UNIVERSIDAD AMAZÓNICA DE PANDO

FAULTAD DE INGENIERÍA Y TECNOLOGÍA

CARRERA DE INGENIERÍA DE SISTEMAS

TEXTO GUIA

ASIGNATURA: AUDITORÍA DE SISTEMAS

Elaborado por: M.Sc. Juan Carlos Huanca Guanca

Período I/2023

Prefacio

Este texto guía, tiene la finalidad de cubrir ese vació bibliográfico existente en relación a los contenidos programáticos de la asignatura de Auditoría de Sistemas de la Carrera de Ingeniería de Sistemas. El contenido, es un compendio desarrollado a partir de la búsqueda de información y libros digitales en la web.

El texto, abarca todos los conceptos relacionados con la auditoría de sistemas, buenas prácticas, auditoría de organización y administración del ambiente informático, los controles de acceso lógicos y físicos para finalizar con la auditoría de la seguridad en los sistemas de bases de datos e internet.

El texto no pretende ser una guía completa en la auditoría de sistemas sin embargo, si aborda los fundamentos y principios de la auditoría de sistemas, de forma que permita al profesional en sistemas especializarse en esta área profesional.

UNIVERSIDAD AMAZÓNICA DE PANDO
FACULTAD DE INGENIERÍA Y TECNOLOGÍA
CARRERA DE INGENENIERÍA DE SISTEMAS
TEXTO GUÍA DE ASIGNATURA

ASIGNATURA: AUDITORÍA DE SISTEMAS
SIGLA: SIS 481
SEMESTRE: NOVENO

MACROPROBLEMA EN RELACIÓN A LA COMPETENCIA DE LA ASIGNATURA

- Sistemas implementados sin una planificación adecuada
- Necesidad de contar con un plan de implementación de sistemas
- Necesidad de valorar si un sistema está funcionando adecuadamente según sus objetivos establecidos
- Exigencias de auditoría de sistemas por parte de los usuarios.

COMPETENCIA DE LA ASIGNATURA

Evalúa la eficiencia y eficacia de la organización y administración de los sistemas y del ambiente informático, para que por medio de cursos alternativos de acción se tomen decisiones que permitan corregir los errores o bien mejorar la forma de actuación en base a normas de auditoría de sistemas de información.

ELEMENTO DE COMPETENCIA	SECCIONES Y CAPÍTULOS DEL LIBRO
EC1: Evalúa los procedimientos y técnicas total o parcialmente del sistema informático con el fin de proteger sus activos y recursos, verificando que sus actividades se desarrollen eficaz y eficientemente de acuerdo a normas de Auditoría de Sistemas.	Capítulo 1: Conceptos generales Capítulo 2: Control interno y auditoría de sistemas de información Capítulo 3: Auditoría de SI vs. Normas de buenas preácticas
EC2: Revisa la seguridad de los Sistemas y el Ambiente Informático de la Organización.	Capítulo 4: Metodologías de control interno, seguridad y la auditoría de sistemas de información (SI) Capítulo 5: El departamento de auditoría de los SI: Organizaciones y funciones
EC3: Verifica el cumplimiento de la normativa y legislaciones vigentes en los sistemas de Información y el ambiente Informático	Capítulo 6: Entorno jurídico de la auditoría de los sistemas de información Capítulo 7: Auditoría de la seguridad física Capítulo 8: La auditoría de la Dirección Informática
EC4: Elabora un informe de Auditoría utilizando estándares ISACA, COBIT	Capítulo 9: Auditoría de Bases de Datos Capítulo 10: Auditoría de redes Capítulo 11: Auditoría de Internet

Indice

PRIMERA PARTE:
AUDITORÍA DE SISTEMAS

Capítulo 1

CONCEPTOS GENERALES

1.1. Introducción del capítulo

El desarrollo normal de las actividades comerciales y financieras de las empresas requiere una constante vigilancia y evaluación; asimismo, las empresas necesitan una opinión, preferiblemente independiente, que les ayude a medir la eficiencia y eficacia en el cumplimiento de sus objetivos. Por lo general, la evaluación consiste en una revisión metódica, periódica e intelectual de los registros,tareas y resultados de la empresa, con lo cual se busca medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones. *Eso es auditoría*.

Los inicios de la auditoría se remontan a la revisión y el diagnóstico quese practicaban a los registros de las operaciones contables de las empresas;después se pasó al análisis, verificación y evaluación de sus aspectos financie- ros; posteriormente se amplió al examen de algunos rubros de la administración, siguiendo con el análisis de aquellos aspectos que intervenían en todas sus actividades y, por último, su alcance se incrementó conforme se avanzó enla llamada revisión integral. Actualmente se ha llegado a las revisiones especializadas de algunas áreas y actividades específicas que se desempeñan enlas instituciones. Entre algunas de estas últimas encontramos: auditoría de sistemas computacionales, auditoría del desarrollo de proyectos de mercadotecnia, auditoría de proyectos económicos, y en sí a muchas ramas de la actividadempresarial.

Con el propósito de dar a conocer cuál ha sido el desempeño y desarrollo de este tipo de trabajos, a continuación, veremos los aspectos más destacados que intervienen en una auditoría, empezando por sus antecedentes, conceptosbásicos y los diferentes tipos o métodos de auditorías, así como sus definiciones. Estos aspectos son sólo una introducción, ya que en capítulos posteriores nos enfocaremos exclusivamente a la auditoría de sistemas computacionales.

1.2. Antecedentes de la auditoría

Conforme se expandía el comercio, después de pasar por el trueque primero en pueblos, ciudades, estados y finalmente en continentes, y motivados por su constante crecimiento, tanto en volumen como en el monto de operaciones comerciales, los incipientes comerciantes tuvieron la necesidad de establecer mecanismos rudimentarios de registro que les permitieran dominar las actividades mercantiles que realizaban. Después, conforme los comerciantes crecieron y se agruparon en gremios y mercados locales, surgió la necesidad de contar con un mejor registro de sus actividades, tanto individuales como conjuntas. Posteriormente, con el crecimiento de estas agrupaciones, que se

convirtieron en incipientes empresas, fue necesario establecer un mayor control para conocer de sus actividades financieras.

Gracias a ese crecimiento se inició el registro de operaciones mercantiles a través de escribas, quienes al principio asentaban dichas operaciones en forma rudimentaria; posteriormente, con el nacimiento de la partida doble y el registro de operaciones financieras, surgió la llamada teneduría de libros. Conforme esta técnica evolucionó, se llegó a impulsar la contabilidad y el registro de operaciones en libros y pólizas. En la actualidad, la contabilidad se lleva a cabo en sistemas de cómputo.

A la par que esto evolucionaba, fue necesario que alguien evaluara que estos registros y resultados fueran correctos y veraces. Entonces se requirió también de alguien que verificara la veracidad y confiabilidad de esas operaciones. En ese momento nació el acto de auditar.

Las primeras revisiones fueron rudimentarias y poco meticulosas, enfocadas exclusivamente a comprobar la veracidad y confiabilidad de los registros contables y su correcta expresión en los resultados que se entregaban; su principal objetivo consistía en saber si las transacciones eran registradas de manera correcta y si las cantidades en ellas asentadas eran exactas. Con ello se buscaba que los encargados de la administración de los negocios llevaran y reportaran con precisión sus anotaciones, para comprobar que no existieran desfalcos ni sustracciones de los bienes que se les encomendaban.

Conforme creció la actividad empresarial y los bancos tuvieron más injerencia en las empresas, a través de la custodia de sus depósitos y el otorgamiento de préstamos a las mismas, se requirió la elaboración de *estados financieros*, en los cuales las empresas anotaban los resultados obtenidos durante los ejercicios anteriores; estos estados financieros también les servían para demostrar su solvencia cuando solicitaban algún préstamo.

En sus inicios, los bancos aceptaban los resultados que emitían las empresas sin objetar sus estados financieros y sin necesidad de dictamen alguno, siempre y cuando estos resultados fueran hechos por un profesional de la contabilidad. Sin embargo, como consecuencia del propio crecimiento de las actividades empresariales, se hizo necesario que el reporte de los resultados de una empresa también fuera avalado por un profesional independiente, a quien se le encargaba que comprobara y dictaminara sobre la veracidad y confiabilidad de los resultados presentados por los financieros de la empresa. Así nació formalmente la actividad del auditor.

1.2.1. Antecedentes históricos de la auditoría

"En tiempos históricos, auditor era aquella persona a quien le leían los ingresos y gastos producidos por un establecimiento (de ahí su raíz latina del verbo **audire***,* oír, es- cuchar*), práctica muy utilizada por civilizaciones muy antiguas [...]"* [1]

Podemos intuir que la primera auditoría nació desde el momento en que fue necesario

rendir cuentas de algún negocio y revisar que éstas fueran correctas; es evidente que dicha función fue evolucionando a la par que el crecimiento de la actividad de registros de operaciones mercantiles. Sin embargo, de acuerdo con los primeros antecedentes de auditoría, ésta nació antes que la teneduría de libros a finales del siglo XV, pero se profesionalizó con la contabilidad financiera a finales del siglo pasado.

Los primeros antecedentes formales se encuentran en 1284, al subir al trono Sancho VI "El Bravo", quien ordenó a algunos de sus hombres de confianza que controlaran el destino de los caudales públicos. Como resultado de esta medida y como producto de su reinado, se originó el tribunal de cuentas en España.[2]

Se estima que el verdadero nacimiento de la auditoría fue a finales del siglo XV,cuando nobles, ricos y familias pudientes de España, Inglaterra, Holanda, Francia y los demás países poderosos de ese entonces, recurrían a los servicios de revisores de cuentas, quienes se encargaban de revisar las cuentas manejadas por los administra- dores de sus bienes, y se aseguraban de que no hubiera fraudes en los reportes que se les presentaban.

El descubrimiento de América (1492) contribuyó también al crecimiento de la actividad de la auditoría, pues la Corona envió visitadores a revisar las cuentas y resultados de sus colonias; dichos visitadores supervisaban que el registro y manejo de las cuentas fueran correctos y emitían una opinión sobre la actuación de los encargados. En México, los virreyes representaban a la Corona y los visitadores venían arevisar el manejo de los tesoros, las recaudaciones, los gastos y la forma en que sus encargados gobernaban en la Nueva España. Igual ocurrió en sus otras colonias deAmérica.

"El origen de los auditores (ESPASA-CALPE, 1988) es la Curia Romana, tiene su ori-gen en la Edad Media [...] El auditor Papae, que en un principio daba consejos en materia de teología [...]; luego ejercía el poder civil y eclesiástico y desde 1831 se entendió en ciertos asuntos disciplinarios."[3]

Aquí se presentan otros de los antecedentes que se pueden citar: a mediados del siglo XIX, la *Ley de Empresas del Reino Unido de Inglaterra*, que impuso la obligación de ejecutar auditorías a los resultados financieros, el balance general, los registros contables y las actividades financieras de las empresas públicas. Dicha costumbre, aun- que no fue de carácter impositivo en Estados Unidos, también se adoptó en las empre-sas de ese país, y se hizo extensiva a los contadores norteamericanos, quienes tuvieron que admitir una práctica similar, principalmente por los requisitos y disposiciones emitidos por la Comisión de Valores y Bolsa, los cuales solicitaban a los auditores independientes que dictaminaran sobre los estados de resultados de las empresas quecotizaban en la Bolsa de Valores de ese entonces.

Otro posible origen lo representaron *los auditores eclesiásticos de la Rota Romana*, a través de tribunales pluripersonales, compuestos por 12 eclesiásticos: ocho italianos, dos españoles, un alemán y un francés.

También se conocieron *los auditores de la Marina y Guerra* en 1894, a quienes se les

considera como los responsables del cumplimiento de las leyes y principios de esta disciplina.

A manera de concentrado de los antecedentes no contables de la auditoría, se pueden señalar los siguientes:

- *Auditores canónigos*
- *Auditores de la nunciatura*
- *Auditores de la Rota Romana*
- *Auditores de la Marina y Guerra*
- *Auditores de camareta*
- *Oidores de la colonia en la Nueva España*

Algunos antecedentes más recientes aparecen con la Revolución Industrial, a partir de la séptima década de 1800; en ese entonces, algunas empresas habían alcanza- do gran auge en las actividades fabriles y mercantiles, lo cual trajo consigo un notablecrecimiento en sus operaciones; obviamente, aumentó también la necesidad de registrar las operaciones contables, y con ello se hizo casi indispensable la existencia de laprofesión de contador para satisfacer esa creciente necesidad. A la par creció la de- manda de ejercer una mayor vigilancia del registro de operaciones financieras y la emisión de resultados financieros que realizaban esos nuevos profesionales, llegando adarse el caso de que el dictamen emitido por un contador independiente, que ejerciera la función de auditor, se consideraba totalmente confiable. Así adquirió popularidad la función de la auditoría y se destacó como una actividad preponderante en la administración de las empresas de ese entonces.

En un principio, la auditoría se consideró como una rama complementaria de la contaduría pública, y sólo se dedicaba a examinar los registros contables y la correcta presentación de los estados financieros de las empresas. Posteriormente, dicha aplicación se extendió a otros campos profesionales para ampliar su revisión; primero a los de carácter administrativo, después a los asociados a otras actividades de la empresa,luego se extendió a las ramas de ingeniería, medicina, sistemas y así sucesivamente, hasta que su práctica alcanzó a casi todas las disciplinas del quehacer humano. A pesar de la amplia gama de áreas en donde se pueden aplicar auditorías, en cualquiera de ellas se tienen que considerar los mismos principios y fundamentos teóricos y prácticos que le dan vigencia a esta profesión.

Aunque la revisión de registros y cuentas se pueden considerar como el inicio de la auditoría, su reconocimiento como profesión se inició en los albores del presente siglo. No obstante, también hay evidencias de que, a mediados del siglo pasado, los británicos, españoles, estadounidenses, e incluso los mexicanos, iniciaron la actividad formal de la auditoría.

Debido a la abundancia de literatura sobre la auditoría financiera, y a la profundidad con que numerosos autores han realizado el análisis a la auditoría de los estados financieros, en este capítulo sólo nos enfocaremos en conocer los antecedentes generales de la auditoría de carácter administrativo y operacional, ya que de la conjugaciónde esos tipos

de auditoría nacieron otros más especializados, entre ellos *la auditoría de sistemas computacionales*.

1.2.2. Antecedentes de la auditoría (siglo XX)

Para hacer las referencias a estas auditorías, vamos a tomar como válidos los antecedentes presentados en la tesis profesional de recientes titulados de la UVM,[4] quienes culminaron su carrera de *Licenciatura en Sistemas de Computación Administrativa*,producto de un profundo estudio e investigación de carácter documental, complementados con otras investigaciones; al respecto encontramos los siguientes datos, enfoca- dos exclusivamente a los antecedentes de la auditoría de carácter administrativo yoperacional, pero que pueden ser válidos como antecedentes para este libro.

En 1912, en el Instituto de Contadores Públicos de España, surge en forma colegiada la actividad del auditor, la cual tuvo una duración muy efímera.

En 1917, el Colegio de Censores de Bilbao.

En 1932, T. G. Rose, consultor inglés en el Instituto de Administración Industrial, expuso la tesis "[...] *Independientemente de la utilidad de la auditoría financiera,también es útil la auditoría administrativa*..."

En 1932, James McKinsey llega a la conclusión de que la empresa tenía que hacer periódicamente una auto auditoría, la cual consistiría en una evaluación de la empresa en todos los aspectos.

En 1936, el Colegio de Contadores Jurados de Madrid.

En 1945, el Instituto de Auditores Internos, en Estados Unidos, proporcionó los primeros escritos sobre lo que sería la auditoría de operaciones, tratando en una discusión de "expertos" lo referente al alcance de la auditoría interna de operaciones técnicas.

En 1946, el Instituto de Censores Jurados de Cuentas de España.

En 1948, Artur H. Kent, funcionario de la empresa Standard Oil of California, hizo importantes aportaciones sobre la auditoría de operaciones.

En 1950, Jackson Martindell, fundador del *American Institute of Management*, desarrolló uno de los primeros programas de auditoría administrativa, con un procedimiento de control directo y un sistema de evaluación, el cual se publicó en sulibro *Apreciación de la gerencia para ejecutores e inversionistas.*

En 1955, Larke A. G. planteó la necesidad de llevar a cabo auto auditorías para las pequeñas empresas, con el fin de evaluar su forma de actuar.

En 1962, Willian P. Leornard realizó un estudio completo de la auditoría administrativa. En

éste trata los métodos para iniciar, organizar, interpretar y presentar una revisión de carácter administrativo.

En 1964, Cadmus y Bradford, quienes eran trabajadores del Instituto de AuditoresInternos (en N. Y.), plantean en su publicación *Operational Auditing Handbook, N.Y.*,la necesidad de una auditoría denominada auditoría operativa, en la cual se selecciona una actividad para un cuidadoso y profundo estudio, apreciación y evaluación.

En 1968, Rigg F. J., autor británico, desarrolló en su país un moderno enfoque dela auditoría administrativa, cuya aplicación se extendió a través de su obra *The Management Audit, the Internal Auditor*.

En 1968, John C. Burton, en su trabajo *The Journal of Accountancy, N. Y.,* planteó la importancia de estudiar de qué índole sería la auditoría administrativa y el grado de calificación del auditor, así como de construir un marco total para la audito- ría administrativa.

En 1969, Langenderfer H. Q. y Robertson J. C. exploraron brevemente el problema de la definición y cuestión de una exposición detallada de la auditoría administrativa. Propusieron también una estructura teórica para extender la función de laauditoría a todos los ámbitos de la empresa, buscando con ello abarcar las audito- rías independientes de gerencias.

En 1970, Keith D. y Bloomstrom R. exponen que las auditorías administrativas sehan desarrollado a través de los años como una forma de evaluar la eficiencia y laeficacia de varios sistemas de una organización, los cuales van desde la responsabilidad administrativa hasta su preocupación social. Esta auditoría se utiliza principal-mente para los propósitos de planeación, entre los cuales están los siguientes:

Investigar empresas para posibles fusiones o adquisicionesDeterminar la solidez de un proveedor principal

Averiguar los puntos débiles y fuertes de una empresa competidora para explorar mejor las ventajas competitivas de la propia empresa

En 1977, Clark C. Arb presenta una perspectiva sobre el conocimiento de la medición de la conducta social de las empresas. En sus conceptos de auditoría social destaca la responsabilidad social, mediciones del comportamiento, auditorías sociales en decisiones administrativas y la implantación de las auditorías.

En 1980, Whitmore G. M. expone que la auditoría administrativa se utiliza para apoyar a los funcionarios públicos y gerentes de empresas privadas. Los aspectos que señala principalmente sobre el uso de esta técnica en el ámbito gubernamental, son las estrategias y los pasos necesarios para la conducción de una auditoría administrativa, haciendo énfasis en sus ventajas.

En 1983, Spencer Hayden expuso la necesidad de evaluar los procedimientos administrativos y de aplicar las correcciones necesarias para lograr una máxima

eficiencia en las actividades futuras. También abundó sobre un procedimiento pro-pio de la auditoría, el tratamiento con detalle del tema de la consultoría administrativa, y enfocó a esta auditoría dentro del camino al cambio organizacional.

En 1984, Robert J. Thierauf habló sobre la auditoría administrativa como una técnica utilizada para evaluar las áreas operacionales de una organización, enfocandosu trabajo desde el punto de vista administrativo.

Podríamos seguir profundizando en los antecedentes de la auditoría en los EstadosUnidos y otros países, pero no es el objetivo de este libro detallar sobre todos los antecedentes de la auditoría administrativa, ni operacional, ni integral ni de cualquier otro tipo, sino que, al presentar estos antecedentes, se busca reconocer que la auditoría de sistemas es el resultado de varias evoluciones de otros tipos de auditorías y que seapoya en ellas para su revisión, incluyendo varias de sus técnicas y metodologías deevaluación.

1.2.3. Antecedentes de la auditoría en México (siglo XX)

En México existe también una gran cantidad de información sobre la auditoría financiera, o por lo menos más que en otros tipos de auditorías. Por esta razón considera- remos únicamente los antecedentes de la auditoría operacional, administrativa e integral. Apoyados en las referencias de la tesis ya citada, a continuación, se muestran,en orden cronológico, los escritores mexicanos más relevantes en este campo[5]

En 1960, A. Mejía Fernández destacó la importancia de la auditoría en su tesis recepcional, *Auditoría de las funciones de la gerencia de las empresas,* presentadaen la FCA de la UNAM en ese año.

En 1962, R. Macías Pineda presentó el trabajo recepcional, *La auditoría administrativa para el curso Teoría de la Administración*, para el Doctorado de Ciencias Administrativas de la Escuela Superior de Comercio y Administración (ESCA) delInstituto Politécnico Nacional.

En 1964, M. D'Azaola S. presentó, en la FCA de la UNAM, la tesis *La revisión del proceso administrativo*.

En 1966, J. A. Fernández Arenas propuso la realización de la auditoría administrativa, combinando los análisis de objetivos, de recursos y del proceso administrativo.

En 1969, Santillán González propuso la realización de la auditoría interna integralmediante una revisión total, tanto de los aspectos financieros como de los aspectos administrativos de las empresas.

En 1970, R. Jiménez Reyes estudió el alcance, desarrollo y planeación de la auditoría administrativa.

En 1978, el Colegio Nacional de Licenciados en Administración (CONLA) publicó, como

resultado del 7º Congreso Nacional de Administración, el trabajo donde seregulan las bases de las normas, alcances del auditor y del informe de auditoría.

En 1978, **S. Cervantes Abreu** presentó un trabajo en ese mismo foro, en el cualanalizó la dinámica de la auditoría administrativa, destacando los cuatro pasos básicos para su desarrollo: *la recolección, la verificación de datos, el estudio de las funciones, la revisión y evaluación del control interno y del informe de la auditoría*.

En 1981, V. M. Rubio y J. Hernández F. presentaron una guía práctica de audito-ría administrativa, como parte de un método para el diagnóstico de la capacidad administrativa de las instituciones públicas y privadas, con el fin de determinar sus puntos vulnerables y sugerir las medidas correctivas.

Así como en el punto anterior, podemos seguir profundizando sobre los antecedentes de la auditoría administrativa, operacional y de otros tipos, pero el enfoque de estecapítulo no es hablar únicamente sobre esas auditorías, sino sobre la auditoría de sistemas. Por esa razón, presentamos exclusivamente lo antes anotado.

1.2.4. Antecedentes de la auditoría de sistemas

Al igual que en los puntos anteriores, en la auditoría de sistemas computacionales también existen antecedentes en el ámbito internacional. Sin embargo, el propósito de este libro no es profundizar en los orígenes de este tipo de auditoría, debido a que seríaocioso y sin ningún beneficio práctico al carecer de evidencias comprobables sobre tales inicios. Sin embargo, para complementar este libro, citaremos a los principales autores sobre este tema en nuestro país:

En 1988, Echenique publicó su libro *Auditoría de sistemas*, en el cual establece las principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico-práctico sobre el tema.

En 1992, Lee presentó un libro en el cual enuncia los principales aspectos a evaluar en una auditoría de sistemas, mediante una especie de guía que le indica alauditor los aspectos que debe evaluar en este campo.

En 1993, **Rosalva Escobedo Valenzuela** presenta en la UVM una tesis de audito- ría a los centros de cómputo, como apoyo a la gerencia, destacando sus aspectos más importantes.

En 1994, G. Haffes, F. Holguín y A. Galán, en su libro sobre auditoría de los estados financieros, presentan una parte relacionada con la auditoría de sistemas, que profundiza en los aspectos básicos de control de sistemas y se complementa con una serie de preguntas que permiten evaluar aspectos relacionados con este campo.

En 1995, Ma. Guadalupe Buendía Aguilar y Edith Antonieta Campos de la O. presentan un tratado de auditoría informática (apoyándose en lo señalado por el maestro Echenique), en el cual presentan metodologías y cuestionarios útiles pararealizar esta especialidad.

. **En 1995, Yann Darrien** presenta un enfoque particular sobre la auditoría de sistemas.

En 1996, Alvin A. Arens y James K. Loebbecke, en su libro *Auditoría. Un enfoque integral*, de Prentice Hall Hispanoamericana, S. A., nos presentan una parte deesta obra como Auditoría de Sistemas Complejos de PED.

En 1996, Hernández Hernández propone la auditoría en informática, en la cual da ciertos aspectos relacionados con esta disciplina.

En 1997, Francisco Ávila obtiene mención honorífica en su examen profesional, en la UVM, Campus San Rafael, con una tesis en la cual propone un caso práctico de auditoría de sistemas realizado en una empresa paraestatal.

En 1998, Yann Darrien presenta *Técnicas de auditoría*, donde hace una propuesta de diversas herramientas de esta disciplina.

En 1998, Mario G. Piattini y Emilio del Peso presentan *Auditoría informática,un enfoque práctico,* donde mencionan diversos enfoques y aplicaciones de esta disciplina.

1.3. Conceptos básicos sobre la auditoría

Como ya hemos mencionado, los campos de aplicación de la auditoría han evoluciona-do mucho, desde su uso en los aspectos netamente contables, hasta su uso en áreas y disciplinas de carácter especial, como la ingeniería, la medicina y los sistemas computacionales. Evidentemente, junto con ese progreso, también se ha registrado el desarrollo de las técnicas, métodos, procedimientos y herramientas de cada uno de estos tiposde auditorías, así como un enfoque cada vez más característico y especializado hacia eluso de técnicas más apegadas al área que se va a evaluar.

Debido a esos constantes cambios, a continuación, citaremos el concepto más amplio de la auditoría, para de ahí analizarlo de acuerdo con lo aportado por la *Real Academia Española* y después, con esa conceptualización, trasladarlo a una propuesta de clasificación de los tipos de auditoría.

En forma general, la definición que se propone para la auditoría es la siguiente:

Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resulta-dos y el cumplimiento de sus operaciones.

Como antecedentes académicos, se encontraron las siguientes expresiones:

Auditor

"Del latín. ***Auditor***, ***oris*** *s. m 1. Persona capacitada para realizar auditorías en empresas u*

otras instituciones. Pertenece a un colegio oficial [...] 3. Auditor de guerra. Funcionario miembro del cuerpo jurídico del ejército que informa en los tribunales militares sobre la interpretación o aplicación de las leyes. 4. [...] auditor de la Rota. Ca- da uno de los doce miembros del tribunal romano de la Rota."[6]

"F. **Auditeur**; It. **uditore**; In., C. P. **uditor**; A.; **Zahöurer***[....] Del latín **uditor**; el que oye, del verbo **audire**. Oír. Anteriormente, oyente."*[7]

Auditoría:

"[...] Supervisión de las cuentas de una empresa, hecha por decisión de un tribunal o a instancias de particular."[8]

"[...] Revisión a la economía de una empresa [...]"[9] *"[...] Revisión de cuentas [...]"*[10]

"1. Profesión de auditor. 2. Despacho o tribunal del auditor. 3. Revisión de cuentas, examen y evaluación de la situación financiera y administrativa de una institución o empresa, realizados por especialistas ajenos a la misma."[11]

"[...] Empleo, cargo de auditor. Tribunal o despacho de auditor."[12]

Audit:

"[...] Revisión o intervención de cuentas [...] Verificar o revisar la contabilidad."[13]

"Es un examen profesional y revisión de los registros, los procedimientos y las transacciones financieras de una organización hechas por especialistas [...] involucrados en la preparación de esos informes. Con base en este examen, en su informe los auditores dan una opinión independiente de la organización de su posición financiera, si los procedimientos y los controles apropiados se han seguido, y si los otros criterios han estado satisfechos en el desembolso de fondos. [...] Una revisión interna, conducida por empleados de la compañía, donde se prueba la suficiencia de los procedimientos y sistemas de contabilidad. [...] para determinar si la corporación encuentra sus responsabilidades a empleados y sociedad."

> *"Constituye adaptación popular del verbo inglés **to Audit**, el cual significa examinar, re- visar cuentas."*

1.4. Clasificación de los tipos de auditorías

Para iniciar nuestro estudio, aquí proponemos que el análisis de los conceptos anteriores se realice al amparo de la siguiente clasificación de los tipos de auditorías, con el fin de identificar los criterios, características y especificaciones de esta disciplina profesional. Posteriormente nos concentraremos exclusivamente en los conceptos y definiciones de la auditoría de sistemas computacionales.

La clasificación que se propone está integrada por el siguiente cuadro:

Auditorías por su lugar de aplicación

- Auditoría externa
- Auditoría interna

Auditorías por su área de aplicación

- Auditoría financiera
- Auditoría administrativa
- Auditoría operacional
- Auditoría integral
- Auditoría gubernamental
- Auditoría de sistemas

Auditorías especializadas en áreas específicas

- Auditoría al área médica (evaluación médico-sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoría laboral
- Auditoría de proyectos de inversión
- Auditoría a la caja chica o caja mayor (arqueos)
- Auditoría al manejo de mercancías (inventarios)
- Auditoría ambiental
- Auditoría de sistemas

Auditoría de sistemas computacionales

- Auditoría informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría alrededor de la computadora
- Auditoría de la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsourcing
- Auditoría ergonómica de sistemas computacionales

1.4.1. Clasificación de la auditoría por su lugar de origen

La primera clasificación se refiere a la forma en que se realiza este tipo de trabajos, y también a cómo se establece la relación laboral en las empresas donde se llevará a cabo la auditoría; esto nos da un origen externo si el auditor no tiene relación directa con la empresa,o un origen interno si existe alguna relación de dicho auditor con la propia empresa.

Auditoría externa

La principal característica de este tipo de auditoría es que la realizan auditores total-

mente ajenos a la empresa, por lo menos en el ámbito profesional y laboral; esto per-mite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación de las actividades y operaciones de la empresa que audita y, por lo tanto, la emisión de resultados será absolutamente independiente. Su definición es la siguiente:

Es la revisión independiente *que realiza un profesional de la auditoría,* con total libertad de criterio y sin ninguna influencia, *con el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de sus resultados financieros. La* relación de trabajo del auditor es ajena a la institucióndonde se aplicará *la auditoría y esto le permite emitir un dictamen libre e independiente.*

Generalmente, estas auditorías externas son realizadas por grandes empresas y despachos independientes de auditores, los cuales, casi siempre gozan de gran popularidad y prestigio dentro del ambiente profesional. El mercado en el cual tienen mayor demanda y aplicación estas auditorías es el ámbito contable, fiscal y financiero de las instituciones, así como en aquellas actividades específicas que demandan una auditoría externa a la empresa cuando existen condiciones especiales que se pretenden evaluar.

