensayos/Campo-a-Aplicaci%C3%B3n-De-Organizaci%C3%B3n-Lineal/2145539.html y fecha de consulta: 10/04/2012)

- Cuando la organización es pequeña no requiere de ejecutivos especializados en las tareas altamente técnicas.
- Cuando la organización está en las etapas iníciales de su historia.
- Cuando las tareas desarrolladas por la organización son estandarizadas, rutinarias y con raras alteraciones o modificaciones, permitiendo plena

concentración en las actividades principales de la organización, ya que la estructura es estable y permanente.

- Cuando la organización tiene corta vida y la rapidez en la ejecución del trabajo se hace más importante que la calidad del trabajo.

Una vez explicado el tipo de estructura organizativa de la empresa para la que vamos a realizar el Plan de Auditoría Informática, vamos a detallar los diferentes departamentos que conforman la empresa.

5.2 Departamentos de la empresa

5.2.1. Departamento de Ventas

En el mercado actual, este departamento cobra mucha importancia, tiene que hacer muchos movimientos para conseguir todos sus objetivos, ya que hay mucha competencia, muchas organizaciones que ofrecen los mismos productos con las mismas calidades y al mismo precio, depende de los profesionales de este departamento que sepan llevarse al cliente a su terreno.

El departamento de ventas se encarga de persuadir al mercado de la existencia de un producto, valiéndose de sus cualidades, su ingenio, de la fuerza de ventas o intermediarios, aplicando las técnicas y políticas de ventas de acuerdo con el producto que se desea comercializar.

Las funciones de este departamento son:

(Dirección Web: http://www.buenastareas.com/ensayos/Funciones-Del-Departamento-De-Ventas/23364.html y fecha de consulta: 10/04/2012)

- Manipular el producto, es decir, analizar las aplicaciones ya existentes, ya que este departamento es el que más contacto tiene con la competencia, es el que mejor visión tiene del exterior, por este motivo puede ayudar a la empresa informándole del estado en el que están las aplicaciones que desarrollaron en tiempos pasados en comparación con los de la competencia, ya que simplemente haciendo determinados

cambios puede que el producto entre a competir con los otros del mercado actual.

- Responsabilidad de que el cliente quede satisfecho con el producto ofertado. El encargado de tener el trato con el cliente juega un papel muy importante ya que debe captar los requisitos que el cliente le está solicitando de una forma clara, si no el resultado del proyecto puede verse gravemente dañado, este es un ejemplo claro que frecuentemente ocurre en el proceso de desarrollo de aplicaciones ya que en numerosas ocasiones el cliente no sabe exactamente lo que quiere y una vez está la aplicación en cuestión medio desarrollada empieza a solicitar modificaciones, las cuales causan retrasos de tiempos, aumento de costes… que el encargado de ventas también deberá tener en cuenta a la hora de realizar las estimaciones.
- Tiene el deber de tener unas estrategias de ventas, condiciones de ventas, reclamaciones y ajustes, calidad del software, créditos y cobros.
- Realiza el financiamiento de las ventas, es decir, las operaciones a crédito y al contado son esenciales para el desenvolvimiento de las transacciones. Para financiar ventas a plazo es necesario que el responsable de ventas este ampliamente relacionado con el de crédito, para determinar los planes de pago que deben adoptarse, la duración del período de crédito, el descuento por pronto pago o los costes financieros a cargar por pago retrasado, es decir, todo lo relacionado con la práctica crediticia.
- El departamento de ventas debe conocer los costes y presupuestos de Ventas para controlar los gastos y planear la ganancia, el ejecutivo de ventas, previa consulta con el personal investigador del mercado con el de contabilidad y el de presupuestos, debe calcular el volumen probable de ventas y sus costos para todo el año.
- Conseguir un buen estudio de mercado, es decir, las preferencias del consumidor, sus hábitos de compra y su aceptación del software o servicio es fundamental para una buena administración de ventas, debido a que se debe recoger, registrar y analizar los datos relativos al carácter, cantidad y tendencia de la demanda, el estudio de mercado

debe incluir el análisis y la investigación de ventas, estudios estadísticos de las ventas, territorio, distribuidores y temporadas; los costos de los agentes de ventas, costos de venta y de operación.

- Debe realizar promociones de venta y publicidad, estas ayudan a estimular la demanda de consumo y contribuir a que las personas de venta, vendan los productos. El responsable de ventas aprueba los planes de promoción y publicidad, los horarios de trabajo, las asignaciones presupuestarias, los medios de propaganda, las promociones especiales y la publicidad en colaboración con los comerciantes.
- También debe lograr una planeación de Ventas, donde el administrador de ventas debe fijar los objetivos de las mismas y determinar las actividades mercantiles necesarias para lograr las metas establecidas. La planeación de ventas debe coordinar las actividades de los agentes, comerciantes y personal anunciador, la distribución física; el personal de ventas, las fechas de los planes de producción, los inventarios, los presupuestos y el control de los agentes de ventas.
- Además debe proveer a los clientes servicios técnicos, los cuales corresponde a los responsables de ventas cuyos productos software requieren de servicios de instalación y técnicos, establecer normas al respecto; tener el equipo y los locales destinados para tal servicio, así como si es necesario dotar de algún tipo de formación al cliente, ya que puede que el software que nuestra organización ofrece requiera de dicha formación.
- El departamento de venta en sí, debe desarrollar de la manera más eficiente el proceso de integración de personal, el cual comprende, buscar, seleccionar y adiestrar al personal de ventas; así como de su compensación económica, supervisión, motivación y control.
- La Administración del departamento de ventas, es responsabilidad del responsable de la misma, el cual debe establecer la organización, determinar los procedimientos, dirigir el personal administrativo, coordinar el trabajo de los miembros del departamento, llevar el registro de las ventas y asignar tareas al personal de este departamento.

5.2.2. Departamento de Recursos Humanos

Los Recursos Humanos son todas aquellas personas que integran o forman parte de una organización. El objeto del Departamento de Recursos Humanos es conseguir y conservar un grupo humano de trabajo cuyas características vayan de acuerdo con los objetivos de la empresa, a través de programas adecuados de reclutamiento, selección, capacitación y desarrollo.

Las funciones del departamento de Recursos Humanos son:

(Dirección Web: http://www.mitecnologico.com/Main/EstructuraFuncionamientoDepartamentoRecursosHumanos y fecha de consulta: 10/04/2012)

- Este departamento es el responsable de la contratación y empleo, esta es una de las funciones que requieren de mayor importancia debido a lo difícil que resulta encontrar a las personas ideales para los puestos vacantes, por lo que es necesario contar con un procesamiento eficaz de reclutamiento y selección de personal, una vez que se tiene a las personas deseadas se procede a la contratación de las mismas, dándoles una introducción acerca de la empresa. Si el puesto vacante se puede cubrir con personal propio de la empresa, entonces se realiza una evaluación de méritos y se le otorga al más capaz.
- Deben realizar la tarea de capacitación y desarrollo, acción que consiste en entrenar y capacitar a todo el personal, ya sea de nuevo ingreso, o no, con el objeto de incrementar el desarrollo personal. La capacitación no se le otorga exclusivamente a los de nuevo ingreso, puesto que nuestros actuales empleados pueden aspirar a un puesto mejor, el cual requiere de una mayor preparación.
- También se encargan de los sueldos y salarios, para poder realizar una justa asignación de sueldos, es necesario elaborar un análisis y evaluación de puestos, sólo así, podremos saber qué cantidad debemos pagar por cada uno de nuestros empleados. Además, hay que considerar que el sueldo está complementado por otros elementos tales como, las vacaciones y la calificación de méritos.

- Realizan las relaciones laborales, es decir, toda relación de trabajo debe estar regulada por un contrato ya sea colectivo o individual, en el que se estipularán los derechos y obligaciones de las partes que lo integran. Su objetivo es mantener una buena relación de trabajo y disciplina. Por otra parte, la comunicación es de vital importancia para toda organización, ya que por medio de esta se puede mantener una adecuada relación de trabajo.
- También es el responsable de realizar los servicios y prestaciones que la organización necesite, la organización puede ofrecer a sus trabajadores con el fin de hacer más atractivo su empleo, una serie de prestaciones distintas, tales como, actividades recreativas, actividades culturales, prestaciones en especie, reconocimientos…
- Asimismo son los responsables de mantener una higiene y seguridad industrial, consiste en llevar un registro de las causas que originan principalmente el absentismo y los accidentes de trabajo, así como de proporcionar a sus empleados los servicios médicos necesarios, y las medidas de higiene y seguridad requeridas para el buen desempeño de sus labores.
- Igualmente son los encargados de realizar la planeación del propio departamento, la cual consiste en realizar periódicamente una auditoría de los empleados para ver si están desempeñando satisfactoriamente sus labores, pudiendo rotar a los que considere inapropiados para dicho puesto.

5.2.3. Departamento de Finanzas

Esta función es de vital importancia, ya que toda empresa trabaja en constantes movimientos de dinero. Esta área se encarga de la obtención de fondos y del suministro del capital que se utiliza en el funcionamiento de la empresa, procurando disponer de los medios económicos necesarios para cada uno de los departamentos, con el objetivo de que puedan funcionar correctamente. El área de finanzas tiene implícito el objetivo del máximo aprovechamiento y administración de los recursos financieros.

Las funciones de este departamento son:
(Dirección Web:
http://webdelprofesor.ula.ve/nucleotrujillo/anahigo/guias_finanzas1_pdf/tema1.pdf, http://www.hondutel.hn/leytransparencia/funciones/gerenciafinanzas.pdf y fecha de consulta 10/04/2011)

- Estudiar y proponer, de acuerdo a los lineamientos generales que imparta la Dirección, el proyecto de presupuesto de la organización, en conformidad con las normas vigentes, la asignación de los recursos presupuestarios a los establecimientos de acuerdo con los programas de salud, las modificaciones presupuestarias que el estado de avance de la ejecución aconseje y la distribución de los aportes, según las posibilidades de ingresos.
- Velar por la correcta utilización de los recursos financieros.
- Participar en la ordenación, coordinación, supervisión y control de las operaciones financieras, contables y presupuestarias, con arreglo a las normas y demás disposiciones.
- Elaborar, en los plazos que se establezcan, los informes requeridos por el Sistema de Contabilidad, tanto de ejecución presupuestaria, movimiento de fondos y cuentas complementarias como de contabilidad de bienes y contabilidad general.
- Confeccionar el balance presupuestario y patrimonial anual de la organización de acuerdo con las normas y procedimientos referentes a la materia.
- Confeccionar y mantener actualizado el inventario de los bienes muebles e inmuebles de la organización.
- Recibir, recopilar, elaborar y consolidar la información financiera que requieran los distintos niveles directivos y unidades asesoras de la organización para formular planes y programas y adoptar decisiones.
- Revisar la facturación por atenciones prestadas.
- Velar por la correcta utilización de los aportes para pago de subsidios por incapacidad laboral, controlando que éstos se paguen de acuerdo a las normas e instrucciones vigentes.

- Desempeñar las demás funciones y tareas que le encomienden el Director de la organización.

5.2.4. Departamento de Contabilidad

El Departamento de Contabilidad se encarga de instrumentar y operar las políticas, normas, sistemas y procedimientos necesarios para garantizar la exactitud y seguridad en la captación y registro de las operaciones financieras, presupuestales y de consecución de metas de la entidad, a efecto de suministrar información que ayude a la toma de decisiones, a promover la eficiencia y eficacia del control de gestión, a la evaluación de las actividades y facilite la fiscalización de sus operaciones, cuidando que dicha contabilización se realice con documentos comprobatorios y justificativos originales, y vigilando la debida observancia de las leyes, normas y reglamentos aplicables.

Las funciones de este departamento son:

(Direcciones Web: http://www.utp.ac.pa/departamento-de-contabilidad ,http://actualicese.com/actualidad/2005/05/08/conocimientos-funciones-y-responsabilidades-del-cargo-de-coordinador-de-contabilidad/ http://www.buenastareas.com/ensayos/Funciones-De-Un-Departamento-De-Contabilidad/3617338.html y fecha de consulta: 10/04/2011)

- Establecer y operar las medidas necesarias para garantizar que el sistema de contabilidad de la organización este diseñado para que su operación facilite la fiscalización de los activos, pasivos, ingresos, costos, gastos, avance en la ejecución de programas y en general de manera que permitan medir la eficacia y eficiencia del gasto.
- Realizar las acciones necesarias para garantizar que el sistema contable de la organización, así como las modificaciones que se generen por motivos de su actualización, cuenten con las autorizaciones legales para su funcionamiento y operación.
- Llevar a cabo la contabilidad de la organización en los términos que establece la Ley de Presupuesto, Contabilidad y Gasto.

- Emitir por escrito las principales políticas contables necesarias para asegurar que las cuentas se operen bajo bases eficientes y consistentes, así como para la clara definición y asignación de responsabilidades de empleados y fiscalizadoras de información relativa a los activos, pasivos, ingresos costos, gastos y avance en la ejecución de programas.
- Registrar y controlar los recursos financieros provenientes del calendario financiero presupuestario, los que otorgan las instituciones para el desarrollo de proyectos de investigación.
- Controlar las disponibilidades de las cuentas bancarias de cheques y de inversión, realizando conciliaciones mensuales contra los saldos reportados en los estados de cuenta bancarios, para garantizar la exactitud en el registro de fondos, y apoyando a una correcta toma de decisiones.
- Depurar permanentemente los registros contables y presupuestales.
- Preparar y presentar los datos que conforman la Cuenta, el Sistema Integral de Información, el Informe Presidencial, las reuniones para Junta Directiva, el Comité de Control y Auditoría, y demás información complementaria que requieran las autoridades competentes respecto de las actividades desarrolladas en el ámbito de su competencia.
- Realizar las demás actividades que le sean encomendadas por la Subdirección de Recursos Financieros, afines a las funciones y responsabilidades inherentes al cargo.
- Coordinar, orientar y apoyar las actividades del personal adscrito al área de su competencia.

5.2.5. Departamento de desarrollo de aplicaciones informáticas

Así como hay departamentos que por definición deben existir, están aquellos que se forman por necesidades especificas y a su vez los que se les considera de lujo para dar una mejor imagen o por qué no, porque están de moda.

Hasta hace algunos años un departamento de desarrollo de aplicaciones informáticas solo lo consideraban aquellas organizaciones con los suficientes

recursos para mantenerlo, aún cuando no generara ingresos, pero poco a poco esta idea ha dejado de existir para convertirse en la convicción de que un departamento de desarrollo de aplicaciones informáticas es de vital importancia dentro de la compañía ya que es el encargado de proveer a esta, de información, lo cual en nuestros días es indispensable para la sobrevivencia de las empresas.

El departamento de desarrollo de aplicaciones informáticas es el área de una organización que se encarga de proveer de información así como de las herramientas necesarias para manipularla. Es el departamento que auxiliado con el equipo de cómputo, es capaz de convertir simples datos en información, es el encargado, de satisfacer las necesidades y preparación computacional a todos los miembros de una empresa, y es el responsable de ofrecer soluciones informáticas y el equipo necesario para su implementación.

Se le llama departamento de Informática por ser precisamente el proveedor de información, sin embargo también es llamado departamento de Sistemas porque es precisamente a través de Sistemas de Información, que se ofrecen la mayoría de las soluciones.

El trabajo medular de un departamento de Informática se hace, a través de un Sistema de Información. El conocimiento de sistemas de información abarca tanto perspectivas técnicas como conductuales, destacando la conciencia de las dimensiones de administración, organización y tecnológicas de los mismos. Los sistemas de información definen cinco retos claves para los administradores de hoy día, el reto del negocio estratégico; el reto de la globalización, el reto de la arquitectura de la información; el reto de la inversión en sistemas de información y el reto de la responsabilidad y control.

Proporcionan soluciones reales en los distintos tipos de sistemas de información en las organizaciones actuales: Sistemas de procesamiento de las operaciones comerciales, Sistemas de automatización del conocimiento/trabajo en la oficina, Sistemas de información para la administración, Sistema de soporte a las decisiones, y Sistemas de soporte para la gerencia. Estos sistemas sirven para diversos fines al dar apoyo a los diferentes niveles y funciones de la organización.

También se utilizan los Sistemas de Información en los negocios para obtener una ventaja competitiva. Los sistemas estratégicos de información han transformado los productos y servicios de las instituciones, las relaciones con los clientes y los proveedores y las operaciones internas. Para emplear estratégicamente los sistemas de información, las instituciones tienen que sufrir cambios técnicos y sociales.

Los sistemas de información quedan delineados de acuerdo con la estructura organizacional, la cultura de los procesos políticos y la administración, ya que la tecnología de la información puede influir también a las instituciones.

Un sistema de información puede definirse técnicamente como un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución. Además, para apoyar a la toma de las decisiones, la coordinación y el control, los sistemas de información pueden también ayudar a los administradores y al personal a analizar problemas, visualizar cuestiones complejas y crear nuevos productos.

La principal función de un departamento de Informática es crear y ofrecer sistemas de información que permitan dar solución a las necesidades informáticas y de toma de decisiones de una institución.

Es necesario hacer notar que el departamento de Informática es un departamento de servicio, y que nuestros clientes pueden ser los demás departamentos que conforman nuestra organización o usuarios/clientes externos que quieren utilizar nuestros servicios, que quieran que el departamento de desarrollo de aplicaciones informáticas les desarrolle determinadas aplicaciones para poder mejorar la manera de obtener, manejar su información. Los productos que ofrece este departamento son servicios y se pueden agrupar en las siguientes funciones: (direcciones Web: http://www.monografias.com/trabajos-pdf/administracion-informatica/administracion-informatica.pdf http://colima.inea.gob.mx/index.php/departamentos/depto-informatica/funciones.html http://www.buenastareas.com/ensayos/Funciones-Departamento-De-Inform%C3%A1tica/1859211.html y fecha de consulta: 10/04/2012)

- La administración y mantenimiento de los sistemas existentes en el grupo.
- Asesoría y capacitación a los diferentes departamentos y empresas del grupo.
- Estudios de factibilidad, compra e instalación de equipo
- Evaluación y adquisición de software y paquetería.
- Desarrollo de nuevos sistemas tanto para la propia organización como para organizaciones externas.
- Elaboración de manuales y documentación
- Administración y mantenimiento de ordenadores, redes y equipo.
- Revisión periódica de las necesidades de información.
- Mantenimiento y reparación de equipo de cómputo.
- Control de compras de todo lo relacionado con equipo, software, consumibles y accesorios computacionales.
- Implementación y administración de los servicios de Internet e Intranet.