Ventajas

Al no tener ninguna dependencia de la empresa, el trabajo de estos auditores es total-mente independiente y libre de cualquier injerencia por parte de las autoridades de la empresa auditada.

* P

ara el mejor entendimiento y distinción entre cada uno de los tipos de auditoría que se proponen, en cada definición se ponen en cursivas sus aspectos más sobresalientes; el propósito es que usted, amigo lector, pueda distinguir la esencia de cada descripción.

En su realización, estas auditorías pueden estar apoyadas por una mayor experiencia por parte de los auditores externos, debido a que utilizan técnicas y herramientas que ya fueron probadas en otras empresas con características similares.

Estas auditorías tienen gran aceptación en las empresas para certificar registros contables, impuestos y resultados financieros. Además, sus dictámenes pueden ser válidos para las autoridades impositivas, y con ello pueden satisfacer requisitos de carácter legal, siempre que sean realizadas por auditores de prestigio que tengan el reconocimiento público.

Desventajas

La principal desventaja es que, como el auditor conoce poco la empresa, su evaluación puede estar limitada a la información que pueda recopilar.

Dependen en absoluto de la cooperación que el auditor pueda obtener de parte delos

auditados.

Su evaluación, alcances y resultados pueden ser muy limitados.

Muchas auditorías de este tipo se derivan de imposiciones fiscales y legales quepueden llegar a crear ambientes hostiles para los auditores que las realizan.

En algunos casos son sumamente costosas para la empresa, no sólo en el aspecto numerario, sino por el tiempo y trabajo adicional que representan.

Auditoría interna

En la realización de estos tipos de evaluación, el auditor que lleva a cabo la auditoría labora en la empresa donde se realiza la misma y, por lo tanto, de alguna manera está involucrado en su operación normal; debido a esto, el auditor puede tener algún tipo de dependencia con las autoridades de la institución, lo cual puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa. La definición que se sugiere es:

Es la revisión que realiza un profesional de la auditoría, cuya relación de traba-jo es directa y subordinada a la institución *donde se aplicará la misma, con el propósito* de evaluar en forma interna *el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreasadministrativas, así como evaluar la razonabilidad en la emisión de sus resulta-dos financieros. El objetivo final* es contar con un dictamen interno *sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados y funcionarios de las áreas que se auditan.*

Ventajas

Debido a que el auditor pertenece a la empresa, casi siempre conoce s actividades, operaciones y áreas; por lo tanto, su revisión puede ser más profunda y con un mayor conocimiento de las actividades, funciones y problemas de la institución. Por esta razón, el contenido de su informe es mucho más valioso.

El informe que rinde el auditor, independientemente del resultado, es sólo de carácter interno y por lo tanto no sale de la empresa, ya que únicamente le sirve a las autoridades de la institución.

Esta auditoría consume sólo recursos internos, por lo tanto no representa ninguna erogación adicional para la empresa en la cual se realiza.

Es de gran utilidad para la buena marcha de la empresa, ya que permite detectar problemas y desviaciones a tiempo.

Puede llevarse un programa concreto de evaluación en apoyo a las autoridades de la empresa, lo cual ayudará a sus dirigentes en la evaluación y la toma de decisiones.

Desventajas

Su veracidad, alcance y confiabilidad pueden ser limitados, debido a que puede haber

cierta injerencia por parte de las autoridades de la institución sobre la forma de evaluar y emitir el informe.

En ocasiones la opinión del auditor tal vez no sea absoluta, debido a que, al laborar en la misma empresa donde realiza la auditoría, se pueden presentar presiones, compromisos y ciertos intereses al realizar la evaluación.

Se pueden presentar vicios de trabajo del auditor con relativa frecuencia, ya sea enlas formas de utilizar las técnicas y herramientas para aplicar la auditoría, como en laforma de evaluar y emitir su informe sobre la misma.

1.4.2. Clasificación de auditorías por su área de aplicación

La clasificación aquí propuesta se refiere al ámbito específico donde se llevan a cabo las actividades y operaciones que serán auditadas, ubicando a cada tipo de auditoría de acuerdo con el área de trabajo e influencia de la rama o especialidad que será evaluada.En atención a dicho criterio, y debido a que podemos encontrar un sinnúmero de clasificaciones de estos tipos de auditorías, todas válidas, para nuestro análisis de los *conceptos generales* sólo nos concentraremos en presentar su clasificación y una breve definición de cada uno de los tipos, tomando en cuenta solamente su área de aplicación sin ir más allá, es decir, no se analizarán sus ventajas ni desventajas.

Auditoría financiera (contable)

Inicialmente llamada auditoría contable, en realidad fue el primer tipo de auditoría que existió en el ámbito comercial; en este tipo de auditoría la principal actividad del auditor consiste en revisar la correcta y oportuna aplicación de los registros contables y operaciones financieras de las empresas, con el propósito de comprobar que la emisión de los resultados financieros de un ejercicio fiscal cumpla con los principios contables que regulan las actividades del contador público y así poder emitir un dictamensobre sus resultados financieros. La definición que analizaremos es la siguiente:

Es la revisión sistemática, explorativa y crítica que realiza un profesional dela contabilidad *a los* libros y documentos contables, a los controles y registros de las operaciones financieras y a la emisión de los estados financieros *de unaempresa, con el fin de evaluar y opinar sobre la razonabilidad, veracidad, con-fiabilidad y oportunidad* en la emisión de los resultados financieros *obtenidos durante un periodo específico o un ejercicio fiscal. El propósito final es* emitirun dictamen contable *sobre la correcta presentación de los resultados financieros a los accionistas, clientes, autoridades fiscales y terceros interesados,* en relación con las utilidades, pago de impuestos y situación financiera y económica *de la institución.*

Actualmente este tipo de auditoría se complementa con un análisis financiero de los resultados obtenidos durante dicho ejercicio, para lo cual se utilizan diversas técnicas de la ingeniería financiera y del análisis contable.

Auditoría administrativa

Después de lo anterior, el siguiente paso de la auditoría, muy importante, por cierto, fue ampliar su ámbito de evaluación a las actividades administrativas de las empresas. Los auditores ya no se contentaban solamente con auditar los resultados financieros de las empresas, sino que les hacía falta completar su trabajo; por eso procedieron a evaluarel adecuado cumplimiento de las funciones, actividades y operaciones de la empresa, principalmente en el aspecto administrativo. Por esta razón se le llamó auditoría administrativa. Su definición es la siguiente:

Es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa *de una empresa, en cuanto a* su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades *que regulan susoperaciones.* Su propósito es evaluar tanto el desempeño administrativo de las áreas de la empresa, como la planeación y control de los procedimientos deoperación, y los métodos y técnicas de trabajo *establecidos en la institución, incluyendo la observancia de las normas, políticas y reglamentos que regulan el uso de todos sus recursos.*

Inicialmente esta auditoría fue aplicada por contadores, pero debido a su propiocampo de acción, así como a la importancia de esta materia, se extendió con rapidez ala profesión de licenciado en administración y carreras similares, siendo éste uno de losprincipales espacios de acción de estos profesionales. Entre los primeros representantesdel tema se encuentran Leonard, de Estados Unidos, y Fernández Arena, de México.

Auditoría operacional

En un principio formó parte de la evaluación a las operaciones contables y administrativas de las empresas, pero su peso e importancia fueron tales que fue necesario hacer auditorías a las operaciones de toda la institución, dándose así una nueva especialidad, no sólo en el campo de los administradores, sino en otras áreas especializadas como la ingeniería, relaciones laborales y otras ramas que la utilizaban para evaluar las operaciones de cualquier área de una institución.

Incluso en algunos casos fue de gran utilidad para el campo de organización, métodos y procedimientos, las actividades fabriles y en sí de la ingeniería aplicada. La definición propuesta es la siguiente:

Es la revisión exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que éstas sean, *tanto en el establecimiento y cumplimiento de los métodos, técnicas y procedimientos de trabajo necesarios para el desarrollo de sus operaciones, encoordinación con los recursos disponibles, como en las normas, políticas, lineamientos y capacitación que regulan el buen funcionamiento de la empresa.*

Auditoría integral

Debido al constante crecimiento de las ramas en las que se podía utilizar la auditoría, y a que cada vez existía una mayor interrelación entre todas las operaciones y actividades de una empresa, casi siempre vinculadas entre sí pero distintas con relación a su contribución a la actividad fundamental de la empresa, surgió la necesidad de avanzaren la rama de

auditoría, con el fin de buscar una forma de evaluación global de todas las áreas que participan en la vida productiva de las corporaciones. Por tal razón hubola exigencia de encontrar mecanismos especiales con los cuales se pudieran evaluar conjuntamente todas esas actividades.

Tras varias experimentaciones se logró lo anterior mediante la participación de ungrupo interdisciplinario de profesionales de diversas especialidades, quienes se agruparon en torno a la disciplina de la auditoría con el fin de poder evaluar conjuntamente todas las áreas, actividades, funciones y operaciones de las instituciones. La definición de esta auditoría es la siguiente:

Es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empre- sa, con el propósito de evaluar, de manera integral, *el correcto desarrollo de las funciones* en todas sus áreas administrativas, *cualesquiera que éstas sean, así como de evaluar sus resultados conjuntos y relaciones de trabajo, comunicaciones y procedimientos interrelacionados que regulan la realización de las actividades compartidas para alcanzar el objetivo institucional; dicha revisión selleva a cabo también a las normas, políticas y lineamientos sobre el uso de todos los recursos de la empresa.*

El propósito fundamental de este nuevo tipo de auditoría tan especializado es poder auditar de manera conjunta todas las actividades, funciones y operaciones de todas las áreas de una empresa, con la posibilidad de evaluar al total de las ramas que conforman una empresa. En esta auditoría se conjuga la participación colegiada de muchos profesionales de distintas especialidades, quienes aparentemente no tienen relación entre sí por lo diferente de sus áreas de actuación, pero que al conjuntar sus trabajos contribuyen en gran medida a elevar los alcances, la profundidad y eficacia de la evaluación de todas las áreas de una misma empresa.

Auditoría gubernamental

Esta auditoría se realiza debido a que los gobiernos federales, estatal y/o municipal son los responsables de captar los ingresos aportados por los contribuyentes, y son también los encargados de manejar los egresos de carácter público para proporcionar el bienestar de la sociedad. Se realiza también debido a lo especializado que resulta el manejoapropiado de las actividades y operaciones gubernamentales requeridas para satisfacer las necesidades de la población, y debido al cúmulo de funciones especializadas de gobierno, las cuales regulan la actuación de una entidad gubernamental a otra, aparente-mente distintas entre sí.

Todo esto en conjunto hace que su evaluación sea también muy especializada ycon características muy particulares, ya que existe la necesidad de una vigilancia más detallada de las funciones gubernamentales. Esta vigilancia debe ser muy estrecha en cuanto al adecuado manejo y cumplimiento de los programas, ingresos, egresos, acciones y funciones por parte de quienes tienen esta responsabilidad ante la sociedad, y además se debe vigilar que todas esas acciones gubernamentales se cumplan con-forme a lo regulado en las leyes federales, estatales y/o municipales.

Debido al alto grado de especialidad que se requiere para auditar estas actividades y resultados gubernamentales, la auditoría tradicional fue incapaz de evaluar esta necesidad. Por esta razón nació la llamada auditoría gubernamental, la cual se puede definir de la siguiente manera:

Es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones de una entidad gubernamental, *cualquiera que sea lanaturaleza* de las dependencias y entidades de la Administración Pública Federal. *Esta revisión se ejecuta con el fin de evaluar el correcto desarrollo de las* funciones de todas las áreas y unidades administrativas de dichas entidades, así como los métodos y procedimientos *que regulan las actividades* necesariaspara cumplir con los objetivos gubernamentales, estatales o municipales; *también se lleva a cabo en la* aplicación y cumplimiento de presupuestos públicos,programas, normas, políticas y lineamientos *que regulan la participación de los recursos de la entidad en la prestación de servicios a la sociedad.*

Esta definición nos indica claramente cómo se satisfizo la necesidad de evolucionar hacia una auditoría más especializada con la cual se pudiera evaluar la correctaaplicación de los presupuestos y gastos del gobierno, y con la que se tuviera la suficiente capacidad para dictaminar acerca del adecuado cumplimiento de las actividades que son encomendadas a las diferentes dependencias gubernamentales e instituciones paraestatales de la federación, los estados y municipios, mediante las técnicas y procedimientos de la auditoría.

Auditoría informática

Motivada por lo especializado de las actividades de cómputo, así como por el espectacular avance que han tenido estos sistemas en los últimos años, ha surgido una nueva necesidad de evaluación para los auditores, quienes requieren una especialización cada vez más profunda en sistemas *computacionales* para dedicarse a este tipo de auditorías. Por ello nació la necesidad de evaluar no sólo los sistemas, sino también la in-formación, sus componentes y todo lo que está relacionado con dichos sistemas. Ladefinición propuesta es la siguiente:

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisiónse realiza de igual manera a la gestión informática, el aprovechamiento de sus re-cursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. *El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados enla institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.*

Las definiciones anteriores son las más comunes y conocidas en el ambiente de la auditoría; sin embargo, existen otros tipos de auditorías más especializados, por lo quees

de suma importancia conocer las definiciones de esos modelos, mismas que se presentan a continuación. Con esto se pretende establecer los diferentes criterios y áreas especializadas de evaluación que existen en esta materia para que el lector conozca dichos tipos de auditorías y pueda llegar a dominar su aplicación.

1.4.4. Definiciones de auditorías especializadas en áreas específicas

El avance de la auditoría no se detiene y requiere una mayor especialización en la evaluación de las áreas y ramas del desarrollo tecnológico de nuestros días; por esta razón, las auditorías son cada vez más singulares y tienen aplicaciones muy peculiares, las cuales están enfocadas a satisfacer las necesidades concretas de revisión y dictamen, según la especialidad de que se trate.

Es evidente que estos tipos de auditorías requieren algo más que el uso de métodos, técnicas, herramientas y procedimientos tradicionales de la auditoría, ya que deben evolucionar y adaptarse a las necesidades específicas de cada una de las áreas en don- de se llevará a cabo la evaluación. Por ello cada día se tecnifican más las auditorías.

Existen muchos tipos de auditorías especializadas, pero de entre todas ellas citaremos sólo las siguientes:

- *Auditoría al área médica (evaluación médico-sanitaria)*
- *Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)*
- *Auditoría fiscal*
- *Auditoría laboral*
- *Auditoría de proyectos de inversión*
- *Auditoría a la caja chica o caja mayor (arqueos)*
- *Auditoría al manejo de mercancías (inventarios)*
- *Auditoría ambiental*

A continuación, se proponen las definiciones formales para cada uno de los tiposde auditoría aquí expuestos, con el propósito de dar a conocer sus antecedentes y conceptos generales. En estas definiciones no se presenta ningún comentario adicional.

Auditoría al área médica (evaluación médico-sanitaria)

Es la evaluación sistemática, exhaustiva y especializada que se realiza a las ciencias médicas y de la salud, aplicada sólo por especialistas de disciplinasmédicas o similares, *con el fin de emitir un dictamen especializado sobre el correcto* desempeño de las funciones y actividades del personal médico, paramédico, técnicos en salud y similares, *así como sobre la atención que las dependencias y el personal de esta especialidad prestan a pacientes, familia- res y proveedores.*

Auditoría al desarrollo de obras y construcciones(evaluación de ingeniería)

Es la revisión técnica especializada que se realiza a la edificación de construcciones, cimientos, obra negra, acabados y servicios urbanísticos complementarios de casas,

edificios, puentes, caminos, presas y cualquier otro tipo deconstrucción, *ya sea de tipo civil y/o arquitectónico; dicha revisión se realiza también a los planos, presupuestos, adquisiciones, cálculos y programas deobra, así como al cumplimiento y desarrollo de estas. Su propósito es* emitir un dictamen especializado sobre la correcta aplicación de las técnicas, cálculos, métodos y procedimientos de la ingeniería civil y la arquitectura.

Auditoría fiscal

Es la revisión exhaustiva, pormenorizada y completa que se realiza a los registros y operaciones contables *de una empresa, así como la evaluación de la correcta elaboración de los resultados financieros de un ejercicio fiscal, con el propósito de* dictaminar sobre el correcto ejercicio financiero y la razonabilidad en la presentación de los estados de resultados y, como consecuencia de ello, comprobar el correcto pago de los impuestos y demás contribuciones tributarias, *tanto de la empresa como de sus empleados, acreedores y compradores.*

Auditoría laboral

Es la revisión y evaluación especializadas que se realizan a las actividades, funciones y operaciones relacionadas con el factor humano *de una empresa; su propósito* es dictaminar sobre el adecuado cumplimiento en la selección, capacitación y desarrollo del personal, la correcta aplicación de las prestaciones sociales y económicas, el establecimiento de las medidas de seguridad e higiene en la empresa, la elaboración de los contratos colectivos e individuales de trabajo, los reglamentos internos de trabajo, *normas de conducta y demás actividades que intervienen en la gestión de personal de una empresa.*

Auditoría de proyectos de inversión

Es la revisión y evaluación que se realizan a los planes, programas y ejecución de las inversiones de los recursos económicos de una institución pública o privada, con el propósito de dictaminar sobre el uso y control correctos de esos recursos, evaluando que su aplicación sea exclusivamente para cumplir el objetivo del proyecto. *Dicha revisión se realiza también a la ejecución y control de los presupuestos, a la adquisición y uso de recursos conforme a las normas y al cumplimiento correcto de las demás actividades especializadas del ejercicio presupuestal.*

Auditoría a la caja chica o caja mayor (arqueos)

Es la revisión periódica del manejo del efectivo que se asigna a una persona o área de una empresa, y de los comprobantes de ingresos y egresos generados por sus operaciones cotidianas; *dicha revisión se lleva a cabo con el fin de verificar el adecuado manejo, control y custodia del efectivo disponible para gas-tos menores, así como de evaluar el uso, custodia y manejo correctos de los fondos de la empresa. Por lo general, estas revisiones se realizan en forma periódica y de manera exhaustiva, dependiendo del monto asignado.*

Auditoría al manejo de mercancías (inventarios)

Es la revisión física que se realiza a través del conteo (inventarios) de los bienes, productos

y materias primas, intermedias o de consumo final *de una empresa, los cuales se encuentran almacenados para su consumo final o para su distribución a clientes y terceros;* su propósito es verificar que las existencias físicas concuerden con los registros contables, con los justificantes de las salidas y entradas y con las incidencias de éstas, *así como verificar el correcto manejo y control de las entradas, salidas, registros y ajustes necesarios que sehacen conforme a las características y políticas de la institución.*

Auditoría ambiental

Es la evaluación que se hace de la calidad del aire, la atmósfera, el ambiente,las aguas, ríos, lagos y océanos, así como de la conservación de la flora y la fauna silvestres, con el fin de dictaminar sobre las medidas preventivas y, en su caso, correctivas que disminuyan y eviten la contaminación *provocada por los individuos, las empresas, los automotores y las maquinarias, y así preservar lanaturaleza y mejorar la calidad de vida de la sociedad.*

Es indudable que existen más definiciones y tipos de auditorías especializadas; sin embargo, no citaremos más conceptos, esto obedece a que la intención de este libro no es presentar ni hacer un tratamiento de las diferentes formas de auditar, sino pre- sentar algunas definiciones de auditoría con el único propósito de que, a usted, amigo lector, le sirvan de referencia para entender los antecedentes e importancia de la auditoría de sistemas computacionales, la cual trataremos más adelante.

Auditoría de sistemas computacionales (Auditoría informática)

Motivados por la importancia de continuar con la exposición de las definiciones de cada uno de los tipos de auditorías, y debido a que la esencia de este libro es enfatizar la trascendencia, utilidad y especialidad de la *auditoría de sistemas computacionales (ASC),* a continuación, presentamos cada una de las definiciones de auditorías especializadas de los sistemas computacionales, las cuales se aplican para las diferentes áreas y disciplinasde este ambiente informático. Estas definiciones contendrán únicamente la exposición delos principales conceptos de esta auditoría y, si es el caso, un breve comentario, ya queen los siguientes capítulos profundizaremos en su estudio y aplicaciones.

Las definiciones propuestas para la auditoría de sistemas computacionales son las siguientes:

- Auditoría informática
- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría en el entorno de la computadora
- Auditoría sobre la seguridad de sistemas computacionales

- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsorcing
- Auditoría ergonómica de sistemas computacionales

A continuación, únicamente se hace la presentación de las definiciones de cadauno de los tipos de auditoría que se proponen en este estudio. Posteriormente se tratarán las aplicaciones específicas de cada clasificación.

Auditoría informática

Esta primera definición se cita sólo de manera general, debido a que alrededor de es- ta conceptualización se engloban todas las demás definiciones de auditoría de sistemas, la cual se conoce también como auditoría en sistemas, auditoría en informática o con otros nombres similares. Esta auditoría se presenta en esta parte con el fin decompletar las definiciones de auditoría, ya que a lo largo de este libro no se utilizará más este concepto de auditoría global, sino que se particularizará de acuerdo con cada especialidad. La definición de auditoría de sistemas es la siguiente:

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.** *El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los da- tos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa.*

* Aunque a primera vista pareciera que estas definiciones son repetitivas, tanto en sus conceptos, alcances y con- tenidos, me tomé la libertad literaria para presentar en esta parte cada una de las definiciones tal y como es, con el único propósito de que sirvan de referencia e identificación para un mejor entendimiento de cada una de las descripciones de auditoría. Espero que usted, amigo lector, me otorgue la dispensa necesaria para tolerar la aparente repetición de conceptos.

** La letra cursiva de los párrafos nos indica los aspectos más relevantes de la clasificación.

Auditoría con la computadora

En este tipo de auditoría se puede distinguir como factor fundamental que su evaluación

se realiza con el apoyo de los sistemas computacionales, aunque pudiera darse elcaso de que la auditoría no se refiera a la evaluación de estos sistemas, sino a cualquier otra disciplina ajena a ellos. Lo relevante es que dichos sistemas se utilizan paraayudar en tal evaluación. Su definición es la siguiente:

Es la auditoría que se realiza con el apoyo de los equipos de cómputo y susprogramas para evaluar cualquier tipo de actividades y operaciones, no necesariamente computarizadas, pero sí susceptibles de ser automatizadas; *dicha auditoría se realiza también a las actividades del propio centro de sistemas y asus componentes. La principal característica de este tipo de auditoría es que,sea en un caso o en otro, o en ambos, se aprovecha la computadora y sus pro-gramas para la evaluación de las actividades a revisar, de acuerdo con las necesidades concretas del auditor, utilizando en cada caso las herramientas especiales del sistema y las tradicionales de la propia auditoría.*

Auditoría sin la computadora

En este tipo de auditoría se busca evaluar a los sistemas desde una óptica tradicional, contando con el apoyo de las técnicas y procedimientos de evaluación acostumbrados y sin el uso de los sistemas computacionales, aunque éstos sean los que se evalúen.Por lo general, esta auditoría se enfoca en los aspectos operativos, financieros, administrativos y del personal de los centros de sistemas computacionales. Su definición esla siguiente:

Es la auditoría cuyos métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional *del comportamiento y validez de las transacciones económicas, administrativas y operacionales* de un área decómputo, *y en sí de todos los aspectos que afectan a las actividades en las quese utilizan sistemas informáticos,* pero dicha evaluación se realiza sin el uso delos sistemas computacionales. *Es también la* evaluación tanto a la estructura de organización, funciones y actividades de funcionarios y personal de un centro de cómputo, así como a los perfiles de sus puestos, *como de los reportes, informes y bitácoras de los sistemas, de la existencia y aplicación de* planes, programas y presupuestos *en dicho centro, así como del uso* y aprovechamiento de los recursos informáticos *para la realización de actividades, operaciones y tareas. Asimismo, es la evaluación de los* sistemas de seguridad y prevenciónde contingencias, de la adquisición y uso del hardware, software y personal informático, *y en sí de todo lo relacionado con el centro de cómputo, pero sin eluso directo de los sistemas computacionales.*

Auditoría a la gestión informática

Esta auditoría es, por lo general, de carácter administrativo y operacional; con su realización se busca evaluar la actividad administrativa de los centros de cómputo, con todo lo que conlleva esta gestión. La definición propuesta es la siguiente:

Es la auditoría cuya aplicación se enfoca exclusivamente a la revisión de lasfunciones y actividades de tipo administrativo que se realizan dentro de uncentro de cómputo, *tales como la* planeación, organización, dirección y control*de dicho centro. Esta auditoría se realiza también con el fin* de verificar el cumplimiento de las funciones y actividades

asignadas a los funcionarios, emplea- dos y usuarios *de las áreas de sistematización, así como para revisar y evaluar* las operaciones del sistema, el uso y protección de los sistemas de procesa-miento, los programas y la información. *Se aplica también para verificar el correcto desarrollo, instalación, mantenimiento y explotación de los sistemas de cómputo, así como sus equipos e instalaciones. Todo esto se lleva a cabo con el propósito de dictaminar sobre la adecuada gestión administrativa de los sis-temas computacionales de una empresa y del propio centro informático.*

Auditoría al sistema de cómputo

Esta auditoría es más especializada y concreta, y está enfocada hacia la actividad y operación de sistemas computacionales, con mucho más de evaluación técnica y especializada de éstos y de todo lo relacionado con esta especialidad. Su definición es la siguiente:

Es la auditoría técnica y especializada que se enfoca únicamente a la evaluación del funcionamiento y uso correctos del equipo de cómputo, su hardware, software y periféricos asociados. Esta auditoría también se realiza a la composición y arquitectura de las partes físicas y demás componentes del hardware, incluyendo equipos asociados, instalaciones y comunicaciones internas o ex ternas, *así como al* diseño, desarrollo y uso del *software de operación, de apoyo y de aplicación, ya sean sistemas operativos, lenguajes de procesamiento y programas de desarrollo, o paquetería de aplicación institucional que se utiliza en la empresa donde se encuentra el equipo de cómputo que será evaluado. Se incluye también* la operación del sistema.

* Aunque aparentemente esta definición y la siguiente son muy similares a la anterior, cada una tiene diferencias sustanciales, aunque también similitudes. La intención de presentarla así, con aparentes repeticiones, es que el lector capte la esencia de cada auditoría, la cual se utilizará de acuerdo a las necesidades concretas de evaluación, eligiendo el tipo de auditoría más adecuado a sus requerimientos de evaluación, a fin de que sea más completa y de mayor alcance.

Auditoría alrededor de la computadora

En este tipo de auditoría se trata de evaluar todo lo que involucra la actividad de los sistemas computacionales, procurando, de ser posible, dejar a un lado todos los aspectos especializados, técnicos y específicos de los sistemas, a fin de evaluar únicamente las actividades vinculadas que se llevan a cabo alrededor de éstos. La definición pro- puesta es la siguiente:

Es la revisión específica que se realiza a todo lo que está alrededor de un equipo de cómputo, como son sus sistemas, actividades y funcionamiento, *haciendo una evaluación de sus métodos y procedimientos de acceso y procesamiento de datos, la emisión y almacenamiento de resultados, las actividades de planeación y presupuestación del propio centro de cómputo, los aspectos operacionales y financieros, la gestión administrativa de accesos al sistema, la atención a los usuarios y el desarrollo de nuevos sistemas, las comunicaciones internas y externas y, en sí, a todos aquellos aspectos que contribuyen al*

buen funcionamientode un área de sistematización.

Auditoría de la seguridad de los sistemas computacionales

Hablar de seguridad es un aspecto muy importante en los sistemas computacionales, lo cual en algunos casos puede estar relacionado con otras auditorías aquí presenta- das. Sin embargo, por lo especializado y profundo del tema, es indispensable que se evalúe por separado; por esta razón se propone la siguiente definición:

Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, *así como a las actividades, funciones y acciones preventivas y correctivas que con- tribuyan a* salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. *Es también la revisión de los planes de contingencia y medidas de protección para la información, losusuarios y los propios sistemas computacionales, y en sí para todos aquellosaspectos que contribuyen a la protección y salvaguarda en el buen funciona- miento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos.*

Auditoría a los sistemas de redes

Es reciente el crecimiento e importancia que han cobrado las redes de cómputo, razón por la cual es necesario enfocar la auditoría hacia este campo específico; no obstante, en ciertos casos, esta evaluación parecería estar contemplada en algunos tipos de auditoría aquí señalados. Su definición es la siguiente:

Es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de re- des, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración *y demás aspectos que repercuten en su* instalación, administración, funcionamiento y aprovechamiento. *Es también larevisión del software institucional, de los recursos informáticos e informaciónde las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.*

Auditoría integral a los centros de cómputo

Esta definición trata de agrupar a todos los tipos de auditoría que se analizan en estas conceptualizaciones, buscando concentrar todas las evaluaciones bajo una misma auditoría con un enfoque global del área de sistemas, según su tipo y tamaño. La definición que se propone es la siguiente:

Es la revisión exhaustiva, sistemática y global que se realiza por medio de un equipo multidisciplinario de auditores, de todas las actividades y operaciones de un centro de sistematización, *a fin de evaluar,* en forma integral, *el uso adecuado de sus sistemas de cómputo, equipos periféricos y de apoyo para el pro-cesamiento de información de la empresa, así como* de la red de servicios de una empresa *y el desarrollo correcto de las funciones de sus áreas, personaly usuarios. Es también la revisión de la administración del*

sistema, del manejo y control de los sistemas operativos, lenguajes, programas y paqueterías de aplicación, así como de la administración y control de proyectos, la adquisición del hardware y software institucionales, de la adecuada integración y usode sus recursos informáticos y de la existencia y cumplimiento de las normas, políticas, estándares y procedimientos que regulan la actuación del sistema, del personal y usuarios del centro de cómputo. Todo esto hecho de maneraglobal por medio de un equipo multidisciplinario de auditores.

Auditoría ISO-9000 a los sistemas computacionales

Las empresas en el mundo han adoptado la calidad ISO-9000 como parte fundamental de sus actividades. Por esta razón, los sistemas están relacionados también con este tipo de auditorías de certificación de calidad, las cuales son muy especializadas y específicas en cuanto a los requerimientos establecidos en ellas. La definición propuestaes la siguiente:

Es la revisión exhaustiva, sistemática y especializada que realizan únicamente los auditores especializados y certificados en las normas y procedimientos ISO-9000, *aplicando exclusivamente los lineamientos, procedimientos e instrumentos establecidos por esta asociación. El* propósito fundamental de esta revisión es evaluar, dictaminar y certificar que la calidad de los sistemas computacionales de una empresa se apegue a los requerimientos del ISO-9000.

Auditoría outsourcing

Otra de las especialidades que se ha adoptado en los sistemas computacionales, es la relacionada con la prestación de servicios de cómputo a las empresas, los cuales abarcan desde la maquilación de sus actividades computacionales, hasta la asesoría y soporte computacional a sus propios sistemas; por esta razón, se requiere de una especialización en la evaluación de estos servicios. La definición que se propone es la siguiente:

Es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad en el servicio de asesoría o procesamiento externo de información *que proporciona* una empresa a otra. *Esto se lleva a cabo con el fin derevisar la confiabilidad, oportunidad, suficiencia y asesoría* por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades *que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas.*

Auditoría ergonómica de sistemas computacionales

Uno de los aspectos menos analizados en el área de sistemas es la afectación que causan el mobiliario y los propios sistemas computacionales en los usuarios de computadoras; estos aspectos pueden llegar a influir en el bienestar, salud y rendimiento de los usuarios, razón por la cual se deben considerar mediante una auditoría especializada. Su definición es la siguiente:

Es la revisión técnica, específica y especializada que se realiza para evaluar lacalidad,

eficiencia y utilidad del entorno hombre-máquina-medio ambiente querodea el uso de sistemas computacionales en una empresa. *Esta revisión se rea- liza también con el propósito de evaluar la correcta adquisición y uso del mobiliario, equipo y sistemas*, a fin de proporcionar el bienestar, confort y comodidad que requieren los usuarios *de los sistemas de cómputo de la empresa, así como* evaluar la detección de los posibles problemas y sus repercusiones, y la determinación de las soluciones relacionadas con la salud física y bienestar delos usuarios de los sistemas *de la empresa.*

Las definiciones anteriores fueron presentadas de manera general, con el único propósito de identificar los tipos de auditorías de sistemas que serán tratados a lo largo de este libro. Más adelante se dará la profundidad que demanda cada una de estas auditorías.

1.5. Objetivos generales de la auditoría

A continuación, como complemento de los conceptos generales, se señalarán de manera muy general los objetivos que se pretende alcanzar con una auditoría, con la única intención de que el lector empiece a comprender las bases sobre las que descansa el desarrollo de una auditoría, cualquiera que ésta sea. Entre esos objetivos encontramos los siguientes:

- *Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.*

- *Hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa.*

- *Evaluar el cumplimiento de los planes, programas, políticas, normas y lineamientos que regulan la actuación de los empleados y funcionarios de una institución, así como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.*

- *Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.*

Cabe aclarar que los objetivos antes enunciados son de carácter general; sin embargo, pueden adecuarse al tipo de auditoría que se pretenda realizar, siendo indispensable que antes de iniciar la evaluación de algún área primero se establezcan de manera precisa los objetivos que se pretende cubrir con esa auditoría, a fin de contar con su existencia, difusión y cumplimiento.

Debido a la importancia que tiene el objetivo en cada tipo de auditoría, en el siguiente capítulo se hace un enunciado específico de los principales objetivos de lapropuesta de clasificación de auditoría.

1.6. Marco esquemático de la auditoría de sistemas computacionales

Evaluación a:

Hardware

Plataforma de hardwareTarjeta madre Procesadores
Dispositivos periféricos Arquitectura del sistema

Instalaciones eléctricas, de datos y de telecomunicaciones
Innovaciones tecnológicas de hardware y periféricos

Software

Plataforma del softwareSistema operativo

Lenguajes y programas de desarrollo

Programas, paqueterías de aplicación y bases de datos
Utilerías, bibliotecas y aplicaciones

Software de telecomunicación Juegos y otros tipos de software

Gestión informática

Actividad administrativa del área de sistemasOperación del sistema de cómputo Planeación y control de actividades

Presupuestos y gastos de los recursos informáticosGestión de la actividad informática

Capacitación y desarrollo del personal informático

Administración de estándares de operación, programación y desarrolloInformación

Administración, seguridad y control de la información

Salvaguarda, protección y custodia de la información
Cumplimiento de las características de la información

Diseño de sistemas

Metodologías de desarrollo de sistemas Estándares de programación y desarrolloDocumentación de sistemas

Bases de datos

Administración de bases de datosDiseño de bases de datos

Metodologías para el diseño y programación de bases de

datosSeguridad, salvaguarda y protección de las bases de datos

Seguridad

Seguridad del área de sistemasSeguridad física

Seguridad lógica

Seguridad de las instalaciones eléctricas, de datos y de telecomunicaciones

Seguridad de la información, redes y bases de datos Administración y control de las bases de datos Seguridad del personal informático

Redes de cómputo

Plataformas y configuración de las redesProtocolos de comunicaciones

Sistemas operativos y software Administración de las redes de cómputo Administración de la seguridad de las redes

Administración de las bases de datos de las redes

Especializadas

Outsourcing

Helpdesk

Ergonomía en sistemas computacionalesISO-9000

Internet/intranet Sistemas multimedia

SEGUNDA PARTE : AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Capítulo 2

CONTROL INTERNO Y AUDITORÍA DE SISTEMAS DE INFORMACIÓN

2.1 INTRODUCCIÓN

La información que es tratada en una organización es un recurso critico que debería ser protegido, ya que la misma es la base de la mayoría de las decisiones que son adoptadas a lo largo del tiempo.

Para tener una seguridad razonable sobre si la información es exacta y completa. estar disponible cuando se necesita y ser confidencial, la implementación de controles internos informáticos es necesario y además ayudan a cumplir con las exigencias legales en materias de Derecho Informático y a asegurar que los sistemas automáticos de procesamiento de la información funcionan de acuerdo con lo que se espera de ellos.

Los escándalos contables de principios de la década han provocado un aumento en la sensibilización, tanto de los reguladores como de las organizaciones (públicas y privadas)

por el control interno. La existencia de una nueva normativa al respecto (por ejemplo, la Sarbannes Oxley Act, el informe COSO...), las necesidades de transparencia en la gestión como un activo más de las organizaciones o la búsqueda de la eficiencia en los procesos internos han actuado durante los últimos años como catalizadores para la mejora de los mecanismos de control interno en las organizaciones.

Entramos así en una fase de madurez de las organizaciones, en las que la mejora de la eficiencia y el control de sus actividades comienzan a ser una de las necesidades básicas.

Dentro de las diferentes actividades que componen la estrategia de control interno de las organizaciones, el control sobre la gestión de los sistemas de información día a día adquiere una mayor relevancia. Para ello podemos encontrar, de manera inmediata, algunas razones:

- La creciente dependencia de las organizaciones y sus procesos (tanto internos como externos) respecto a sus sistemas de información.

- Derivado de lo anterior, el aumento de la complejidad de los mismos, con entornos heterogéneos y abiertos, a la vez que integrados.
- El éxito de las estrategias de externalización de la gestión de los sistemas de información, con los que la dependencia de los sistemas de información se refuerza con la dependencia de uno o varios proveedores de servicio.
- La globalización.
- La gestión de la calidad total (TQM- Total Quality Management).

Prueba de la mayor importancia que el control sobre la gestión de los sistemas de información gana día a día es el hecho de que, por ejemplo, la normativa europea de autorización de organismos pagadores define, como uno de sus cuatro grandes criterios de autorización, el del fomento del uso de los sistemas de información como soporte a todos sus procesos y el del establecimiento de un Sistema Integrado de Gestión de la Seguridad (SGSI), que no es más que el reflejo del aumento del nivel de control sobre los Sistemas de Información.

Así mismo se incorpora a las Organizaciones la función de auditoria informática inicialmente como apoyo a la auditoria financiera y posteriormente, surgen nuevas funciones en cuyos principales impulsores, podemos encontrar:

- Los reguladores, que empezaron a generar normativa específica aplicable sobre los sistemas de información de las organizaciones y sus procesos de gestión. Los ejemplos más conocidos son la Ley Orgánica de Protección de Datos (LOPD en adelante en este documento), pendiente de desarrollo, estando subsistente el Reglamento de Medidas de Seguridad recogido en el Real Decreto 994/1999, que desarrollaba la anterior Ley de Protección de Datos conocida como LORTAD, o la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI), que ha sido

elaborada por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología, en cumplimiento de lo dispuesto en el artículo 33 de la citada Ley.

- Los sistemas de comercio electrónico, tanto entre organizaciones (B2B), como orientada a clientes finales (B2C), que han impulsado la mejora de los procesos de comercialización de productos pero a la vez han abierto la puerta a nuevos riesgos derivados de la necesidad de "abrir" los sistemas de información de las organizaciones a terceros.
- El aumento de la complejidad de los sistemas de información y la dependencia de las organizaciones respecto a los mismos.

2.2 LAS FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICOS

2.2.1 Control Interno Informático

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

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

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

Como principales objetivos podemos indicar los siguientes:

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

Realizar en los diferentes sistemas (centrales, departamentales, redes locales, PC, etc.) y entornos informáticos (producción, desarrollo o pruebas) el control de las diferentes

actividades operativas sobre:

- El cumplimiento de procedimientos, normas y controles dictados. Merece resaltarse la vigilancia sobre el control de cambios y versiones del software.
- Controles sobre la producción diaria.
- Controles sobre la calidad y eficiencia del desarrollo y mantenimiento del software y del servicio informático.
- Controles en las redes de comunicaciones.
- Controles sobre el software de base.
- Controles en los sistemas microinformáticos.
- La seguridad informática (su responsabilidad puede estar asignada a control interno o bien puede asignársele la responsabilidad de control dual de la misma cuando está encargada a otro órgano):
- Usuarios, responsables y perfiles de uso de archivos y bases de datos.
- Normas de seguridad.
- Control de información clasificada.
- Control dual de la seguridad informática.
- Licencias y relaciones contractuales con terceros.
- Asesorar y transmitir cultura sobre el riesgo informático.

2.2.2 Auditoria informática

La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias parar determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoria informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoria:

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

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

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

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

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informativas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informativos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

2.2.3 Control Interno y auditoría informáticos: campos análogos

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

Aunque ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar (véase figura 2.1).

	CONTROL INTERNO INFORMÁTICO	AUDITOR INFORMÁTICO
SIMILITUDES	Personal interno. Conocimientos especializados en Tecnología de la Información. Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.	
DIFERENCIAS	Análisis de los controles en el día a día. Informa a la Dirección del Departamento de informática. Sólo personal interno. El alcance de sus funciones es únicamente sobre el Departamento de Informática.	Análisis de un momento informático determinado. Informa a la Dirección General de la Organización. Personal interno y/o externo. Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

Figura 2.1 Similitudes y diferencias entre control interno y auditoría informáticos

2.3 SISTEMA DE CONTROL INTERNO INFORMÁTICO

2.3.1 Definición y tipos de controles internos

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

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

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

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

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

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

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

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

informáticos.

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

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

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

2.3.2 Implantación de un sistema de controles internos informáticos

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- Entorno de red: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entomos de base que soportan aplicaciones criticas y consideraciones relativas a la seguridad de la red.
- Configuración del ordenador base: configuración del soporte fisico, entorno del sistema operativo, software con particiones, entomos (pruebas y real), bibliotecas de programas y conjunto de datos.
- Entorno de aplicaciones: procesos de transacciones, sistemas de gestión de bases de datos y entornos de procesos distribuidos.

- Productos y herramientas: software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

- Seguridad del ordenador base: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

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

- **Gestión de sistemas de información:** políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.
- **Administración** de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.
- **Seguridad:** incluye las tres clases de controles fundamentales implantados en el software del sistema: integridad del sistema, confidencialidad (control de acceso) y disponibilidad.
- **Gestión del cambio:** separación de las pruebas y la producción a nivel de software y controles de procedimientos para la migración de programas software aprobados y probados.

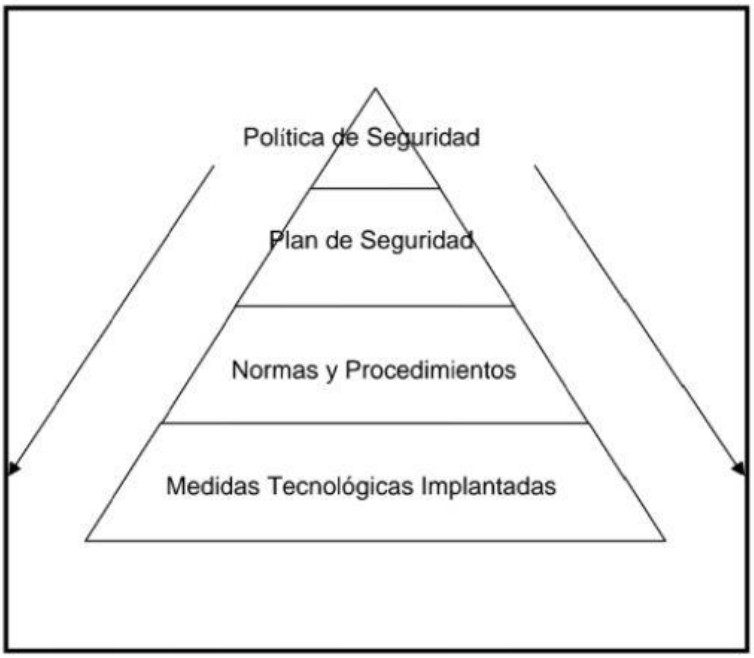

Figura 2.2. Implantación de política y cultura sobre seguridad.

La implantación de una política y cultura sobre la seguridad requiere que sea realizada por fases (véase en la figura 1.2) y esté respaldada por la Dirección. Cada función juega un papel importante en las distintas etapas:

- **Dirección de Negocio o Dirección de Sistemas de Información (SI):** han de definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.

- **Dirección de Informática:** ha de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de Informática mediante la creación y publicación de procedimientos, estándares, metodología y normas, aplicables a todas las áreas de Informática así como a los usuarios, que establezcan el marco de funcionamiento.
- **Control Interno Informático:** ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y diseñarlos conforme a los objetivos de negocio y dentro del marco legal aplicable. Éstos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles establecidos de Control Interno Informático informando de las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios crea convenientes en los controles, así como transmitirá constantemente a toda la organización de Informática la cultura y políticas del riesgo informático. (Véase figura 1.3).

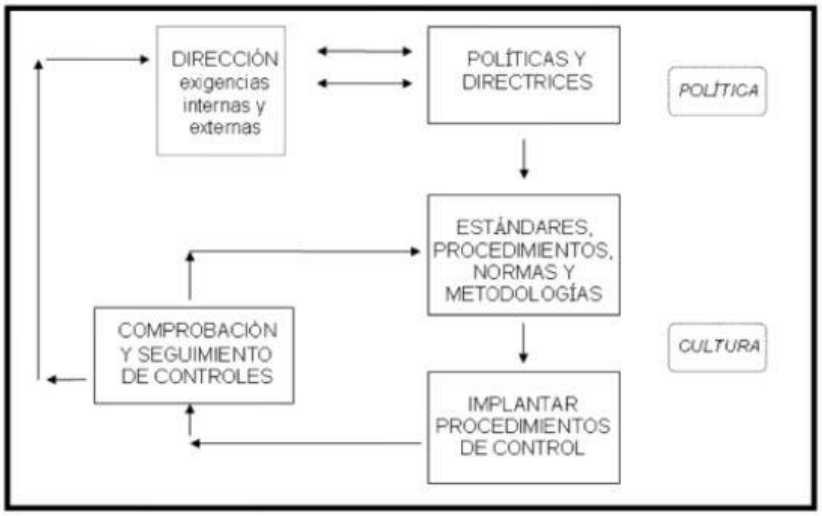

Figura 2.3. Funcionamiento del control interno informático

- Auditor interno/externo informático: ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo con el nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

A continuación, se indican algunos controles internos (no todos lo que deberían definirse) para sistemas de información, agrupados por secciones funcionales, y que

serían los que Control Interno Informático y Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

a. Controles generales organizativos

- Políticas: deberán servir de base para la planificación, control y evaluación por la Dirección de las actividades del Departamento de Informática.
- Planificación:
  - Plan Estratégico de Información, realizado por los órganos de la Alta Dirección de la Empresa donde se definen los procesos corporativos y se considera el uso de las diversas tecnologías de información así como las amenazas y oportunidades de su uso o de su ausencia.
  - Plan Informático, realizado por el Departamento de Informática, determina los caminos precisos para cubrir las necesidades de la Empresa plasmándolas en proyectos informáticos.
  - Plan General de Seguridad (fisica y lógica), que garantice la confidencialidad, integridad y disponibilidad de la información.
  - Plan de emergencia ante desastres, que garantice la disponibilidad de los sistemas ante eventos.
- Estándares: que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas.
- Procedimientos: que describan la forma y las responsabilidades de ejecutoria para regular las relaciones entre el Departamento de Informática y los departamentos usuarios.
- Organizar el Departamento de Informática en un nivel suficientemente superior de estructura organizativa como para asegurar su independencia de los departamentos usuarios.
- Descripción de las funciones y responsabilidades dentro del Departamento con una clara separación de las mismas.
- Políticas de personal: selección, plan de formación, plan de vacaciones y evaluación y promoción.
- Asegurar que la Dirección revisa todos los informes de control y resuelve las excepciones que ocurran.
- Asegurar que existe una política de clasificación de la información para saber dentro de la Organización qué personas están autorizadas y a qué información.
- Designar oficialmente la figura de Control Interno Informático y de Auditoría Informática (estas dos figuras se nombrarán internamente en base al tamaño del Departamento de Informática).

b. Controles de desarrollo, adquisición y mantenimiento de sistemas de información

Para que permitan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones:

- Metodología del ciclo de vida del desarrollo de sistemas: su empleo podrá garantizar a la alta Dirección que se alcanzarán los objetivos definidos para el sistema. Éstos son algunos controles que deben existir en la metodología:
    - La alta Dirección debe publicar una normativa sobre el uso de metodología de ciclo de vida del desarrollo de sistemas y revisar ésta periódicamente.
    - La metodología debe establecer los papeles y responsabilidades de las distintas áreas del Departamento de Informática y de los usuarios, así como la composición y responsabilidades del equipo del proyecto.
    - Las especificaciones del nuevo sistema deben ser definidas por los usuarios y quedar escritas y aprobadas antes de que comience el proceso de desarrollo.
    - Debe establecerse un estudio tecnológico de viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis coste-beneficio -de cada alternativa-.
    - Cuando se seleccione una alternativa debe realizarse el plan director del proyecto. En dicho plan deberá existir una metodología de control de costes.
    - Procedimientos para la definición y documentación de especificaciones de: diseño, de entrada, de salida, de ficheros, de procesos, de programas, de controles de seguridad, de pistas de auditoría, etc.
    - Plan de validación, verificación y pruebas.
    - Estándares de prueba de programas, de prueba de sistemas.
    - Plan de conversión; prueba de aceptación final.
    - Los procedimientos de adquisición de software deberán seguir las políticas de adquisición de la Organización y dichos productos deberán ser probados y revisados antes de pagar por ellos y ponerlos en uso.
    - La contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto.
    - Deberán prepararse manuales de operación y mantenimiento como parte de todo proyecto de desarrollo o modificación de sistemas de información, así como manuales de usuario.
- Explotación y mantenimiento: el establecimiento de controles asegurará que los datos se tratan de forma congruente y exacta y que el contenido de sistemas sólo será modificado mediante autorización adecuada. Éstos son algunos de los controles que se deben implantar:
    - Procedimientos de control de explotación.

- Sistema de contabilidad para asignar a usuarios los costes asociados con la explotación de un sistema de información.
- Procedimientos para realizar un seguimiento y control de los cambios de un sistema de información.

c. Controles de explotación de sistemas de información

- Planificación y Gestión de recursos: definir el presupuesto operativo del Departamento, Plan de adquisición de equipos y gestión de la capacidad de los equipos.
- Controles para usar, de manera efectiva, los recursos en ordenadores:
  - Calendario de carga de trabajo. o Programación de personal.
  - Mantenimiento preventivo del material.
  - Gestión de problemas y cambios.
  - Procedimientos de facturación a usuarios.
  - Sistema de gestión de la biblioteca de soportes.
- Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y control de cambios.
- Seguridad física y lógica:
  - Definir un grupo de seguridad de la información, siendo una de sus funciones la administración y gestión del software de seguridad, revisar periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes.
  - Controles físicos para asegurar que el acceso a las instalaciones del Departamento de Informática queda restringido a las personas autorizadas.
  - Las personas externas a la Organización deberán ser acompañadas por un miembro de la plantilla cuando tengan que entrar en las instalaciones.
  - Instalación de medidas de protección contra el fuego.
  - Formación y concienciación en procedimientos de seguridad y evacuación de edilicio.
  - Control de acceso restringido a los ordenadores mediante la asignación de un identificador de usuario con palabra clave personal e intransferible.
  - Normas que regulen el acceso a los recursos informáticos.
  - Existencia de un plan de contingencias para el respaldo de recursos de ordenador críticos y para la recuperación de los servicios del Departamento Informático después de una interrupción imprevista de los mismos.

d. Controles en aplicaciones

Cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, validez y mantenimiento completos y exactos de los datos. Las cuestiones

más importantes en el control de los datos son:

- Control de entrada de datos: procedimientos de conversión y de entrada, validación y corrección de datos.
- Controles de tratamientos de datos para asegurar que no se dan de alta, modifican o borran datos no autorizados para garantizar la integridad de los mismos mediante procesos no autorizados.
- Controles de salidas de datos: sobre el cuadre y reconciliación de salidas, procedimientos de distribución de salidas, de gestión de errores en las salidas, etc.

e. Controles específicos de ciertas tecnologías

- Controles en Sistemas de Gestión de Bases de Datos:
    - El software de gestión de bases de datos para prever el acceso a, la estructuración de y el control sobre los datos compartidos deberá instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno.
    - Que están definidas las responsabilidades sobre la planificación, organización, dotación y control de los activos de datos, es decir, un administrador de datos.
    - Que existen procedimientos para la descripción y los cambios de datos así como para el mantenimiento del diccionario de datos.
    - Controles sobre el acceso a datos y de concurrencia.
    - Controles para minimizar fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación.
    - Controles para asegurar la integridad de los datos: programas de utilidad para comprobar los enlaces físicos —punteros-asociados a los datos, registros de control para mantener los balances transitorios de transacciones para su posterior cuadre con totales generados por el usuario o por otros sistemas.
- Controles en informática distribuida y redes:
    - Planes adecuados de implantación, conversión y pruebas de aceptación para la red.
    - Existencia de un grupo de control de red.
    - Controles para asegurar la compatibilidad del conjunto de datos entre aplicaciones cuando la red es distribuida.
    - Procedimientos que definan las medidas y controles de seguridad a ser usados en la red de informática en conexión con la distribución del contenido de bases de datos entre los departamentos que usan la red.

- Que se identifican todos los conjuntos de datos sensibles de la red y que se han determinado las especificaciones para su seguridad.
- Existencia de inventario de todos los activos de la red.
- Procedimientos de respaldo del hardware y del software de la red.
- Existencia de mantenimiento preventivo de todos los activos.
- Que existen controles que verifican que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.
- Controles de seguridad lógica: control de acceso a la red, establecimiento de perfiles de usuario.
- Procedimientos de cifrado de información sensible que se transmite a través de la red.
- Procedimientos automáticos para resolver cierres del sistema.
- Monitorización para medir la eficiencia de la red.
- Diseñar el trazado físico y las medidas de seguridad de las líneas de comunicación local dentro de la organización.
- Detectar la correcta o mala recepción de mensajes.
- Identificar los mensajes por una clave individual de usuario, por terminal y por el número de secuencia del mensaje.
- Revisar los contratos de mantenimiento y el tiempo medio del servicio acordados con el proveedor con objeto de obtener una cifra de control constante.
- Determinar si el equipo multiplexor/concentrador/procesador frontal remoto tiene lógica redundante y poder de respaldo con realimentación automática para el caso de que falle.
- Asegurarse de que haya procedimientos de recuperación y reinicio.
- Asegurarse de que existan pistas de auditoria que puedan usarse en la reconstrucción de los archivos de datos y de las transacciones de los diversos terminales. Debe existir la capacidad de rastrear los datos entre la terminal y el usuario.
- Considerar circuitos de conmutación que usen rutas alternativas para diferentes paquetes de información provenientes del mismo mensaje; esto ofrece una forma de seguridad en caso de que alguien intercepte los mensajes.

- Controles sobre ordenadores personales y redes de área local:
  - Políticas de adquisición y utilización.
  - Normativas y procedimientos de desarrollo y adquisición de software de aplicaciones.
  - Procedimientos de control del software contratado bajo licencia.

- Controles de acceso a redes, mediante palabra clave, a través de ordenadores personales.
- Revisiones periódicas del uso de los ordenadores personales.
- Políticas que contemplen la selección, adquisición e instalación de redes de área local.
- Procedimientos de seguridad física y lógica.
- Departamento que realice la gestión y soporte técnico de la red. Controles para evitar modificar la configuración de una red. Recoger información detallada sobre los minis existentes: arquitectura (CPU, Discos, Memoria, Streamers, Terminales, etc.), conectividad (LAN, mini to host, etc.), software (sistema operativo, utilidades, lenguajes, aplicaciones, etc.), servicios soportados.
- Inventario actualizado de todas las aplicaciones de la Entidad.
- Política referente a la organización y utilización de los discos duros de los equipos, así como para la nomenclatura de los archivos que contienen, y verificar que contiene al menos: obligatoriedad de etiquetar el disco duro con el número de serie del equipo, creación de un subdirectorio por el usuario en el que se almacenarán todos sus archivos privados, así como creación de un subdirectorio público que contendrá todas las aplicaciones de uso común para los distintos usuarios.
- Implantar herramientas de gestión de la red con el fin de valorar su rendimiento, planificación y control.
- Procedimientos de control de los file-transfer que se realizan y de controles de acceso para los equipos con posibilidades de comunicación. Políticas que obliguen a la desconexión de los equipos de las líneas de comunicación cuando no se está haciendo uso de ellas.
- Adoptar los procedimientos de control y gestión adecuados para la integridad, privacidad, confidencialidad y seguridad de la información contenida en redes de área local.
- Cuando exista conexión PC-Host, comprobar que opera bajo los controles necesarios para evitar la carga/extracción de datos de forma no autorizada.
- Contratos de mantenimiento (tanto preventivo como correctivo o detectivo).
- Cuando en las acciones de mantenimiento se requiera la acción de terceros o la salida de los equipos de los límites de la oficina, se deberán establecer procedimientos para evitar la divulgación de información confidencial o sensible.

- Mantener un registro documental de las acciones de mantenimiento realizadas, incluyendo la descripción del problema y la solución dada al mismo.
- Los ordenadores deberán estar conectados a equipos de continuidad (UPS, grupo, etc.).
- Protección contra incendios, inundaciones o electricidad estática. Control de acceso físico a los recursos microinformáticos: Llaves de PC. Áreas restringidas. Ubicación de impresoras (propias y de red). Prevención de robos de dispositivos. Autorización para desplazamientos de equipos. Acceso físico fuera de horario normal.
- Control de acceso físico a los datos y aplicaciones: almacenamiento de disquetes con copias de backup u otra información o aplicación, procedimientos de destrucción de datos e informes confidenciales, identificación de disquetes/cintas, inventario completo de disquetes almacenados, almacenamiento de documentación.
- En los computadores en que se procesen aplicaciones o datos sensibles instalar protectores de oscilación de línea eléctrica y sistemas de alimentación ininterrumpida.
- Implantar en la red local productos de seguridad así como herramientas y utilidades de seguridad.
- Adecuada identificación de usuarios en cuanto a las siguientes operaciones: altas, bajas y modificaciones, cambios de password, explotación del log del sistema.
- Controlar las conexiones remotas in/out (CAL): Módems, Gateway, Mapper.
- Procedimientos para la instalación o modificación de software y establecer que la dirección es consciente del riesgo de virus informáticos y otros software maliciosos, así como de fraude por modificaciones no autorizadas de software y daños.
- Controles para evitar la introducción de un sistema operativo a través de disquete que pudiera vulnerar el sistema de seguridad establecido.

f. Controles de Calidad

- Existencia de un Plan General de Calidad basado en el Plan de la Entidad a Largo Plazo y el Plan a Largo Plazo de Tecnología. Este Plan General de Calidad debe promover la filosofía de mejora continua y debe dar respuestas a preguntas básicas de "qué", "quién" y "cómo".
- Esquema de Garantía de Calidad: la Dirección de Informática debe establecer una norma que establezca un Esquema de Garantía de

Calidad que se refiera tanto a las actividades de desarrollo de proyectos, como a las demás actividades de Informática. Las normas deben establecer los tipos de actividades para garantizar calidad (como revisiones, auditorías, inspecciones, etc.) que deben ser realizadas para lograr los objetivos del Plan General de Calidad.