Nuestros clientes pudiéramos clasificarlos de la siguiente manera:

- Los ejecutivos. Son aquellos que se encuentran en la parte superior de la estructura organizacional, ellos requieren de nuestros servicios en forma de información pura, es decir no requieren de sistemas o programas que les permitan procesar ni capturar información, a ellos se les debe proveer de herramientas sencillas que les aporte información concisa que les sirva para la toma de decisiones.
- Los jefes y coordinadores. Son aquellos que se encuentran en la parte media del organigrama, ellos supervisan las labores y entregan resultados. Requieren de nuestros servicios a través de programas y sistemas que les permitan visualizar y supervisar el trabajo de sus subordinados, que les permita también, manejar la información que resulta de las operaciones diarias y a su vez que puedan, generar informes para presentar resultados. La información a este nivel es un poco más a detalle y este tipo de usuario tiene la facilidad de operarla.
- Los auxiliares administrativos, operadores, secretarias que operan directamente los sistemas. Son aquellos que su trabajo es alimentar los sistemas con datos para obtener información, estos son nuestros

clientes más numerosos y requieren de nuestros programas para realizar su trabajo.

- Los trabajadores en general. Estos son los que sin utilizar sistema alguno, requieren también de información o servicio, es decir para cobrar requieren que se ejecute el proceso de nómina que es sin duda todo un sistema.
- Los clientes externos. Que al igual que los anteriores requieren de la información generada por los diferentes sistemas y servicios.

Todos los anteriores requieren además de sistemas, capacitación, documentación, adiestramiento, instalación y demás servicios que ofrece el departamento.

Los objetivos básicos de este departamento son:

(Direcciones Web:http://www.peru.gob.pe/docs/PLANES/10018/PLAN_10018_MOF%20GERENCIA%20DE%20INFORMATICA%20Y%20PLANEAMIENTO_2009.pdf http://ahome.gob.mx/1174/files/transparencia/Manual%20de%20funciones/MANUAL%20DE%20FUNCIONES%20DE%20INFORMATICA.pdf http://www.monografias.com/trabajos-pdf/administracion-informatica/administracion-informatica.pdf http://www.munivaldivia.cl/administracion/informatica/informatica.html http://www.bn.com.pe/transparenciabn/mof/dpto-de-informatica.pdf y fecha de consulta: 11/04/2011)

- El objetivo básico del departamento de desarrollo de aplicaciones informáticas consiste en suministrar la información que se necesita para controlar la estrategia y llevar a cabo las diferentes funciones de la empresa, ya sea la propia empresa al que pertenece este departamento o empresas externar a las que van destinas nuestros producto, así como de las herramientas necesarias para su manipulación.
- Aunque el objetivo es único y primordial, se dice que es inalcanzable ya que es el fin al que se debe llegar, y el fin marcará la terminación de todo. Al objetivo uno se acerca y los avances hacia él, se miden por medio de metas, las cuales son concretas y alcanzables.

- Desde la creación del departamento se marcaron un conjunto de metas, las cuales se han ido alcanzando conforme pasa el tiempo, sin embargo al cumplir el ciclo administrativo, planeación y control, y revisar los planes de acción y los logros obtenidos, se replantean nuevas metas que muchas veces son las mismas con algunas innovaciones o mejoras, pudiendo centrarnos en las siguientes como principales y constantes.
- Constituir el grupo como una sola institución e implementar un sistema de información único que funcione para todas las áreas.
- Estandarizar los equipos y sistemas.
- Crear y aplicar un plan de capacitación y adiestramiento constante y eficaz.
- Crear y llevar a cabo un plan de renovación y actualización de equipo y software.
- Mantener la integridad de la información.
- Crear un plan efectivo de contingencia.
- Elaborar programas y sistemas confiables y operativos que faciliten las labores de los empleados y logren ahorros considerables y la toma de
- buenas decisiones.
- Tener documentados todos los sistemas.
- Crear un plan y llevar a cabo las acciones necesarias para salvaguardarnos del problema del año.
- Crear un ambiente sano y cordial entre el personal del departamento y para con los demás usuarios.
- Mantenernos como un departamento líder en los servicios que ofrecemos.

5.2.5.1 Organigrama del Departamento de desarrollo de aplicaciones informáticas

(Direcciones Web: http://www.monografias.com/trabajos-pdf/administracion-informatica/administracion-informatica.pdf http://www.bn.com.pe/transparenciabn/mof/dpto-de-informatica.pdf http://es.scribd.com/doc/60046252/2/Organigrama-del-Departamento-de-Informatica y fecha de consulta: 10/04/2011)

5.2.5.1.1 Jefe de Informática

El jefe de informática tiene la responsabilidad de todas las actividades en la interviene información, incluyendo proceso de datos, soporte técnico, metodología y aplicaciones. También es responsable de los aspectos básicos del personal y administración que pertenecen a su área de actividad.

Algunas de sus funciones son:

- Gestionar las relaciones con los proveedores externos y los eventuales prestadores de servicio.
- Gestionar las relaciones con otros departamentos de la organización para establecer los planes de acción.
- Definir y controlar el presupuesto o una parte del mismo.
- Organizar el departamento informático en todas sus facetas, como el personal, de organización, distribución, horarios, vacaciones…
- Colaborar, aportar sus conocimientos en la definición de la estrategia y los objetivos informáticos.
- Supervisar la implantación y desarrollo de los proyectos informáticos que lleve a cabo el departamento.
- Garantizar la fiabilidad, la coherencia y la evolución del Sistema Informático tanto de punto de vista funcional como del técnico.

5.2.5.1.2 Jefe de Explotación

El jefe de explotación es el encargado de planificar, organizar y controlar el área de explotación, siendo el responsable de todas las actividades relativas a la explotación y producción de los ordenadores tanto de la misma organización como de las externas.

Algunas de sus funciones principales son:

- Coordinar las actividades y recursos técnicos, materiales y de los equipos de soporte en lo que se refiere a sistemas operativos, bases de datos y comunicaciones.
- Resolver las incidencias que los sistemas puedan ocasionar.

- Analizar y decidir la opción óptima del software a utilizar, asi como sus posteriores actualizaciones.
- Planificar, supervisar y coordinar el desarrollo, implantación y mantenimiento de los sistemas operativos, bases de datos, software…
- Garantizar que todo funciones correctamente y tener planes de contingencia preparados para sí fallase alguna cosa poder solucionarlo lo antes posible.
- Responsabilidad de la atención a los usuarios.
- Responsabilidad de garantizar el adecuado nivel de servicio en la explotación de los servicios informáticos.
- Técnico de Explotación
- Esta persona se encarga de proporcionar el conocimiento necesario de instalación y mantenimiento de los servicios de redes, de los equipos y sistemas informáticos.
- Algunas de sus funciones son:
- Definir los procesos, los documentos y ejecutar su control.
- Responsable del buen funcionamiento del sistema informático y sus resultados.
- Gestionar las incidencias y asegurar las soluciones.
- Asegurar el buen funcionamiento físico de los sistemas informáticos.

5.2.5.1.3 Responsable de Calidad

El responsable de este departamento creará el plan de calidad del producto, diseñará y gestionará el despliegue necesario para ejecutar y coordinar las pruebas y revisiones del software. Otras de sus funciones son coordinar y dirigir las actividades relacionadas con gestión de la calidad en todas sus áreas: productos, procesos y procedimientos, y supervisar el cumplimiento de la normativa de calidad, organizando las actividades relativas a la mejora de procesos en todas las áreas. Este responsable puede ayudarse de determinadas herramientas que sirven para analizar el código y determinar su calidad en función de sus líneas de código, como por ejemplo, nos informa de variables declaradas que nunca se utilizan, código repetido, código poco claro…

Dentro de las funciones principales son:

- Verificar el desarrollo y aplicación de la normativa de calidad.
- Cooperar en la determinación de los objetivos de calidad.
- Dirigir la realización del manual de calidad de la compañía, así como realizar las modificaciones pertinentes.
- Responsable de la adecuación entre los desarrollos realizados y las directrices establecidas.
- Definir las normas de desarrollo en colaboración con la Dirección de Informática.
- Implementar y vigilar el cumplimiento de la política de calidad de la empresa.
- Motivar y coordinar los equipos de desarrollo en el marco de aplicación de las normas y métodos en vigor.
- Asegurar la definición de las directrices de calidad, su aplicación así como la estandarización.
- Poner en marcha los procedimientos de prueba y de control de calidad.
- Asegurar la coherencia y la coordinación de su trayectoria con la política global de la organización.
- Tomar a su cargo la campaña de las pruebas de cara al conjunto de los usuarios finales.
- Participar en la distribución de las ediciones originales de las aplicaciones y de los documentos a las entidades de producción garantizando un alto nivel de calidad.
- Garantizar una calidad permanente a través de los procedimientos y de las herramientas.

5.2.5.1.4 Jefe de Desarrollo

El jefe de desarrollo debe garantizar que se produce lo esperado en el tiempo esperado y con el coste esperado. Es labor del jefe de desarrollo decidir cual es el que mejor se adapta a la situación concreta a la que se enfrenta para minimizar la inversión requerida y obtener los resultados esperados.

Algunas de sus funciones son:

- Participa en el proceso de construcción aplicando técnicas de Ingeniería de Software.
- Realizar estimaciones del software a construir.
- Interpretar el diseño y realizar adaptaciones cuando sea necesario.
- Coordinar y llevar a cabo revisiones de código.
- Controlar factores de calidad en la producción del código fuente.
- Dominar las tecnologías y lenguajes empleados para la construcción del software, sirviendo de apoyo a los programadores.
- Dominar técnicas de depuración de errores. La localización y corrección sistemática de errores en el código fuente exige un profundo conocimiento del lenguaje utilizado, las tecnologías empleadas y el sistema operativo, así como de conceptos fundamentales de bases de datos, teoría de sistemas operativos y redes, entre otras.

5.2.5.1.5 Analista

La responsabilidad de los Analistas es elaborar un catálogo detallado de requisitos que permita describir con precisión el sistema de información, para lo cual mantendrán entrevistas y sesiones de trabajo con los usuarios, actuando del interlocutor entre estos y el equipo de proyecto en lo que a requerimientos se refiere. Estos requisitos permiten a los analistas elaborar los distintos modelos que sirven de base para el diseño, obteniendo los modelos de datos y de procesos en el caso del análisis estructurado y los modelos de clases e interacción de objetos en análisis orientado a objeto. Así mismo realizan la especificación de las interfaces entre el sistema y el usuario.

Algunas de las funciones principales son:

- Idear, desarrollar y mantener, y perfeccionar los programas lógicos que rigen el funcionamiento general de las computadoras.
- Mantener actualizados y en buen funcionamiento las bases de datos y los sistemas de gestión de datos para garantizar la validez e integridad de la información registrada.
- Crear y desarrollar lenguajes informáticos.
- Realizar investigaciones acerca de los principios y métodos informáticos.
- Desarrollar y mantener los soportes lógicos y programas, y la estructura

y sistemas de datos.

- Analizar las necesidades de los usuarios y determinar programas, configuraciones y soportes lógicos.

5.2.5.1.6 Programador

La función del programador, miembro del equipo de proyecto, es construir el código que dará lugar al producto resultante en base al diseño técnico realizado por el analista o analista programador, generando también el código asociado a los procedimientos de migración y carga inicial de datos. Igualmente se encarga de elaborar, desarrollar, ensayar y mantener en buen estado los soportes lógicos y/o los programas informáticos, para cubrir las necesidades de los usuarios. Combinándolo con la realización de las pruebas unitarias y participando en las pruebas de conjunto de la aplicación.

Algunas de las funciones son:

- Determinar en colaboración con los Analistas informáticos los objetivos perseguidos con los distintos programas, la naturaleza y fuentes de datos que habrá que introducir y ordenar, y establecer los controles necesarios.
- Elaborar gráficos y diagramas para describir y determinar en que secuencias habrá que proceder al registro y tratamiento de los datos.
- Desarrollar y proporcionar documentación detallada sobre los programas informáticos, utilizando para ello diversos lenguajes de programación.
- Ensayar los programas elaborados para eliminar o corregir deficiencias o errores.
- Mantener actualizados los programas.

5.6.1.1.7 Jefe de Sistemas

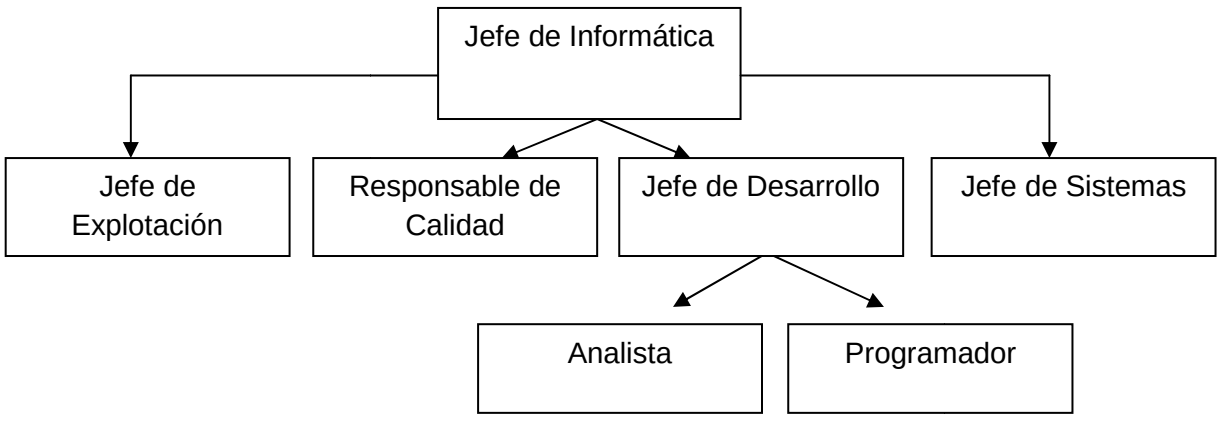
Es el encargado de administrar la red, programar, mantener y coordinar el funcionamiento de los sistemas informático, administrando para ello el equipo de cómputo y aprovechando este recurso para optimizar las actividades de las direcciones y jefaturas haciendo más eficiente el trabajo de cada una de las áreas de la organización. Deberá propiciar que las operaciones se realicen de forma automatizada, incluyendo firmas electrónicas y de que se produzca

oportunamente la información.

Algunas de las funciones son:

- Planificar, supervisar y coordinar el mantenimiento de sistemas operativos, software de mercado y propio, básico o de soporte.
- Definir y actualizar software básico.
- Actualizar y decidir la alternativa óptima de software de mercado a adquirir. Diseñar, en conexión con la Dirección de Informática, la política de hardware, redes y comunicaciones, respecto a adquisiciones, sustituciones, etc.
- Resolver y coordinar las incidencias de los sistemas.
- Dirigir las actividades y recursos, técnicos, materiales y los equipos de soporte en materia de sistemas operativos, bases de datos y comunicaciones.
- Establecer un programa de detección de virus y vacunas apropiadas.
- Desarrollar aplicaciones específicas para las diversas áreas.
- Instalar y configurar de acuerdo a las necesidades de la red, los equipos de nueva adquisición.
- Reinstalar los equipos cuando se trasladen a una nueva ubicación.

En la figura 5.2.5.1 podemos observar cómo queda la jerarquía entre los diferentes miembros del departamento de desarrollo de aplicaciones informáticas:



5.2.5.1 Organigrama del Departamento de desarrollo de aplicaciones informáticas

5.3 Resumen

Como hemos podido comprobar en este capítulo pretendemos explicar el tipo de organización a la que vamos a realizar el plan de auditoría, hemos explicado cuales son las funciones a rasgos generales que debe realizar cada departamento para conseguir que la organización pueda funcionar correctamente, centrándonos en el departamento que más nos interesa, el departamento de desarrollo de aplicaciones informáticas, ya que es sobre este departamento, sobre el cual vamos a realizar el plan de auditoría, y más concretamente sobre las funciones de desarrollo de aplicaciones que realizan las personas que forman parte de este departamento, por este motivo además de explicar las funciones del departamento en general lo hemos detallado un poco más explicando cuales son las personas específicas de este departamento y cuales son las funciones que deben realizar dentro de su departamento.

En el próximo capítulo vamos a realizar el plan de auditoría para el departamento de informática, en concreto para el desarrollo de las aplicaciones, como hemos comentado anteriormente, veremos en un principio la importancia que tiene realizar un plan de auditoría y por consiguiente el propio plan de auditoría a este departamento en cuestión y sus funciones, además de acotar cuales son las funciones o tareas, y por tanto los objetivos a controlar, que son responsabilidad del departamento.

5.4 Bibliografía del capítulo 5

5.4. 1 Libros, Apuntes, Artículos

Autores: Rafael Bernal Montañés i Óscar Coltell Simón. **Título:** Auditoría de los sistemas de información. **Año:** 1996.**Fecha de la consulta:** 21/01/2012.

Título: Dirección y gestión de los sistemas de información en la empresa, Una visión integradora 2º Edición. **Año:** 2006. **Fecha de la consulta:** 21/01/2012.