- Compatibilidad de la revisión de Garantía de Calidad con las Normas y Procedimientos habituales en las distintas funciones de Informática.
- Metodología de Desarrollo de Sistemas: la Dirección de Informática de la Entidad debe definir e implementar Normas para desarrollos de Sistemas y adoptar una Metodología de Desarrollo de Sistemas para administrar y gestionar dicho proceso en base al tipo de sistemas de cada Entidad.
- Actualización de la Metodología de Desarrollo de Sistemas respecto a Cambios en la Tecnología.
- Coordinación y Comunicación: la Dirección de Informática debe establecer un procedimiento para asegurar estrecha coordinación y comunicación con los Usuarios de la Entidad e Informática. Este proceso debe hacerse mediante métodos estructurados, utilizando la Metodología de Desarrollo de Sistemas para asegurar la obtención de soluciones de Informática de calidad que cumplan con las necesidades de la Entidad.
- Relaciones con Proveedores que Desarrollan Sistemas: existencia de un proceso que asegure buenas relaciones laborales con proveedores que desarrollan sistemas para la Entidad. Este proceso debe hacer que el usuario y el Proveedor del sistema acuerden criterios de aceptación y administración de cambios, problemas durante el desarrollo, funciones del usuario, herramientas, software, normas y procedimientos.
- Normas de Documentación de Programas: existencia de Normas de Documentación de Programas las cuales deben ser comunicadas e impuestas al personal pertinente. La metodología debe asegurar que la documentación creada durante el desarrollo del sistema o proyecto respete estas Normas.
- Normas de Pruebas de Programas: la Metodología de Desarrollo de Sistemas de la Entidad debe incorporar Normas que se refieran a los Requisitos de las Pruebas de Programas, Comprobación, Documentación y Retención del material, para probar cada una de las unidades del software a ser puesto en producción.
- Normas respecto a la Prueba de Sistemas: la Metodología de Desarrollo de Sistemas de la Entidad debe incorporar Normas que se refieran a los Requisitos de las Pruebas de Sistemas, Comprobación, Documentación y Retención del material, para probar de manera global el funcionamiento de cada sistema a ser puesto en producción.

- Pruebas Piloto o en Paralelo: la Metodología de Desarrollo de Sistemas de la Entidad debe definir las circunstancias bajo las cuales se efectuarán Pruebas Piloto o en Paralelo de programas o sistemas.
- Documentación de las Pruebas de Sistemas: la Metodología de Desarrollo de Sistemas de la Entidad debe establecer, como parte de cada desarrollo, implementación o modificación, que se documenten los resultados de las Pruebas de Sistemas.
- Evaluación del cumplimiento de Garantía de Calidad de las Normas de Desarrollo

2.4 CONCLUSIONES

Vivimos en un mundo completamente globalizado y dinámico. Los avances tecnológicos se suceden, lo único permanente es el cambio y no podemos ignorarlo a pesar de los riesgos que conlleva. Pero debemos reconocer la existencia de riesgos que implica el uso de la tecnología, para poder, dentro de lo posible, neutralizarlos, minimizando su impacto sobre la organización.

Actualmente, toda organización moderna es, por definición, informático-dependiente. A poco que lo pensemos, la información es uno de los activos más valiosos de la organización. Esto lamentablemente se entiende cuando se vuelve inaccesible, porque se destruye o es robada e implica un serio traspié para la empresa.

El sistema de políticas y procedimientos organizacionales para custodia y salvaguarda de sus activos se ve influido y modificado por el proceso informático.

Por lo tanto, es necesaria la existencia de un control interno informático como herramienta de una adecuada gestión de los Sistemas de Información.

Muchos de los problemas informáticos se originan dentro de la misma empresa. Por ello es cada vez más necesario un completo análisis del tráfico de:

- Los correos electrónicos corporativos.
- Las páginas web que se visitan desde los ordenadores de la empresa.

El sistema de control interno informático será más eficiente en una organización inmersa en tecnología cuando se le dote de herramientas modernas de supervisión. Esto ayuda a que la organización logre adecuados niveles de excelencia en la custodia y aprovechamiento de su información.

La organización moderna aprovecha las potencialidades del proceso informático, pero ello implica una nueva realidad, es decir, nuevos riesgos:

- Todos los procesos críticos de negocio se encuentran automatizados.
- La tecnología cliente servidor, el uso de Bases de Datos, el uso de Internet y de las intranets corporativas llevan a que la información almacenada esté distribuida geográficamente (descentralizada).

- Posibilidades para modificar información mediante accesos no controlados en los sistemas.
- A consecuencia de lo anterior, necesidad de implementar en los sistemas controles informáticos.

En el momento en el que las organizaciones adquieren conciencia sobre la necesidad de aumentar el nivel de control sobre la gestión de sus sistemas de información, surge la siguiente pregunta: ¿pero qué es realmente la auditoria informática y cómo puede ayudarme? Es natural esta duda desde la perspectiva de que, tradicionalmente, los departamentos de control interno o auditoría interna están compuestos por perfiles muy cercanos al negocio, principalmente financiero y, en algunos casos, operativo.

En el momento en el que el auditor informático comienza a plantearse objetivos de control sobre quién debe acceder a qué información, qué puede hacer con ella, o a cuestionarse la integridad de la misma, comienza a necesitar y a obtener un conocimiento profundo sobre los procesos de negocio de la compañía.

Por otra parte, la integración de dichos procesos en aplicaciones informáticas provoca que gran parte de los controles que se aplican sobre los mismos se definan en dichas aplicaciones. A partir de este instante, la labor del auditor informático comienza a confluir con la del auditor financiero, adquiriendo una doble versión de especialista en la definición de procesos de control interno en los procesos de negocio y en su aplicación o análisis sobre los sistemas de información que los soportan.

En definitiva, el papel actual del auditor informático dentro de las organizaciones lo podemos resumir en dos grandes tareas principales:

- Apoyo al auditor interno, en la definición y aplicación de controles internos sobre los procesos de Negocio, Estratégicos y de Soporte de la Organización, en tanto que gran parte de los mismos se aplican desde sus sistemas de información.
- Auditoria de la gestión de los sistemas de información, que se plantea básicamente dos objetivos:
    - Que los sistemas de información soportan adecuada y eficientemente los procesos de negocio de las organizaciones.
    - Que la información tratada por los sistemas de información dispone de un nivel de seguridad adecuado a su valor y a los riesgos asociados a su uso.

2.5 LECTURAS RECOMENDADAS

EDP Auditing. Auerbach Publications.

Fitzgerald, Jerry. Controles internos para sistemas de computación. Ed. Limusa Wiley.

Martin, James. Security, Accuracy and Privacy in Computer System. Ed. Prentice

Hall.

Instituto Auditores Internos de España. Control interno, auditoria y seguridad informática.

2.6. BIBLIOGRAFIA

Miguel Ángel Davara Rodríguez, Rosa María García Ontoso, Juan Manuel Fernández López, Emilio del Peso Navarro. Actualidad Informática Aranzadi. N° 34- Enero 2000.

Ramos Suárez Fernando. Nuevo reglamento de Seguridad para la Protección de Ficheros Automatizados con datos de Carácter Personal: ¿Obstáculo o ayuda al desarrollo de la empresa? Derecho .org.

Sánchez Blanco, Ángel. Internet, Sociedad, empresa y Poderes Públicos. Edit. Comarca. 2000.

SEDISI, Guía de la Seguridad Informática. (Asociación Española de Empresas de Tecnologías de la Información). Abril 1997.

Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports. SEC. Agosto 2003.

PCAOB Release, An Audit of Infernal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. N°. 2004-001, marzo 2004.

2.7 CUESTIONES DE REPASO

1. ¿Qué cambios en las empresas provocan tensión en el control interno existente?
2. ¿Cuáles son las funciones del control interno informático?
3. ¿Cuáles son los objetivos de la Auditoria Informática?
4. ¿Cuáles son las semejanzas y diferencias entre Control Interno y Auditoria Informática?
5. Ponga ejemplos de controles correctivos en diversas áreas informáticas.
6. ¿Cuáles son los principales controles en el área de desarrollo?
7. ¿Qué procesos definiría para controlar la informática distribuida y las redes?
8. ¿Qué controles se deberían establecer en las aplicaciones?
9. ¿Cómo justificaría ante un directivo de empresa la inversión necesaria en control y auditoría informática?
10. Describa la informática como modo de estructuración de las empresas.

Capítulo 3

AUDITORÍA DE SI vs. NORMAS DE BUENAS PRÁCTICAS

3.1 INTRODUCCIÓN

Desde hace varios años la sociedad está asistiendo a un raudal de publicaciones de normas' y "buenas prácticas" sobre la gestión y la seguridad de las Tecnologías de la Información y las Comunicaciones (TI, en adelante), algunas totalmente nuevas, otras con actualizaciones periódicas y otras simplemente "remozadas".

En muchos de estos casos, estas normas y buenas prácticas están relacionadas concretamente con el gobierno de TI, o bien con ciertos aspectos, procesos o actividades, concretos dentro del conjunto global, conglomerado y complejo que supone la totalidad de los elementos "tecnológicos" que soportan la actividad de una entidad'.

La implantación de una norma, en un entorno de TI, no es un obstáculo para que los auditores de Sistemas de Información (SI)3 puedan realizar su cometido principal: emitir un informe o dictamen independiente, basado en pruebas independientes, para la Dirección de una Entidad, sobre la confianza que puede depositar en su TI, como soporte de su "negocio" e identificando los riesgos que TI puede implicar para acometer los objetivos de la actividad de su entidad.

A continuación se analizan algunas de estas normas y buenas prácticas para TI desde la perspectiva de la auditoria de SI, ya que se pueden establecer sinergias desde la metodología de auditoria de SI y las normas, aunando cometidos comunes.

3.2 AUDITORÍA DE SI VERSUS COBIT

3.2.1 La auditoría de SI

La famosa y limitada consideración de "caja negra" en relación a la tecnología siempre ha suscitado inquietudes en los responsables de las entidades, públicas o privadas, con respecto a la "veracidad" de la información que almacenaba y procesaba "el ordenador".

Es a finales de la década de 1960 cuando comienzan a aparecer publicaciones con las primeras normas o guías para la auditoria de lo que hoy llamamos Sistemas de Información. Estas publicaciones fueron realizadas por: entidades de auditores, asociaciones profesionales, especialmente de auditores, de proveedores de equipos y software.

A modo de ejemplo, entre muchos otros, la publicación por IBM, de su A Management System for the Information Business en 1981 (GE20-0662- I a 4), que abarcaba en sus cuatro volúmenes los siguientes temas, tan de actualidad hoy:

- Visión general de la Dirección / Gerencia (Management Overview, en inglés).
- Misión de los servicios de los sistemas de información (The Information Systems Service Mission, en inglés).
- Misión del Desarrollo de sistemas de información (The Information Systems Development Misión, en inglés).
- Dirección y Gestión de los recursos de sistemas de información (Managing Information Systems Resouces, en inglés).

En la década del 1970 (concretamente se funda en 1967) se consolida la que hoy se llama Information Systems Audit and Control Association (ISACA), siendo aún hoy la única entidad, a nivel mundial, de los auditores de SI, y que gestiona una certificación en esta materia: Certified Information Systems Auditor (CISA). Esta asociación, que está presente en más de 140 países, a través de más de 170 capítulos (Chapters, en inglés) en todo el mundo, establece normas y procedimientos para la función de la auditoría de SI y los profesionales que las realizan.

Las preocupaciones fundamentales con respecto a la tecnología aludidas anteriormente siguen siendo las mismas o se han incrementado con la evolución tecnológica. Estas inquietudes tanto de la Dirección de una entidad, como de sus accionistas o de la sociedad en general, se pueden concretar en:

- La veracidad de la información en cuanto a su totalidad y exactitud, procesada por los sistemas de tecnología.
- La utilización racional y ajustada a las necesidades reales de los recursos tecnológicos.
- El "mantenimiento" o "sostenibilidad" de la estructura tecnológica y su crecimiento no debe ser traumático en el soporte de nuevas actividades.
- La confidencialidad de la información.
- La protección de sus activos, especialmente el software y la información.

Por lo tanto, aquellas necesidades de tener una opinión independiente sobre estos temas, aludidos de forma genérica, no sólo se ha consolidado, sino que aumenta en la medida que aumentan las amenazas y vulnerabilidades para la información y la sustentación de los procesos de negocio, con los avances tecnológicos.

La "caja negra es cada vez más compleja, dispersa, y si se quiere opaca: Internet, Comunicaciones vía satélite, PALMS, todo tipo de soportes informáticos, aplicaciones complejas que modifican los procesos operativos, como los ERP, etc.

Esta necesidad de una auditoria de SI, independiente y objetiva, está impactando no sólo al ámbito "voluntario" del gobierno de TI, sino que también comienza a verse reflejada en la legislación, como por ejemplo: el requerimiento del Reglamento de Seguridad para ficheros de datos personales automatizados, de realizar una auditoria de

las medidas organizativas y técnicas cada dos años; y la famosa ley Sarbanes Oxley, etc.

Para centrar el tema con respecto al objetivo de este capitulo y de esta sección, de la "Auditoría de SI versus COBIT", es necesario situarse primero en la definición de qué es la auditoría de SI. Existen muchas definiciones, pero con dos, de las más difundidas, es suficiente':

- La Auditoria de TI es un proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo los fines de la organización y utiliza eficientemente los recursos.
- La Auditoria de TI es el mecanismo/proceso metodológico para valorar y evaluar la confianza que se puede depositar en TI.

Son varios los elementos de estas definiciones que merecen un análisis por el contenido critico que tienen con respecto a la función y "misión" de la auditoria de SI:

- La palabra "información" en los "apellidos" del auditor, ya sea Sistemas de Información o Tecnologías de la Información, indica claramente el fundamento principal: la fiabilidad de la información procesada, disponible y suministrada a través de procesos tecnológicos.
- La auditoria de SI sigue un proceso metodológico en sus revisiones y debe identificar la adecuación de los controles, su nivel de cumplimiento y, fundamentalmente, identificar los riesgos para el negocio. Es decir, la auditoria de SI no se limita a determinar que existe tal o cual control, sino que va más allá: si el control ha sido diseñado adecuadamente para el objetivo que se pretende, es eficiente (eficacia versus coste), si se cumple con eficacia en el tiempo y, sumariamente, si los riesgos de TI, relacionados con este control, están mitigados.

La auditoría de SI distingue entre dos grandes grupos los controles en un entorno de TI:

- Los controles sobre las infraestructuras de tecnologías.
- Los controles imbuidos en las propias aplicaciones o software para la gestión de la actividad del negocio.

Estas dos vertientes, aunque han evolucionado en el tiempo, están vigentes en su base conceptual desde hace más de 30 años: cualquier deficiencia en los controles de la infraestructura tendrá una gran posibilidad de afectar directa o indirectamente en los controles de las aplicaciones o sistemas del negocio, y por ende en la fiabilidad de la información procesada.

Tanto la revisión, como parte de las tareas de la auditoria de TI tanto de los controles de infraestructura como de los de aplicación, que son convergentes, requieren una visión global y metodológica del auditor de SI, sobre la organización y gestión de TI, como un todo.

Por esa razón, cuando el auditor de SI se encuentra en una entidad donde se ha implantado COBIT, encontrará que su labor de revisión se ve allanada, no ya solamente por la conciencia y compromiso de la Dirección en la implantación de este modelo y por ende con el control de TI, sino que el modelo COBIT tiene bastantes referencias a la auditoría de SI como factor esencial de una opinión independiente.

3.2.2 COBIT

COBIT (Control Objectives for Information and Related Technology) es un modelo/conjunto estructurado de buenas prácticas y metodologías para su aplicación, cuyo objetivo es facilitar el gobierno de TI.

El Information Technology Govemance Inslitute' publicó recientemente la edición 4.0 de COBIT. Esta nueva edición enfatiza el cumplimiento de normas y legislación, sin invalidar los conceptos fundamentales de las versiones anteriores. Esta edición 4.0, realizada como una actualización para reflejar el estado del arte en los temas del gobierno de la tecnología de la información (TI), incluye fundamentalmente mejoras y avances en esta actividad, al mismo tiempo que tiene en cuenta un criterio de practicidad y facilidad para su implementación.

COBIT apoya y sustenta el gobierno de TI, proporcionando un marco de referencia que asegure que:

- La tecnología de la información está alineada con el negocio, contribuyendo, al mismo tiempo, a la maximización de los beneficios.
- Los recursos de TI (humanos y técnicos) son utilizados de forma responsable.
- Los riesgos de TI son gestionados y dirigidos adecuadamente.

Es decir, que primero se tiene en cuenta la actividad de una entidad, sus objetivos, los riesgos y sus recursos y a partir de este conocimiento se pueden establecer los objetivos de control que se quieren alcanzar.

La gran ventaja es que COBIT entiende a la tecnología de la información como un TODO de servicio (entendiendo el servicio como un activo), y no de forma parcial.

Otra acertada característica de COBIT es su estructuración o esquema de presentación. Está estructurado con criterios prácticos en un orden lógico y racional de mayor nivel a menor nivel en la gestión y dirección de TI. Esta organización de las buenas prácticas permite una mayor comprensión del esquema, la graduación en su implantación, su revisión y actualización periódica sin tener que cambiar todo el esquema, a la vez que el enfoque de procesos permite una mayor adaptabilidad a los procesos de negocio y operativos de una organización. A su vez permite visualizar la interrelación entre los objetivos de control de alto nivel y de detalle, dentro de cada dominio o proceso, según su agrupación por actividades, y según los requerimientos para estos controles.

Esta perspectiva es adecuada, ya que los controles internos en TI, como en cualquier otro aspecto de los procesos de una entidad, deben relacionarse siempre entre sí, en cuanto a sus objetivos, eficiencia y complementariedad en la mitigación de riesgos,

evitando su consideración aislada. Cualquier consideración aislada de los controles distorsiona la utilidad y resultados de un proceso de análisis y evaluación de riesgos.

COBIT 4.0 estructura **en 34 objetivos de control de alto nivel para los procesos de TI, que están agrupados en 4 dominios de actividades típicas** del gobierno de TI (o que cualquier gobierno de TI debería incluir para ser realista y eficiente).

Los 4 dominios de actividades, son los siguientes:

- PLANIFICAR y ORGANIZAR (P0)7
- ADQUIRIR e IMPLEMENTAR (AI)8
- ENTREGAR y DAR SOPORTE (DS)9
- MONITORIZAR y EVALUAR (ME)10

Es decir, se empieza planificando y organizando TODAS las actividades de TI, y no un área en especial (Desarrollo, explotación, etc.) o un aspecto en concreto (la continuidad de los servicios, por ejemplo).

Por cada uno de los procesos, y por cada uno de los objetivos de control de alto nivel, COBIT 4.0 proporciona los objetivos de control de detalle o del nivel siguiente. En total son 215 objetivos de control de detalle.

Todos los objetivos de control, tanto los de alto nivel como los de detalle, están debidamente fundamentados y contienen en explicaciones de sus propósitos y alcances.

Pero la estructuración y mera descripción de los objetivos de control por dominios no es suficiente para implantar adecuadamente un gobierno de TI y asegurar que estas buenas prácticas logren el objetivo previsto.

Por esta razón, COBIT incluye además otros elementos a considerar que están relacionados con los requerimientos del negocio con respecto a los servicios y recursos de TI:

- **Requerimientos del Negocio con respecto a TI:** Efectividad o Eficacia; Eficiencia; Confidencialidad; integridad; Disponibilidad; Cumplimiento y Confiabilidad.
- **Recursos de TI afectados:** Aplicaciones; Información; Infraestructura y Personal.
- **Áreas Centrales para el Gobierno de TI:** Alineación Estratégica; Entrega y Servicio que añada valor; Gestión de los Recursos; Gestión del Riesgo y Medición del Rendimiento.
- **Objetivos de Control de Detalle:** enumeración de los Objetivos de Detalle con sus oportunas explicaciones sobre su propósito y alcance, por objetivo de alto nivel.
- **Directrices de Gestión:** guía sobre las interrelaciones con otros Dominios y Objetivos de Control de Alto Nivel, señalando tanto la relación de recepción (input) de otros objetivos de control e inclusive externos al esquema COBIT, como la entrega (output) hacia otros.

- **Responsabilidades por los distintos niveles de Dirección y Gerencia:** incluyen tanto la Alta Gerencia, como a unidades de negocio, hasta la Auditoria de TI.
- **Cuadro de objetivos y métricas aplicables:** objetivos y métricas aplicables para el objetivo de control de que se trate, y así mismo los indicadores para la respectiva medición
- **Modelo de Madurez:** criterios para considerar en cada nivel.

En su planteamiento COBIT tiene presente el tradicional esquema que diferencia entre los controles generales de TI (Desarrollo de Sistemas, Gestión de Cambios, Seguridad, Producción, entre otros) y los controles de las Aplicaciones de Negocio (Totalidad, Exactitud; Validez; Autorización y Segregación de Funciones, entre otros).

En cuanto a la evaluación del riesgo, COBIT no proporciona ninguna herramienta específica al respecto, y referencia de forma primordial al Enterprise Risk Management—Integrated Framework, 2004, del Committee of Sponsoring Organisations of the Treadway Commission (COSO). Pero sí considera que el riesgo de TI debe estar en consonancia, si existe, con el Modelo de Evaluación del Riesgo de Negocio.

Existen otras normas para TI con las que el modelo Cona 4.0 está relacionado, que son complementarios a este modelo. La (SACA y el ITGI han publicado y continúan publicando distintos documentos para facilitar la implantación práctica de esta complementariedad. Por ejemplo: con ITIL, ISO/IEC 27000, etc.

C0BiT 4.0 es una herramienta critica que abarca la gestión integral de TI, y que puede verse complementada con esas otras normas para profundizar en aquellos controles de este modelo, es decir, pasar del "debe hacerse", al "cómo se hace".

3.2.3. Convergencia de la Auditoría de SI y COBIT

En estos momentos, después de varios años de andadura del COBIT, ya no se le confunde con una metodología de auditoría de SI. Por lo tanto, el objetivo de esta sección es definir el marco de actuación de los auditores de SI en relación a este modelo.

Esta confusión se debía, quizás, a la estrecha relación de COBiT con la ISACA. Por lo tanto, tanto Cofia- como las normas, directrices y procedimientos que comparten el mismo lenguaje, y esta es, en ocasiones, una facilidad para los auditores de TI.

Con la versión 3 se editó una guía de auditoria para COBiT. Sin embargo esta guía no constituía una metodología de auditoria, ni normas ni directrices de auditoría. En principio, establecía un marco de actuación de los auditores de SI, basados en la metodología de auditoria de la ISACA.

"...los auditores como requerimiento general deben proporcionar una garantía (assurance) y recomendaciones en relación a los controles en una entidad:

- Proporcionar una garantía razonable de que se alcanzarán con los objetivos de control.
- Identificar si existen debilidades significativas en estos controles.
- Sustanciar el riesgo que puede estar asociado a estas debilidades.
- Recomendar o asesorar a la Gerencia sobre las acciones correctivas que deberían ser tomadas".

Esta referencia en COBIT 3 a la auditoria de SI indicaba concretamente los siguientes fundamentos de la función de la auditoria de TI, en consonancia con los de la ISACA:

- **Obtención de un conocimiento:** las tareas de auditoria que deben ser realizadas para conocer y documentar objetivos de negocio, riesgos respectivos y medidas de control relevantes, así como las actividades que dan fundamento a los objetivos de control así como las necesarias para identificar las medidas y procedimientos de control establecidos, y que se llevan a cabo.
- **Evaluación de la adecuación:** las tareas de auditoría que deben ser realizadas en la apreciación de la eficacia de los mecanismos de control que se llevan a cabo o del grado hasta el cual el objetivo de control es alcanzado. Es decir, básicamente, decidir qué, en qué oportunidad y cómo realizar las pruebas.
- **Evaluación del cumplimiento:** las tareas de auditoria que deben ser realizadas para asegurar que los mecanismos de control establecidos están funcionando tal como se estableció, consistentemente y de forma continuada, para poder emitir una conclusión sobre la adecuación del entorno de control.
- **Fundamentar el riesgo:** las tareas de auditoría que deben realizarse para fundamentar o "sustanciar" el riesgo de un objetivo de control que no se cumple, utilizando técnicas analíticas y/o consultando fuentes alternativas. El objetivo es soportar una opinión y provocar que la Dirección tome acciones. No obstante, esta guía sigue siendo muy válida ya que contiene una descripción amplia y detallada de cómo realizar la auditoria de los controles de alto nivel y de detalle, indicando tipo de pruebas, posibles riesgos en caso de deficiencias, etc."

En definitiva el auditor de SI debe actuar frente a una implantación de COBIT como en cualquier otra auditoria. No se limitará a contestar a un cuestionario de si existe o no determinado control:

- Analizará los riesgos dentro del alcance y objetivo de la auditoria en cuestión.
- Identificará el modelo y los controles que supuestamente mitigan los riesgos identificados.
- Realizará sus pruebas sobre los controles y el impacto de las deficiencias de control.
- Obtendrá sus conclusiones y emitirá su informe o dictamen independiente, indicando fundamentalmente los riesgos para el negocio.

COBIT 4 indica en su documento de entorno ("framework") que los auditores de TI deben aplicar su metodología y sus guías de auditoria. La orientación de COBIT es fundamentalmente el "negocio", es decir, la actividad de una entidad, pero no se puede negar su gran utilidad también para los auditores, como sustentación del modelo de control de TI a evaluar. El auditor de TI tiene que opinar sobre los riesgos de TI, no limitarse a indicar que determinado control del modelo fue implantado o no.

A lo largo de todo el documento Cona, la auditoria de TI está presente y es aludida en distintas circunstancias, no como mera comprobación del modelo, sino como un elemento activo en la ayuda a la implantación de este modelo y en su mejora.

Por cada control de alto nivel, dentro de cada dominio, COBIT, en las referencias a las responsabilidades relacionadas, incluye una referencia a la auditoria.

Por ejemplo en el Dominio de Planificación y Organización, en el control de alto nivel sobre la Planificación de un plan estratégico de TI, se indica a la Auditoria con la responsabilidad de:

- Identificación de dependencias críticas y rendimientoI2 actual: el auditor debe ser consultado.
- Construcción de un plan estratégico para TI: el auditor debe ser consultado.
- Construcción de planes tácticos para TI: el auditor debe ser informado.

En estas tablas de referencia debe tenerse en cuenta que auditoria ha sido incluida en el mismo apartado que "Cumplimiento Legar", Riesgos y Seguridad (como conceptos globales). En estas dos últimas funciones, sí es posible que, en determinados casos, sean "responsables" de una acción determinada, sin embargo nunca debe serlo el auditor, para mantener su independencia. Por lo tanto, estas tablas, tal y como indica COBIT, son guías, no "obligaciones" mandatorias.

También la función de auditoría está reflejada en otros mecanismos relevantes de COBIT, como por ejemplo en las métricas. Entre las referencias de este tipo, se puede ilustrar con la del Dominio de Adquisición e Implementación, en el control de alto nivel de Instalación y Acreditación de soluciones y cambios, donde se considera, como un indicador, los errores o deficiencias indicados en informes de auditoría interna o externa.

Otro ejemplo se encuentra en el Dominio de Monitorización y Evaluación, en los objetivos de control de detalle para el control de alto nivel: monitorización y evaluación del control interno, donde existe otra referencia a la auditoria de TI. El control de detalle ME2.5 — Aseguramiento del Control Interno indica que debería obtenerse un aseguramiento independiente sobre el control interno, a través de auditoria interna o externa.

En este mismo dominio, en el objetivo de control de alto nivel monitorización y evaluación del control interno, menciona entre las actividades que deben implantarse la evaluación del rendimiento de las revisiones y auditorías independientes.

La auditoría de TI no cambia en la aplicación de sus normas, metodología y

procedimientos porque esté implantado el modelo COBIT, más bien, esta situación es una ayuda, ya que contará con mejores evidencias, y dispondrá de registros más fiables sobre la realización de los controles.

Por ejemplo, las normas de auditoría de TI siguientes son totalmente aplicables dentro de un contexto COBIT:

- S I - Estatuto de Auditoría
- S2 - Independencia
- S3 - Ética Profesional y normas aplicables
- S4 - Competencia Profesional
- S5 – Planificación
- S6 - Realización del Trabajo de Auditoria o Supervisión, Evidencia, y Documentación.
- S7 - Informes
- S8 - Actividades de Seguimiento
- S9 - Irregularidades y actos ilegales
- S 10 - Gobierno de TI
- S11 - Uso de Evaluación del Riesgo en la planificación de auditoría
- S12 - Materialidad • SI3 - Uso del trabajo de expertos
- S13 - Evidencia de Auditoria

De la misma forma que son aplicables muchas de las directrices de auditoria de SI: G4: Extemalización de las actividades de TI a otras organizaciones; G6: Conceptos de Materialidad para la auditoria de SI; 610: Muestreo estadístico; 616: Impacto de terceras partes en los controles de TI de la organización; G31: Privacidad; G36: controles biométricos; entre otras.

3.3 AUDITORÍA DE LOS SISTEMAS DE GESTIÓN EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES -TICS

3.3.1 Introducción

Nuestro planteamiento acerca de los Sistemas de Gestión pretende centrarse en el análisis de los mismos desde la perspectiva de la Gestión del Conocimiento.

Podemos afirmar que el ciclo de Deming -con el acrónimo PDCA- es un ciclo de mejora continua, donde cabe distinguir las siguientes fases:

- **Plan**: planificación de objetivos y procesos necesarios para alcanzar los resultados de acuerdo a las políticas de la empresa.
- **DO**: implantación de los procesos.
- **Check**: revisión y monitorización de los procesos.
- **Act**: ejecutar acciones para mejorar continuamente los procesos.

Los ámbitos donde el PDCA puede considerarse como el auténtico motor y el conocimiento de las TIC es muy variado: va desde la Seguridad de los Sistemas de

Información, pasando por la ingeniería del Software, hasta la calidad en los servicios TIC, etc.

El conocimiento vendría a ser la guía de buenas prácticas que, desde la perspectiva de los Sistemas de Información, lo definimos como repositorio o base de datos de controles. (Véase figura 2.1).

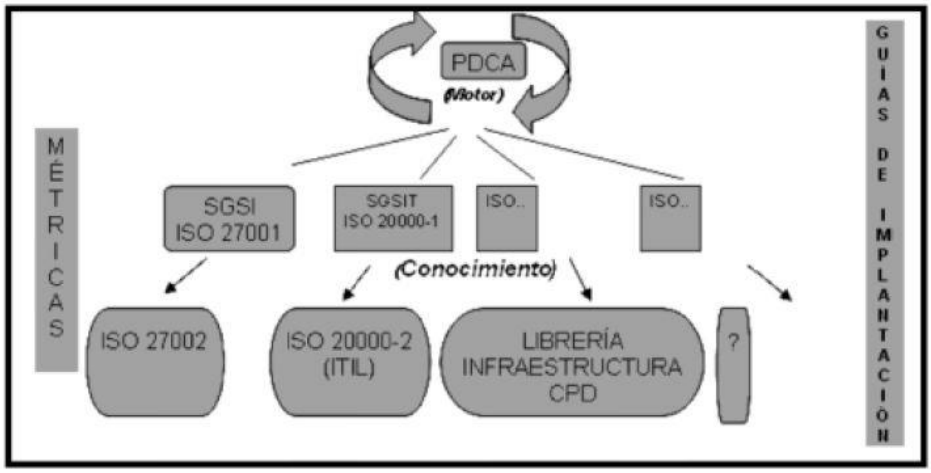

Figura 2.1. Sistemas de gestión de TIC

Los dos sistemas de Gestión del sector de las TIC que están siendo más implantados por las empresas ya sean grandes corporaciones o PYMES son los denominados SGSI y SGSTI, que pasamos a definir:

- **SCSI** —Sistema de Gestión de la Seguridad de la Información: —basado en la Norma UNE ISO / IEC 27001: 2007 (Motor -PDCA-) y en la Norma UNE ISO /IEC 27002 (Conocimiento-Guía de buenas prácticas-Repositorio de Controles para la seguridad en TIC).
- **SGSTI** —Sistemas de Gestión del Servicio de Tecnologías de la Información-: basado en la Norma UNE ISO/ IEC 20000- 1: 2005 (Motor -PDCA-) y en la Norma UNE ISO/IEC 20000 — 2 (Conocimiento-Código de buenas prácticas-Repositorio de controles).

La principal ventaja que presentan estos sistemas de Gestión en las TIC la constituye su capacidad de integración con otros sistemas ya muy difundidos en las empresas, como son el Sistema de Gestión de Calidad (UNE 1SO 9001) y el sistema Medioambiental (UNE ISO 14000), etc. Por este motivo, con su implementación se logra que las TIC queden integradas y alineadas con otros procesos del negocio.

3.3.2 La implantación de un Sistema de Gestión en las TIC

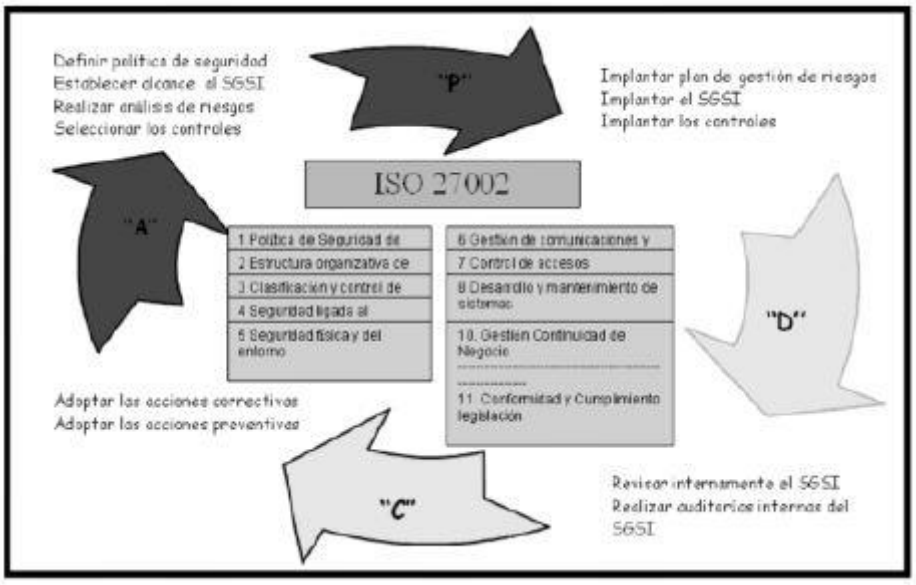

Figura 2.2. Implantación SGSI OSO 27001)

Su implantación lleva aparejada la implementación de las fases de un PDCA (véase figura 2.2). siguiendo los puntos de la Norma UNE ISO/IEC 27001: 2007 desde el apartado 4 al 8 de la Norma antes indicada.

Se hace un especial énfasis en el análisis y gestión de los riesgos y la asignación de controles que minimicen estos riesgos, utilizando una de las muchas metodologías de análisis de riesgos que existen en el mercado, y aplicando los controles que se estimen adecuados de la UNE ISO 27002 (Conocimiento).

3.3.3 Auditoría Interna

En el apartado 6 de la Norma UNE ISO 27001 se define el concepto de Auditoría Interna del SGSI; se define como una revisión independiente del SGSI. Dicha independencia supone obviamente la exigencia de que la persona que lleve a cabo la Auditoría Interna no puede estar vinculada en forma alguna a la implantación ni a la gestión del SGSI.

Si utilizamos el concepto de Motor — Conocimiento, la auditoría interna se podría definir como la revisión del motor y de los controles implementados (conocimiento).

Para esta revisión independiente o Auditoria de SGSI se podrá utilizar la metodología que recomienda uno de los gurús de la Auditoria de Sistemas de Información, RON WELER, denominada Risk—based approach, que cita en su libro Conceptual Foundations and Practice; versión española adaptada por los autores EDR-Evaluación de Riesgos.

Dicha metodología consiste en realizar Pruebas de Cumplimiento; es decir, comprobar que los controles están implementados, funcionan adecuadamente y cumplen los objetivos para los cuales fueron implementados, tanto para los procesos del PDCA -Motor- como para los controles implantados del repositorio Conocimiento-.

No obstante y como complemento a las Pruebas de cumplimiento que se realicen, existe

la posibilidad adicional de ampliación de pruebas —Pruebas Sustantivas- con el objetivo de constatar con una mayor certeza el cumplimiento de los controles.

3.3.4 El proceso de Certificación de los Sistemas de Gestión de las TIC

Se puede considerar el proceso de certificación como el reconocimiento formal por parte de un tercero independiente de un determinado sistema de Gestión. (Véase en la figura 2.3).

La certificación de un sistema de Gestión de las TIC no es obligatoria, pero lo cierto es que las empresas que optan por certificarse mantienen sus sistemas de gestión con una mayor dedicación en el ciclo de mejora continua y en su búsqueda por alcanzar la excelencia.

El esquema de certificación sigue la secuencia especificada en la figura 23 que detallamos brevemente:

- Presentación de solicitud formal ante el organismo de certificación, adjuntando la información solicitada por el organismo en dicha solicitud.
- Revisión del Manual del sistema de Gestión y los procedimientos por el Auditor externo del organismo certificador.
- Visita Previa del Auditor externo del organismo Certificador (Pre-Auditoría en las instalaciones de la empresa cliente). Para realizar esta Pre-Auditoría, el auditor externo revisará el Motor del Sistema de Gestión y emitirá un Informe con observaciones al respecto.
- Pasado un tiempo prudencial el auditor de la certificadora realizará la Auditoría del Sistema de Gestión, revisando el Motor y el Conocimiento con la metodología EDR anteriormente aludida.

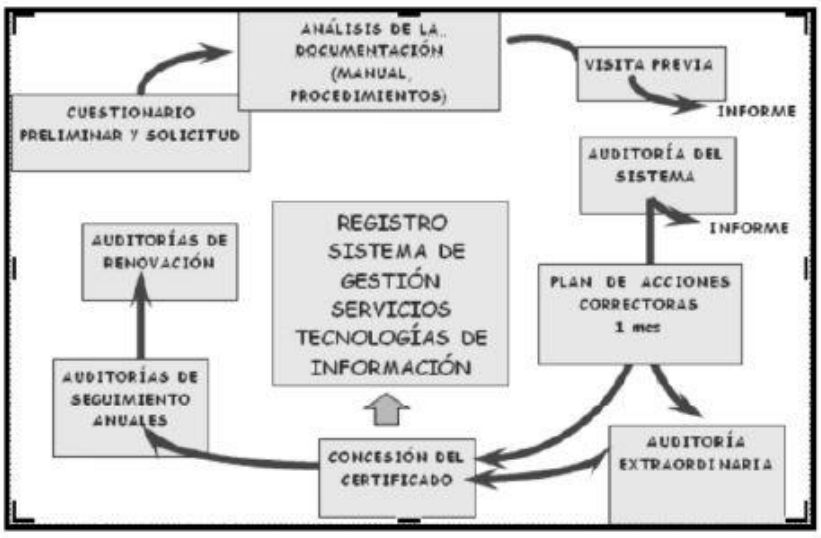

Figura 2.3. Modelo de certificación de sistemas de gestión de TIC

El resultado de dicha Auditoria quedará plasmado en un informe de Auditoría Inicial con

no conformidades. En caso de existir no conformidades de importancia, la certificación podría quedar suspendida pendiente de rectificación.

Para el caso de detectarse no conformidades "menores", se emitirá una certificación con reservas, quedando pendientes las oportunas rectificaciones cuya subsanación deberá ser constatada por el Auditor en la auditoría de seguimiento.

Una vez otorgada la certificación, el organismo certificador llevará a cabo anualmente Auditorías de seguimiento para determinar si su sistema de Gestión de las TIC sigue cumpliendo con las Normas (Motor).

El tiempo de la Certificación es de tres años, realizándose al tercer año la Auditoría de Renovación que es similar a la Auditoría Inicial.

Como se puede apreciar en estas nuevas auditorías de Sistemas de Gestión de TIC, se sigue el proceso de la Auditoría de Sistemas de Información, salvedad hecha de la inclusión del novedoso concepto de Motor-Conocimiento, que hemos intentado resumir al máximo en este capítulo.

3.4 CONCLUSIONES

La implantación de normas y modelos de gestión de TI puede colaborar y ayudar a las entidades a lograr sus objetivos de negocio, aumentando la confianza que pueden depositar en sus sistemas y tecnologías de la información.

La auditoría de SI se verá beneficiada con la implantación de estas normas en que tendrá mejores evidencias y sustentación de los controles implantados en un entorno de TI.

No obstante, es necesario tener en cuenta el objetivo de la auditorio, si es dentro del marco de la certificación de una norma (en muchos casos la comprobación de la aplicación de los requisitos establecidos en la norma respectiva), o como un dictamen independiente con un alcance y objetivo determinado, para informar a la Dirección de una entidad, o por requerimientos externos, si existen deficiencias en la gestión de TI, en su acepción más global, para el negocio, en el presente o en un futuro cercano.

3.5 REFERENCIAS Y BIBLIOGRAFÍA

www.itgi.org

www.isaca.org

COBIT 4

IT Assurance Framework Draft - Agosto 2007

http://europa.eu.int/eur_ex/lex/JOHtml.do?uri=0J:L:2005:077:SOM:EN:HTML

Information Security Harmonisation—Classification of Global Guidance - www.isaca.org

Sarbanes-Oxley Act Compliance - Strategies for Implementing an Audit Committee Complaints Procedure - By Mathias Strasser y Edgar Weippl - Joumal - Volume 5 - 2006 - www.isaca.org

Security standards and frameworks - Bob Violino -bviolino@optonline.net. - COMPUTERWORLD

Challenges of compliance - The Cobit bridge - Kenneth Licw - COMPUTERWORLD - Vol.12 - Junio 2006

Alphabet Soup: Cobit. ITIL and ISO - www.csoonline.com - Febrero 2006

COBIT MAPPING: MAPPING OF ISO/IEC 17799:2000 WITH COBIT, 2° ed. - www.isaca.org - www.itgi.org

COBIT MAPPING: OVERVIEW OF INTERNATIONAL IT GUIDANCE, r ed.- www.isaca.org - www.itgi.org

COBIT MAPPING: MAPPING OF SEI'S CMM FOR SOFTWARE WITH COBIT 4.0 - ITGI 2006 - www.isaca.org - wwwitgi.org

Convergent Security Risks in Phvsical Security Systems and - IT Infrastructures - (Informe donde participan las siguientes organizaciones: ASIS Intemational (ASIS), Information Systems Security Association (ISSA) y la !SACA. - 2005

!T Control Objectives for Sarbanes-Oxley, ed. - Septiembre 2006 -www.isaca.org - wwwitgi.org

Guidance on Aligning COBIT. ITIL and !SO /7799 - By Gary Hardy Joumal on line - 2006 - www.isaca.org

ITGI Issues Val IT—New IT Value Framework - www.isaca.org -www.itgi.org

Control Practices"- www.isaca.org - www.itgi.org

Governance of Outsourcing - ITGI. 2005 - www.itgi.org

COBIT MAPPING: MAPPING OF PMBOK WITH COBIT 4.0 - Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBOKgI Guide) — Third Edition - 2006

Information Risks: - Whose Business - Are They? - ITGI - 2006

3.6 CUESTIONES DE REPASO

1. Defina brevemente qué es el Ciclo de Deming. ¿De qué fases consta?

2. ¿Cuál es la relación entre el motor y el PDCA en los Sistemas de Gestión de las TIC?
3. ¿Qué es el conocimiento en el modelo Motor - Conocimiento de los Sistemas de Gestión de las TIC?
4. En un SGSI-Sistema de Gestión de la Seguridad de la Información, ¿cuál seria la base o fundamento del sistema?
5. En la metodología Evaluación de Riesgos, explique brevemente las pruebas de cumplimiento y sustantivas.
6. En un modelo de Certificación de Sistemas de Gestión de TIC, explique brevemente qué es la Visita previa y la Auditoría Inicial.

Capítulo 4

METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD *Y* LA AUDITORÍA DE SISTEMAS DE INFORMACION

4.1 INTRODUCCIÓN A LAS METODOLOGÍAS

Según el diccionario de la lengua "MÉTODO es el modo de decir o hacer con orden una cosa". Así mismo, define el diccionario la palabra "METODOLOGÍA como el conjunto de métodos que se siguen en un trabajo científico o en una exposición doctrinal, que permiten abordar éste de forma organizada y consecuente".

Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad que llamaremos METODOLOGÍA.

La Informática ha sido tradicionalmente una materia compleja en todos sus aspectos. Y ha sido necesario por ello la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, y como no, la auditoría de los sistemas de información.

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de "acierto /error.

Asi mismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si uno solo lo hiciera. Es por ello lo habitual del uso de metodologías en las empresas auditoras/consultoras profesionales, desarrolladas por los más expertos, y de esta manera se pueden conseguir resultados homogéneos en equipos de trabajo heterogéneos.

La proliferación de metodologías en el mundo de la auditoria y el control informáticos se pueden observar en los primeros años de la década de los 80 paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos). Pero el uso de métodos de auditoria es casi paralelo al nacimiento de la informática,

Dentro del mundo de la informática existen muchas disciplinas en las que el uso de metodologías es una práctica habitual. Una es la seguridad de sistemas de infonnación.

Aunque de forna simplista se trata de identificar la seguridad in fonnática a la

seguridad lógica de los sistemas, nada está mas lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

Este y no otro debe ser el campo de actuación de un auditor informático del siglo XXI, en uno de los grandes símbolos del desarrollo tecnológico de la época de la humanidad que nos ha tocado vivir.

Si definimos la "SEGURJDAD DE LOS SISTEMAS DE INFORMACIÓN" como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoria es una de sus figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

Por tanto, el nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

Resumiendo, la informática en una entidad crea unos riesgos informáticos, de los que hay que proteger y preservar a la entidad con un entramado de contramedidas, y la calidad y la eficacia de las mismas es el objetivo a evaluar para asi poder identificar sus puntos débiles y poder mejorarlos. Ésta es una de las funciones de los auditores informáticos.

Por tanto, debemos profundizar más en ese entramado de contramedidas, para ver qué papel tienen las metodologías y los auditores en el mismo..

Para explicar este aspecto diremos que cualquier concramedida nace de la composición de varios factores.

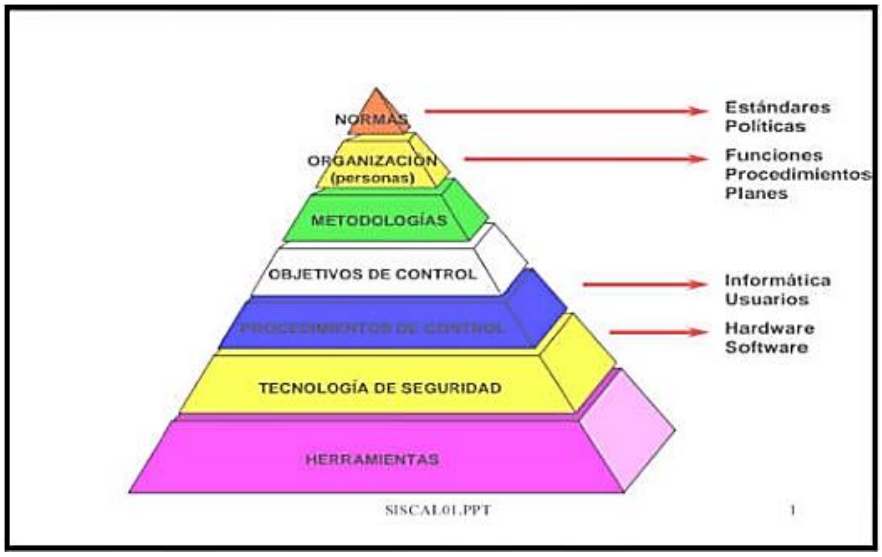

Figura 3.1. Factores que intervienen en la composición de contramedida

Todos los factores de la pirámide intervienen en la composición de una

contramedida.

LA NORMATIVA debe definir de forma clara y precisa todo lo que debe existir y cumplirse, tanto desde el punto de vista conceptual como práctico, desde lo general a lo particular. Debe inspirarse en estándares, políticas, marco jurídico, políticas y normas de empresa, experiencia y práctica profesional. Desarrollando la normativa, debe alcanzarse el resto del "gráfico valor". Se puede dar el caso en que una normativa y su carácter disciplinario sean el único control de un riesgo, pero no es frecuente.

LA ORGANIZACIÓN son personas con funciones especificas, y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Este es el aspecto más importante, dado que sin él, nada es posible. Se pueden establecer controles sin alguno de los demás aspectos. pero nunca sin personas. Son estas las que realizan los procedimientos y desarrollan los Planes (Plan de Seguridad, Plan de Contingencias, auditorías, cte.).

LAS METODOLOGÍAS son necesarias para realizar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

LOS OBJETIVOS DE CONTROL son los objetivos a cumplir en el control de los procesos. Este concepto es el más importante después de **"LA ORGANIZACIÓN"**, y solamente de un planteamiento correcto de los mismos, saldrán unos procedimientos eficaces y realistas.

LOS PROCEDIMIENTOS DE CONTROL sor los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivo* de control y. por tanto, deben de estar documentados y aprobados por la Dirección.

La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al "control o contramedida", pero no debemos olvidar que "UNA HERRAMIENTA NUNCA ES UNA SOLUCIÓN SINO UNA AYUDA PARA CONSEGUIR UN CONTROL MEJOR". Sin la existencia de estos procedimientos, las herramientas de control son solamente una anécdota

Dentro de la **TECNOLOGIA DE SEGURIDAD** están todos los elementos, ya sean hardware o software, que ayudan a controlar un riesgo informático. Dentro de este coocepto están los cifradores, autentificadores. equipos "tolerante* al fallo", las herramientas de control, etc.

LAS HERRAMIENTAS DE CONTROL son elementos software que permiten definir uno o varios procedimientos de control, para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí y la calidad de cada uno está relacionada con la de los demás. Cuando se evalúa el nivel de Seguridad de **Sistemas** en una institución, se están evaluando todos estos factores **(pirámide)** y se plantea

un **Plan de Seguridad** nuevo, que mejore todos los factores, aunque conforme vayamos realizando los distintos proyectos del plan, no irán mejorando todos por igual. Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

Llamaremos PLAN DE SEGURIDAD a una estrategia planificada de acciones y proyectos que lleven a un sistema de información y a sus centros proceso de una situación inicial determinada (y a mejorar) a una situación mejorada. (véase en la figura 3.2).

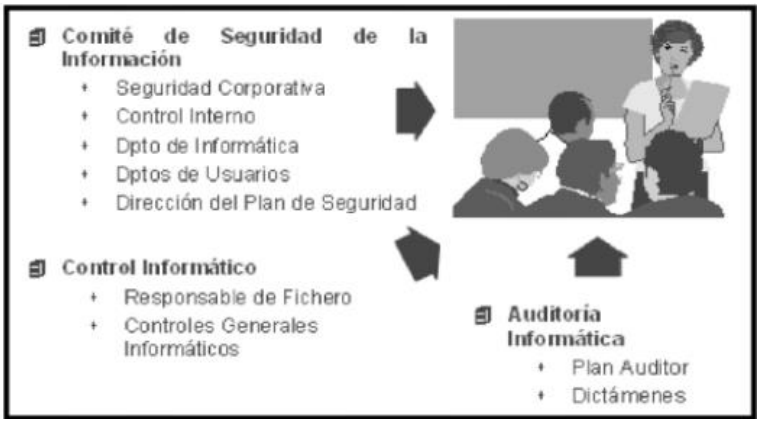

Figura 3.2. Organización de la seguridad de sistemas en las organizaciones

En la figura 3.2 se muestra la organización de la seguridad de sistemas en la empresa. Por una parte un comité que seria el director de la estrategia y de las políticas. Y por otra parte control interno y auditoría informáticos. La función de control interno se ve involucrada en la realización de los procedimientos de control y es una labor de dia a día. La función de auditoria informática está centrada en la evaluación de los distintos aspectos que designe su PLAN AUDITOR, con unas características de trabajo que son las visitas concretas al centro, coa objetivos concretos y tras terminar su trabajo, la presentación del informe de resultados. Por tanto las características de su función son totalmente distintas. Lógicamente también sus métodos de trabajo.

Queda pues decir que ambas funciones deben ser independientes de la informática, dado que por la disciplina laboral, la labor de las dos funciones quedaría mediatizada y comprometida. Esto es lo que se llama "segregación de funciones" entre éstas y la informática. Nos quedaría decir que en organizaciones muy grandes, incluso con dependencias multinacionales, se tiende a estructuras organizativas más complejas. Así mismo por la tendencia a descentralizar la función o crear figuras paralelas. Pero tenemos que decir que no son más que variantes de las dos funciones clásicas, auditoría y control o seguridad. Asi es que hasta dentro de las organizaciones profesionales existen las dos funciones diferenciadas en sus credenciales y certificaciones.

También conviene aclarar que, aunque en algunos foros se utiliza el concepto seguridad integral tratando de unir dos sectores absolutamente diferenciados

como son el de la seguridad de la información y la seguridad ñsica (o seguridad electrónica), nada más lejos de la realidad que este tópico que *se* ha escuchado desde hace muchos años, y que no es nada objetivo. Porque que en un sistema de videovigilancia en IP se protejan los datos con una VPN no significa que sean dos sectores convergentes. El sector de la seguridad flsica tiene coches blindados y no significa que confluyan este sector y el del automóvil.

4.2 METODOLOGÍAS DE EVALUACIÓN DE SISTEMAS

4.2.1 Conceptos fundamentales

Las metodologías que se usan en el mundo de la seguridad de sistemas son todas las necesarias para realizar un plan de seguridad y además las **de** auditoria informática.

Las dos metodologías de evaluación de sistemas por antonomasia son las de ANÁLISIS DE RIESGOS y las de AUDITORÍA INFORMÁTICA, con dos enfoques distintos. La auditoria informática sólo identifica el nivel de "exposición" por la falta de controles, mientras que el análisis de riesgos facilita la "evaluación" **de los riesgos, y recomienda acciones en base al costo-beneficio de las mismas,**

Introduzcamos una serie de definiciones para profundizar en estas metodologías:

- AMENAZA: una(s) persona(s) o cosa(s) vista como posible fuente de peligro o catástrofe. Ejemplos: inundación, incendio, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.
- VULNERABILIDAD: la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático, Ejemplo falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de sopones magnéticos, falta de separación de entornos en el sistema, falta de cifrado en las telecomunicaciones, etc.
- RIESGO: la probabilidad de que una amenaza llegue a acaecer por la existencia de una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes.
- EXPOSICIÓN O IMPACTO: la evaluación del efecto del riesgo. Ejemplo: es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc.

Las amenazas reales se presentan de forma compleja y son difieiles de predecir. Ejemplo: por varias causas se rompen las dos entradas de agua e inundan las líneas telefónicas (pues existe un poro en el cable) y hay un cortocircuito, y se quema el transformador de la central local. En estos casos la probabilidad resultante es muy dificil de calcular.

Las metodologías de análisis de riesgos se utilizan desde los años 70 en la industria del seguro basándose en grandes volúmenes de datos estadísticos agrupados en tablas actuarias

Se emplearon en la informática en los 80, y adolecen del problema de que los registros estadísticos de incidentes son escasos y por tanto el rigor científico de los cálculos probabilísticos es pobre. Aunque existen bases de incidentes en varios países, estos datos no son muy fiables por varios motivos: la tendencia a la ocultación de los afectados, la localización geográfica, las distintas mentalidades, la informática cambiante, que los riesgos se presentan en un período de tiempo solamente (ventana de criticidad), etc.

Todos los riesgos que se presentan podemos:

- EVITARLOS (por ejemplo: no construir un centro donde hay peligro constante de inundaciones)
- TRANSFERIRLO (por ejemplo: uso de un centro de cálculo contratado)
- REDUCIRLO (por ejemplo: sistema de detección y extinción de incendios).
- ASUMIRLOS. Que es lo que se hace si no se controla el riesgo en absoluto.

Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo más baja posible o al menos quede reducida de una forma razonable en costo-beneficio.

4.2.2 Tipos de metodologías

Todas las metodologías existentes desarrolladas y utilizadas en la auditoria y el control informáticos se pueden agrupar en dos grandes familias. Estas son:

- Cuantitativas: basadas en un modelo matemático numérico que ayuda a la realización del trabajo.

- Cualitativas: basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo y seleccionar en base la experiencia acumulada.

4.2.2.1 Metodologías cuantitativas

Diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencias son datos de probabilidad de ocurrencia (riesgo) de un evento, y que se deben extraer de un registro de incidencias donde el número de incidencias tienda al infinito o sea

suficientemente grande. Esto no pasa en la práctica y se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar en el método a elegir entre varias contramedidas podríamos aceptarlo.

Hay varios coeficientes que conviene definir:

- ALE (Annualized Loss Expentacy): multiplicar la pérdida máxima posible de cada bien/recurso por la amenaza con probabilidad más alta.
- Reducción del ALE (Annualized Loss Expectancy): es el cociente entre el coste anualizado de la instalación y el mamenimicnto de la medida contra el valor total del bien/recurso (activo) que se está protegiendo, en tanto por ciento.
- Retomo de la inversión (ROi): ALE original menos ALE reducido (como resultado de la medida), dividido por el coste anualizado de la medida.

Todos estos coeficientes y otros diseñados por los autores de las metodologías son usados para el juego de simulación que permite elegir entre varias contramedidas en el análisis de riesgos. Esto es, en el proceso metodológico del análisis de riesgos, tras identificar activos, amenazas, debilidades, siempre habrá entre varias opciones de plan de contramedidas a elegir. El modelo o juego de ensayo que me permite elegir el más apropiado en cada caso se llama "qué pasa si", *y* cada metodología usa uno distinto que la caracteriza.

Por tanto vemos con claridad dos grandes inconvenientes de estas metodologías, que son por una parte la debilidad de los datos, de la probabilidad de ocurrencia, por los pocos registros de incidentes y la poca significación de los mismos a nivel mundial. Y además la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden acaecer. Frente a la ventaja de poder usar un modelo matemático para el análisis.

4.2.2.2 Metodología cualitativa / subjetivas

Basadas en métodos estadísticos y lógica borrosa. Precisan de un profesional experimentado. Pero requieren menos recursos humanos/tiempo que las metodologías cuantitativas.

La tendencia de uso de la realidad es la mezcla de ambas. En la figura 3.3 se observa un cuadro comparativo entre ambas.

4.2.3 Metodologías más comunes

Las metodologías más comunes que podemos encontrar de evaluación de sistemas son de análisis de riesgos o de diagnósticos de seguridad, las de plan de contingencias y las de auditoría de controles generales.

4.2.3.1 Metodologías análisis de riesgos

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas

Existen dos tipos: las cuantitativas y las cualitativas. Existen gran cantidad de ambas clases y citaremos algunas de ellas.

El esquema básico de una metodología de análisis de riesgos es en esencia el representado en la figura 3.4.

4.2.3.2 Comparación

	CUANTITATIVA	CUALITATIVA
PROS	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra justificante para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Incluye factores intangibles.
CONTRAS	Estimación de probabilidad de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodología estándares. Difíciles de mantener o modificar. Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Pueden excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Identificación de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. Dependencia de un profesional.

Figura 4.3. Tipos de metodologías para el análisis de riesgo

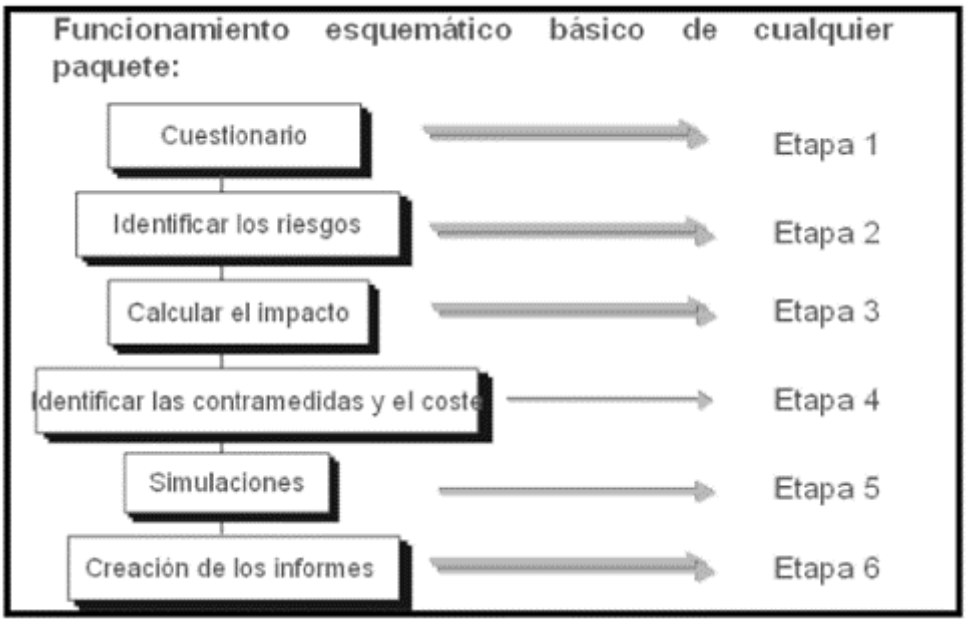

Figura 4.4. Funcionamiento del software del análisis de riesgo

En base a unos cuestionarios se identifican vulnerabilidades y riesgos, se evalúa el impacto, para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante pues mediante un juego de simulación (que llamaremos "¿qué pasa si?...") analizamos el efecto de las distinta contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad), que compondrá el informe final de la evaluación.