5.4.2 Webs

Títulos: Tipos de Empresa, Tipos de estructuras organizativas. **Año:** 2009**. Fecha de la consulta:** 11/01/2012. **Dirección:** http://www.mailxmail.com/curso-administracion-empresas-organizacion/tipos-estructuras-organizativas

Autor: LIC. Adafrancys Salazar - Richard Maggiorani. **Título:** Estructura organizativa y tipo de organigrama. **Año:** 2005. **Fecha de la consulta:** 12/01/2012. **Dirección:** http://www.gestiopolis.com/recursos4/docs/ger/estrorgorg.htm

Título: Fundamentos de estructura organizativa. **Fecha de la consulta:** 12/01/2012. **Dirección:** http://es.scribd.com/doc/6286437/Tipos-de-Estructura-Organizacional

6. Plan de auditoría del desarrollo de aplicaciones informáticas

6.1 Introducción a la auditoría en el desarrollo de aplicaciones informáticas: Importancia, características, áreas, objetivos, guías y técnicas de control

En este apartado seguimos el Libro: Autores: Mario G. Piattini, Emilio del Peso. (2001): Auditoría Informática, Un enfoque práctico, 2º Edición. 2001

La importancia de que una organización cuente con unos procedimientos de control es aceptado como garantía de que la organización está gestionando de forma eficaz orientándose a la consecución de los objetivos marcados. La función auditora es precisamente la encargada de comprobar y analizar la existencia de que estos procedimientos de control se están definiendo y aplicando correctamente, determinando las deficiencias que existan al respecto y los riesgos asociados a estas carencias de control.

6.1.1 Importancia de la auditoría del área de desarrollo

Aunque cualquier área de un departamento es susceptible de ser auditada, hay una serie de factores que hacen especialmente importante el área de desarrollo frente a otras áreas dentro del departamento de desarrollo de aplicaciones informáticas, algunos de los factores que podemos destacar son:

- Los avances en tecnología de los computadores han hecho que actualmente el principal factor de éxito de la información sea la mejora de la calidad del software.
- El gasto destinado a software es cada vez más superior al que se destina a hardware.
- El software como producto es muy difícil de validar. Por ello para poder incrementar la calidad del software y disminuir los costes de mantenimiento debemos proporcionar un mayor control en el proceso de desarrollo.

- El índice de fracasos en proyectos de desarrollo es demasiado alto, lo cual nos hace ver el mal o nulo funcionamiento de los controles en este proceso.
- 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.

En la mayoría de los casos para realizar el análisis de un sistema y cuáles son sus procedimientos, es necesario utilizar algún tipo de cuestionario, programa de trabajo o listas de controles. No todos los auditores le dan la misma importancia a los cuestionarios, ya que piensan que la respuesta del tipo 'si' o 'no' son poco realistas y en ocasiones no nos llevan a ninguna situación clara.

Las cuestiones resultan útiles para analizar métodos y procedimientos, pero no permiten comprobar elementos de datos o activos aislados ni demuestran que el procedimiento que se investiga se cumple siempre.

Existen muchos tipos de controles: controles de gestión, operativos, de procedimientos, de rendimiento y de datos.

6.1.2 Características de un sistema de control

Un verdadero sistema de control reúne las siguientes características:

1. Establecimiento de estándares, normas o necesidades, esto incluiría definir con detalle la precisión con la que se deben medir las necesidades. Del mismo modo también debería incluir el periodo durante el cual se van a solucionar dichas necesidades, ya que se va a fijar la frecuencia de admisión de los informes, que deberán adecuarse al problema que se esté tratando.
2. El registro del rendimiento real. Estos registros van a clasificar la información de manera que se adapta a la ordenación de objetivos que se haya fijado.
3. La comparación periódica del rendimiento con los objetivos.
4. Informes de excepción, que notifiquen y expliquen las diferencias que existen entre los objetivos y el rendimiento durante ese período.
5. Acciones correctoras que obliguen a que las actividades vuelvan a obedecer las pautas exigidas. Existen tres tipos posibles de acciones correctoras:
    a. repetir la operación después de eliminar la causa del error, para que se ejecute correctamente,

b. asegurarse de que en el futuro las cosas vayan según los planes, pero aceptando que no se puede modificar lo sucedido y que el error se va a quedar sin corregir, y

c. ajustar las necesidades en un futuro próximo de modo que se cumplan los objetivos generales durante un periodo de tiempo restante, aunque no sea posible alterar lo que haya ocurrido ya.

6. El repaso conjunto de estándares, para utilizarlos en el futuro.

En muchos sistemas de control, la definición de estándares es un problema, porque las condiciones pueden variar mientras se ejerce el control, o podría haberse dado una falta de conocimiento y experiencia cuando se fijaron los estándares por primera vez.

Los objetivos de control sirven para mantener el nivel necesario de autoridad, propiedad y exactitud en los trabajos, y obtener los resultados puntualmente. El ámbito de control es la cantidad de información o actividad relacionada con ella que está sometida a una acción de control.

6.1.3 Áreas de control de un sistema informático

Las áreas de control de un sistema informático son las siguientes:

- Controles gerenciales.
- **Controles del desarrollo**, adquisición y mantenimiento de sistemas de información.
- Controles generales de sistemas de información: operaciones.
- Controles de aplicación.
- Controles de la tecnología.

En este proyecto vamos a tratar sobre la auditoría del área de control de desarrollo de aplicaciones informáticas que como hemos comentado anteriormente resultan de las más interesantes, donde para cada objetivo de control se especificarán una o más técnicas de control, también denominadas simplemente controles, que contribuyen a lograr el cumplimiento de dicho objetivo.

6.1.4 Áreas de control y secciones de control del desarrollo de aplicaciones informáticas

En el área de control de desarrollo de aplicaciones informáticas hay varias secciones, tareas que se deben realizar de una forma específica y controlada para que todo fluya con normalidad y exactitud, cada una de estas secciones constituye un objetivo de control por separado.

6.1.5 Objetivos de control, y guías o técnicas de control del área de desarrollo de aplicaciones informáticas

Todos los **objetivos de control** que vamos a detallar posteriormente son aquellas tareas que la organización debe realizar y tener controladas para que se realicen de la manera adecuada. Para el auditor, estos objetivos de control son las expectativas que tiene acerca del proyecto, que si no se cumplen se introducirán en el informe que eleve a la dirección. Para cada uno de estos objetivos de control se especificará una o más **guías de auditoría o técnicas de control**, mediante estas guías el auditor pretende averiguar si los objetivos mencionados anteriormente se cumplen con exactitud.

6.2. Controles de desarrollo de aplicaciones informáticas

El proceso seguido por una organización en el desarrollo de aplicaciones informáticas debería tratar de alcanzar la efectividad, ahorro y eficiencia del sistema, la integridad de datos, protección de recursos, y el cumplimiento de las leyes y regularizaciones. El uso de una metodología de ciclo de vida de desarrollo de aplicaciones informáticas efectiva, debería proporcionar a la alta dirección de la organización una razonable garantía de que estos objetivos serán alcanzados. Es decir, cada organización debe establecer una metodología para el proceso de desarrollo de aplicaciones informáticas y asignar responsabilidades en cada una de las fases del proceso para que sea posible progresar de una manera más fácil en el diseño y el desarrollo de aplicaciones informáticas.

Áreas a controlar:

- La metodología y responsabilidades del proceso de desarrollo de aplicaciones informáticas
- Las funciones y responsabilidades de cada individuo
- Proceso de actualización de la metodología que sigue la organización en el proceso desarrollo de aplicaciones informáticas

6.2.1 Área a controlar sobre la metodología y responsabilidades del proceso de desarrollo de aplicaciones informáticas

Objetivo de control. El jefe del departamento de desarrollo de aplicaciones informáticas debe utilizar una política, la cual tiene que constar por escrito, en la que se utiliza una metodología para el proceso de desarrollo de aplicaciones como medio de estructuración y control del proceso de desarrollo de aplicaciones informáticas.

Guía de control. Se debe revisar dicha metodología del proceso del desarrollo de aplicaciones de la organización:

1. Revisar la metodología del proceso de desarrollo de aplicaciones de la organización que está actualmente en vigor en la organización y determinar si se utiliza una aproximación estructurada además de determinar si es consistente con los conceptos prácticos empleados en el campo de la computación.

2. Evaluar si cada fase del proceso de desarrollo de aplicaciones de la organización da lugar a un producto cuantificable sobre el cual se pueda hacer una revisión y aprobación final antes de pasar a la siguiente fase.

3. Decidir si la metodología del proceso de desarrollo de aplicaciones de la organización proporciona un mecanismo adecuado para tener controlados los cambios en los requerimientos durante la duración del proyecto.

4. Comprobar la metodología que sigue la organización para determinar si el énfasis puesto sobre cada fase cumple los requisitos de seguridad y los controles internos.

5. Comprobar la extensión, familiaridad de la formación y experiencia que tienen los miembros del departamento de desarrollo de aplicaciones informáticas y del usuario con el uso de la metodología del proceso de desarrollo de aplicaciones de la organización.

6. Determinar si los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización son obligatorios o consecutivos y valorar si estos pueden ser flexibles en el uso de la metodología si las condiciones del proyecto varían, en función, por ejemplo, de si los proyectos son grandes o pequeños.

7. Determinar si se permiten desviaciones de la metodología, revisar cuando pueden ocurrir estas desviaciones, y comprobar si deben ser documentadas y aprobadas.

8. Determinar si la metodología del proceso de desarrollo de aplicaciones informáticas de la organización contiene todos los estándares y requisitos de documentación y programación para los usuarios, programadores, desarrolladores de aplicaciones, analistas y el personal encargado del procesamiento de los datos del departamento de desarrollo de aplicaciones informáticas, departamento informático.

9. Averiguar si la metodología del proceso de desarrollo de aplicaciones informáticas contiene especificaciones de las tecnologías de bases de datos a utilizar, así como la selección e instalación de productos software legal.

10. Determinar si la metodología del proceso de desarrollo de aplicaciones informáticas de la organización está usándose en el desarrollo de software actualmente. Valorar la adecuación, actualización, y adaptabilidad de la metodología para que si cambiamos la tecnología se pueda determinar el grado de riesgo que puede existir en el desarrollo de software de acuerdo con esta.

En el cuadro nº. 6.2.1 se resume el Objetivo y la Guía de control sobre la metodología y responsabilidades del proceso de desarrollo de aplicaciones

Objetivo a controlar: La metodología y responsabilidades del proceso de desarrollo de aplicaciones
Objetivo de control: Se revisará la utilización de una metodología para el proceso de desarrollo: - para cada participante - para las diferentes fases de la metodología del ciclo de vida, **Guía de control** 1. Revisar la metodología que se utiliza 2. Revisar que cada fase da lugar a un producto cuantificable 3. Revisar si la metodología controla la posibilidad de cambios en los requerimientos 4. Comprobar que énfasis puesto en cada fase es el adecuado para cumplir los requisitos de seguridad y control interno. 5. Familiaridad entre metodología y usuarios 6. Comprobar si los requisitos son flexibles en el uso de la metodología si las condiciones del proyecto varían. 7. Determinar si existen desviaciones de la metodología 8. Determinar si la metodología contiene todos los estándares necesarios para los participantes 9. Comprobar si la metodología contiene especificaciones de la tecnología de base de datos, y software legal **10.** Determinar si la metodología está usándose adecuadamente

Fuente: Elaboración propia basada en la documentación del punto 6.2.1.

Cuadro nº. 6.2.1. Resumen de Objetivo a controlar sobre la metodología y responsabilidades del proceso de desarrollo de aplicaciones. Objetivo de control y Guía de control

6.2.2 Las funciones y responsabilidades de cada individuo

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización tiene que especificar en cada etapa todas las funciones del departamento desarrollo de aplicaciones informáticas, así como de los usuarios y del resto del personal, para así poder planificar, revisar, implementar y auditar los productos finalizados por el proceso de desarrollo de aplicaciones informáticas.

Guía de control. Se revisará la asignación de las funciones y responsabilidades de cada empleado luego se amplía con usuarios??? para las diferentes fases de la

metodología del ciclo de vida, proceso de desarrollo de aplicaciones informáticas de la organización.

1. Determinar si el jefe del departamento ha utilizado una política declarada por escrito definiendo aquellas funciones y responsabilidades que tiene cada persona en el proceso de desarrollo de aplicaciones informáticas. Estas funciones deberían incluir a la dirección, a los usuarios finales, al propio equipo del proyecto, al equipo que controla la calidad y el procesamiento de los datos del departamento desarrollo de aplicaciones informáticas.

2. Evaluar si, en cada fase del proceso del desarrollo de aplicaciones de la organización, se pueden modificar las metas, la dirección del desarrollo, el esfuerzo en la dedicación del desarrollo y si se permite el poder decidir si se pasa a la siguiente fase.

3. Determinar si todas las funciones y responsabilidades, realizadas por el equipo del desarrollo de aplicaciones informáticas, están claramente establecidas en la metodología del proceso de desarrollo de aplicaciones informáticas de la organización y además averiguar hasta qué punto se le permite al jefe de proyecto tomar decisiones sobre los costes, presupuestos y resto de tareas.

4. Determinar cómo han sido seleccionados los responsables del departamento de usuario para el equipo del proyecto y hasta qué punto se ve involucrado el departamento de usuario en el proceso de desarrollo de aplicaciones informáticas. Verificar que las responsabilidades asignadas se ajustan con sus capacidades.

5. Controlar en qué medida, bajo la metodología de desarrollo de aplicaciones informáticas de la organización, se ven involucrados en el proceso de desarrollo de aplicaciones informáticas los miembros o el miembro de control de calidad del departamento de desarrollo de aplicaciones informáticas, departamento desarrollo de aplicaciones informáticas.

6. Revisar las disposiciones de la metodología del proceso de desarrollo de aplicaciones de la organización para cada cosa manteniendo una separación de deberes, y asegurar una adecuada supervisión de los controles.

En el cuadro nº. 6.2.2 se resume el Objetivo y la Guía de control sobre las funciones y responsabilidades de cada individuo

Las funciones y responsabilidades de cada individuo
Objetivo de control: Se revisará la asignación de las funciones y responsabilidades: - de cada participante - para las diferentes fases de la metodología del ciclo de vida, **Guía de control** 1. Política declarada por escrito, incluyendo a todos 2. a) Modificaciones, b) Paso a la fase siguiente 3. a) Funciones y responsabilidades en la Metodología, b) Toma de decisiones sobre los costes, presupuestos y resto de tareas por el jefe de proyecto 4. Revisar las selección de los participantes 5. Involucración de cada miembro 6. Adecuada supervisión de los controles

Fuente: Elaboración propia basada en la documentación del punto 6.2.2.

Cuadro nº. 6.2.2 Resumen de Objetivo a controlar sobre las funciones y responsabilidades de cada individuo. Objetivo de control y Guía de control

6.2.3 Proceso de actualización de la metodología que sigue la organización en el proceso desarrollo de aplicaciones informáticas

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería ser revisada de forma periódica por la alta dirección de la organización y así asegurar que se proporcionan procedimientos y técnicas aceptadas y actualizadas en los sistemas de informática.

Guía de control. Se examinarán los mecanismos de la organización para revisar la actualización y la adecuación de la metodología del ciclo de vida, proceso de desarrollo de aplicaciones informáticas.

1. Determinar si existe una manera sistemática para revisar de forma periódica la adecuación y actualización de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización y examinar las evaluaciones más prioritarias de esta metodología.

2. Determinar si se mantiene un registro con las revisiones y modificaciones de la metodología que se utiliza en el proceso de desarrollo de aplicaciones informáticas de la organización.

En el cuadro nº. 6.2.3 se resume el Objetivo y la Guía de control sobre el proceso de actualización de la metodología que sigue la organización en el proceso de desarrollo de aplicaciones.

Proceso de actualización de la metodología que sigue la organización en el proceso desarrollo de aplicaciones informáticas
Objetivo de control: Revisión y actualización de la metodología utilizada.
Guía de control 1. Revisar si existe una forma periódica de revisar la metodología 2. Revisar el registro de modificaciones

Fuente: Elaboración propia basada en la documentación aportada en el capítulo 6.2.3.

Cuadro nº. 6.2.3 Resumen de Objetivo a controlar sobre el proceso de actualización de la metodología que sigue la organización en el proceso de desarrollo de aplicaciones. Objetivo de control y Guía de control

6.3 Objetivos y Guías de Control por fases del proyecto de desarrollo de aplicaciones informáticas

6.3.1 Iniciación del proyecto

Una metodología del proceso de desarrollo de aplicaciones informáticas tendría que tener al departamento usuario involucrado en la identificación del ámbito del proyecto de desarrollo de aplicaciones informáticas. La información para el desarrollo de aplicaciones informáticas debería definirse en formularios escritos, diseños funcionales y técnicos, los cuales deben estar cerrados tanto por parte del cliente como por el

propio personal del departamento desarrollo de aplicaciones informáticas antes de comenzar el proceso de desarrollo de la aplicación informática en cuestión.

Objetivos a controlar:

- Definición del proyecto
- Participación del departamento usuario/cliente en la iniciación del proyecto
- Relación de los miembros del equipo del proyecto y sus responsabilidades
- Definición de los requisitos para la realización del desarrollo de la aplicación
- Aprobación del proyecto

6.3.1.1 Definición del proyecto

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería crear una documentación claramente escrita, que detallara cada una de las tareas a realizar, como se van a realizar y en que tiempos se deben realizar antes de comenzar a trabajar en el proyecto.

Guía de control. Se deberán examinar las metas y propósitos del proyecto de desarrollo de aplicaciones informáticas de la organización antes de comenzar a trabajar en él.

1. Determinar que la metodología del proceso de desarrollo de aplicaciones informáticas de la organización exige los requisitos de solicitud y que estos incluyen la siguiente información:

a. Las razones para realizar el proyecto, incluyendo:
   a.1 Una exposición de los problemas que se van a remediar.

   a.2 Una exposición de las necesidades para la nueva aplicación informática expresadas en términos que realzan las habilidades de la organización para alcanzar estas metas.

   a.4 Las oportunidades que serían proporcionadas para incrementar el ahorro o eficiencia de la aplicación.

   a.5 El control interno o seguridad necesaria que sería satisfecho por el proyecto.

b. Ambiente del proyecto.

c. Alcance del proyecto.
d. Restricciones del proyecto.
e. Beneficios del proyecto.
f. El usuario del proyecto.