De forma genérica las metodologías existentes se diferencian en:

- Si son cuantitativas o cualitativas, o sea si para el "Qué pasa si ...." utilizan un modelo matemático o algún sistema cercano a la elección subjetiva. Aunque bien pensado al aproximar las probabilidades por esperanzas matemáticas subjetivamente, las metodologías cuantitativas, aunque utilicen aparatos matemáticos en sus simulaciones, tienen una gran componente subjetiva.
- Y además se diferencian en el propio sistema de simulación.

En el INFOSEC'92 proyecto S2O14 se identificaron 66 metodologías de las cuales por limitaciones de tiempo se analizaron sólo 12 con sus respectivos paquetes y así el informe de este trabajo acabó siendo un contraste de las prestaciones de dichos paquetes según los fabricantes y la opinión de los consultores del equipo. Estos métodos analizados eran: NALIZY, BDSS, BIS RISK ASSESOR, BUDDY SYSTEM, COBRA, CRAMM, DDIS MARION AP+, MELISA, RISAN, RISKPAC, RISKWATCH.

Después de estas metodologías han nacido muchas otras, como por ejemplo la MAGERIT (desarrollada por la administración española), Octave, PRJMA, etc.

En la figura 3.5 se muestran las metodologías más destacables en la actualidad.

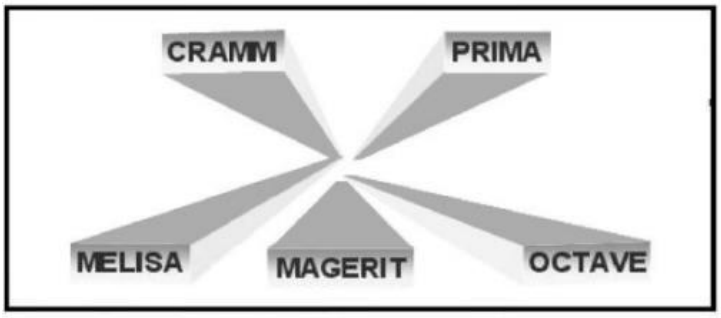

Figura 3.5. Principales métodos de análisis y gestión de riesgos

PRIMA (Prevención de riesgos informáticos con metodología abierta)

Es un compendio de metodologías españolas desarrolladas entre los años 1990 y la actualidad con un enfoque subjetivo.

Sus características esenciales son:

- Cubrir las necesidades de los profesionales que desarrollan cada uno de los proyectos necesarios de un plan de seguridad.
- Fácilmente adaptable a cualquier tipo de herramienta.
- Posee cuestionarios de preguntas para la identificación de debilidades o faltas de controles.
- Posee listas de ayuda para los usuarios menos experimentados de debilidades, riesgos y contramedidas (sistema de ayuda).
- Permite fácilmente la generación de informes finales.
- Las "Listas de ayuda" y los cuestionarios son abiertos y por tanto es posible introducir información nueva o cambiar la existente. De ahí la expresión Abierta de su nombre.
- Tiene un "¿qué pasa si … ?" cualitativo pero al tener capacidad de aprendizaje con su uso posee en su base de conocimiento una base o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo.

En las figuras 3.6 y 3.7 se expone la metodología de análisis de riesgos PRIMA.

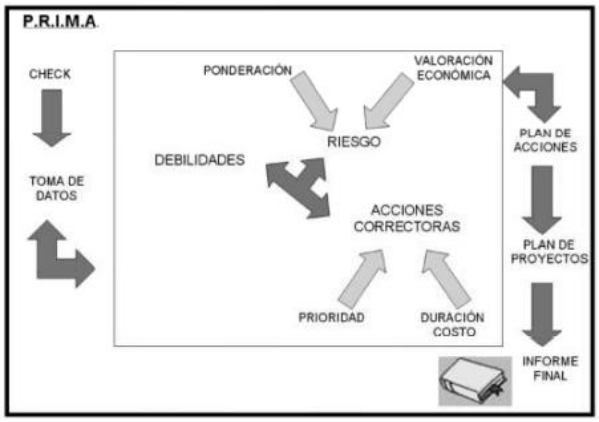

Figura 3.6. Conceptas básicos de la metodología PRIMA

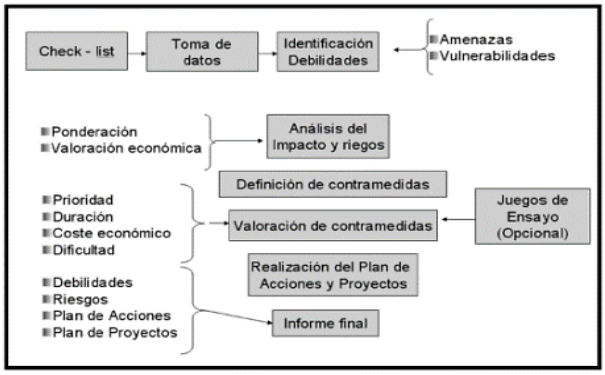

Figura 3.7. Fases de la metodología PRIMA

4.2.3.3 Plan de contingencias

El auditor debe conocer perfectamente los conceptos de un plan de contingencias para poder auditarlo.

Hay varias formas de llamarlo pero conviene no confundir los conceptos que se manejan alrededor de los nombres.

El plan de contingencias y de recuperación de negocio es lo mismo, pero no así el plan de restauración interno. Este va enfocado hacia la restauración del C.P.D., pero sobre eventos que suceden dentro del entorno (caídas del sistema, roturas leves, etc.), y que su duración no afecta gravemente a la continuidad del negocio.

También se manejan a veces los conceptos de plan de contingencias informático y plan de contingencias corporativo, cuyos conceptos son sólo de alcance. El corporativo cubre no sólo la informática sino todos los departamentos de una entidad, y puede incluir también el informático como un departamento más. Frecuentemente se realiza el informático.

El Plan de Contingencias es una **estrategia planificada** constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa.

Esa estrategia materializada en un manual es el resultado de todo un proceso de análisis y definiciones que es de lo que existen metodologías. O sea las metodologías que existen versan sobre el proceso necesario para obtener dicho plan.

Es muy importante tener en cuenta que el concepto a considerar es "la continuidad en el negocio"; estudiar todo lo que puede paralizar la actividad y producir pérdidas. Todo lo que no considere este criterio no será nunca un plan de

contingencias.

FASES DE UN PLAN. Las fases de un plan son las siguientes:

FASE 1: ANÁLISIS Y DISEÑO. Se estudia la problemática, las necesidades de recursos, alternativas de respaldo y se analiza el coste/beneficio de las mismas, Esta es la fase más importante pudiendo llegarse al final de la misma hasta la inclusión la conclusión de que no es viable o es muy costoso el seguir. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas

Las de **Risck Análisis** se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Los registros de incidentes al igual que hablamos en las metodologías de análisis de riesgos son escasos y poco fiables, aun así es más fácil encontrar este tipo de metodologías que las segundas.

Las tareas de esta fase en las metodologías de Risck Análisis son las siguientes:

1. Identificación de amenazas.
2. Análisis de la probabilidad de materialización de la amenaza.
3. Selección de amenazas.
4. Identificación de entornos amenazados.
5. Identificación de servicios afectados.
6. Estimación del impacto económico por paralización de cada servicio
7. Selección de los servicios a cubrir.
8. Selección final del ámbito del Plan.
9. Identificación de alternativas para los entornos.
10. Selección de alternativas.
11. Diseño de estrategias de respaldo.
12. Selección de la estrategia de respaldo.

Las de **Bussincs lmpact** se basan en el estudio del impacto (pérdida económica o de imagen) que ocasiona la falla de algún recurso de los que soporta la actividad del negocio. Estas metodologías son más escasas pero tienen grandes ventajas como es el mejor entendimiento del proceso, o el menor empleo de tiempo de trabajo por ir más directas al problema.

Las tareas para las de Bussines lmpact son las siguientes:

1. Identificación de servicios finales.
2. Análisis del impacto. En estas metodologías se evalúan los daños económicos y de imagen y otros aspectos no económicos, lo que les da una ventaja en los casos en los que intervienen otros valores que no sean los económicos.
3. Selección de servicios críticos.
4. Determinación de recursos de soporte.
5. Identificación de alternativas para entornos.
6. Selección de alternativas.

7. Diseño de estrategias globales de respaldo.
8. Selección de la estrategia global de respaldo.

Como puede verse el enfoque de esta segunda es más práctico y directo y se va más directo a las necesidades reales de la entidad sin tener que justificar con datos de probabilidades que aportan poco por la pobreza de los datos. Estas se basan en hechos ciertos, que se analizan y se justifican económicamente. Permiten por tanto hacer estudios costo/beneficio que justifican las inversiones con más rigor que los estudios de probabilidad que se obtienen con los análisis de riesgos.

Hay un factor importante a determinar en esta fase que es el "Time Frarne", o tiempo que la empresa puede asumir con paralización de la actividad operativa antes de incurrir en pérdidas significativas. Este factor marcará las estrategias de recuperación y se extraerá del análisis del impacto.

FASE II: **DESARROLLO DEL PLAN.** Esta fase y la tercera son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando así la documentación del plan.

Es en esta fase cuando se analiza la vuelta a la nonnalidad dado que pasar de la situación normal a la "alternativa" debe concluirse con la reconrracción de la situación inicial antes de la contingencia, y esto es lo que no todas las merodologfas incluyen.

FASE III: PRUEBAS *Y* MAN TENIMIENTO. En esta fase se definen las pruebas, sus características, sus ciclos y se realiza la primera prueba como comprobación de todo el trabajo realizado y mentalizar al personal implicado.

Así mismo se define la estrategia de mantenimiento, la organización destinada a ello y la normativa y procedimientos necesarios para llevarlo a cabo.

HERRAMIENTAS. En este caso como en todas las metodologías la herramienta es una anécdota y lo importante es tener y usar la metodología apropiada y más tarde desarrollar la herramienta que se necesite.

4.3 LAS METODOLOGIAS DE AUDITORÍA INFORMÁTICA

Las únicas metodologías que podemos encontrar en la auditoria informática son dos familias distintas: las auditorias de controles generales como producto estándar de las compañías auditoras profesionales, que son una homologación de las mismas a nivel internacional, y las metodologías de los auditores internos

El objetivo de fas auditorias de controles generales es "dar una opuuon sobre la fiabilidad de los datos del ordenador para la auditoria financiera". El resultado externo es un escueto informe como parte del informe de auditoria, donde se destacan las vulnerabilidades encontradas.

Están basadas en pequeños cuestionarios estándares. que dan como resultado informes muy generalitas, Tienen apartados para definir "pruebas" y anotar sus resultados. Ésta es una característica clara de la diferencia con las metodologías de evaluación de la consultoría como las de análisis de riesgos que no las tienen, aunque también tratan de identificar vulnerabilidades o falta de controles. O sea la realización de pruebas es consustancial a la auditoría, dado que el trabajo de consultoría como el análisis de riesgos espera siempre de la colaboración del analizado, y por el contrario la auditoria debe demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener el apartado de las pruebas, llegando al extremo de que hay auditorias que se basan sólo en pruebas corno la "auditoria de integridad".

Estas metodologías están muy desprestigiadas pero no porque sean malas en si mismas, sino porque dependen mucho de la experiencia de los profesionales que las usan y existe una práctica de utilizarlas profesionales sin ninguna experiencia. Ninguna de esta metodologías usa de ayudas de contramedidas, llegándose a la aberración de que se utilizan metodologías de análisis de riesgos para hacer auditorías.

Todas estas anomalías nacen de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil y rápida que le permita empezar su trabajo rápidamente. Esto es una utopía. El auditor informático necesita de una larga experiencia tutelada y una gran formación tanto auditora como informática. Y esta formación debe ser adquirida mediante el estudio y la práctica tutelada.

Llegamos al punto en el que es necesario decir que la metodología de auditor interno debe ser diseñada y desarrollada por el propio auditor y esta será la significación de su grado de experiencia y habilidad.

Por tanto entre las dos metodologías de evaluación de sistemas (análisis de riesgos y auditoría) existen similitudes y grandes diferencias. Ambas tienen papeles de trabajo obtenidos del trabajo de campo tras el plan de entrevistas, pero los cuestionarios son totalmente distintos. Los de la figura 3.6 son de análisis de riesgos y son preguntas dirigidas a la identificación de la falta de controles. Se ven dirigidas a consultores por la planificación de los tiempos, y por ser preguntas más concretas.

En el punto 3 se expone un ejemplo real de una metodología de auditor interno necesaria para revisar cualquier aplicación. Como se ve en el ejemplo está formada por recomendaciones de plan de trabajo y de todo el proceso que debe seguir. También define el objetivo de la misma, que habrá que describirlo en el memorándum de apertura al auditado. Así mismo describe en forma de cuestionarios genéricos, con una orientación de los controles a revisar.

En este caso del auditor interno informático le servirá de guía para confeccionar el programa real de trabajo de la auditoría. El auditor deberá hacer los cuestionarios más detallados si así lo estima oportuno y definir cuantas pruebas estime oportunas.

Así mismo si cuando empieza una auditoría, el auditor detecta vías alternativas a revisar, su deber es seguirlas cambiando el plan de trabajo. Por tanto el concepto de las metodologías de análisis de riesgos de "tiempos medidos" es más bien para consultores profesionales que para auditores internos. Estos, aunque deben planificar sus tiempos, en principio no debe ser nunca su factor principal, dado que su función es vigilancia y esta se cumple si el auditado se siente vigilado.

El auditor interno debe hacerse sus metodologías necesarias para auditar los distintos aspectos o áreas que defina en el plan auditor que veremos en el siguiente punto.

El esquema metodológico del auditor está definido por el plan auditor que vemos a continuación

4.3.1 Ejemplo metodología auditoría de una aplicación

METODOLOGÍA DE TRABAJO

REVISIÓN DE CONTROLES SOBRE APLICACIONES

OBJETIVO: determinar que los sistemas producen informaciones exactas y completas al momento oportuno. Este área de trabajo es tal vez el más importante en el trabajo de auditorias informáticas,

4.3.1.1 Programa de la revisión

1. Identificar el área a revisar (por ejemplo a partir del calendario de revisiones), notificar al responsable del área y prepararse utilizando papeles de trabajo de auditorías anteriores.

2. Identificar las informaciones necesarias para la auditoria y para las pruebas.

3. Obtener informaciones generales sobre el sistema operacional. En esta etapa, se definen los objetivos y el alcance de la auditoria, y se identifican los usuarios específicos que estarían afectados por la auditoria (plan de entrevistas); el auditor aprende en qué consiste el entorno a revisar, y explica por qué se hace la auditoria.

   Obtener una comprensión detallada de la aplicación/sistema. Aquí, se pasan entrevistas con los usuarios y el personal implicado en el sistema a revisar; se examina la documentación de usuarios, de desarrollo, de operación, se identifican los aspectos más importantes del sistema (entrada, tratamiento, salida de datos), la periodicidad de procesos, los programas fuentes, características y estructuras de ficheros de datos; y pistas de auditoria.

4. Identificar los puntos de control críticos en el sistema operacional. Utilizando organigramas de flujos de informaciones, identificar los puntos de control

críticos en entrevistas con los usuarios y el personal operacional, y con el apoyo de la documentación sobre el sistema. El auditor tiene que identificar los peligros y los riesgos que podrían surgir en cada punto. Los puntos de control críticos son aquellos puntos donde el riesgo es más grave, es decir, donde la necesidad de un control es más importante. A menudo, son necesarios controles en los puntos de interface entre procedimientos manuales y automáticos.

5. Diseño y elaboración de los procedimientos de la auditoria.

6. Ejecución de pruebas en los puntos críticos de control. Se podría incluir la determinación de las necesidades de herramientas informáticas de ayuda a la auditoria no informática. Una revisión del cumplimiento de los procedimientos se hace para verificar el buen seguimiento de estándares y procedimientos formales, y de los procesos descritos por los organigramas de flujos. Así se verifican los controles internos del cumplimiento de a) planes, políticas, procedimientos, estándares, b) la ética del trabajo de la organización, c) requerimientos legales, d) principios generales de contabilidad y e) prácticas generales de informática.

7 Se hacen revisiones sustantivas y pruebas, como resultado de la revisión del cumplimiento de procedimientos. Si las conclusiones de la revisión de cumplimentación eran generalmente positivas, se podrían limitar las revisiones sustantivas. Dentro de este punto del programa de la revisión podríamos analizar si existen los siguientes controles.

8 Evaluación de la revisión y/o resultados de pruebas. En esta etapa se identifican y se evalúan los puntos fuertes y débiles de los procedimientos y prácticas de control interno en relación con su adecuación, eficiencia y efectividad. Cuando se identifique una debilidad, se determinará su causa. Se elaboran las conclusiones basadas sobre la evidencia; lo que deberá ser suficiente, relevante, fiable, disponible, comprobable y útil.

9 Preparación del informe. Recomendaciones.

4.3.1.2 Controles

- Revisar procedimientos escritos para iniciar, autorizar, recoger, preparar y aprobar los datos de entrada, en la forma de un manual de usuario. Verificar que los usuarios entienden y siguen estos procedimientos.
- Que se dé la forrnación del "uso del Terrninal'' necesaria a los usuarios.
- Revisar los documentos fuente u otros documentos para determinar si son numerados. También revisar códigos de identificación de transacciones y otros campos de uso frecuentes, para determinar si son codificados previamente para minimizar errores en los procesos de preparación, entrada y conversión de datos.
- Cuando sea necesario, veri ficar que todos los datos de entrada en un

sistema pasan por validación y registro antes de su tratamiento.

- Determinar si los usuarios preparan totales de control de los datos de entrada por terminales, Comprobar la existencia de una reconciliación de los totales de entrada con totales de salida.
- Comprobar la existencia y seguimiento de calendarios de entrada de datos y de distribución de informes (listados).
- Determinar si el archivo y retención de documentos fuente y otros formularios de entrada es lógica y accesible, y que cumple las normas y requerimientos legales
- Revisar los procedimientos de corrección de errores.
- Comprobar la existencia de períodos para documentos fuentes y soportes magnéticos.

CONTROLES DE ENTRADA DE DATOS

- Establecer los procedimientos de entrada y control de datos, que explican las revisiones necesarias de entradas y salidas, con fecha limite, criterios de validación de datos de entrada; códigos, mensajes y detección de errores; la corrección de errores y la reentrada de datos.
- Para sistemas interactivos, verificar el uso de métodos preventivos para evitar la entrada incorrecta de datos funciones de ayuda a la pantalla, formatos fijos, el uso de menús y mensajes para el operador.
- Para sistemas interactivos, determinar la grabación de datos de entrada con fecha y hora actual, así como con una identificación del usuario/terminal y ubicación.
- Revisar los logs de acceso por lineas de telecomunicaciones para determinar posibles accesos y entradas no autorizados.
- Revisar los programas para determinar si contienen procesos internos de validación de datos (por ejemplo chequeos de dígitos, test razonables, número de cuentas, etc.). Evaluar su exactitud.
- Comparar, validar, apuntar y recalcular campos o elementos de datos críticos, por métodos manuales o automáticos.
- Para sistemas interactivos, determinar que los datos se verifican al momento de su entrada en el sistema.
- Comprobar que los usuarios revisan regularmente las tablas internas del sistema para validar sus contenidos.
- Revisar funciones matemáticas que redondean cálculos para ver si tienen implicaciones negativas.
- Determinar que existen pistas de auditoria adecuadas en el diccionario de datos. Identificar la interrelación entre los programas y los datos para dejar la posibilidad de seguir la pista de datos dentro de programas y sistemas errores.
- Revisar los procedimientos de corrección de errores.
- Identificar con los usuarios cualquier código de errores críticos que deberían aparecer en momentos específicos, pero que nunca surgen¿Se han desactivado los códigos o mensajes de error?

CONTROLES DE TRATAMIENTO Y ACTUALIZACIÓN DE DATOS

- Ver si hay establecidos controles internos automatizados de proceso, tales como rutinas de validación, al momento de la actualización de los ficheros de transacción, referencia y maestro.
- Identificación de transacciones por códigos de transacción y otros indicadores.
- Revisión del log de transacciones para identificar problemas encontrados por el operador y las medidas seguidas.
- Restricción de la posibilidad de pasar por encima de procesos de validación.
- Aceptación por los usuarios finales de todas las transacciones y cálculos de la aplicación.
- Revisar los totales de control de entrada de datos.
- Verificar que existen totales de control para confirmar la buena interface entre tareas o programas.
- Comprobar que existen validaciones entre totales de control, manuales y automáticos, en puntos del interface entre procesos manuales y automatizados.
- Verificar que los logs de actividad de sistemas se revisan por los responsables operacionales para investigar accesos y manipulaciones no autorizados.
- Ver los controles sobre la entrada de datos.

CONTROLES DE SALIDAS DE DATOS

- Determinar si los usuarios comparan totales de control de los datos de entrada con totales control de datos de salida.
- Determinar si control de datos revisa los informes de salida (listados) para detectar errores evidentes tales como: campos de datos que faltan, valores no razonables o formatos incorrectos.
- Verificar que se hace una identificación adecuada sobre los informes, por ejemplo nombre y número de informe, fecha de salida, nombre de área/departamento, página y totales y control si son necesarios.
- Comparar la lista de distribución de informes con los usuarios que los reciben en realidad. ¿Hay personas que reciben el informe que no deberían recibirlo?
- Verificar que los informes que pasan de aplicabilidad se destruyen, y que no pasan simplemente a la basura, sin seguridad de destrucción.
- Revisar la justificación de informes, que existe una petición escrita para cada uno y que se utilizan realmente y que está autorizada la petición.
- Verificar la existencia de períodos de retención de informes y su suficiencia.
- Revisar los procedimientos de corrección de los datos de salida.

CONTROLES DE DOCUMENTACIÓN

- Verificar que dentro de las actividades de desarrollo y mantenimiento de

aplicaciones se producen documentación de sistemas, programas, operaciones y funciones y procedimientos de usuario.

- Existencia de un persona específica encargada de la documentación y que mantiene un archivo de documentos ya distribuidos y a qué personas.
- Comprobar que los jefes de área se informen de faltas de documentación adecuada para sus empleados.
- Destrucción de toda la documentación de antiguos sistemas
- Que no se aceptan nuevas aplicaciones por los usuarios sin una documentación completa.
- Actualización de la documentación al mismo tiempo que los cambios y modificaciones en los sistemas.
- La existencia de documentación de sistemas, de programas. de operación y de usuario para cada aplicación ya implantada.

CONTROLES DE BACKUP Y REARRANQUE

- Existencia de procedimientos de backup y rcarranquc documentados y comprobados para cada aplicación en uso actualmente.
- Procedimientos escritos para la transferencia de materiales y documentos de backup entre el C.P.D. principal y el sitio de backup (centro altemativo). Mantenimiento de un inventario de estos materiales.
- Existencia de un plan de contingencia.
- Identificación de aplicaciones y ficheros de datos críticos para el plan de contingencia.
- Revisar los contratos del plan de contingencia y backup para determinar su adecuación y actualización.
- Pruebas de aplicaciones criticas en el entorno de backup, con los materiales del plan de contingencia (soportes magnéticos, documentación, personal, etc.).
- Determinación de cada aplicación que se revisa si es un sistema crítico y debería incluirse en el plan de contingencia.
- Grabación de todas las transacciones ejecutadas por teleproceso, cada día; para facilitar la reconstrucción de ficheros actualizados durante el dia en caso de fallo del sistema.
- Existencia de procesos manuales para sistemas criticos en el caso del fallo de contingencia.
- Actualización del plan de contingencia cuando es necesario; pruebas anuales.

CONTROLES SOBRE PROGRAMAS DE AUDITORÍA

- Distribución de políticas y procedimientos escritos a auditores y responsable de áreas sobre la adquisición. desarrollo y uso de software de auditoria.
- Uso de software de auditoria únicamente por personas autorizadas.
- Participación del auditor en la adquisición, modificación/adaptación, instalación de paquetes de software de auditoría.
- Participación por el auditor en la planificación, diseño, desarrollo e

implantación de software de auditoria desarrollado internamente.

- Formación apropiada para los auditores que manejan software de auditoría.
- Participación por el auditor en todas las modificaciones y adaptaciones del software de auditoría, que sea de fuera o propio. Acrualización de la documentación de software.
- Verificación de que los programas de utilidad se utilizan correctamente (cuando no se puede utilizar el software de auditoria auditoria).
- Revisión de tablas de contraseñas para asegurar que no se guardan identificaciones y contraseñas de personas que han causado baja.

CONTROLES DE LA SATISFACCIÓN DE LOS USUARIOS

- Disponibilidad de políticas y procedimientos sobre el acceso y uso de la información.
- Resultados fiables, completos, puntuales y exactos de las aplicaciones
- (integridad de datos).
- Utilidad de la información de salida de la aplicación en la toma de decisión por los usuarios.
- Comprensión por los usuarios de los informes e informaciones de salida de las aplicaciones.
- Satisfacción de los usuarios con la información que produce la aplicación.
- Revisión de los controles de recepción. archivo. protección y acceso de datos guardados sobre todo tipo de soporte.
- Participación activa de los usuarios en la elaboración de requerimientos de usuarios, especificaciones de diseno de programas y revisión de resultados de pruebas.
- Controles por el usuario en la transferencia de informaciones por intercambio de documentos.
- Resolución fácil de problemas, errores, irregularidades y omisiones por buenos contactos entre usuarios y el personal del C.P.D.
- Revisiones regulares de procesos que podrían mejorarse por automatización de aspectos paniculares o reforzamientos de procesos manuales.

4.3.1.3 Informes

Las recomendaciones son razonables, verificables, interesantes económicamente y tienen en cuenta el tamaño de la organización.

Para ser efectivo, el informe da crédito al personal del área revisado cuando se corrigen por ellos debilidades encontradas.

El informe tiene un tono constructivo. Si es apropiado se anotan los puntos fuertes.

El lenguaje utilizado debería contener un mínimo de términos técnicos. No tardarán más que cuatro semanas como máximo, después de las visitas al área revisada.

Para su distribución, se preparará un resumen del informe.

Después de la revisión del informe final con los responsables del área revisada se distribuirá a las otras personas autorizadas.

El área tiene la posibilidad de aceptar o rechazar cada punto de control. Todos los puntos rechazados se explicarán por escrito. El área acepta los riesgos implícitos de la debilidad encontrada por el auditor.

Se hace un seguimiento de la implantación de fas recomendaciones, para asegurarse que el trabajo de revisión produce resultados concretos.

4.4 EL PLAN AUDITOR INFORMÁTICO

Es el esquema metodológico más importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que realiza en la entidad. Debe estar en sintonía con el plan auditor del resto de los auditores de la entidad.

Las partes de un plan auditor informático deben ser al menos fas siguientes:

- Funciones. Ubicación de la figura en el organigrama de la empresa.
- Debe existir una clara segregación de funciones con la Inforrnática y de control interno informático y esté debe ser auditado así mismo. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.
- Procedimientos para las distintas tareas de fas auditorias. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoria, redacción de informe final, etc.
- Tipos de auditorias que realiza. Metodologías y cuestionarios de las mismas. Ejemplo: revisión de la aplicación de facturación, revisión de fa LOPD, revisión de seguridad fisica, revisión de control interno, etc. Existen tres tipos de auditorías según su alcance, fa Full o completa de una área (ejemplo: control interno, informática), limitada a un aspecto (ejemplo: una aplicación, la seguridad lógica, el software de base, etc.), la Corrective Action Review (CAR) que es la comprobación de acciones correctivas de auditorias anteriores.
- Sistema de evaluación y los distintos aspectos que evalúa.
- Independientemente de que exista un plan de acciones en el informe final, debe hacerse el esfuerzo de definir varios aspectos a evaluar como nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc. y realizar una evaluación global de

resumen para toda la auditoría. Esta evaluación en nuestro país suele hacerse en tres niveles que son "Bien, Regular, o Mal", significando la visión de grado de gravedad. Esta evaluación final nos servirá para definir la fecha de repetición de la misma auditoría en el futuro según el nivel de exposición que se le haya dado a este tipo de auditoria en cuestión. (Véase figura 3.8).

- Nivel de exposición. Como ejemplo podemos ver la figura 3.8. El nivel de exposición es en este caso un número del uno al diez definido subjetivamente y que me permite en base a la evaluación final de fa última auditoria realizada sobre ese tema definir la fecha de la repetición de la misma auditoria. Este número no conviene confundirlo con ninguno de los parámetros utilizados en el análisis de riesgos que está enfocado a probabilidad de ocurrencia. En este caso el valor del nivel de exposición significa la suma de factores como impacto, peso del área, situación de control en el área. O sea se puede incluso rebajar el nivel de un área auditada porque está muy bien y no merece la pena revisarla tan a menudo. Lista de distribución de informes.

- Seguimiento de las acciones correctoras.

- Plan quinquenal. Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación además de las repeticiones y añadido de las auditorias no programadas que se estimen oportunas deberán componer anualmente el plan de trabajo anual.

- Plan de trabajo anual. Deben estimarse tiempos de manera racional y componer un calendario que una vez terminado me dará un resultado de horas de trabajo previstas y por tanto los recursos que se necesitarán.