2 .Determinar, revisando los registros de los proyectos que todos los requisitos fueron preparados, revisados, y aprobados de acuerdo con la metodología del proceso de desarrollo de aplicaciones que la organización está utilizando.

En el cuadro nº. 6.3.1.1 se resume el Objetivo y la Guía de control sobre la definición del proyecto

Definición del proyecto
Objetivo de control: Revisión de la que metodología incluye un documento con las tareas a realizar.
Guía de control 1. Determinar que la metodología incluye los requisitos y que estos incluyen: a) Exposición del problema, b) Exposición de las necesidades, c) Incremento del ahorro o eficiencia, d) Seguridad que satisfaga el proyecto, e) ambiente del proyecto, f) alcance del proyecto, g) restricciones del proyecto, h) beneficios del proyecto y i) el usuario del proyecto. 2. Revisar que los requisitos fueron preparados, revisados y aprobados.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.1.1.

Cuadro nº. 6.3.1.1 Resumen de Objetivo a controlar sobre la definición del proyecto. Objetivo de control y Guía de control

6.3.1.2 Participación del departamento usuario/cliente en la iniciación del proyecto

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería promover la participación de los responsables del departamento usuario/cliente afectado en la definición y autorización del proyecto de desarrollo de aplicaciones.

Guía de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización será revisada por los participantes del departamento usuario.

1. Revisar los documentos del jefe del departamento de desarrollo de aplicaciones informáticas y los planes de los proyectos a desarrollar para determinar la participación del departamento usuario en el proyecto y en los procesos generales de definición y autorización de los proyectos de desarrollo de aplicaciones informáticas.

2. Entrevistar las direcciones del departamento usuario/cliente afectado para determinar su composición en los proyectos de desarrollo de aplicaciones informáticas en aquello que les esté afectando, y así determinar la naturaleza y extensión de la participación en la definición y aprobación de estos proyectos.

3. Revisar cuales son los presupuestos del departamento usuario afectado para identificar el reparto de tiempo de los miembros del departamento a los proyectos de desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.1.2 se resume el Objetivo y la Guía de control sobre la participación del departamento usuario/cliente en la iniciación del proyecto.

Participación del departamento usuario/cliente en la iniciación del proyecto
Objetivo de control: Revisión de que la metodología promueve la implicación del departamento usuario/cliente
Guía de control 1. Revisar la documentación para determinar la implicación 2. Entrevistar al departamento usuario para saber su participación 3. Revisar los presupuestos del departamento usuario/cliente

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.1.2.

Cuadro nº. 6.3.1.2 Resumen de Objetivo a controlar la participación del departamento usuario/cliente en la iniciación del proyecto. Objetivo de control y Guía de control

6.3.1.3 Relación de los miembros del equipo del proyecto y sus responsabilidades

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería especificar las bases para asignar que miembros de la organización son los más adecuados para realizar cada proyecto de desarrollo de aplicaciones informáticas.

Guía de control. Se revisaran las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para asignar personal al equipo de proyecto y definir cuáles son sus responsabilidades.

1. Identificar, para los proyectos de desarrollo de aplicaciones informáticas, cuales son las personas encargadas del proyecto, los nombres de todos los que componen el equipo del proyecto, y cuáles son sus responsabilidades.

2. Evaluar los antecedentes y cualidades de las persona que van a formar parte del equipo de trabajo para la realización del proyecto, para saber si las tareas que se les han asignado a cada uno de ellos son las apropiadas para los conocimientos que posee cada miembro del grupo.

3. Determinar si los responsables del departamento usuario involucrado en los proyectos seleccionados de desarrollo de aplicaciones informáticas tienen miembros de su departamento participando en los equipos del proyecto y evaluar si estas personas tienen:

    a. Un amplio conocimiento de las necesidades de información que requiere la aplicación que se va a desarrollar.
    b. La habilidad para trabajar con los otros miembros del equipo en el proyecto.
    c. El mismo conocimiento del alcance y objetivo de la aplicación a desarrollar como los otros miembros del equipo.

En el cuadro nº. 6.3.1.3 se resume el Objetivo y la Guía de control sobre la relación de los miembros del equipo y sus responsabilidades.

Relación de los miembros del equipo y sus responsabilidades
Objetivo de control: La metodología debería especificar cuáles son las mejores funciones para cada miembro **Guía de control** 1. Identificar miembros del equipo y sus responsabilidades 2. Saber si la tareas asignadas son la más apropiadas para cada miembro 3. Determinar la participación de los miembros del dep. usuario/cliente y que estos tienen: a) conocimiento de las necesidades, b) habilidades, c) conocimiento alcance y objetivo.

Fuente: Elaboración propia basada en la documentación del punto 6.3.1.3.

Cuadro nº. 6.3.1.3 Resumen de Objetivo a controlar sobre la relación de los miembros del equipo y sus responsabilidades. Objetivo de control y Guía de control

6.3.1.4 Definición de los requisitos para la realización del desarrollo de la aplicación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas debería facilitar que los requisitos de información existentes como los que se acuerden posteriormente debieran estar claramente definidos antes de que el proyecto de desarrollo de aplicaciones informáticas sea aprobado.

Guía de control. Las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización serán revisadas para determinar que la información requerida para el proyecto de la organización será revisada para el proyecto de desarrollo de aplicaciones.

1. Controlar, para los proyectos de desarrollo de aplicaciones informáticas, la adherencia a los requisitos e documentación de la metodología del proceso de desarrollo de aplicaciones. En particular, verificar que:

    a. Las descripciones de los sistemas existentes son adecuados y se pueden utilizar como base para estudiar las necesidades de la nueva aplicación informática propuesta.

b. Han sido identificados claramente aquellos aspectos del sistema existente que se deben cambiar para la aplicación propuesta.
c. Han sido evaluados por el departamento desarrollo de aplicaciones informáticas los requisitos de información para la integridad, consistencia, y viabilidad de procesamiento que serán satisfechos para la nueva aplicación informática.
d. Ha sido revisados y aprobados por los responsables del departamento usuario involucrados en el proyecto de desarrollo estos requisitos de información.

En el cuadro nº. 6.3.1.4 se resume el Objetivo y la Guía de control sobre la definición de los requisitos para la realización del desarrollo de aplicaciones.

Definición de los requisitos para la realización del desarrollo de la aplicación
Objetivo de control: Revisión que la metodología facilita que los requisitos estén claramente definidos
Guía de control 1. Comprobar adherencia entre requisitos y la documentación de la metodología, en concreto: a) descripciones de sistemas existentes son adecuadas, b) identificados aspectos a cambiar, c) evaluados los requisitos, d) revisado y aprobados por en dep. usuario/cliente.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.1.4.

Cuadro nº. 6.3.1.4 Resumen de Objetivo a controlar sobre la definición de los requisitos para la realización del desarrollo de aplicaciones. Objetivo de control y Guía de control

6.3.1.5 Aprobación del proyecto

Objetico de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería facilitar la aprobación de los miembros designados por la dirección a cada proyecto a desarrollar antes de comenzar a trabajar en la siguiente etapa.

Guía de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización se revisará que facilite la aprobación de los miembros

designados por la dirección a cada proyecto a desarrollar antes de comenzar a trabajar en la siguiente etapa.

1. Determinar, revisando los registros de los proyectos de desarrollo de aplicaciones informáticas, que se haya preparado un informe que englobe todos los puntos establecidos como requisitos de la aplicación a desarrollar y que estén definidos los requisitos de información del proyecto.

2. Comprobar, que el jefe del departamento de aplicaciones informáticas y del departamento de usuario ha revisado los informes de cada miembro que forman parte del proyecto de desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.1.5 se resume el Objetivo y la Guía de control sobre la aprobación del proyecto.

Aprobación del proyecto
Objetivo de control: Revisión de que la metodología facilita la designación de cada miembro para cada tarea
Guía de control 1. Comprobar que se ha hecho un informe que aporta toda la información 2. Comprobar que el resp. del dep. usuario ha revisado dichos informes.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.1.5.

Cuadro nº. 6.3.1.5 Resumen de Objetivo a controlar sobre la aprobación del proyecto. Objetivo de control y Guía de control

6.3.2 Estudio de la viabilidad

Objetivo de control. Una metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar un estudio de la viabilidad para alcanzar las metas de la aplicación a desarrollar junto con el análisis de coste y beneficio para cada aplicación a desarrollar.

Guía de control. Se comprobaran las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización que exigen el análisis de líneas alternativas de acción para satisfacer los requisitos de información establecidos para el nuevo proyecto a desarrollar.

Objetivos a controlar:

- Estudio de viabilidad en la tecnología utilizada

6.3.2.1 Estudio de la viabilidad en la tecnología utilizada

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones de la organización debería facilitar un examen de la viabilidad técnica de cada alternativa para satisfacer los requisitos de información establecidos para la nueva aplicación.

Guía de control. Revisar, para los proyectos de desarrollo de aplicaciones, el informe preparado de viabilidad técnica de cada una de las alternativas para cada proyecto de desarrollo de aplicaciones seleccionado.

1. Evaluar la forma en la cual este informe debe incluir los puntos siguientes:

    a. Necesidades del los miembros que forman parte del equipo y su disponibilidad.
    b. Necesidades de software, hardware y su disponibilidad.
    c. Restricciones de tiempo y espacio vigentes.
    d. Viabilidad operacional de la nueva aplicación dentro de la unión del hardware, software, y ambiente de comunicaciones de la organización.
    e. Consideraciones legales relacionadas con la transferencia de datos.
    f. Restricciones legales relativas al uso de tecnología y la manera para obtener la aprobación de la autoridad correspondiente.

2. Verificar, para los proyectos de desarrollo de sistemas de aplicaciones informáticas de la organización, los responsables del departamento usuario afectado y el departamento de desarrollo de aplicaciones Informáticas han añadido a la viabilidad:
    a. El plan de datos y equipamiento necesario.
    b. La formación de los miembros o usuarios indicados.

c. Los controles adecuados sobre los test de programas y datos.
d. La recogida y análisis de los datos relevantes.
e. Los escritos de los informes requeridos.

3. Determinar, con una revisión de la documentación de los test de los proyectos de desarrollo de aplicaciones informáticas realizados:
   a. La fuente, tipo, y adecuación del generador de test.
   b. Los datos de transacciones reales.
   c. El análisis de los resultados de los test.

En el cuadro nº. 6.3.2.1 se resume el Objetivo y la Guía de control sobre el estudio de viabilidad en la tecnología utilizada.

Estudio de viabilidad en la tecnología utilizada
Objetivo de control: Revisión de que la metodología facilita examen de viabilidad técnica
Guía de control 1. Revisar el informe preparado y que este incluye: a) necesidades de los miembros, b) necesidades software, hardware, c) restricción tiempo, d) viabilidad operacional, e) legalidad transferencia de datos, f) restricciones legales 2. Verificación de que los responsables dep, informática y dep usuario/cliente incluyen: a) plan datos y equipamiento, b) formación usuarios afectados, c) controles sobre test y datos, d) regida y análisis de datos, e) escritos de los informes 3. Determinar con revisión de los test: a) fuente, tipo y adecuación del generador de test, b) datos de transacciones reales, c) análisis de los resultados.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.2.1.

Cuadro nº. 6.3.2.1 Resumen de Objetivo a controlar sobre el estudio de viabilidad en la tecnología utilizada. Objetivo de control y Guía de control

6.3.3 Desarrollo e Implantación

Una metodología del proceso de desarrollo de aplicaciones debería asegurar, que están establecidos los objetivos de programación para el proyecto, las

responsabilidades para la programación están asignadas, que los sistemas manuales están preparados, además de todos los estándares de testeo, los criterios de aceptación y validación de aplicaciones están creados para cada proyecto de desarrollo de aplicaciones informáticas.
Objetivos a controlar:

- Los objetivos de programación
- Documentación detallada de programas
- Paquetes de aplicaciones software
- Programación de la aplicación a desarrollar
- Manual de mantenimiento y operaciones
- Manuales de usuario
- Plan de formación
- Estándares de testeo de las aplicaciones
- Estándares de pruebas de la aplicación
- Documentación del testeo de la aplicación
- Evaluación de los resultados de los test
- Análisis de la documentación de conversión

6.3.3.1 Los objetivos de programación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones de la organización debería exigir que se cree un informe por escrito con los objetivos de programación que se van a realizar para cada proyecto de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán los requisitos que los informes por escrito de los objetivos de programación a conseguir para todos los proyectos de desarrollo de aplicaciones están en los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas.

1. Revisar la documentación para los proyectos de desarrollo de aplicaciones informáticas y determinar si ésta incluye unos informes adecuados declarando los objetivos de programación a realizar en el desarrollo de aplicaciones

informáticas, y si estas se ajustan a las disposiciones relativas de la metodología del proceso de desarrollo de aplicaciones de la organización.

En el cuadro nº. 6.3.3.1 se resume el Objetivo y la Guía de control sobre el desarrollo e implantación.

Desarrollo e implantación
Objetivo de control: Revisión de que la metodología incluye escrito con objetivos de programación
Guía de control 1. Revisar documentación para comprobar la inclusión de estos escritos

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.1.

Cuadro nº. 6.3.3.1 Resumen de Objetivo a controlar sobre el desarrollo e implantación. Objetivo de control y Guía de control

6.3.3.2 Documentación detallada de programas

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones de la organización debería exigir que esté creada una documentación muy bien detallada de los programas para cada proyecto de desarrollo de aplicaciones.

Guía de control. Se revisarán los requisitos de la metodología del proceso de desarrollo de aplicaciones de la organización para determinar que para cada proyecto de desarrollo de aplicaciones de información esté creada una documentación claramente detallada de programas.

1. Revisar las descripciones que forman parte de la documentación del programa y determinar su extensión para saber si se ajusta a la descripción definida en la aplicación original.

2. Revisar si en la documentación de los proyectos de desarrollo de aplicaciones esta la información de la descripción lógica claramente y consistentemente escrita para la documentación de los proyectos de desarrollo de aplicaciones

ya que personas no familiarizadas deben ser capaces de entender sus funciones.

3. Determinar, mediante una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas, si la metodología del proceso de desarrollo de aplicaciones informáticas de la organización exige que se prepare un diagrama de flujo para cada proyecto y comprobar si esta documentación existente cumple este requisito.

4. Hablando con el administrados de la base de datos de la organización y con una revisión de la documentación de los proyectos, comprobar si los datos elementales utilizados por los proyectos seleccionados:
   a. Tienen designados unos propietarios.
   b. Están apropiadamente descritos.
   c. No están en conflicto con otras definiciones en la base de datos.

En el cuadro nº. 6.3.3.2 se resume el Objetivo y la Guía de control sobre la documentación detallada de programas.

Documentación detallada de programas
Objetivo de control: Revisión de que la metodología exige la creación de una documentación bien detallada
Guía de control 1. Revisar que la documentación se ajusta a las descripciones originales 2. Revisar que la documentación incluye la descripción lógica 3. Determinar la exigencia de la creación de un diagrama de flujo 4. Comprobar que los datos utilizados tienen: a) designados propietarios, b) descritos correctamente, c) sin conflictos con otras definiciones.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.2.

Cuadro nº. 6.3.3.2 Resumen de Objetivo a controlar sobre la documentación detallada de programas. Objetivo de control y Guía de control

6.3.3.3 Paquetes de aplicaciones software

Objetivos de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar paquetes software que satisfagan las necesidades de un proyecto de desarrollo así como ser compatible con las operaciones de procesamiento de datos existentes en el departamento que satisfagan las necesidades de un proyecto de desarrollo de aplicaciones determinado. Los procedimientos de adquisición del software debería seguir las políticas de la organización, y estos deberían ser testados y revisados antes de ser utilizados.

Guía de control. Se revisarán las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización que gestionan la adquisición de paquetes de aplicaciones software.

1. Revisar, los contratos de adquisición de los paquetes de software para cada proyecto de desarrollo de aplicaciones y así poder determinar si:

    a. Las condiciones de compra se ajustan a las políticas que fueron aprobadas por escrito por los miembros del departamento usuario afectado y el departamento de desarrollo aplicaciones informáticas.
    b. La documentación suministrada con estos paquetes y los controles proporcionados en los programas son los adecuados.
    c. Los paquetes fueron testeados y revisados antes de ser utilizados y pagados.

En el cuadro nº. 6.3.3.3 se resume el Objetivo y la Guía de control sobre los paquetes de aplicaciones software.

Paquetes de aplicaciones software
Objetivo de control: Revisión de que la metodología incluye paquetes software adecuados para cada desarrollo
Guía de control
1. Revisar los contratos de adquisición y determinar si: a) condiciones de compra, b) la documentación suministrada por los paquetes, c) los paquetes se testearon y revisaron antes de pagarse y utilizarse.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.3.

Cuadro nº. 6.3.3.3 Resumen de Objetivo a controlar sobre los paquetes de aplicaciones software. Objetivo de control y Guía de control

6.3.3.4 Programación de la aplicación a desarrollar

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar un contrato para la realización de la programación de la aplicación, los proyectos finales que se entregan al cliente deben estar testeados por las personas responsables propias de equipo de desarrollo antes de que se pague y sean entregados al cliente.

Guía de control. Revisar que este contrato está claramente detallado en la metodología del proceso de desarrollo de aplicaciones informáticas de la organización.

1. Revisar, para los proyectos de desarrollo de aplicaciones informáticas seleccionados, los requisitos de los servicios del contrato de programación para determinar cuál es:
   a. La razonabilidad de los requisitos.
   b. La aprobación de tales requisitos antes de adquirir los servicios.

2. Determinar, con entrevistas y una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas, si el proveedor del contacto de servicios de programación recibió consejos adecuados de los estándares de documentación de programas de la organización, así como de las disposiciones de las declaraciones de los objetivos de programación del proyecto.

3. Revisar que la documentación del contrato de los servicios de programación de aplicaciones informáticas y determinar si fueron testados por el grupo de desarrollo de aplicaciones más en concreto los responsables de calidad y que fueron aprobados de acuerdo con las disposiciones del contrato y de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización.

En el cuadro nº. 6.3.3.4 se resume el Objetivo y la Guía de control sobre la programación de la aplicación a desarrollar.

Programación de la aplicación a desarrollar
Objetivo de control: Revisión del contrato para la programación de la aplicación
Guía de control 1. Revisión de los requisitos de contrato para terminar: a) razonabilidad de los requisitos, b) aprobación de los mismos 2. Comprobar que los estándares de documentación de programas utilizados son adecuados. 3. Comprobar que todo el código programado fue testeado por los responsables.

Fuente: Elaboración propia basada en la documentación aportada en el capítulo 6.3.3.4.

Cuadro nº. 6.3.3.4 Resumen de Objetivo a controlar sobre la programación de la aplicación a desarrollar. Objetivo de control y Guía de control

6.3.3.5 Manual de mantenimiento y operaciones

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debe exigir la preparación de manuales de mantenimiento y operaciones adecuadas como parte de cada proyecto de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización que debe exigir promover la preparación de manuales de mantenimiento como parte de cada proyecto de desarrollo de aplicaciones informáticas.

1. Verificar que la metodología del proceso de desarrollo de aplicaciones informáticas de la organización contiene toda la documentación de los manuales de ejecución para cada proyecto de desarrollo de aplicaciones informáticas.

2. Comprobar que la documentación de los proyectos de desarrollo de aplicaciones informáticas a desarrollar y que los manuales de ejecución de operaciones individuales:

   a. Se ajustan a la metodología del proceso de desarrollo de aplicaciones informáticas de la organización.
   b. Son accesibles y comprensibles para los operadores.
   c. Son utilizados en los test del software.

3. Verificar, para los proyectos de desarrollo de aplicaciones informáticas seleccionados, que para cada paso del trabajo los manuales de ejecución de los operadores individuales especifican:
   a. La función del programa.
   b. Los requisitos hardware.
   c. Los requisitos software.
   d. Explicación de todos los mensajes de consola, junto con la respuesta adecuada del operador.
   e. Identificación adecuada de las etiquetas de los ficheros de salida.
   f. Puntos adecuados de reinicio o procedimientos de notificación de errores o condiciones de fallos.
   g. Controles checkpoint para manejar de forma adecuada el control de ejecución en ejecución.

En el cuadro nº. 6.3.3.5 se resume el Objetivo y la Guía de control sobre el manual de mantenimiento y operaciones.

Manual de mantenimiento y operaciones
Objetivo de control: Revisión de que la metodología exige la preparación de manuales de mantenimiento y operaciones
Guía de control 1. Comprobar que la metodología contiene los manuales 2. Comprobar que los manuales de ejecución: a) se ajustan a la metodología, b) accesibles y comprensibles, c) utilizados en los test 3. Comprobar que los manuales especifica: a) la función del programa, b) los requisitos hardware, c) los requisitos software, d) explicación de tdos los mensajes de consola, e) identificación adecuada de las etiquetas de los ficheros de salida, f) puntos adecuados de reinicio, g) controles checkpoint.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.5.

Cuadro nº. 6.3.3.5 Resumen de Objetivo a controlar sobre el manual de mantenimiento y operaciones. Objetivo de control y Guía de control

6.3.3.6 Manuales de usuario

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debe exigir promover la preparación de manuales de usuario como parte de cada proyecto de desarrollo de aplicaciones informáticas.

Guía de control. Se revisaran las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización obligando la preparación de manuales adecuados de usuario como parte de cada proyecto de desarrollo de aplicaciones informáticas.

1. Verificar que la metodología del proceso de desarrollo de aplicaciones informáticas de la organización define la documentación o manual para cada proyecto de desarrollo de aplicaciones informáticas.

2. Verificar, mediante entrevistas y revisiones la documentación de los proyectos de desarrollo de aplicaciones informáticas seleccionados y comprobar que los manuales de usuario incluyen la adecuada información sobre:

a. Especificaciones y diseños de entrada de datos.
b. Formas de presentar datos al departamento desarrollo de aplicaciones informáticas.
c. La responsabilidad para resolver errores u otras incongruencias.
d. La asignación de prioridades de procesamiento.
e. La lógica, seguridad, vigencia y disposiciones de las salidas.
f. La lógica de programación.
g. El registro de aprobación de usuario.
h. El registro de solicitudes y aprobaciones de cambios de la aplicación.
i. Procedimientos para encender y apagar terminales y servidores.
j. Descripción de los mapas de la pantalla del terminal y de los comandos disponibles.
k. Especifica claramente la forma de utilizar cada una de las pantallas, indicando que datos son dependientes de otros.
l. Específica la funcionalidad de cada una de las pantallas.

3. Verificar, mediante la realización de entrevista y revisiones de la documentación de los proyectos de desarrollo de aplicaciones informáticas que los manuales de usuario

están distribuidos de acuerdo a la metodología del proceso de desarrollo de aplicaciones informáticas y que estos manuales son utilizados en el testeo del software.

En el cuadro nº. 6.3.3.6 se resume el Objetivo y la Guía de control sobre los manuales de usuario.

Manuales de usuario
Objetivo de control: Revisión de que la metodología exige la preparación de manuales de usuario
Guía de control 1. Revisar que está definido el manual para cada proyecto j. Comprobar que los manuales incluyen: a) especificaciones y diseños de entrada de datos, b) formas de presentar datos, c) responsabilidad para resolver errores, d) la asignación de prioridades, e) lógica, seguridad, vigencia y disposiciones de las salidas, f) lógica de programación, g) el registro de aprobación de usuario, h) registro de solicitudes y aprobaciones de cambios de la aplicación, i) procedimientos para encender y apagar terminales y servidores, j) descripción de los mapas, k) especifica utilización de cada pantallas, l) específica la funcionalidad de las pantallas.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.6.

Cuadro nº. 6.3.3.6 Resumen de Objetivo a controlar sobre los manuales de usuario. Objetivo de control y Guía de control

6.3.3.7 Plan de formación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debe exigir un plan para formar a los grupos de mantenimiento y operaciones del departamento usuario afectado y departamento de aplicaciones informáticas como una parte de cada proyecto de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para llevar a cabo un plan

de coordinación para la formación de los miembros de los departamentos usuario y los grupos de mantenimiento y operaciones del departamento de aplicaciones Informáticas.

1. Revisar la documentación de los proyectos de desarrollo de aplicaciones informáticas, comprobar si hay un plan escrito para formar a cada miembro del departamento usuario y a los de mantenimiento y operaciones del departamento de aplicaciones Informáticas además de verificar que el plan deja suficiente tiempo para completar las actividades de formación requeridas.

2. Verificar, entrevistando a los usuarios de los proyectos de desarrollo de aplicaciones informáticas para comprobar que planes han sido ejecutados, y la completitud de la información proporcionada.

En el cuadro nº. 6.3.3.7 se resume el Objetivo y la Guía de control sobre el plan de formación.

Plan de formación
Objetivo de control: Revisión de que la metodología exija un plan para formar los grupos de mantenimiento
Guía de control 1. Determinar si hay un escrito para formar a cada miembro que vaya estas funciones. 2. Revisar la completitud de la formación proporcionada.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.3.7.

Cuadro nº. 6.3.3.7 Resumen de Objetivo a controlar sobre el plan de formación. Objetivo de control y Guía de control

6.3.4 Testeo y Pruebas

6.3.4.1 Estándares de testeo y pruebas de las aplicaciones

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar los estándares para el testeo e implementación de la nueva aplicación a desarrollar.

Guía de control. Se revisaran las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización que establece los estándares de testeo e implementación del software.

1. Verificar que la metodología del proceso de desarrollo de aplicaciones informáticas de la organización establece los estándares adecuados para el testeo e implementación de la aplicación creada.

2. Verificar que no se queda ninguna función por terminar de programar, que el código ejecutado fue testeado y que los resultados se ajustan a las especificaciones del proyecto original.

3. Revisar los estándares de testeo de aplicaciones informáticas individuales proporcionados por la metodología del proceso de desarrollo de aplicaciones informáticas de la organización.

4. Determinar si se proporcionan adecuados estándares para la participación de los responsables del departamento usuario/cliente, de los miembros de programación y control de calidad del departamento de aplicaciones Informáticas, en la preparación de los datos del test para revisar y aprobar los resultados del test.

En el cuadro nº. 6.3.4.1 se resume el Objetivo y la Guía de control sobre los estándares de testeo de las aplicaciones

Estándares de testeo de las aplicaciones
Objetivo de control: Revisión de que la metodología proporciona estándares para el testeo e implementación
Guía de control 1. Revisar que la metodología establece los estándares adecuados 2. Comprobar que esta todo programado, testeado y los resultados son los esperados. 3. Revisar los estándares de pruebas. 4. Determinar que los estándares utilizados son los adecuados.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.4.1.

Cuadro nº. 6.3.4.1 Resumen de Objetivo a controlar sobre los estándares de testeo de las aplicaciones. Objetivo de control y Guía de control

6.3.4.2 Documentación del testeo de la aplicación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar por escrito las actividades y los resultados del testeo de la aplicación que haya desarrollado el equipo de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones del proceso de desarrollo de aplicaciones informáticas de la organización que requieren que los resultados de los test de la aplicación sean incluidos en el registro escrito de las actividades del proyecto para todos los proyectos de desarrollo de aplicaciones informáticas.

1. Determinar, con una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas seleccionados, si:
    a. La aplicación fue testeada de acuerdo con el plan de verificación, validación y test.
    b. Todos las funcionalidades más críticas de la aplicación fueron incluidos en el proceso de testeo.
    c. Los materiales de testeo fueron adecuadamente controlados durante el proceso de testeo.
    d. Los resultados del proceso fueron aprobados por los responsables del departamento usuario afectado y por el departamento de desarrollo de aplicaciones informáticas y el responsable del control de calidad del departamento.
    e. El registro de este proceso de testeo y aprobación fue correcto.
    f. Se incluyó un informe escrito de los resultados en los informes de las actividades del equipo de desarrollo de aplicaciones informáticas.

2. Averiguar, a través de entrevistas con los responsables del departamento usuario afectado del proyecto en cuestión y documentación aportada de los proyectos de desarrollo de aplicaciones informáticas, si los responsables del departamento usuario fueron conscientes de la importancia del proceso de testeo, participando de una forma adecuada, y fueron responsables y consecuentes de aprobar los resultados del proceso de testeo.

3. Clarificar, si los controles de acceso y autorización fueron adecuadas mediante una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas.

4. Determinar si se han desarrollados procedimientos por escrito para mantener la adecuación de estos controles durante el funcionamiento de la aplicación por parte tanto, de los responsables del departamento usuario como los por parte del equipo de trabajo de departamento de desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.4.2 se resume el Objetivo y la Guía de control sobre la documentación del testeo de la aplicación.

Documentación del testeo de la aplicación
Objetivo de control: Revisión de que la metodología incluye por escrito las actividades y los resultados del testeo
Guía de control 1. Determinar si: a) La aplicación fue testeada, b) todas las funcionalidades críticas fueron testeadas, c) los materiales utilizados fueron los correctos, d) resultado aprobados por dep. usuario y dep. informática, e) el registro y aprobación fue correcto, f) se incluye informe con los resultados 2. Comprobar si los responsables fueron conscientes, participaron, responsables y consecuentes del proceso de testeo 3. Determinar si los controles de acceso y autorización fueron adecuados 4. Determinar si hay escritos que garanticen la futura adecuación de estos controles.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.4.2.

Cuadro nº. 6.3.4.2 Resumen de Objetivo a controlar sobre la documentación del testeo de la aplicación. Objetivo de control y Guía de control

6.3.4.3 Evaluación de los resultados de los test

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería promover, como parte de cada proyecto de desarrollo de aplicaciones informáticas, que los resultados del testeo de la aplicación sean evaluados y aprobados por los responsables del departamento usuario/cliente así como del departamento de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones del proceso de desarrollo de aplicaciones de la organización que verifican que los resultados de los test han sido evaluados y aprobados por los responsables del departamento usuario y los miembros del departamento de desarrollo de aplicaciones encargados.

1. Determinar, con la revisión de la documentación de los test de los proyectos de desarrollo de aplicaciones informáticas, si los resultados previstos fueron desarrollados antes que los obtenidos por el test de la aplicación en la realidad, que fueron comprobados los dos resultados, y que ambos coincidieron. Cuando los resultados de los test difieren de los previstos, el auditor debería examinar estas diferencias y obtener una explicación de los individuos involucrados en el proceso de revisión y aprobación de los resultados del test.

2. Determinar, con una revisión de la documentación de los test de los proyectos de desarrollo de aplicaciones informáticas, si contienen informaciones como:
    a. Listados de los datos de los test.
    b. Informes o salidas de la aplicación.
    c. Las entradas relevantes del log de la aplicación.

3. Determinar, con una revisión de la documentación de los test de los proyectos de desarrollo de aplicaciones informáticas, si se hicieron test de backups y restauraciones, responsabilidades y capacidades, planes de fallos, y planes de contingencias, y si los resultados de estos fueron evaluados y aprobados por los responsables del departamento usuario y los miembros del departamento desarrollo de aplicaciones informáticas encargados de tal responsabilidad.

En el cuadro nº. 6.3.4.3 se resume el Objetivo y la Guía de control sobre la evaluación de los resultados de test.

Evaluación de los resultados de test
Objetivo de control: Revisar que la metodología exige que los resultados del testeo se evaluados y aprobados
Guía de control 1. Determinar que los resultado previstos fueron desarrollados antes de los obtenidos y que coinciden 2. Comprobar que la documentación de test contiene: a) listado de datos de test, b) informes de la aplicación, c) entradas relevantes 3. Revisar que se hicieron test de backups y restauraciones, responsabilidades y capacidades, planes de fallos, y planes de contingencias, y si los resultados de estos fueron evaluados y aprobados.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.4.3.

Cuadro nº. 6.3.4.3 Resumen de Objetivo a controlar sobre la evaluación de los resultados de test. Objetivo de control y Guía de control

6.3.4.4 Análisis de la documentación del testeo

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería promover, que antes de la conversión, los responsables del departamento del desarrollo de aplicaciones informáticas asegurase que la documentación de todos los programas, los manuales de usuario y los de operación, estén completos y listos para ser utilizados por el personal del mismo y del departamento usuario.

Guía de control. Se revisarán las disposiciones del proceso de desarrollo de aplicaciones informáticas de la organización para verificar la exactitud de la documentación, confirmando que los responsables del departamento de desarrollo de aplicaciones informáticas y del departamento usuario revisaron la exactitud de la información.

1. Revisar los test, tanto de los responsables del departamento de desarrollo de aplicaciones informáticas con el usuario, para determinar que se terminó la documentación antes de la conversión.

2. Revisar la documentación de la nueva aplicación para determinar si incluye la documentación.

En el cuadro nº. 6.3.4.4 se resume el Objetivo y la Guía de control sobre el análisis de la documentación e conversión.

Análisis de la documentación del testeo
Objetivo de control: Revisión de que antes de la conversión toda la información este detallada **Guía de control** 1. Revisión de los test 2. Revisar la documentación de la nueva aplicación.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.4.4.

Cuadro nº. 6.3.4.4 Resumen de Objetivo a controlar sobre el análisis de la documentación del testeo. Objetivo de control y Guía de control

6.3.4.5 Test de aceptación final

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería promover, como una parte del test de aceptación final una evaluación de los resultados de test por los responsables del departamento usuario y del departamento de desarrollo de aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones del proceso de desarrollo de sistemas de la organización que requieren de los responsables del departamento usuario y de los miembros del departamento de desarrollo de aplicaciones informáticas encargados la evaluación de los resultados del test de aceptación final o de control de calidad para las nuevas aplicaciones informáticas.

1. Verificar que la metodología del proceso de desarrollo de aplicaciones informáticas de la organización define los estándares adecuados para el test de aceptación final de las nuevas aplicaciones informáticas.

2. Determinar, con una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas, si los responsables del

departamento usuario y los miembros del departamento de desarrollo de aplicaciones informáticas, tanto programadores, analistas… como el responsable de calidad, participaron en la evaluación del desarrollo de la nueva aplicación.

3. Determinar si cualquier ineficiencia encontrada en la conversión fue remitida antes de que la aplicación fuese declarada operacional.

En el cuadro nº. 6.3.4.5 se resume el Objetivo y la Guía de control sobre el test de aceptación final.

Test de aceptación final
Objetivo de control: Revisión de que la metodología promueve una evaluación de los resultados de test
Guía de control 1. Verificar que la metodología define estándares adecuados para el test de aceptación final 2. Verificar que todos los miembros que forman parte del desarrollo participaron en la evaluación.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.4.5.

Cuadro nº. 6.3.4.5 Resumen de Objetivo a controlar sobre el test de aceptación final. Objetivo de control y Guía de control

6.3.5 Operación y mantenimiento

Una metodología del proceso de desarrollo de aplicaciones informáticas de la organización debe asegurar, para cada proyecto de desarrollo de aplicaciones informáticas, que están establecidos los objetivos de programación para el proyecto, los procedimientos de operaciones y mantenimiento están establecidos para asegurar que los datos son procesados exacta y consistentemente y que el contenido del sistema será modificado solamente con la apropiada autorización.

Objetivos a controlar:

- Procedimientos de control de operaciones
- Control de costes

- Modificaciones de la aplicación
- Re-evaluación de los requisitos del usuario/cliente

6.3.5.1 Procedimientos de control de operaciones

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería asegurar que se han instalado adecuadamente los procedimientos para controlar las actividades de procesamientos de datos de una nueva aplicación informática.

Guía de control. Se revisará las disposiciones del proceso de desarrollo de aplicaciones informáticas de la organización para determinar que se han implantado adecuados procedimientos para controlar las actividades de procesamiento de datos de una nueva aplicación informática.

1. Determinar, con una revisión de la documentación de los proyectos de desarrollo de aplicaciones informáticas, si los procedimientos de control establecidos por los responsables del departamento usuario y el departamento de desarrollo de aplicaciones informáticas son adecuados a los tipos de los ficheros manteniendo las transacciones procesadas por la nueva aplicación.