- Debemos hacer notar que es interesante tener una herramienta programada con metodología abierta que permita confeccionar los cuestionarios de las distintas auditorías y fácilmente cubrir los hitos y fases de los programas de trabajo una vez definida la metodología completa. Esto se puede hacer sin dificultad con cualquier herramienta potente que existe en la actualidad.

- Las metodologías de auditoria informática son del tipo cualitativo/subjetivo. Podemos decir que son las subjetivas por excelencia. Por tanto están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continuada. Sólo asi esta función se consolidará en las entidades, esto es, por el "respeto profesional" a los que ejercen la función.

Ciclo	Nivel de Exposición	Evaluación	Frecuencia/Visitas
1	10-9	B	18 meses
		R	9 meses
		M	6 meses
2	8-7	B	18 meses
		R	9 meses
		M	6 meses
3	6-5	B	24 meses
		R	18 meses
		M	12 meses
4	4-1	B	36 meses
		R	24 meses
		M	18 meses

Figura 3.8. Ciclo de auditorí

4.5 CONCLUSIONES

Son muchas pues las metodologías que se pueden encontrar en el mundo de la auditoría informática y control interno. Muchas las hemos visto en este capítulo. Pero como resumen se podría decir que la metodología es el fruto del nivel profesional de cada uno y su visión de cómo conseguir un mejor resultado en el nivel de control de cada entidad, aunque el nivel de control resultante debe ser similar.

Pero en realidad todas ellas son herramientas de trabajo, mejores o peores, que ayudan a conseguir mejores resultados. Sólo resta animar a los profesionales que lean este libro a trabajar con las únicas herramientas verdaderas de la auditoria y el control... "la actitud y la aptitud", con una actitud vigilante y una formación continuada.

4.6 LECTURAS RECOMENDADAS

Jim A. Schweitzer. Administración de la seguridad de la información (Administrativo. Electrónico y Medidas Legales e Información Comercial del Proyecto). Traseros. ISBN0-409-90195-4.J.M. l-anvctc. La Seguridad Informática (Metodología). Ediciones Arcadia.ISBN 84-86299-13-6.J.M. Lamere. La securité des petits et moyens systèmes informatiques. Dunodinformática. ISBN 2-04-018721-9.yo. M. Lamere. Y. l-eroux, J. Orly. La securité des rescata (Métodos* et técnicas). Dunod informatique. ISBN 2-01-018886-X.

4.7 CUESTIONARIO

1. ¿Qué diferencias y similitud» existen entre las metodologías cualitativas y las cuantitativas? ¿Qué ventajas y qué inconvenientes tienen?

2. ¿Cuáles son los componentes de una contra medida o control ipirimide de la seguridad)? ¿Qué papel desempeñan las herramientas de control? ¿Cuáles son las herramientas de control m is frecuentes?

3. ¿Qué tipos de metodologías de Plan de Contingencias existen? ¿En qué se diferencian? ¿Qué es un Plan de Contingencias?

4. ¿Qué metodologías de auditoria informática existen? ¿Para qué se usa cada una?

5. ¿Qué es el nivel de exposición y para qué sirve?

6. ¿Qué diferencias existen entre las figuras de auditoría informática y control interno informático? ¿Cuáles son las funciones más importantes de éste?

7. ¿Cuáles son las dos metodologías más importantes para el control interno informático? ¿Para qué sirve cada una?

8. ¿Qué papel tienen las herramientas de control en los controles?

9. ¿Cuáles son los objetivos de control en el acceso lógico?

10. ¿Qué es la certificación de seguridad? ¿Que aporta la ISO 17799? ¿Qué metodologías se utilizan en el desarrollo de un SGSJ?

TERCERA PARTE: 3. AUDITORÍA DE ORGANIZACIÓN Y ADMINISTRACIÓN DEL AMBIENTE INFORMÁTICO

CAPITULO 5

EL DEPARTAMENTO DE AUDITORÍA DE LOS SI: ORGANIZACIONES Y FUNCIONES

5.1 INTRODUCCIÓN

El presente capítulo del libro pretende mostrar al lector cuáles son las responsabilidades de un Departamento de Auditoría de los Sistemas de Información (en adelante SI), así como aspectos clave para poder desarrollar dichas responsabilidades dentro de una Organización, sea tanto una Institución pública (Universidad, Hospital, etc.), una empresa pública o privada. e independientemente de su tamaño, diversidad geográfica u objeto social. Por tanto, un aspecto clave para el entendimiento del presente capitulo es la consideración de la función de auditoría de SI dentro de una entidad como una parte de la función de auditoría interna de dicha entidad, y algunas consideraciones las abordaremos desde la óptica de esta última función.

El capítulo está estructurado siguiendo las etapas cronológicas desde la creación de un departamento de Auditoria de los SI, a saber:

- Establecimiento de la Misión y Responsabilidades del Departamento de Auditoria de los SI.
- Definición de la Organización del Departamento de Auditoría de los SI.
- Elaboración de los planes de trabajo del Departamento de Auditoría de los SI.
- Establecimiento de una metodología para la ejecución de los trabajos de Auditoría de los SI.
- Y finalmente abordaremos cuestiones relativas a los recursos humanos que componen el Departamento de Auditoria de los SI.

Como podrá comprobar el lector, el enfoque dado a este capítulo pretende ser sumamente práctico e intentará ayudarle para el establecimiento de un Departamento de Auditoria de los SI en su Organización. Nos apoyaremos en otros capítulos del presente libro donde se definen y detallan técnicas para la elaboración de procesos y actividades que a lo largo del presente capitulo establecemos como tareas a desarrollar por un Departamento de Auditoria de los SI.

Consideramos a lo largo de las siguientes páginas al Departamento de Auditoria de los SI como una Unidad interna dentro de la organización, y la exposición parte, por tanto, de este punto de partida. Se indica esta premisa porque es posible que la función 0 labor de auditar los Sistemas de Información de una organización se realice a través de personal externo especialmente contratado para tal fin, sin la necesidad de mantener

un Departamento específico para acometer dicha función.

Casi siempre cuando se manejan diferentes alternativas, cada una de ellas presenta ventajas e inconvenientes respecto a las demás. No es objeto del presente capitulo identificar u opinar acerca de los beneficios de dotar a la organización de un departamento interno que audite los SI, o sobre la opción de ejecutar dicha función externamente a través de consultoras especializadas. LO considero un apasionante debate, pero no es el objeto del presente capítulo.

5.2 MISIÓN DEL DEPARTAMENTO DE AUDITORÍA DE LOS SI

La Misión principal de la función de auditoría de los SI es proveer a los órganos de gobierno y a los de gestión de una organización de una seguridad razonable que los sistemas de control interno de los recursos de información de dicha organización están bien definidos y efectivamente administrados, y que apoyan y ayudan a la creación de valor de la organización.

Embebida en la definición de la misión hemos deslizado tres aspectos importantes:

- Para quién desarrolla su labor la función de auditoría de SI órganos de gobierno y a los de gestión...).
- Qué debe realizar (... que los sistemas de control interno...).
- Sobre qué debe actuar (… recursos de información...).

Dichos conceptos son importantes de entender para llegar a delimitar en su totalidad la misión de la función de auditoría de SI. Dedicaremos un breve espacio para ello, no obstante, en la bibliografía puede el lector encontrar textos que profundizan sobre los aspectos que a continuación trataremos y sobre otros relacionados. Animo al lector a su lectura.

Comenzando con la definición de la misión encontramos que la función de la auditoría de SI es proveer a los órganos de gobierno y a los de gestión de una organización. Nos encontramos por tanto con una primera clasificación, característica o catalogación sobre las funciones que administran y dirigen una organización y, como veremos en el próximo capítulo, para la función de auditoria es muy importante diferenciarlas.

Comencemos definiendo a los órganos de gobierno. que podemos establecer como los Órganos colegiados que dirigen la marcha de una empresa supervisando y guiando la actuación de la dirección. Son los responsables de establecer las metas, objetivos y las políticas, y se suelen plasmar en el Consejo de Administración.

Los órganos de gestión o dirección de una organización son los responsables de las diferentes unidades de negocio o soporte que existen dentro de la organización, y que se suelen plasmar en un Comité de Dirección bajo la responsabilidad de un director general.

Prosiguiendo la definición establecida de la misión podemos leer de los sistemas de control interno..., en este punto he de indicarle al lector que intentar resumir en un

breve texto una explicación relativa al control interno es tarea harto complicada y que existe, como ya hemos mencionado, abundante literatura al respecto. No obstante, vamos a describir algunos puntos importantes.

El informe COSO del "Committee of Sponsoring Organizations" en su primera versión define el control interno de la siguiente manera:

"El control interno es un proceso, ejercido por el consejo de administración de la entidad, los gestores y otro personal de la organización, diseñado para proporcionar seguridad razonable respecto a la consecución de los objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento con leyes y regulaciones.

Ahondemos sobre esta definición y resaltemos algunos aspectos importantes:

Establece que el control interno es un proceso, por tanto, es algo que sucede y evoluciona con el tiempo persiguiendo un fin, por tanto, es un medio para conseguir un fin no un fin en sí mismo.

- Que es ejecutado por toda la organización en su conjunto, desde los máximos órganos de dirección o administración hasta los niveles operativos. Por tanto, involucra y responsabiliza a todo el personal de la organización.
- Indica que se ejecuta por las personas. es por tanto una acción continuada y no un conjunto de políticas, normas o buenas prácticas.
- Cuyo fin es proporcionar seguridad razonable, nunca absoluta, para facilitar la consecución de los objetivos de la organización (aquello para 10 que existe).

Ahora bien, como establecemos en la propia definición de la misión de la auditoria de SI, ésta se circunscribe a los recursos de información de la organización. Intentemos definir con mayor claridad este punto.

Intuitivamente podemos establecer que los recursos de información son todos aquellos activos que necesita utilizar la organización para poder dotarse de adecuados sistemas de información que soporten sus procesos operativos o de negocio, así como para transmitir y sintetizar información hacia sus órganos de gestión y administración, hacia reguladores externos, accionistas, empleados, proveedores y público en general.

Intentemos desglosar dichos activos (ver figura 5.1):

- **Datos;** obviamente la información está compuesta por cientos, miles, millones tal vez, de datos, que combinándose de forma lógica y estructura producen la información. Por tanto, los datos son los "átomos" de la información.
- **Software de Aplicaciones**; los datos para combinarse y estructurarse necesitan aplicaciones que los presenten de forma lógica y entendible para sus usuarios, de forma que dichos datos aporten información al usuario de dicha aplicación.

- **Tecnología;** para poder desarrollar y ejecutar las aplicaciones de software la organización necesita contar con activos de hardware y software de base, así como redes de comunicación, sobre los que construirlos y operarlos.
- **Instalaciones;** se debe contar con ubicaciones físicas donde alojar la tecnología que necesita la organización.
- **Personas;** lógicamente todos los activos anteriores no pueden ser explotados y ejecutados sin la necesaria participación de recursos humanos especializados en estas labores.

Acabamos por tanto de establecer la misión de la función o departamento de auditoría de los SI, y a partir de ella desarrollaremos los aspectos o atributos que dicha función o departamento debe contener para conseguir su fin.

Figura 5.1. Recursos de información

5.3 ORGANIZACIÓN DEL DEPARTAMENTO DE AUDITORÍA DE LOS SI

Una vez definida la misión vamos a establecer cuáles son los objetivos y las funciones y/o responsabilidades de la función 0 departamento de auditoría de los SI, que podemos explicitar de la siguiente forma:

5.3.1 Objetivos

Podemos destacar:

- Revisar la existencia y suficiencia de los controles de los Recursos de Información que soportan los procesos de negocio.
- Validar que los Recursos de Información apoyan los objetivos de negocio y cumplen los requerimientos establecidos.
- Analizar los nuevos riesgos derivados de las nuevas tecnologías y de los nuevos negocios.
- Formar y divulgar respecto de los riesgos y amenazas que se derivan de una inadecuada utilización de los Recursos de Información.

Los dos primeros apartados de los objetivos están claramente alineados con la misión de evaluar el control interno de los recursos de información, mientras que los dos últimos apartados se focalizan más en el rol de apoyo y consejo que la función de auditoría de los SI debe aportar a la organización, en especial a sus órganos de gobierno

y de dirección.

Por tanto, es importante notar esa doble vertiente que debe ejecutar la función de auditoría de SI, por una parte:

- Revisar, evaluar y validar que el control interno de los recursos de información es adecuado y apoya los objetivos del negocio. Un objetivo sobre lo que la organización ya tiene establecido, ya ejecuta, y cuyo fin es mejorarlo.

Y por otra:

- Identificar nuevos riesgos relativos a las tecnologías de la información, difundiendo y sensibilizando a la organización para que los mitigue de forma adecuada. Un objetivo sobre lo que acontece y acontecerá en relación a las tecnologías de la información, y cuyo fin es estar preparado.

5.3.2 Ubicación en la Organización

Revisando la misión que exponíamos en el apartado anterior podemos establecer que, dado que el auditor de SI debe revisar el control interno de los recursos de información y ésta afecta a toda la organización, debe por tanto ubicarse en un punto del organigrama de la organización que le dote de total independencia del resto de unidades, y además de suficiente autoridad para poder ejercer su labor.

Es por ello que la función de auditoría de SI no puede en modo alguno estar incluida en el departamento de Sistemas de Información de una compañía, puesto que le limitaría claramente su independencia en la ejecución de sus trabajos de auditoria al tener que estar evaluando procesos que están bajo la responsabilidad del cargo al que a su vez también reportaría el departamento de auditoría de SI.

Desgraciadamente en diferentes organizaciones nos encontramos con este hecho que limita totalmente el trabajo del auditor, e impide que todo el valor que puede, y debe aportar a la organización, se desarrolle completamente.

La ubicación de la función de auditoría de los SI dentro de una organización debe estar englobada con la función de la auditoría interna de dicha organización. En la actualidad existen normativas, tanto nacionales como internacionales, así como buenas prácticas de gobierno corporativo, que establecen y/o recomiendan la posición y el rol que debe tener la función de auditoría interna en una organización, que podríamos esquematizar según se muestra en la figura 5.2.

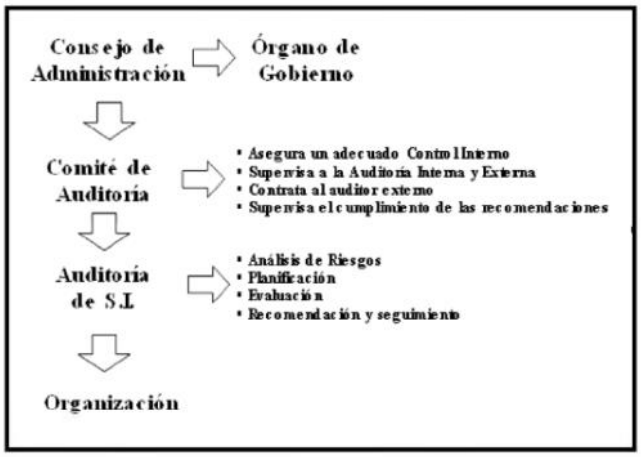

Figura 5.2. Posición de la auditoria de SI

Y que establecen o recomiendan que:

- La función de auditoría interna es un órgano dependiente del Consejo de Administración, a través del Comité de Auditoría por delegación, que tiene la responsabilidad de supervisar, controlar y designar al responsable de la función.

- El personal de auditoría interna no asumirá responsabilidades operativas. y actuará con independencia de criterio respecto a las otras unidades de la organización.

- La función de auditoría interna tenga total acceso a los registros, archivos, documentos y fuentes de información de la organización necesarios para el adecuado ejercicio de su labor.

Esquemáticamente la posición adecuada de la unidad de auditoría interna en el organigrama de una organización se muestra en la figura 5.3.

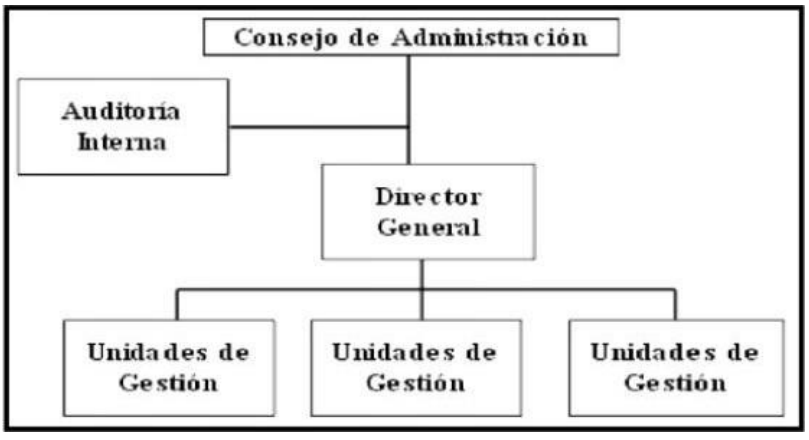

Figura 5.3. Posición de la unidad de auditoría interna en la organización

5.3.3 Recursos necesarios

para poder desarrollar su función el departamento de auditoría de SI debe contar con los recursos suficientes„ los cuales podemos clasificarlos en:

- Recursos Humanos. Personal de la unidad para desarrollar la misión definida al departamento. Parte de este aspecto lo trataremos en este apartado, la relacionada con la organización y localización de las personas, y Otra parte, la que se corresponde con su perfil profesional, en el apartado 7.6.
- Recursos técnicos. Son los recursos necesarios para que el personal del departamento de auditoría de SI puedan desarrollar eficaz y eficientemente su labor. Básicamente estarán relacionados Con sistemas o herramientas de información.
- Recursos económicos- los cuales deberán ser presentados y aprobados por el Comité de Auditoría.

De estos tres tipos no cabe duda que el más crítico es el primero, los recursos humanos, el personal que forma parte del departamento de auditoría de SI y desarrolla sus tareas. Las labores realizadas por un auditor no pueden ser sustituidas por ninguna herramienta ni tecnología. Si bien éstas últimas pueden mejorar y hacer más eficiente el trabajo de un auditor. el trabajo de auditoria descansa de forma casi absoluta y completa en la labor de los auditores.

Como veremos en los siguientes apartados, el auditor debe entender el entorno o proceso que está analizando, identificar sus aspectos clave, evaluar el diseño establecido, probar si los controles existentes operan satisfactoriamente y finalmente informar sobre sus hallazgos. En todo este proceso, y para algunas tareas más que veremos que desarrolla la función de la auditoria de SI, el recurso humano es difícilmente sustituible.

Por tanto, el aspecto clave para conseguir un buen departamento de auditoría de SI es dotarlo de miembros preparados y cualificados para tal fin. Este punto lo desarrollaremos en el apartado 5.6.

5.3.4 Estructura del departamento de auditoría de SI

Para dimensionar y estructurar el departamento de auditoría de SI debemos lógicamente tomar parámetros de la organización donde dicho departamento estará inmerso. Algunos de los parámetros clave son:

- Tamaño de la organización; no principalmente en su vertiente de plantilla de trabajadores ni en volumen de negocio o ventas, sino en su faceta de diversidad de procesos de negocio que desarrolla, diversificación de productos o servicios que proporciona. Posiblemente las anteriores variables estén relacionadas, pero es importante focalizarse en la última.
- Dependencia; de los negocios de la organización de las TI' posiblemente el parámetro más importante en el análisis que estamos efectuando. Este valor debería estar claramente recogido en el análisis de riesgos que sería deseable realizara la organización.

- Tecnología de los Sistemas de Información: debemos considerar el grado de centralización/descentralización de los Sistemas, las diferentes tecnologías usadas, número y localización d importancia de los procesos externalizados.
- Ubicación geográfica; localización geográfica de los diferentes centros productivos o de gestión de la entidad, y su importancia relativa en los procesos de negocio.

Al menos estos cuatro parámetros nos ayudarán a establecer dos aspectos clave de la estructura del departamento de auditoría de SI:

- Dimensión del departamento: número de personas que deben formar parte de ella.
- Localización del departamento; lugares físicos donde contar con recursos del departamento.

Lógicamente cada Organización es diferente a las demás, independientemente que operen en el mismo sector o región, por tanto, es sumamente difícil poder aportar estándares a esas dos cuestiones. Cada entidad debe analizar su propia organización y valorar cómo y dónde establecer la función de auditoría de SI. Una actitud prudente sería establecer un plan a diferentes años, con un crecimiento periódico previsto, que permita ir ajustándolo hasta encontrar la dimensión y localización óptima.

Respecto a la dimensión, no cabe duda que ese aspecto está muy relacionado, no solamente a los cuatro parámetros anteriormente descritos, sino también a la sensibilidad que los órganos de gobierno y dirección de la organización tengan sobre el control interno.

Referente a la localización resaltar algunas ideas al respecto:

- Es importante que la función de auditoria esté presente en aquellas ubicaciones geográficas que sean importantes para el negocio de la organización. Concentrar totalmente la función de auditoria puede provocar pérdida de conocimiento sobre la realidad de dichas localizaciones.
- La localización de los recursos del departamento de auditoría de SI debe estar alineada con la estructura topológica de los SI de la organización, para de esa forma ser más eficientes en la labor de auditoría,
- Los aspectos relacionados con la metodología y herramientas con las que acometer los trabajos de auditoría de SI deben ser únicos y por tanto pueden ser definidos y gestionados desde una única ubicación.

Otros aspectos de interés para evaluar cada alternativa son:

- Interés en mantener una mayor proximidad con los gestores de cada empresa.
- Política interna de distribución de costes.
- Grado de especialización de cada negocio con el consiguiente efecto en el perfil de conocimientos de los auditores que los revisan.

5.3.5 El Estatuto de auditoría de SI

Para poder desarrollar la misión y funciones definidas al departamento de auditoría de

SI ésta debe contar con un Estatuto o marco normativo que básicamente le proporcione sobre toda la organización e independencia de sus órganos de gestión y dirección. Estos dos atributos son esenciales para el correcto y adecuado desempeño de las labores que debe desarrollar un auditor de sistemas, y su inexistencia puede hacer fracasar la función de auditoría de los SI o limitarla de tal forma que puede que su actividad no tenga sentido dentro de la organización.

Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna establecen que "El propósito, la autoridad y la responsabilidad de la actividad de la auditoría interna deben estar formalmente definidos en un Estatuto el cual debe estar aprobado por el Consejo de Administración de la organización.

En el Estatuto se debe establecer la posición de la función de auditoría interna dentro de la organización, autorizar el acceso a toda la información de la Organización necesaria y relevante para el ejercicio de su función y establecer el alcance o ámbito de actuación de la auditoría interna. Debe especificarse que en el ejercicio de sus funciones actúa por delegación del Consejo y del Comité de Auditoría.

El Estatuto debe ser público dentro de la organización y suficientemente divulgado entre los miembros de la dirección para garantizar el entendimiento de la labor y así como las responsabilidades de la auditoría interna, y para promover su adecuada y necesaria colaboración.

Por tanto, una de las primeras labores a acometer por quien desee implantar una función de auditoría de SI es elaborar un Estatuto en consonancia con lo que aconsejan las Normas Internacionales para el Ejercicio Profesional de la Auditoria.

Nótese que como ya hemos indicado, y recomendado anteriormente, en la gran mayoría de los casos el departamento de auditoría de SI estará englobado en la Unidad de Auditoría Interna y por tanto su Estatuto será el mismo para ambos.

5.3.6 Referencias sobre la función de auditoría de SI

Terminaremos el apartado 3 con una serie de referencias relativas a la función de auditoría de SI que aporten al lector datos comparativos.

El GAIN del año 2007 expone que un 65% de las empresas encuestadas contaban con un departamento o grupo de auditoría de SI. Desgraciadamente en España, según el estudio realizado por KPMG, ISACA[80] Capitulo de Madrid y el IA1[81] durante el año 2005, únicamente el 33% informaban sobre la existencia de dicha función. El GAIN 2007 muestra que el 96% de los departamentos de auditoría de SI están inmersos dentro de la unidad de auditoría interna.

El ll Estudio sobre la situación de la Auditoría Interna en España de la firma KPMG emitido en 2005 indica que, para las empresas encuestadas, el promedio de la ratio de nº auditores internos'n^0 empleados es de 0,22% y el informe GAIN 2007 que el porcentaje de auditores informáticos es del 18% del total de auditores internos. Este último indica que el de la actividad de auditoría de SI es contratada externamente a firmas especializadas.

5.4 PLANIFICACIÓN DEL TRABAJO DE AUDITORÍA DE SI

Para llevar a cabo la misión definida al departamento de auditoría de SI hemos de evaluar el sistema de control interno de los recursos de información de la organización, y esta tarea la realizaremos a través de evaluaciones o revisiones de auditoría. Por tanto, la labor principal, y a la que está destinada la práctica totalidad de la plantilla del departamento de auditoría de SI, es a la realización de trabajos de auditoría. Para poder establecer cuáles son los trabajos a realizar. asi como criterios para su priorización, debemos contar con alguna metodología que nos guíe.

En los siguientes apartados vamos a indicar un método para acometer esta labor, se muestra en la figura 5.4.

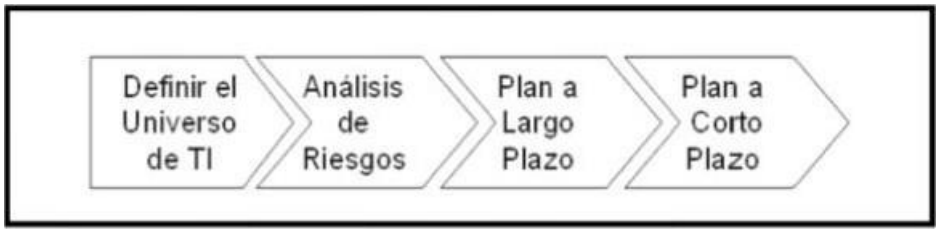

Figura 5.4. Planificación de trabajo de auditoría de SI

5.4.1 Definir el Universo de TI

El primer reto que debemos afrontar para efectuar una planificación de trabajos de auditoría es la de establecer qué se debe auditar. Poder enmarcarlo, acotarlo y definirlo es condición necesaria para elaborar posteriormente el plan. Seguramente esta es la labor más compleja y está marcada por dos casuísticas:

- La total integración de los sistemas de información en los procesos operativos de las organizaciones. Este hecho provoca que determinar dónde termina el proceso puramente operativo y dónde comienza el proceso informático sea totalmente imposible.
- La heterogeneidad de las TI de cada organización los convierte en únicos, es lo que las guías GTAG llaman "el efecto copo de nieve". LO cual provoca que difícilmente dos organizaciones cuenten con universos de TI homólogos.

Como indicamos la misión de la función de la auditoria de SI es evaluar el sistema de control interno de los recursos de información de una organización, los cuales ya habíamos desglosado en:

- Datos
- Software de Aplicaciones
- Tecnología
- Instalaciones
- Personas

Por tanto, ya tenemos un primer nivel de detalle que puede ayudar a establecer el universo de TI en cada organización.

Otra forma de abordar este problema es considerando. no sólo los recursos de información, sino también los procesos operativos que son necesarios para que dichos recursos provean de información a la organización, siguiendo la metodología COBIT y tal y como se muestra en la figura 5.5.

En donde, además de considerar los recursos de TI, se tiene en cuenta que es necesario ejecutar los siguientes procesos para aportar adecuados SI a la organización:

- Planificación y Organización.
- Desarrollar, implantar y mantener aplicaciones.
- Explotación y soporte.
- Supervisión y control.

Otra forma de abordar el problema es acudir a las guías GTAG que establecen de una forma muy simple y esquemática los siguientes niveles para un entorno de Tl:

- La dirección de TI.
- La infraestructura técnica.
- Las aplicaciones.
- Las conexiones externas

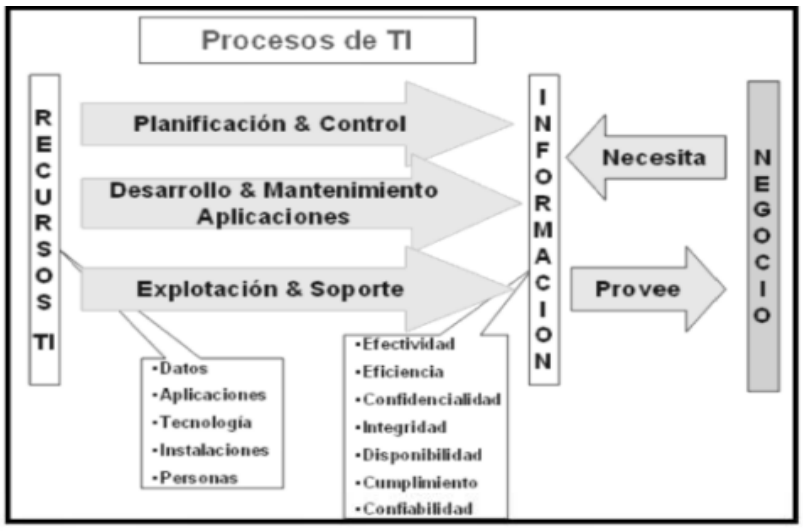

Figura 5.5. Procesos de TI

Que si bien simplifica enormemente el universo de Tl Si puede servir de punto de partida para su definición en organizaciones pequeñas y poco complejas.

La forma por tanto de acometer este primer paso será muy específica en cada organización.

5.4.2 Análisis de Riesgos

El siguiente paso una vez se tiene definido y catalogado el universo de TI Objeto de auditoría, es establecer una medida de importancia relativa de cada uno de los elementos de dicho universo, en relación a los riesgos de cada uno de los ítems de dicho universo. Para ello la técnica propuesta es realizar un análisis de riesgos de cada

elemento mediante una metodología de análisis de riesgos de TI.

No es objeto del presente capitulo mostrar las diferentes metodologías existentes. puesto que tal fin podría ser objeto, no sólo de un capítulo entero, sino tal vez de un libro. Por tanto, en este punto únicamente quiero trasladar algunos aspectos que considero de interés.