2. Determinar que los procedimientos de control incluyen controles adecuados de distribución de salidas, de manera que solamente las reciba el personal autorizado del departamento usuario afectado.

3. Determinar que están identificados, controlados, corregidos y adecuadamente reprocesados los procedimientos que aseguran los errores durante la vida de la nueva aplicación.

4. Determinar que los procedimientos aseguran que las funciones de las operaciones clave, incluyen las operaciones de programas de aplicaciones, seguridad de datos, introducción de datos, además de que las bases de datos hayan sido desarrolladas por diferentes individuos y que esta separación de deberes ha sido forzada por los responsables del departamento desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.5.1 se resume el Objetivo y la Guía de control sobre el procedimiento de control de operaciones.

Procedimiento de control de operaciones
Objetivo de control: Revisión de que la metodología asegure que se han instalado los procedimientos para el control las actividades de procesamiento de datos
Guía de control 1. Determinar si los procedimientos de control establecidos son los adecuados 2. Determinar que existen controles adecuados en la distribución de las salidas Determinar que están identificados, controlados, corregidos y reprocesados los procedimientos que aseguran los errores de la aplicación.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.5.1.

Cuadro nº. 6.3.5.1 Resumen de Objetivo a controlar sobre el procedimiento de control de operaciones. Objetivo de control y Guía de control

6.3.5.2 Control de costes

Objetivo de control. El sistema de contabilización de la organización debería almacenar, analizar, e informar de los costes asociados con el funcionamiento de la nueva aplicación.

Guía de control. Se revisará los procedimientos de contabilidad usados rutinariamente para almacenar, analizar, e informar de los costes asociados con el funcionamiento de la nueva aplicación informática.

1. Revisar los procedimientos usados por el sistema de contabilización de la organización para registrar, analizar, e informar los costes asociados con el funcionamiento de la nueva aplicación informática.

2. Verificar que los procedimientos son adecuados y que han sido revisados y aprobados por los responsables del departamento usuario afectado y el departamento de desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.5.2 se resume el Objetivo y la Guía de control sobre el control de costes.

Control de costes
Objetivo de control: El sistema de contabilización debe controlar los costes de la aplicación
Guía de control 1. Revisar los procedimientos que utiliza este sistema 2. Verificar que los procedimientos son los adecuados

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.5.2.

Cuadro nº. 6.3.5.2 Resumen de Objetivo a controlar sobre el sobre el control de costes. Objetivo de control y Guía de control

6.3.5.3 Modificaciones de la aplicación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería establecer procedimientos para controlar los cambios de todas las aplicaciones informáticas.

Guía de control. Se revisarán las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para determinar que se han controlado los cambios de la aplicación.

1. Determinar con una revisión de la documentación de las aplicaciones informáticas si los cambio de estas aplicaciones se han registrado y procesado de una forma oportuna.

2. Determinar si los cambios propuestos a estas aplicaciones están aprobados por los responsables del departamento usuario afectado antes de comenzar a trabajar.

3. Determinar que todos los registros de los cambios actualmente hechos, incluyendo las revisiones de los diagramas de flujo de datos y la evaluación y aprobación de los resultados de los test, están incorporados en la documentación acumulada por el departamento de desarrollo de aplicaciones informáticas.

En el cuadro nº. 6.3.5.3 se resume el Objetivo y la Guía de control sobre la modificación de la aplicación.

Modificación de la aplicación
Objetivo de control: Revisión de que la metodología establezca procedimientos para controlar los cambios
Guía de control 1. Revisar si se registran los cambios 2. Revisar que los cambios están aprobados 3. Revisar que los cambios están en la documentación del proyecto

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.5.3.

Cuadro nº. 6.3.5.3 Resumen de Objetivo a controlar sobre la modificación de la aplicación. Objetivo de control y Guía de control

6.3.5.4 Re-evaluación de los requisitos del usuario/cliente

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería promover revisiones periódicas de los requisitos de usuario para comprobar si estos pueden haber cambiado desde el principio de la toma de requerimientos.

Guía de control. Se revisarán las disposiciones del proceso de desarrollo de aplicaciones informáticas de la organización para verificar que las revisiones periódicas de los requisitos de usuario para la aplicación en cuestión son realizadas.

1. Determinar con una revisión de las peticiones de cambios de la aplicación informática, la extensión de las necesidades de usuario insatisfechas.

2. Determinar, mediante entrevistas o la distribución de un cuestionario, la naturaleza de los cambios solicitados en estas aplicaciones por los responsables del departamento usuario afectado.

3. Verificar que la información es proporcionada por la aplicación en cuestión a los usuarios en un formato adecuado y de una forma exacta, oportuna, completa y fidedigna.

En el cuadro nº. 6.3.5.4 se resume el Objetivo y la Guía de control sobre la re-evaluación de los requisitos del usuario/cliente.

Re-evaluación de los requisitos del usuario/cliente
Objetivo de control: Revisar que la metodología incluye revisiones periódicas de los requisitos
Guía de control 1. Determinar las necesidades de usuario insatisfechas 2. Determinar la naturaleza de los cambios 3. Revisar que la información proporcionada es exacta y fidedigna

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.5.4.

Cuadro nº. 6.3.5.4 Resumen de Objetivo a controlar sobre la re-evaluación de los requisitos del usuario/cliente. Objetivo de control y Guía de control

6.3.6 Revisión post-implantación

Una metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar una revisión en conjunto, después de que haya sido implantada la aplicación informática, para asegurar que el esfuerzo produjo una aplicación que cumple las necesidades del usuario y los objetivos expuestos, obteniendo beneficios anticipados, y ajustándose a los requisitos de la metodología.

Objetivos a controlar:

- Plan de revisión de post-implantación
- Evaluación de resultados
- Evaluación de los requisitos del usuario
- Evaluación del análisis coste y beneficio
- Evaluación de la adherencia a los estándares de desarrollo
- Informe de recomendaciones de la revisión de post-implantación

6.3.6.1 Plan de revisión de post-implantación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería proporcionar, como parte integrante de las

actividades del equipo del proyecto, el desarrollo de un plan de revisión de la post-implantación de cada nueva aplicación informática.

Guía de control. Se revisarán los requisitos del proceso del desarrollo de aplicaciones de la organización para verificar que, como parte integrante de las actividades del equipo del proyecto, el desarrollo de un plan de revisión de la post-implantación de todas las aplicaciones informáticas a desarrollar.

1. Determinar, revisando la documentación de las aplicaciones informáticas a desarrollar, si se creó un plan de revisión de post-implantación del equipo del proyecto de desarrollo, el cual incluye:

    a. Una fecha proyectada para la revisión, la cual proporciona suficiente tiempo para que el sistema sea completamente operacional.
    b. La acumulación de datos para realizar la revisión.
    c. Persona encargada de realizar la revisión.
    d. Los objetivo definidos para la revisión.
    e. El alcance y naturaleza de la revisión y los recursos requeridos por esta.
    f. La preparación y emisión de un informe de los resultados de la revisión.

En el cuadro nº. 6.3.6.1 se resume el Objetivo y la Guía de control sobre el plan de revisión post-implantación

Plan de revisión post-implantación
Objetivo de control: Revisión de que la metodología incluye un plan de revisión post-implantación
Guía de control 1. Revisar si se creó un plan de revisión que incluya: a) fecha de revisión, b) acumulación de datos, c) persona encargada, d) los objetivos, e) alcance, naturaleza y recursos requeridos, f) preparación y emisión de un informe

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.6.1.

Cuadro nº. 6.3.6.1 Resumen de Objetivo a controlar sobre el plan de revisión post-implantación. Objetivo de control y Guía de control

6.3.6.2 Evaluación de resultado

Objetivo de control. La metodología del proceso de desarrollo de desarrollo de aplicaciones informáticas de la organización debería exigir una revisión de post-implantación valorando si los objetivos del sistema han sido alcanzados.

Guía de control. Se revisarán los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para asegurarse de que, mediante el uso de una revisión post-implantación de una aplicación informática, los objetivos del sistema han sido alcanzados.

1. Determinar, con un examen de la documentación de las aplicaciones informáticas desarrolladas, si la revisión de post-implantación compara la aplicación existente con las especificaciones relevantes, especialmente en estos términos:
   a. Datos procedentes de backup y restauración.
   b. Mantenimiento de la segregación de deberes.
   c. Controles sobre las interfaces con otras aplicaciones y sistemas.
   d. Medidas de seguridad.
   e. Documentación distribuida a los usuarios.

En el cuadro nº. 6.3.6.2 se resume el Objetivo y la Guía de control sobre la evaluación del resultado.

Evaluación del resultado
Objetivo de control: Revisión de que la metodología incluye un plan de revisión valorando si se alcanzaros los objetivos
Guía de control
1. Revisar que la documentación de post- implantación incluye: a) datos procedentes de backup y restauración, b) mantenimiento de la segregación de deberes, c) controles sobre las interfaces con otras aplicaciones, d) medidas de seguridad, e) documentación distribuida a los usuarios.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.6.2.

Cuadro nº. 6.3.6.2 Resumen de Objetivo a controlar sobre la evaluación del resultado. Objetivo de control y Guía de control

6.3.6.3 Evaluación de los requisitos del usuario/cliente

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas debería exigir que una revisión de post-implantación que valorará si las necesidades del usuario han sido llevadas a cabo por la aplicación.

Guía de control. Se revisará los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para asegurar que, mediante el uso de una revisión post-implantación de la aplicación en cuestión, las necesidades del usuario han sido llevadas a cabo por la aplicación.

1. Determinar, con entrevistas o cuestionarios, si en las revisiones de post-implantación realizadas a las aplicaciones en cuestión y las necesidades del usuario han sido llevadas a cabo mediante estas aplicaciones.

2. Verificar estas revisiones mediante un análisis del uso real que se está haciendo de la aplicación y las propuestas de cambios que se han hecho desde que se implantó la aplicación.

En el cuadro nº. 6.3.6.3 se resume el Objetivo y la Guía de control sobre la evaluación de los requisitos del usuario/cliente.

Evaluación de los requisitos del usuario/cliente
Objetivo de control: Revisión de que la metodología garantice que en la revisión post-implantación se analice si la necesidades del usuario han sido satisfechas
Guía de control 1. Revisar que las necesidades han sido cumplidas 2. Analizar el uso real de la aplicación

Fuente: Elaboración propia en la documentación del capítulo 6.3.6.3.

Cuadro nº. 6.3.6.3 Resumen de Objetivo a controlar sobre la evaluación de los requisitos del usuario/cliente. Objetivo de control y Guía de control

6.3.6.4 Evaluación del análisis coste y beneficio

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería exigir que una revisión post-implantación de una aplicación informática valorara si el coste efectivo del sistema se ajusta a los costes y beneficios originales proyectados por este.

Guía de control. Se examinarán los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para verificar que, mediante una revisión post-implantación de una aplicación, el coste efectivo de la misma se ajusta a los costes y beneficios originales proyectados por este.

1. Verificar, con un examen de la documentación de los proyectos de desarrollo de aplicaciones informáticas, la exactitud del proceso de estimación del coste, comparando los costes totales del proyecto con los establecidos inicialmente.

2. Determinar, con un examen de la documentación de los proyectos de desarrollo de aplicaciones informáticas, el grado en el que los beneficios cuantificables y no cuantificables asociados con la aplicación han sido realizados y comparados con los originalmente estimados.

3. Evaluar la admisibilidad de las razones citadas para las diferencias entre los costes y beneficios estimados y determinar si la alta dirección o el departamento de desarrollo de aplicaciones informáticas han sido prevenidos con las copias de los análisis que identifican estas diferencias.

En el cuadro nº. 6.3.6.4 se resume el Objetivo y la Guía de control sobre la evaluación del análisis coste y beneficio.

Evaluación del análisis coste y beneficio
Objetivo de control: Revisar que la metodología exija que se revise si el coste efectivo del sistema se ajusta a los costes y beneficios originales proyectados
Guía de control 1. Revisar la exactitud de la estimación del coste 2. Saber el grado en que los beneficios han sido realizados 3. Evaluar las diferencias entre los costes beneficios estimados y los reales.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.6.4.

Cuadro nº. 6.3.6.4 Resumen de Objetivo a controlar sobre la evaluación del análisis coste y beneficio. Objetivo de control y Guía de control

6.3.6.5 Evaluación de la adherencia a los estándares de desarrollo

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería exigir una revisión post-implantación de un sistema de información operacional valorara si el equipo del proyecto se adhiere a las disposiciones de la metodología.

Guía de control. Se examinarán los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para determinar que una revisión de post-implantación de una aplicación informática evaluó la adherencia del equipo del proyecto a las disposiciones de la metodología.

1. Verificar, con el examen de la documentación de los proyectos de desarrollo de aplicaciones informáticas, que hubo:
   a. Una documentación completa.
   b. Adherencia a las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización.
   c. Una adecuada participación en el proyecto de los miembros del departamento usuario/cliente afectado.

2. Verificar, mediante entrevistas con los participantes del equipo del proyecto, que los recursos de los miembros del equipo, la organización del equipo, y las comunicaciones fueron adecuadas para los proyectos de desarrollo de aplicaciones informáticas de la organización

En el cuadro nº. 6.3.6.5 se resume el Objetivo y la Guía de control sobre la evaluación de la adherencia a los estándares de desarrollo

Evaluación de la adherencia a los estándares de desarrollo
Objetivo de control: Revisar que la metodología exige que en la revisión post-implantación valorara si el equipo se adhiera a la metodología **Guía de control** 1. Verificar que hubo: a) documentación completa, b) adherencia de la metodología, c) adecuada participación del dep. usuario/cliente 2. Verificar que los recursos utilizados fueron adecuados.

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.6.5.

Cuadro nº. 6.3.6.5 Resumen de Objetivo a controlar sobre la evaluación de la adherencia a los estándares de desarrollo. Objetivo de control y Guía de control

6.3.6.6 Informe de recomendaciones de la revisión de post-implantación

Objetivo de control. La metodología del proceso de desarrollo de aplicaciones informáticas de la organización debería exigir que los resultados de la revisión de post-implantación de una aplicación informática sean sometidos a los responsables del departamento usuario/cliente afectado por la aplicación y a la dirección del departamento de aplicaciones informáticas.

Guía de control. Se revisarán los requisitos de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización para verificar que la revisión de post-implantación de una aplicación informática ha sido sometida a los responsables del departamento usuario afectado por la aplicación y a la dirección del departamento de aplicaciones informáticas.

1. Determinar, con un examen de la documentación de la aplicación informática en cuestión, si el informe de los resultados de las revisiones de post-implantación fue preparado y aprobado.

2. Determinar que estos informes fueron comunicados a los responsables del departamento usuario afectado por la aplicación informática y a la dirección del departamento de aplicaciones informáticas.

3. Verificar la naturaleza de las acciones tomadas sobre las recomendaciones del informe.

En el cuadro nº. 6.3.6.6 se resume el Objetivo y la Guía de control sobre el informe de recomendaciones de la revisión de post-implantación,

Informe de recomendaciones de la revisión de post-implantación
Objetivo de control: Revisar que la metodología exija que la revisión post-implantación haya sido sometida por el dep. usuario/cliente y por el de informática
Guía de control 1. Revisar que el informe de los resultados de las revisiones de post-implantación fue preparado y aprobado 2. Revisar que los informes fueron comunicados a los miembros correspondientes 3. Verificar la naturaleza

Fuente: Elaboración propia basada en la documentación del capítulo 6.3.6.6.

Cuadro nº. 6.3.6.6 Resumen de Objetivo a controlar sobre el informe de recomendaciones de la revisión de post-implantación. Objetivo de control y Guía de control

6.4 Resumen

Como podemos comprobar a lo largo de este capítulo pretendemos detectar y esclarecer todos los pasos que se deben seguir durante el ciclo de vida del desarrollo de aplicaciones informáticas, para ellos hemos identificado como objetivos de control aquellas tareas, documentos…que se deberían realizar, que debería existir para que el desarrollo de aplicaciones informáticas se realice de una forma correcta, fidedigna y adecuada a las leyes. Con esto lo que pretendemos es que tanto los miembros que forman parte del equipo de desarrollo como los que forman parte del departamento usuario/cliente tengan una forma clara y sin ningún tipo de duda de cómo se debe realizar sus tareas, que responsabilidades debe adquirir cada miembro del equipo, tener claramente los conocimientos que tiene cada persona para qué a la hora de asignar tareas podamos ser más eficientes, ya que si cada uno sabe perfectamente que debe hacer y como lo debe hacer seremos mucho más competitivos y productivos.

6.5 Bibliografía del capítulo 6

6.5.1 Libros, Apuntes, Artículos

Autores: Rafael Bernal Montañés i Óscar Coltell Simón. **Título:** Auditoría de los sistemas de información. **Año:** 1996. **Fecha de la consulta:** 21/03/2012.

Autores: Carmen de Pablos Heredero, José Joaquín López-Hermos Agius, Santigo Martín-Romo Romero, Sonia Medina Salgado, Antonio Monteri Navarro, Juan José Nájera Sanchez. **Título:** Dirección y gestión de los sistemas de información en la empresa, Una visión integradora 2º Edición. **Año:** 2006. **Fecha de la consulta:** 20/03/2012.

Autores: Mario G. Piattini, Emilio del Peso. **Título:** Auditoría Informática, Un enfoque práctico 2º Edición. **Año:** 2001. **Fecha de consulta:** 10/04/2012

6.5.2 Webs

Títulos: Auditoría Informática. **Fecha de la consulta:** 15/03/2012. **Dirección:** http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Fecha de la consulta: 16/03/2012. **Dirección:** http://www.slideshare.net/janethvalverdereyes/planeacion-de-la-auditoria-informatica

Fecha de la consulta: 16/03/2012. **Dirección:** http://prezi.com/q7rneahg1eg_/plan-de-auditoria-informatica/

Bibliografía acumulada

1. Libros, Apuntes, Artículos

Autor: David Lorente Guzmán. **Asignatura:** Auditoría de los Sistemas de Información, ETS de Ingeniería Informática de la UPV, Plan de Estudios de ITIG, Curso 2009-2010, **Fecha de consulta:** 25/09/2011. **Dirección:** http://www.inf.upv.es/webei/webETSIA/la_escuela/titulaciones/ITIG01/lista_optativas_con_info.php#ausi

Autores: Bernal Montañés, Rafael y Coltell Simón, Oscar (1996). **Título:** Auditoría de los sistemas de información. Universidad Politécnica de Valencia, Servicio de Publicaciones. **Año:** 2008. **Fecha de la consulta:** 27/09/2011

Autores: Carmen de Pablos Heredero, José Joaquín López-Hermos Agius, Santigo Martín-Romo Romero, Sonia Medina Salgado, Antonio Monteri Navarro, Juan José Nájera Sanchez. **Título:** Dirección y gestión de los sistemas de información en la empresa, Una visión integradora 2º Edición. **Año:** 2006. **Fecha de la consulta:** 20/03/2012.

Autores: Mario G. Piattini, Emilio del Peso. **Título:** Auditoría Informática, Un enfoque práctico 2º Edición. **Año:** 2001. **Fecha de consulta:** 10/04/2012

2 Webs

http://www.monografias.com (Fecha de consulta: 26/05/2011)

http://www.eumed.net/cursecon/libreria/rgl-genaud/1i.htm (Fecha de consulta: 26/05/2011)

http://www.wikilearning.com/monografia/fundamentos_teoricos_de_la_auditoria_vinculados_a_la_calidad-antecedentes_historicos_de_la_auditoria/12675-1 (Fecha de consulta: 06/06/2011)

http://www.monografias.com/trabajos16/auditoria-de-informacion/auditoria-de-informacion.shtml (Fecha de consulta: 06/06/2011)

http://www.eumed.net/libros/2006a/jcmn/1c.htm (Fecha de consulta: 08/08/2011)

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

www.**itgi**.org (Fecha de la consulta: 23/07/2011)

http://www.theiia.org/ (Fecha de la consulta: 24/07/2011)

http://www.iso.org/ (Fecha de la consulta: 26/07/2011)

http://www.iai.es/ (Fecha de la consulta: 27/07/2011)

http://es.wikipedia.org/wiki/CISA (Fecha de la consulta: 24/07/2011)

http://www.theiia.org/certification/certified-internal-auditor/ (Fecha de la consulta: 27/07/2011)

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

https://www.isaca.org/Pages/default.aspx (Fecha de la consulta: 23/07/2011)

http://www.marblestation.com/?p=645 (Fecha de la consulta: 18/09/2011)

www.**iso**.ch/(Fecha de la consulta: 26/07/2011)

http://www.itil-officialsite.com/ (Fecha de la consulta: 26/07/2011)

Autor: Ángela Jiménez. **Fecha de la consulta:** 25/09/2011. **Dirección:** http://www.uclm.es/area/aef_TO/pdf//publicaciones/AngelaJimenez_Tema5.pdf

Autor: Eduardo Horacio Quinn. **Título:** Auditoría Informática dentro de las etapas de análisis. **Fecha de la consulta:** 25/09/2011. **Dirección:** http://www.monografias.com/trabajos5/audi/audi.shtml

Institución: Ministerio de Hacienda y Administraciones Públicas, D.G. de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. **Título:** MAGERIT, versión 2. **Año:** 2010. **Fecha de la consulta:** 07/01/2012. **Dirección:** http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184

(Direcciones Web: http://www.monografias.com/trabajos-pdf/administracion-informatica/administracion-informatica.pdf http://www.bn.com.pe/transparenciabn/mof/dpto-de-informatica.pdf http://es.scribd.com/doc/60046252/2/Organigrama-del-Departamento-de-Informatica y fecha de consulta: 10/04/2011)

Títulos: Tipos de Empresa, Tipos de estructuras organizativas. **Año:** 2009**. Fecha de la consulta:** 11/01/2012. **Dirección:** http://www.mailxmail.com/curso-administracion-empresas-organizacion/tipos-estructuras-organizativas

Autor: LIC. Adafrancys Salazar - Richard Maggiorani. **Título:** Estructura organizativa y tipo de organigrama. **Año:** 2005. **Fecha de la consulta:** 12/01/2012. **Dirección:** http://www.gestiopolis.com/recursos4/docs/ger/estrorgorg.htm

Título: Fundamentos de estructura organizativa. **Fecha de la consulta:** 12/01/2012. **Dirección:** http://es.scribd.com/doc/6286437/Tipos-de-Estructura-Organizacional

Títulos: Auditoría Informática. **Fecha de la consulta:** 15/03/2012. **Dirección:** http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

Fecha de la consulta: 16/03/2012. **Dirección:** http://www.slideshare.net/janethvalverdereyes/planeacion-de-la-auditoria-informatica

Fecha de la consulta: 16/03/2012. **Dirección:** http://prezi.com/q7rneahg1eg_/plan-de-auditoria-informatica/

Anexos

Anexo 1. Cuestionario

PREGUNTA	RESPUESTA	
	SÍ	NO
6.2.1 Las responsabilidades en el proceso de desarrollo de aplicaciones		
¿El jefe del departamento de desarrollo de aplicaciones informáticas utiliza una política por escrito, en la que utiliza una metodología para el proceso de desarrollo de aplicaciones informáticas?		
¿Le sirve esto como medio de estructuración y control del proceso del desarrollo de aplicaciones informáticas?		
¿Cada fase del proceso de desarrollo de aplicaciones informáticas de la organización da lugar a un producto cuantificable sobre el cual se puede hacer una revisión y aprobación final para pasar a la siguiente fase?		
¿El énfasis puesto sobre cada fase cumple los requisitos de seguridad?		
¿Entre los miembros del departamento de desarrollo de aplicaciones informaticas y los miembros del equipo usuario existe una relación consolidada y experiencia con el uso de seguir una metodología para el desarrollo de aplicaciones informáticas?		
¿Los requisitos de la metodología para el proceso de desarrollo de aplicaciones informáticas son obligatorios?		
¿Estos pueden ser flexibles en función de si las condiciones varían, ejemplo proyecto grande o pequeño?		
¿Se permiten desviaciones de la metodología utilizada para el proceso de desarrollo de aplicaciones informáticas?		
¿Estas desviaciones están documentadas?		
¿Estas desviaciones están aprobadas?		
¿La metodología utilizada para el desarrollo de aplicaciones informáticas		

contiene unos estándares y requisitos de documentación y programación para los usuarios, programadores, analistas y personal encargado del procesamiento de los datos?		
¿La metodología utilizada en el proceso de desarrollo de aplicaciones informáticas contiene información sobre la tecnología que se utilizara para la base de datos?		
¿La metodología utilizada en el proceso de desarrollo de aplicaciones informáticas contiene información sobre la selección e instalación de los productos software legal?		
¿Para el desarrollo de aplicaciones informáticas se está usando una metodología?		
¿Esta metodología está actualizada y es adaptable si realizamos cualquier cambio en la tecnología?		
6.2.2 La funciones y responsabilidades de cada individuo		
¿El jefe del departamento ha utilizado una política declarada por escrito definiendo aquellas funciones y responsabilidades que tiene cada persona en el proceso de desarrollo de aplicaciones informáticas?		
¿La metodología que sigue la organización especifica todas las funciones del departamento de desarrollo de aplicaciones informáticas?		
¿La metodología que sigue la organización especifica las responsabilidades que tiene cada persona a la hora del desarrollo de aplicaciones informáticas?		
¿La metodología que sigue la organización especifica todas las funciones de la dirección de la organización?		
¿La metodología que sigue la organización especifica las responsabilidades que tiene cada persona perteneciente a la alta dirección?		
¿La metodología que sigue la organización especifica todas las funciones de los usuarios finales?		
¿La metodología que sigue la organización especifica las responsabilidades que tienen los usuarios finales?		
¿La metodología que sigue la organización especifica todas las funciones de los miembros del equipo de desarrollo de aplicaciones informáticas?		

¿La metodología que sigue la organización especifica las responsabilidades que tiene los miembros del equipo de desarrollo de aplicaciones informáticas?		
¿En cada fase del proceso de desarrollo de aplicaciones informáticas se pueden modificar las metas?		
¿En cada fase del proceso de desarrollo de aplicaciones informáticas se puede modificar la dirección de desarrollo?		
¿En cada fase del proceso de desarrollo de aplicaciones informáticas se puede modificar el esfuerzo en dedicación al desarrollo?		
¿En cada fase del proceso de desarrollo de aplicaciones informáticas se permite el poder decidir si pasamos a la siguiente fase?		
¿El jefe del proyecto de desarrollo de aplicaciones informáticas puede tomar decisiones sobre los costes?		
¿Es la alta dirección la que toma las decisiones sobre los costes?		
¿El jefe del proyecto de desarrollo de aplicaciones informáticas puede tomar decisiones sobre los presupuestos?		
¿Es la alta dirección la que toma las decisiones sobre los presupuestos?		
¿El jefe del proyecto de desarrollo de aplicaciones informáticas puede tomar decisiones sobre el resto de tareas?		
¿Es la alta dirección la que toma las decisiones sobre el resto de tareas?		
¿Los responsables del departamento usuario están involucrados con el equipo de de desarrollo de aplicaciones informáticas?		
¿Los responsables del departamento usuario tienen reuniones periódicas con los miembros del equipo de departamento de desarrollo de aplicaciones informáticas?		
¿Los responsables del departamento usuario tienen responsabilidades que se ajustan a sus capacidades?		
¿Están involucrados en el proceso de desarrollo de aplicaciones informáticas los miembros o el miembro que se encarga del control de calidad del departamento de desarrollo de aplicaciones informáticas?		
¿Se garantiza de que antes que se entregue la aplicaciones los miembro que se encargan del control de calidad pasen las pruebas necesarias para que la aplicaciones sea entregada?		

6.2.3 Proceso de actualización de la metodología que utiliza la organización para el desarrollo de aplicaciones		
¿La metodología que utiliza la organización en el proceso de desarrollo de aplicaciones informáticas se revisa periódicamente por la alta dirección?		
¿La metodología que utiliza la organización en el proceso de desarrollo de aplicaciones informáticas se revisa periódicamente por los jefes del departamento de desarrollo de aplicaciones informáticas?		
¿Se mantiene un registro con las revisiones y modificaciones de la metodología que se utiliza en el proceso de desarrollo de aplicaciones informáticas?		
6.3.1.1 Definición del proyecto		
¿La metodología utilizada por la organización promueve la creación de un documento que detalle claramente cada uno de las tareas a realizar antes de comenzar a realizar el propio desarrollo?		
¿Están documentadas las razones para la realización del proyecto?		
¿Están documentados los problemas que se van a solucionar si es que los hay?		
¿Están expuestas las necesidades para la realización de la nueva aplicación?		
¿Está documentado el alcance de la nueva aplicación?		
¿Están documentadas las restricciones de la nueva aplicación?		
¿Están documentados los beneficios de la nueva aplicación?		
¿Fueron revisados y aprobados todos los requisitos de acuerdo a la metodología que utiliza la organización?		
6.3.1.2 La participación del departamento usuario/cliente en la iniciación del desarrollo de la aplicación		
¿En la metodología utilizada se promueve la participación de los responsables del departamento usuario/cliente en el proceso de desarrollo de aplicaciones informáticas?		
¿Los responsables del departamento usuario/cliente hacen reuniones periódicas con los responsables del departamento de desarrollo de aplicaciones informáticas para aclara los requisitos y aprobación de la		

aplicación a desarrollar?		
¿El departamento usuario/cliente ha detallado claramente cuál es el presupuesto del que dispone para el desarrollo del proyecto?		
6.3.1.3 Relación de los miembros del equipo del proyecto y sus responsabilidades		
¿La metodología que utiliza la organización en el desarrollo de aplicaciones informáticas especifica las bases para asignar que miembros de la organización son los más adecuados para realizar el proyecto en cuestión?		
¿La metodología que utiliza la organización en el desarrollo de aplicaciones informáticas especifica las bases para asignar cuales son las responsabilidades de cada miembro que forma parte del departamento de desarrollo de aplicaciones informáticas?		
¿Antes de asignarle a cada miembro del equipo cual es la función que debe desempeñar se han evaluado sus antecedentes y cualidades?		
¿Los responsables de departamento usuario/cliente tienen miembros participando activamente junto con los miembros del departamento de desarrollo de aplicaciones informáticas?		
¿Los responsables del departamento usuario/cliente tienen un amplio conocimiento detallado sobres la información que requiere la aplicación a desarrollar?		
¿Los responsables del departamento usuario/cliente tiene las habilidades necesarias para trabajar junto con los otros miembros del equipo del proyecto de desarrollo de aplicaciones informáticas?		
¿Los responsables de departamento usuario/cliente tienen los mismos conocimientos sobre el alcance y los objetivos de la aplicación a desarrollar que los otros miembros del equipo?		
6.3.1.4 Definición de los requisitos para la realización del desarrollo de la aplicación		
¿La metodología del proceso de desarrollo de aplicaciones informáticas facilita que los requisitos de información existentes así como los que se acuerden posteriormente estén claramente definidos antes de que el proyecto sea aprobado?		
¿Es controlada la adherencia a los requisitos y documentación de la metodología del proceso de desarrollo de aplicaciones en los proyectos		

de desarrollo de aplicaciones informáticas?		
¿Las descripciones de los sistemas existentes son adecuadas y si se pueden utilizar como base para estudiar las necesidades de la nueva aplicación informática propuesta?		
¿Han sido identificados claramente aquellos aspectos del sistema existente que se deben cambiar para la aplicación propuesta?		
¿Se ha evaluado por el departamento de desarrollo de aplicaciones informáticas los requisitos de información para la integridad, consistencia y viabilidad para la nueva aplicación?		
¿Los requisitos tomados han sido revisados y aprobados por los responsables del departamento usuario/cliente afectados en el proyecto de desarrollo de aplicaciones?		
6.3.1.5 La aprobación del proyecto		
¿La metodología que utiliza la organización para el proceso de desarrollo de aplicaciones informáticas facilita la aprobación de los miembros designados por la dirección del proyecto a desarrollar antes de comenzar a trabajar en la siguiente etapa?		
¿Se ha preparado un informe que engloba todos los puntos establecidos como requisitos de la aplicación a desarrollar?		
¿En este informe están bien definidos los requisitos para el desarrollo de la aplicación en cuestión?		
¿Tanto el jefe del departamento de desarrollo de aplicaciones informáticas como el responsable de departamento usuario/cliente han revisado los informes que realiza cada miembro del departamento de desarrollo de aplicaciones informáticas?		
6.3.2.1 Estudio de la viabilidad en la tecnología utilizada		
¿La metodología que utiliza la organización proporciona un estudio de la viabilidad para alcanzar las metas de la aplicación a desarrollar junto con el análisis de coste y beneficio?		
¿La metodología utilizada facilita un examen de la viabilidad de cada alternativa posible para satisfacer los requisitos de información establecidos para la nueva aplicación?		
¿Existe un informe que estudia la viabilidad para cada una de las alternativas para el desarrollo de la aplicación en cuestión?		

¿Este informe incluye las necesidades y disponibilidades de los miembros que forman parte del equipo de desarrollo de aplicaciones informáticas?		
¿El informe incluye las necesidades de software y hardware que se necesitan para el proceso de desarrollo de aplicaciones informáticas?		
¿El informe incluye la viabilidad de operaciones de la nueva aplicación?		
¿El informe incluye las consideraciones legales relacionadas con la transferencia de datos que se deben tener a la hora del desarrollo de aplicaciones?		
¿Tanto los responsables del departamento usuario/cliente como los del departamento de desarrollo de aplicaciones informáticas han añadido a la viabilidad el plan de datos y equipamiento del proyecto?		
¿Tanto los responsables del departamento usuario/cliente como los del departamento de desarrollo de aplicaciones informáticas han añadido a la viabilidad la formación tanto de los miembros del departamento de desarrollo de aplicaciones informáticas como la de los miembros del departamento usuario/cliente?		
¿Tanto los responsables del departamento usuario/cliente como los del departamento de desarrollo de aplicaciones informáticas han añadido a la viabilidad los controles adecuados sobre los test de programas, ficheros y datos?		
¿Tanto los responsables del departamento usuario/cliente como los del departamento de desarrollo de aplicaciones informáticas han añadido a la viabilidad la recogida y análisis de los datos relevantes?		
¿Tanto los responsables del departamento usuario/cliente como los del departamento de desarrollo de aplicaciones informáticas han añadido a la viabilidad los escritos de los informes requeridos?		
¿Se ha revisado mediante una revisión de la documentación de los test del proyecto de desarrollo la fuente, tipo y adecuación del generador de test?		
¿Se ha revisado mediante una revisión de la documentación de los test del proyecto de desarrollo los datos de transacciones reales?		
¿Se ha revisado mediante una revisión de la documentación de los test del proyecto de desarrollo el análisis de los resultados de test?		
6.3.3.1 Los objetivos de programación		

¿La documentación que existe para el desarrollo de aplicaciones informáticas incluye unos informes declarando claramente los objetivos de programación para realizar el desarrollo de aplicaciones informáticas?		
6.3.3.2 Documentación detallada de programas		
¿La metodología que utiliza la organización en el proceso de desarrollo de aplicaciones exige que esté creada una documentación muy bien detallada de los programas para este proceso de desarrollo de aplicaciones informáticas?		
¿La documentación de los proyectos de desarrollo de aplicaciones informáticas contiene la información de la descripción lógica claramente detallada tal que si la leyeran personas no familiarizadas con este proyecto pudieran entender las funcionalidades de la misma?		
¿La metodología que utiliza la organización exige que se prepare un diagrama de flujo para el desarrollo de la aplicación informática en cuestión?		
¿Los datos elementales utilizados para el desarrollo de la aplicación en cuestión tienen designados unos propietarios?		
¿Los datos elementales utilizados para el desarrollo de la aplicación en cuestión están apropiadamente descritos?		
¿Los datos elementales utilizados para el desarrollo de la aplicación en cuestión no están en conflicto con otras definiciones en la base de datos?		
6.3.3.3 Paquetes de aplicaciones software		
¿La metodología que utiliza la organización en el proceso de desarrollo de aplicaciones informáticas proporciona paquetes software que satisfacen las necesidades de la aplicación en cuestión?		
¿Los procedimientos de adquisición de software siguen las políticas de la organización, están testeados y revisados antes de ser utilizados?		
¿Las condiciones de compra para la adquisición de los paquetes software se ajustan a las políticas que fueron aprobados por los miembros del departamento usuario/cliente y los del departamento de desarrollo de aplicaciones infromáticas?		
¿La documentación suministrada con los paquetes software adquiridos es adecuada?		

¿Los paquetes software adquiridos fueron testeados y revisados antes de ser utilizados y pagados?		
6.3.3.4 Programación de la aplicación a desarrollar		
¿La metodología que utiliza la organización proporciona un contrato para la realización de la fase de programación de la organización?		
¿Los proyectos finales que se entregan al usuario/cliente están testeados por los responsables del equipo de desarrollo de aplicaciones informáticas?		
¿El contrato especifica claramente cuáles son las condiciones de plazos, presupuesto y requisitos?		
6.3.3.5 Manual de mantenimiento y operaciones		
¿La metodología que utiliza la organización exige la preparación de manuales de mantenimiento?		
¿La metodología que utiliza la organización exige la preparación de operaciones adecuadas?		
¿Los miembros del equipo de desarrollo de aplicaciones informáticas han realizado estos manuales para la nueva aplicación en cuestión?		
¿Estos manuales son comprensibles y accesibles para los miembros del departamento usuario/cliente?		
¿Estos manuales son utilizados en los test de software?		
¿Para cada fase del manual se especifica la funcionalidad del programa?		
¿Para cada fase del manual se especifica los requisitos hardware?		
¿Para cada fase del manual se especifica los requisitos software?		
¿Para cada fase del manual se especifica todos los mensajes de consola con la respuesta adecuada?		
¿Para cada fase del manual se identifican adecuadamente las etiquetas de los ficheros de salida?		
¿Para cada fase del manual se especifica los puntos adecuados de los reinicios?		
6.3.3.6 Manuales de usuario		

¿La metodología que utiliza la organización exige la preparación de manuales de usuario como una parte del proceso de desarrollo de aplicaciones informáticas?		
¿Los miembros del departamento de desarrollo de aplicaciones infromáticas realizan estos manuales de usuario?		
¿Estos manuales de usuario incluyen las especificaciones y diseños de entrada de datos?		
¿Estos manuales de usuario incluyen las formas de presentar los datos al departamento de desarrollo de aplicaciones informáticas?		
¿Estos manuales de usuario incluyen la responsabilidad para resolver errores u otras incongruencias?		
¿Estos manuales de usuario incluyen la asignación de prioridades de procesamiento?		
¿Estos manuales de usuario incluyen la lógica, seguridad, vigencia y disposiciones de las salidas?		
¿Estos manuales de usuario incluyen la lógica de programación?		
¿Estos manuales de usuario incluyen el registro de aprobación usuario?		
¿Estos manuales de usuario incluyen el registro de solicitudes y aprobación de cambios del programa?		
¿Estos manuales de usuario incluyen el procedimiento para encender y apagar terminales y servidores?		
¿Estos manuales de usuario incluyen la forma en que los usuarios deben utilizar la aplicación?		
¿Estos manuales de usuario incluyen la funcionalidad de cada una de las pantallas?		
¿Estos manuales de usuario son utilizados en el testeo de software?		
6.3.3.7 Plan de formación		
¿La metodología que utilizada la organización para el desarrollo de aplicaciones informáticas exige una plan para formar a los grupos del mantenimiento del departamento usuario/cliente?		
¿Existe un plan escrito para formar a cada miembro del departamento usuario y a los de mantenimiento del departamento de desarrollo de		

aplicaciones infromáticas?		
¿Es plan de formación de usuarios deja suficiente tiempo para completar las actividades de formación requeridas?		
6.3.4.1 Estándares de testeo de las aplicaciones		
¿La metodología que utiliza la organización proporciona estándares para el testeo e implementación de aplicación en cuestión?		
¿Los estándares que utiliza la metodología son los adecuados para el testeo de la aplicación desarrollada?		
¿Se revisa que todas la funcionalidades estén programadas, que el código fue testeado y que los resultado se ajustan a las especificaciones iníciales?		
¿La metodología que utiliza la organización proporciona estándares para las pruebas como una parte del desarrollo de la aplicación en cuestión?		
¿Se proporcionan adecuados estándares para la preparación de los responsables del departamento usuario y de departamento de desarrollo de aplicaciones informáticas en la preparación de los datos del test para revisa y aprobar los resultados del test?		
6.3.4.2 Documentación del testeo de la aplicación		
¿La metodología utilizada proporciona un documento por escrito las actividades y los resultados de los test de la nueva aplicación?		
¿La aplicación fue testeada de acuerdo a plan de verificación validación y test?		
¿Todos las funcionalidades más críticas de la aplicación fueron incluidas es en proceso de testeo?		
¿Los materiales que se utilizaron en el testeo fueron adecuadamente controlados?		
¿Los resultado del proceso fueron aprobados tanto por los responsables del departamento usuario como por del departamento de desarrollo de aplicaciones informáticas?		
¿Se incluyó un informe escrito de los resultados en los informes de las actividades del equipo de desarrollo de aplicaciones informáticas?		
¿Los responsables de departamento usuario/cliente han sido		

conscientes de la importancia del proceso de testeo?		
¿Los responsables de departamento usuario/cliente han participado de una forma adecuada, responsable y consecuente con la hora de probar el resultado del testeo?		
¿Se ha desarrollado un documento por escrito tanto por parte del departamento usuario/cliente como por parte del departamento de desarrollo de aplicaciones informáticas que detalle los controles que se deben seguir durante el funcionamiento de la aplicación?		
6.3.4.3 Evaluación de los resultados de los test		
¿Los resultados de los test han sido aprobados tanto por los responsables de departamento usuario/cliente como por los responsables del departamento de desarrollo de aplicaciones informáticas?		
¿Los resultados previstos fueron desarrollados antes de los obtenidos?		
¿Los resultados previstos coinciden con los resultados obtenidos?		
¿La documentación que contiene la información del resultado de los test incluye un listado de los datos obtenidos de los test?		
¿La documentación que contiene la información del resultado de los test incluye las salidas de la aplicación en cuestión?		
¿La documentación que contiene la información del resultado de los test incluye las entradas relevantes del log de la aplicación?		
¿La documentación contiene tests de backups y restauración?		
¿La documentación contiene las responsabilidades y capacidades que tiene cada miembro con la diferentes tareas de testeo?		
6.3.4.4 Análisis de la documentación del testeo		
¿Antes de la entrega se ha verificado la exactitud de la documentación por los responsables tanto del departamento usuario como por los responsables del departamento de desarrollo de aplicaciones informáticas?		
6.3.4.5 Test de aceptación final		
¿Se ha realizado una evaluación de los resultados de test tanto por los responsables del departamento usuario como por parte de los miembros del departamento de desarrollo de aplicaciones informáticas?		

¿La metodología utilizada define los estándares adecuados para el test de aceptación final?		
¿Los responsables del departamento usuario/cliente y del departamento de aplicaciones participan en la evaluación del desarrollo de la aplicación en cuestión?		
¿Si se detecta una ineficiencia durante el test de aceptación final es remitida con anterioridad de que la aplicación sea declarada operacional?		
6.3.5.1 Procedimientos de control de operaciones		
¿La metodología que utiliza la organización asegura la instalación de los procedimientos para controlar las actividades de procesamientos de datos de la nueva aplicación informática?		
¿Se ha comprobado si los procedimientos de control establecidos por los responsables del departamento usuario y el departamento de desarrollo de aplicaciones informáticas son adecuados a los tipos de los ficheros que se han mantenido en las transacciones procesadas por la nueva aplicación?		
¿Los procedimientos de control incluyen los controles adecuados de distribución de salidas?		
¿Estos procedimientos de control son recibidos solamente por el personal autorizado del departamento usuario/cliente afectado?		
¿Han sido identificados, controlados, corregidos y adecuadamente reprocesados los procedimientos que aseguran los errores durante la vida de la nueva aplicación?		
¿Han sido identificados los procedimientos que aseguran los errores durante la vida de la nueva aplicación?		
¿Han sido controlados los procedimientos que aseguran los errores durante la vida de la nueva aplicación?		
¿Han sido corregidos los procedimientos que aseguran los errores durante la vida de la nueva aplicación?		
¿Han sido adecuadamente reprocesados los procedimientos que aseguran los errores durante la vida de la nueva aplicación?		
¿Los procedimientos aseguran que las funciones de las operaciones clave incluyen las operaciones de programas de aplicaciones, seguridad de datos, introducción de datos, han sido desarrolladas por diferentes		

miembros del equipo y que esta separación ha sido forzada por los responsables del departamento		
6.3.5.2 Control de costes		
¿El sistema de contabilización de la organización almacena, analiza e informa de los costes asociados con el funcionamiento de la nueva aplicación?		
¿Se han revisado los procedimientos usados por el sistema de contabilización de la organización para registrar, analizar e informar de los costes asociados con el funcionamiento de la nueva aplicación?		
¿Se ha comprobado que los procedimientos son adecuados y que han sido revisados y aprobados por los responsables del departamento usuario afectado y el departamento de desarrollo de aplicaciones informáticas?		
6.3.5.3 Modificaciones de la aplicación		
¿La metodología que utiliza la organización establece procedimientos para controlar los cambios de la nueva aplicaciones informáticas?		
¿Los cambios de nueva aplicación a desarrollar han sido registrados y procesados de forma oportuna en un documento?		
¿Se ha comprobado si los cambios propuestos de la aplicación en cuestión están aprobados por los responsables del departamento usuario afectado antes de comenzar a trabajar?		
¿Se ha comprobado si todos los registros de los cambios actualmente hechos, incluyendo las revisiones de los diagramas de flujo de datos, la evaluación y aprobación de los resultados de los test, están incorporados en la documentación acumulada por el departamento de desarrollo de aplicaciones informáticas?		
6.3.5.4 Re-evaluación de los requisitos del usuario		
¿La metodología que utiliza la organización realiza revisiones periódicas de los requisitos de usuario para comprobar si estos pueden haber cambiado desde el principio de la toma de requerimientos?		
6.3.6.1 Plan de revisión de post-implantación		
¿La metodología del proceso de desarrollo de aplicaciones informáticas de la organización proporciona, como parte integrante de las actividades del equipo del proyecto, el desarrollo de un plan de revisión de la post-		

implantación de cada nueva aplicación informática?		
¿Se ha revisado la documentación de las aplicaciones informáticas a desarrollar?		
¿Se ha creado un plan de revisión de post-implantación del equipo del proyecto de desarrollo?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye una fecha proyectada para la revisión que proporciona suficiente tiempo para que el sistema sea completamente operacional?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye una acumulación de datos para realizar la revisión?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye a la persona que realiza la revisión?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye los objetivos definidos para la revisión?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye el alcance y la naturaleza de la revisión y los recursos requeridos por esta?		
¿El plan de revisión de post-implantación del equipo del proyecto de desarrollo incluye una preparación y emisión de un informe de los resultados de la revisión?		
6.3.6.2 Evaluación de resultado		
¿La metodología del proceso de desarrollo de aplicaciones informáticas de la organización exige una revisión de post-implantación valorando si los objetivos del sistema han sido alcanzados?		
¿El resultado de la revisión de post-implantación compara el sistema existente con las especificaciones relevantes?		
¿La revisión de post-implantación compara el sistema existente con las especificaciones relevantes procedentes de backup y restauración?		
¿La revisión de post-implantación compara el sistema existente con las especificaciones relevantes de mantenimiento de la segregación de deberes?		
¿La revisión de post-implantación compara el sistema existente con las especificaciones relevantes en los controles sobre las interfaces con otras aplicaciones y sistemas?		

¿La revisión de post-implantación compara el sistema existente con las especificaciones relevantes de las medidas de seguridad?		
¿La revisión de post-implantación compara el sistema existente con las especificaciones relevantes de la documentación distribuida a los usuarios?		
6.3.6.3 Evaluación de los requisitos del usuario		
¿La metodología del proceso de desarrollo de aplicaciones informáticas exige una revisión post-implantación valorando si las necesidades del usuario han sido llevadas a cabo por la aplicación?		
¿Se ha comprobado si en las revisiones de post-implantación realizadas a la aplicación y a las necesidades del usuario se han llevado a cabo mediante estas aplicaciones?		
¿Se ha hecho un análisis del uso real que se está haciendo de la aplicación y de las propuestas de cambios que se han hecho desde que se implantó la aplicación?		
6.3.6.4 Evaluación del análisis coste y beneficio		
¿La metodología del proceso de desarrollo de aplicaciones de la organización exige una revisión post-implantación valorando si el coste efectivo del sistema se ajusta a los costes y beneficios originales proyectados para este?		
¿Se ha comprobado la exactitud del proceso de estimación del coste, comparando los costes totales con los establecidos inicialmente?		
¿Ha sido determinado el grado en el que los beneficios cuantificables y no cuantificables asociados con la aplicación han sido realizados y comparados con los originales estimados?		
¿Ha sido evaluada la admisibilidad de las razones citadas para las diferencias entre costes y beneficios estimados?		
¿La alta dirección o el departamento de desarrollo de aplicaciones informáticas han sido prevenidos con las copias de los análisis que identifican estas diferencias?		
6.3.6.5 Evaluación de la adherencia a los estándares de desarrollo		
¿La metodología del proceso de desarrollo de aplicaciones de la organización exige una revisión post-implantación valorando si el equipo de proyecto se adhiere a las disposiciones de la metodología?		

¿Se ha hecho un examen de la documentación de los proyectos de desarrollo de aplicaciones informáticas para comprobar si el equipo del proyecto se adhiere a las disposiciones de la metodología?		
¿Se comprueba si hay una documentación completa?		
¿Se comprueba si hay una adherencia a las disposiciones de la metodología del proceso de desarrollo de aplicaciones informáticas de la organización?		
¿Se comprueba si hay una adecuada participación en el proyecto de los representantes del departamento usuario afectado?		
¿Los recursos de los miembros del equipo, la organización del equipo y las comunicaciones son las adecuadas para los proyectos de desarrollo de aplicaciones informáticas de la organización?		
6.3.6.6 Informe de recomendaciones de la revisión de post-implantación		
¿Los resultados de la revisión de post-implantación son sometidos por los responsables del departamento usuario afectado por la aplicación?		
¿Los resultados de la revisión de post-implantación son sometidos a la dirección del departamento de aplicaciones informáticas?		
¿El informe de los resultados de las revisiones de post-implantación es preparado y aprobado?		
¿Los informes son comunicados a los responsables del departamento usuario afectado por la aplicación informática?		
¿Estos informes son comunicados a la dirección del departamento de aplicaciones informáticas?		
¿Se ha verificado la naturaleza de las acciones tomadas sobre las recomendaciones del informe?		

Anexo 2. Siglas

TIC	Tecnologías de la Información y la Comunicación
TI	Tecnologías de Información
SI	Sistemas de Información
AAPA	American Association of Public Accountants
IPA	Institute of Public Accountants
AIA	American Institute of Accountants
GAAP	Generally Accepted Accounting Principles
SEC	Securities and Exchange Commission
CAP	Committee on Auditing Procedure
ARS	Accounting Research Division
APB	Accounting Principles Board
ARB	Accounting Research Bulletin
AICPA	American Institute of Certified Public Accountants
SAP	Statements on Auditing Procedure
SAS	Statement son Auditing Standards
FASB	Financial Accounting Standard Board
AFNOR	Asociación Francesa de Normalización
ISACA	Information Systems Audit and Control Association
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CGEIT	Certified in the Governance of Enterprise IT

CRISC	Certified in Risk and Information System Control
CACS	Conferencias del equipo de Auditoría, Control y Seguridad
GRCIT	Conferencia de las TI de Gestión de Riesgos y Cumplimiento
ISRM	Conferencia de la Gestión de Seguridad y Riesgo
COBIT	Control Objectives for Information and related Technology
ValIT	IT Value Delivery
ITAF	Garantía de IT Framework
BMIS	Modelo de negocio de Seguridad de Información
ISACA-CV	Information System Audit and Control Association-Com.Valenciana
ITGIIT	IT Governance Institute
IIA	The Institute of Internal Auditors
ISO	Organización Internacional de Normalización
ECIIA	European Confederation of Institutes of Internal Auditing
CISA	Certified Information System Auditor
CIA	Certificado de Auditor Interno
CISM	Certified Information Security Manager
CGEIT	Certified in the Governance of Enterprise IT
CRISC	Certified in Risk and information System Control
ITIL	Information Technology Infrastructure Library

Anexo 3. Definiciones

Método: Es el modo de decir o hacer con orden una cosa. (Libro: Auditoría de tecnologías y sistemas de información, año 2008, autor: Mario Piattini Velthuis, Emilio del Peso Navarro, María del Peso)

Metodología: se define como el conjunto de métodos que se siguen en un trabajo científico o en una exposición doctrinal, que permite abordar éste de forma organizada y consecuente. (Libro: Auditoría de tecnologías y sistemas de información, año 2008, autor: Mario Piattini Velthuis, Emilio del Peso Navarro, María del Peso)

Materialidad en la auditoría contable o financiera: La información es material si su omisión o distorsión puede influir en las decisiones económicas de los usuarios que se apoyan en los estados financieros. La materialidad depende del tamaño de la partida o del error considerado en las particulares circunstancias de la omisión o distorsión.

Materialidad refiriéndose a una auditoría informática: La materialidad constituye una referencia o un punto de corte antes que una característica cualitativa principal para que la información pueda ser útil. (Contraloría General de la República, MANUAL DE AUDITORÍA GUBERNAMENTAL - MAGU - 1998)