Es fundamental que en el momento de abordar esta tarea se Obtenga información de la organización relativa a su propio análisis de riesgos. Sería deseable que los órganos de gobierno y de gestión de la organización hayan elaborado su propio mapa de riesgos de toda la entidad. Dicho mapa seria, indudablemente, la primigenia fuente de información en este proceso. Desgraciadamente pocas organizaciones cuentan con dicho análisis, o en su defecto con unidades que aglutinen la información relativa a gestión de riesgos regada en sus diferentes unidades.

Por ello es frecuente que esta tarea sea realizada directamente por la unidad de auditoría, y si así ocurre es sumamente importante involucrar durante su proceso a todas las unidades gestoras 0 en su defecto contrastar finalmente con ellas los resultados obtenidos.

A la hora de caracterizar riesgos de los elementos del universo de TI es conveniente al menos tener en cuenta dos:

- Riesgo de Negocio: son aquellos que afectan al normal desarrollo de la actividad evaluada. Se pueden clasificar en riegos de entorno (regulatorios, medioambientales, competencia), Operativos (tecnológicos, de ejecución o explotación, financieros), de información (operacional, financiera, estratégica).
- Riesgo de Auditoría; son los relativos al control interno del ítem evaluado. Consideran aspectos relativos a: manejo de fondos, complejidad de la función, cambios recientes, fraude...

Según la metodología especifica de cada organización, o aquella que se haya tomado para desarrollar esta tarea, al final cada ítem del universo de auditoria se habrá catalogado con valores de uno o varios riesgos, pudiendo obtener un mapa de riesgos, tal y como se muestra en la figura 5.6.

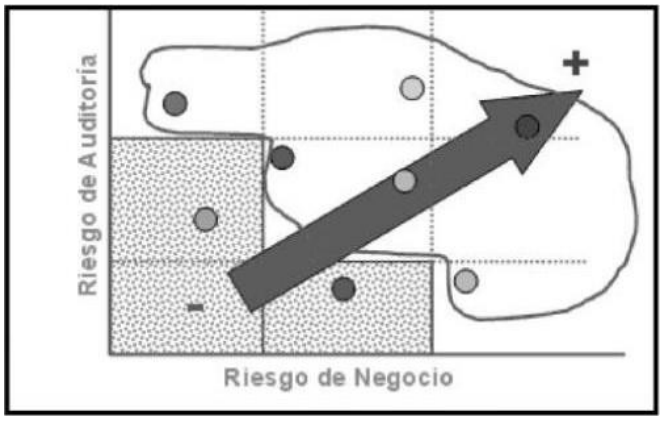

Figura 5.6 Mapa de riesgos

En este mapa esquematizado cada círculo representa un ítem del universo de Tl. y aquellos que se encuentran más cercanos al vértice superior derecho son, lógicamente, lo que tienen mayor riesgo. En el presente esquema hemos mostrado un mapa con dos ejes, pero obviamente se podrían considerar más ejes.

5.4.3 Planificación a Largo Plazo

Una vez establecido el universo de TI, así como determinado cuál es el riesgo de cada elemento de dicho universo (ubicación que ocupa en la matriz de riesgos), el siguiente paso es definir el plan para evaluar si los sistemas de control establecidos en la organización son adecuados y suficientes para mitigar los riesgos identificados.

Para ello el primer paso a realizar es establecer para cada ítem del universo de TI cuáles son los trabajos de auditoria necesarios para evaluar si los riesgos establecidos para dicho ítem se mantienen dentro de los umbrales definidos por la organización. Definiendo para cada uno de los trabajos o auditorías cuáles son sus objetivos principales y sobre qué riesgos de los identificados para ese elemento del universo de Tl. Esquemáticamente se muestra en la figura 5.7.

Nótese que un mismo trabajo, en este caso el "trabajo 12", puede evaluar los riesgos de diferentes ítems 0 elementos de nuestro universo de Tl. Lógicamente también un mismo trabajo puede evaluar dos o más riesgos de un mismo ítem o de diferentes ítems, por tanto, nuestro esquema no es más que un método para acercarse al problema.

Universo Tl	Riesgos	Trabajos Auditoría	Objetivos del Trabajo
ítem I	Riesgo I	Trabajo 1 1	……..
	Riesgo 2	Trabajo 12	…….
ítem 2	Riesgo 3	Trabajo 23	
ítem 3	Riesgo 2	Trabajo 12	

Figura 5.7. Conjunto de trabajos de auditoria

Para realizar esta tarea contamos con una herramienta de incalculable valor, que es la metodología COBIT editada por ISACA, que ya se ha introducido en el capítulo 2. En ella para cada uno de los procesos de Tl se establecen objetivos de control de primer y segundo nivel y pautas para su evaluación. Indudablemente COBIT es el instrumento que nos permitirá ir estableciendo nuestra relación de trabajos de auditoría con los

objetivos a evaluar en cada una de ellas. El lector entenderá que no es objeto del presente capitulo explicar el contenido y uso de la metodología COBIT, pero si es importante que la conozca a fondo para realizar esta tarea en su organización.

Al ejecutar esta tarea debemos intentar no atomizar en exceso los trabajos a realizar de forma que la relación de trabajos necesarios a efectuar se convierta en una lista excesivamente detallada que sea de difícil comprensión para el director de Auditoria o para los componentes del Comité de Auditoría que son quienes finalmente deben aprobarla y, sobre todo, apoyarla para que posteriormente se ejecute. Por tanto, mi consejo en este punto es expresar este conjunto de trabajos con términos que se alejen de la jerga tecnológica en la que abundantemente Caemos las personas involucradas directamente con las TI.

Una vez completado este paso tenemos establecido:

- Universo de Tl; diferenciados cada uno de sus elementos.
- Mapa de Riesgos del universo de TI; con una categorización o priorización de los más importantes o críticos.
- Relación de trabajos de auditoría a realizar para evaluar los riesgos identificados.

Si a esta relación de trabajos además de los objetivos de control a evaluar le introducimos más variables, tales como:

- Periodicidad (anual, bienal...).
- Alcance dentro de la organización (todas las filiales, la matriz, las delegaciones; todos los sistemas de negocio, únicamente el económico. que lógicamente dependerá de cómo he establecido el universo de TI,
- Recursos necesarios (horas/hombre, importe económico…)

podremos establecer para un período de tiempo largo cuáles son los trabajos a acometer y los recursos necesarios para abordarlos. Y, si en este punto, introducimos la información relativa a la clasificación del mapa de riesgos confeccionado, podremos establecer además prioridad en esta lista de trabajos, en función de la criticidad o importancia que hayamos establecido al riesgo que evalúa el trabajo.

Ya tenemos por tanto nuestra Planificación de trabajos de auditoría de SI a largo plazo, ordenada por importancia y definido su alcance y necesidad de recursos. Además, podemos evaluar la posibilidad de eliminar del Plan aquellos trabajos necesarios para abordar los riesgos identificados en nuestro mapa como poco importantes (vértice izquierdo inferior del mapa), acotando más el Plan hacia lo más importante. Este último punto debe ser adecuadamente explicado al Comité de Auditoría para recabar su necesaria aprobación.

Uno de los atributos del Plan son los recursos humanos (horas/hombre) necesarios para abordarlo. Este valor nos permitirá tener un criterio para establecer el tamaño 0 dimensión del departamento de auditoría de SI, así como sus posibles localizaciones (centralizado, varias ubicaciones...). pero a dicho valor debernos añadir otro que es el ciclo o duración temporal que quiera establecer a dicho Plan.

La plantilla necesaria variará lógicamente si el Plan se quiere acometer en tres o en cinco años, y por tanto el valor que se le establezca a este parámetro es muy relevante para la definición del tamaño del departamento de auditoría de SI.

Definir el tiempo de ejecución del Plan o ciclo estará marcado por diferentes variables intrínsecas a cada organización, tales como:

- Nivel de control interno de los SI; si es una organización que tiene unos SI maduros con un adecuado control interno. el ciclo será mayor que Otra organización con una unidad de SI de alto crecimiento reciente y menor nivel de control interno.
- Dependencia de la organización de los SI: una entidad cuyos procesos de negocio están muy vehiculados a través de los SI (como puede ser la banca) deberá tener ciclos más breves.
- Tolerancia al riesgo de la Dirección: se establecerán ciclos diferentes en función de la sensibilización y/o tolerancia al riesgo que tengan los miembros de los órganos de gobierno y dirección de cada organización.

Una vez definido el ciclo ya se puede cerrar y establecer la Planificación a Largo Plazo de duración igual a un ciclo.

5.4.4 Planificación a Corto Plazo

Lógicamente la planificación con una visión temporal de un ciclo, que puede variar entre dos, si es muy breve 0 frecuente. 0 cinco años, hay que trocearla en planes más cortos que permitan establecer objetivos en un menor tiempo y mayor flexibilidad para su ejecución.

Un plan a corto plazo puede acotarse a un ciclo entre un año a un trimestre, si bien la mayoría de las empresas suelen realizar sus planes de forma anual (un 70%. frente a un 14% que lo realiza de forma semestral o trimestral)". Y en ella debemos trasladar aquellos trabajos de la Planificación a Largo Plazo pendientes de realizar y que se hayan evaluado más críticos o importantes.

La Planificación a corto plazo define los trabajos a realizar en un período dado de tiempo y por tanto se descompone en diferentes auditorias, cada una de las cuales tiene sus objetivos establecidos, su alcance y los recursos asignados. Materializándose por tanto en la propia ejecución de dichos trabajos de auditoría.

5.5 METODOLOGÍA DEL TRABAJO DE AUDITORÍA DE SI

El objetivo del presente apartado no es establecer uno o varios métodos para abordar y ejecutar los trabajos que debe realizar un auditor de SI. Ese objetivo se cubre principalmente en la parte o sección ll del presente libro, que aportará al lector información sobre las principales áreas de la auditoria informática y esquemas y metodologías para efectuar el trabajo dentro de cada una de ellas.

En cambio, el objetivo del presente apartado es establecer, en base a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, qué aspectos debe

contener la metodología que guía el trabajo del auditor de SI a lo largo de todas sus tareas. Y establecemos como metodología el conjunto de procedimientos y/o guías que definen la forma de realizar una actividad. Por tanto, tampoco vamos a exponer en relación a las herramientas que debe manejar un auditor de SI, aspecto que se trata en el capítulo 9.

Un procedimiento tiene como fin definir los pasos que deben realizarse para ejecutar una tarea, de tal forma que garantice que, independientemente de quien la ejecuta, ésta se realiza de una forma homogénea y conocida de antemano, y facilitando el desempeño de las labores de quien la ejecuta.

Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, tanto en su apartado de Normas sobre Atributos como sobre Desempeño, nos determinan diferentes procedimientos a considerar, incluido el Consejo para la práctica 2040-1 que establece que el responsable de auditoría interna debe establecer políticas y procedimientos para guiar la actividad de la auditoría interna. A continuación, se muestra de forma resumida y esquemática una metodología que da cumplimiento a las Normas Internacionales, pero animo al lector a leer y familiarizarse con dichas Normas.

Una metodología a implantar en un departamento de auditoría de SI podría esquematizarse según se muestra en la figura 5.8:

Figura 8.5. Metodología para implantar en un departamento de auditoria

Veamos que abarca cada una de sus partes:

1. Administración de la actividad de auditoría.

Bajo este epígrafe englobamos todos los aspectos relacionados con la gestión diaria de la función de auditoría de SI que son:

- La Organización de la propia función, que como hemos indicado debe estar materializada a través de su Estatuto. Además del Estatuto puede establecerse en un procedimiento de mayor detalle la forma cómo se organiza el departamento y las funciones o roles de cada uno de sus componentes.
- La información que la función aporta hacia otros órganos de la organización, tales como Cuadros de Mando para el seguimiento diario de la función o

Memorias anuales. Así Como establecer criterios para clasificar la información que se maneja, y dotarla por tanto de adecuadas medidas de seguridad.
- Procedimientos para realizar el control de calidad interno, y el establecimiento de criterios para la elaboración y mejora de procedimientos internos.
- Desarrollo profesional de la plantilla del departamento, evaluación de sus competencias y definición de planes de formación y mejora.

2. Trabajo de auditoría.

En este conjunto de procedimientos agruparíamos aquellos que enmarcan las labores o actividades relacionadas con el desarrollo de un trabajo de auditoría de SI tales como:

- La Planificación del trabajo, en donde se define cómo se analiza el proceso o área a evaluar y el establecimiento del programa de trabajo.
- Desarrollo del trabajo, los cuales establecen entre otras, la forma de documentar el trabajo de auditoria en los papeles de trabajo, los niveles de supervisión y revisión de dichos papeles y la forma de clasificar las pruebas realizadas.
- Resultado del trabajo, procedimientos relacionados con el formato y forma de emisión y distribución de informes, clasificación y catalogación de las debilidades o excepciones encontradas, y asignación de responsabilidades respecto a las recomendaciones emitidas.

Recuerdo por tanto al lector que el objetivo de este apartado no es mostrar métodos o técnicas sobre cómo abordar ciertos trabajos de auditoría, sino cuál es el armazón metodológico o procedimental con el que se debe dotar a un departamento de auditoría de SI para su adecuado funcionamiento.

5.6 EL EQUIPO DE AUDITORÍA DE SI

En el apartado 5.3.3 hacíamos mención sobre la importancia que tiene la plantilla del departamento de auditoría de SI para el correcto desempeño de sus funciones, dado que la propia naturaleza del trabajo de auditoria es eminentemente un trabajo intelectual y en él el aspecto fundamental y diferencial es la competencia de la persona que 10 ejecuta.

Por tanto, es éste un elemento clave para el éxito de la función de la auditoria de SI y como tal se debe considerar. Se ha establecido y diferenciado este apartado con el fin de trasladar al lector el énfasis de la importancia que se le debe dar a este punto cuando estemos estableciendo o potenciando un departamento de auditoría de SI. Si se quiere que esa iniciativa tenga éxito se debe realizar un esfuerzo en dotar a ese departamento de profesionales que estén altamente cualificados y preparados para desempeñar eficazmente la labor de auditores de SI.

Algunos elementos que se deben considerar en el momento de seleccionar al personal que compondrá la unidad de auditoría de SI:

- Formación; si bien muchos de los profesionales con más antigüedad en este ámbito son titulados superiores en especialidades relacionadas con la economía, dada la naturaleza del trabajo del auditor de SI es adecuado que su formación universitaria esté principalmente relacionada con las Tl, tales Como ingeniero informático 0 de telecomunicación.

- Trato con las personas: dado que a menudo la actividad de un auditor es analizar y evaluar actividades realizadas por otras personas de la organización, que además tienen gran experiencia en ello, es muy importante que las personas que realizan los trabajos de auditoría cuenten con las siguientes aptitudes:
  - Sean empáticos, capaces de colocarse en la posición de la persona auditada.
  - Capacidad para escuchar.
  - Capacidad de negociación.
  - Paciente, prudente y flexible.
  - Con capacidad para defender sus puntos de vista.
- Desarrollo del trabajo: un auditor de SI debe ser ordenado, metódico y con gran capacidad de síntesis. Debe saber trabajar en equipo y tener adecuadas habilidades para la redacción de informes y papeles de trabajo.
- honesto y reservado; la especifica tarea de un auditor de SI le obliga a mantener una conducta ética adecuada, cumpliendo el Código de Ética de ISACA si posee la certificación CISA[8,] y mantener una estricta cautela a la hora de divulgar información.

Es importante destacar que, si bien el aspecto de la formación técnica es tal vez necesario de partida para desempeñar la labor de auditor de SI, los otros aspectos seguramente son los que diferencian y provocan que los auditores que las poseen aportan mayor valor en sus trabajos.

Actualmente la única certificación existente en relación a la formación 0 capacidad de un profesional para desempeñar 0 ejecutar labores de auditoría de sistemas es la certificación CISA. Esta certificación es realizada por la ISACA desde el año 1978 y mantiene un gran prestigio. Por tanto, una adecuada política debe ser promover activamente que todos los miembros del departamento de auditoría de SI sean certificados CISA.

Existen otras certificaciones relacionadas con los sistemas de información y con la auditoría tales como:

- CIA: Certified Internal Auditor, promovida por el Institute Internal Auditor, y que posee también un gran reconocimiento para los profesionales que desarrollan su labor en unidades de auditoría interna.
- CISSP: Security Professional certification, promovida por (ISC), relacionada con la seguridad de los sistemas de información.
- CISM: Certified Information Security Manager, promovida por [SACA y también relacionada con la seguridad de los sistemas de información.
- Las relacionadas con los estándares ISO o británicos de seguridad de la información.

Todas ellas mejoran lógicamente las competencias técnicas de un auditor de sistemas.

5.7 CONCLUSIONES

A modo de conclusión de este Capítulo debemos resaltar tres aspectos clave de un departamento de auditoría de SI:

- Debe estar ubicado dentro de la organización en un punto que le dote de la adecuada autoridad e independencia, y contar con un Estatuto aprobado por el Consejo de Administración y suficientemente divulgado que así lo exprese.

- Para su correcto funcionamiento debe contar con un adecuado esquema metodológico que permita ejecutar sus tareas no solamente de forma homogénea sino también de forma eficaz y eficiente.

- La plantilla que compone el departamento es la pieza clave para que éste aporte realmente valor a la organización, y se convierta en asesor de los órganos de gobierno y de dirección de la entidad en relación a los riesgos de las tecnologías de la información.

5.8 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS

Eduardo Hevia Vázquez. Concepto moderno de la auditoría interna, editado por el Instituto de Auditores Internos de España.

Marco para la práctica profesional de la auditoría interna editado por el Instituto de Auditores Internos de España.

Rafael González Marín. Dirección de organizaciones y auditoría interna, editado por el Instituto de Auditores Internos de España.

Pelegrin García Martinez. Organización, administración y planificación de la función de auditoría interna, editado por el Instituto de Auditores Internos de España.

ll Estudio sobre la situación de la auditoría interna en España de la firma KPMG.

I Estudio sobre la función de la auditoría interna de Sistemas de Información en España de la firma KPMG.

Mario Piattini y Fernando Hervada. Gobierno de las tecnologías y los sistemas de información editado por Ra-Ma.

5.9 CUESTIONES DE REPASO

A continuación, exponemos una serie de preguntas tendentes a reflexionar sobre la materia expuesta en este capítulo.

1. Identifique tres aspectos importantes para evaluar y decidir acerca de la ubicación geográfica de un departamento de auditoría de SI dentro de Su organización.
2. Identifique competencias y/o habilidades que deben tener los auditores de SI.
3. Cuál cree el lector que debe ser la ubicación en el organigrama de su organización del departamento de auditoría de SI.
4. Exponga al menos tres procedimientos que debe contener la metodología de un departamento de auditoría de SI.

5. Defina una estrategia para establecer el universo de TI de su organización.
6. ¿Cuál cree que es el aspecto más relevante para determinar la dimensión de un departamento de auditoría de SI en su organización?
7. Exponga dos aspectos relevantes de la definición de control interno.
8. ¿De qué órgano depende la función de auditoría de SI?
9. ¿Qué son los recursos de información? Nómbrelos.
10. Exponga los pasos en los que se descompone la planificación de auditoría de SI.

CAPITULO 6

ENTORNO JURÍDICO DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

6.1 INTRODUCCIÓN

Hace no muchos años, cuando afrontábamos la tarea de escribir sobre las normas jurídicas que afectaban a la auditoria de los sistemas de información, nos encontrábamos con muy pocas leyes, con lo que con poco espacio podíamos asumir ampliamente el trabajo que nos encomendaban.

Hoy día ya no sucede así y las normas jurídicas referentes a temas tecnológicos crecen exponencial y rápidamente por lo que, para evitar simplemente relacionarlas, hemos optado por elegir unas cuantas, algunas por su importancia y otras por su novedad.

Hacer una selección es algo subjetivo por 10 que somos conscientes de que podemos haber errado en ello y dejada filera algunas ciertamente importantes.

Las áreas seleccionadas, teniendo en cuenta estas consideraciones, han sido:

a. Protección de datos de carácter personal
b. La protección jurídica de los programas de ordenador
c. Los delitos tecnológicos
d. La contratación electrónica
e. La firma electrónica
f. El DNI electrónico
g. El correo electrónico
h. La videovigilancia
i. La ley estadounidense Sarbanes (SQX)

Como se puede ver, tenemos junto a normas antiguas y con un amplio recorrido, otras más modernas y que, sin embargo, por su trascendencia pueden resultar de gran interés para los auditores de los sistemas de información. ¡Esperamos no habernos equivocado en la selección!

Las normas reguladoras de la protección de los datos de carácter personal, la protección jurídica de los programas de ordenador o los delitos tecnológicos han sido ya suficientemente aplicadas por los tribunales y por consiguiente existe una jurisprudencia desarrollada sobre ellas; sin embargo las que regulan el correo

electrónico, que prácticamente ha sustituido al correo postal en el mundo empresarial, la firma electrónica que pretende sustituir a la firma manuscrita o el DNI electrónico que se está implantando y pretende ser el documento ideal de identificación. todos ellos emergen con enorme fuerza en este mundo cambiante que nos ha tocado vivir.

La videovigilancia, que surge como defensa ante los riesgos que tenemos que afrontar en esta sociedad, nos pone frente a la disyuntiva de elegir entre más intimidad o más seguridad.

por último, la Ley estadounidense Sarbanes-Oxley dada la globalización económica que existe, afecta a un buen número de empresas radicadas en nuestro país y por tanto de interés para los auditores de los sistemas de información.

6.2 LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

6.2.1 Legislación

El artículo 18.4 de la Constitución Española de 1978 señala: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos. ‘’

Fruto del mandato constitucional fue la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal (en adelante LORTAD).

Esta ley tenía por objeto según su artículo 1: "limitar el uso de la informática y Otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos " y era de aplicación, de conformidad con su artículo 2.1 a: "los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior. incluso no automatizado. de daros de carácter personal registrados en soporte susceptible de tratamiento automatizado. "

Su desarrollo reglamentario se llevó a cabo a través de tres reglamentos:

- Real Decreto 428/1993, de 26 de marzo. por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.
- Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.
- Real Decreto 994/1999, de ll de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS),

El retraso en la aprobación de este tercer Reglamento dio lugar a una peculiar situación cuyas consecuencias aún perduran, al aprobarse el mismo pocos meses antes de que la ley que desarrollaba, la LORTAD. fuese derogada. En 1995 tuvo lugar la aprobación de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre. relativa a

la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (en adelante Directiva 95/46/CE). La Directiva supuso una ampliación del objeto de la protección de datos puesto que garantiza la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales y del ámbito de aplicación puesto que se aplicará al tratamiento total 0 parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

La trasposición al ordenamiento jurídico español de la Directiva 95/46/CE se llevó a cabo a través de la Ley 15/1999. de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) que es la ley actualmente vigente en esta materia.

No obstante, en su Disposición transitoria tercera declara subsistentes, hasta tanto no se lleve a cabo el desarrollo reglamentario de la Ley, con su propio rango las normas reglamentarias existentes y en especial los Reales Decretos mencionados más arriba, en cuanto no se opusieran a la misma.

En el momento de redactar estas líneas no se ha llevado a cabo el desarrollo reglamentario de la LOPD, aunque está prevista la aprobación en fecha no lejana de un Reglamento de desarrollo que incluirá también las medidas de seguridad aplicables a ficheros automatizados y no automatizados.

6.2.2 Objeto de la protección de datos

Dato de carácter personal según el artículo 3.a) de la LOPD) es: "Cualquier información concerniente a personas físicas identificadas o identificables."

Estos datos deben estar registrados en soporte físico que los haga susceptibles de tratamiento y/o estar almacenados en un fichero. La LOPD distingue en su Título IV entre ficheros de titularidad pública y ficheros de titularidad privada.

La LOPD define el fichero en su artículo 3.b) como "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación. almacenamiento. organización y acceso" mientras que el artículo 3.c) define el tratamiento como "operaciones y procedimientos técnicos de carácter automatizado 0 no, que permitan la recogida. grabación. conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones. consultas, interconexiones y transferencias."

6.2.3 Sujetos protección de datos

Los principales sujetos que podemos tener en cuenta al abordar el tratamiento de los datos de carácter personal son: responsable del fichero o responsable del tratamiento. encargado del tratamiento, responsable propietario del fichero, responsable de seguridad, afectado o interesado y órganos de control.

Responsable del fichero o del tratamiento: según el artículo 3 de la LOPE) es persona

física o jurídica, de naturaleza pública o privada. u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento. '.

Encargado del tratamiento: el artículo 3.g) de la LOPE) lo define como: "la persona física o jurídica, autoridad pública. servicio o cualquier Otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento. ‘’

Responsable propietario del fichero: esta figura no está definida en la ley pero es especialmente útil a la hora de delimitar el nivel de responsabilidad dentro de las organizaciones. Será quien cree el fichero, lo mantenga y disponga las medidas de seguridad que considere necesarias, fije las normas para establecer autorizaciones de acceso solicitando al Departamento de Sistemas de Información la adopción de las medidas necesarias para el buen uso de su fichero.

Responsable de seguridad: según el artículo 16 del RMS será quien se encargue de coordinar y controlar las medidas definidas en el Documento de Seguridad.

Afectado o interesado: según el artículo 3.e) de la LOPD es la persona física titular de los datos que sean objeto del tratamiento. No se refiere la ley pues a personas jurídicas que están fuera de la protección que otorga el derecho a la protección de datos de carácter personal.

Órganos de control: la Agencia Española de Protección de Datos (en adelante AEPD) es el ente encargado de velar por el cumplimiento de la normativa sobre protección de datos. También existen Agencias Autonómicas que ejercen sus competencias cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial. En la actualidad existen la Agencia de Protección de Datos de la Comunidad de Madrid, la Agencia Catalana de Protección de Datos y la Agencia Vasca de Protección de Datos.

6.2.4 Principios protección de datos

Vienen regulados en el Titulo ll de la LOPD y de ellos emanan una serie de obligaciones para el responsable del fichero y, en su caso, para el encargado del tratamiento y una serie de derechos para el afectado o interesado.

Los principios de la protección de datos son:

Artículo 4. Calidad de los datos
Artículo 5. Derecho de información en la recogida de datos
Artículo 6. Consentimiento
Artículo 7. Datos especialmente protegidos
Artículo 8. Datos de salud
Artículo 9. Seguridad de los datos
Artículo 10. Deber de secreto
Artículo 11. Comunicación de datos
Artículo 12. Acceso a los datos por Cuenta de terceros

Principio de calidad

Dentro de este principio se engloban Otros subprincipios:

Pertinencia: supone la obligación para el responsable del fichero de recoger y tratar los datos cuando sean adecuados. pertinentes y no excesivos en relación con las finalidades determinadas, explicitas y legitimas para las que se hubieran obtenido.

Finalidad: los datos de carácter personal objeto de tratamiento no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

Exactitud; los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado, rectificándolos cuando sean inexactos y cancelándolos cuando hayan dejado de ser necesarios 0 pertinentes para la finalidad para la cual hubieran sido recabados.

Lealtad: la ley prohíbe la recogida de datos por medios fraudulentos, desleales e ilícitos.

Principio de información

Según el artículo 5 de la LOPD los interesados a los que se soliciten datos de carácter personal deberán ser informados previamente de modo expreso, preciso e inequívoco de:

- La existencia de un fichero o tratamiento de datos de carácter personal, finalidad de la recogida de éstos y destinatarios de la información.
- El carácter obligatorio 0 facultativo de la respuesta a las preguntas que les sean planteadas.
- Las consecuencias de la Obtención de los datos o de la negativa a suministrarlos.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
- Para algunos autores este principio se viene denominando principio de conocimiento.

Principio de consentimiento

- Según el artículo 3.h) de la LOPD el consentimiento es "toda manifestación de voluntad, libre, inequívoca. especifica e informada, mediante la que el interesado consienta el tratamiento de los datos personales que le conciernen. '

- La regla general es que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa y salvo las excepciones que la propia LOPD contempla en su artículo 6.2.

Datos especialmente protegidos

Los datos especialmente protegidos son:

- Ideología, afiliación sindical, religión y creencias. Para proceder al tratamiento de este tipo de datos es necesario obtener el consentimiento expreso y por escrito del interesado.
- Origen racial. salud y vida sexual. Sólo podrán ser tratados cuando. por razones de interés general, así 10 disponga una ley 0 el afectado consienta expresamente.

Seguridad de los datos

Según el artículo 9 de la LOPD tanto el responsable del fichero como. en su caso, el encargado del tratamiento deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

La ley remite a la vía reglamentaria el establecimiento de los requisitos y condiciones que deben reunir los ficheros que Contengan datos de carácter personal.

Deber de secreto

En virtud de este principio el responsable del fichero y todos aquellos que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos.

Estas obligaciones subsisten aún después de finalizar las relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Comunicación de datos

Según el artículo 3.i) de la LOPD la cesión o comunicación de datos es "toda revelación de datos realizada a persona distinta del interesado. "

Es necesaria la obtención del previo consentimiento del interesado para la comunicación o cesión de los datos a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario salvo las excepciones contenidas en el artículo 11.2 de la LOPD.

Acceso a datos por cuenta de terceros

El artículo 12 de la LOPD regula el supuesto en que un tercero puede acceder a los datos cuando dicho acceso es necesario para la prestación de un servicio al responsable del fichero. Este tercero recibe el nombre de encargado del tratamiento y en este caso el acceso no se considera cesión o comunicación de datos.

La relación entre responsable del fichero y encargado del tratamiento debe estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido y en el que deberá constar expresamente:

- Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- Que no los aplicará o utilizará con fin distinto al que figure en dicho contrato.
- Que no los comunicará, ni siquiera para su conservación, a otras

Se estipularán las medidas de seguridad que el encargado del tratamiento está obligado a implementar de acuerdo con la Ley.

Una vez cumplida la prestación, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte 0 documentos en que conste algún dato de carácter personal objeto del tratamiento.

El único responsable ante los entes de control es el responsable del fichero, pero si el encargado del tratamiento destina los datos a otra finalidad. los comunica o utiliza incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

6.2.5 Derechos de las personas

La LOPD regula los derechos de las personas en el Título III. De ellos, cuatro integran el contenido del derecho a la protección de datos de carácter personal: derecho de acceso, derecho de rectificación y cancelación, derecho de oposición.

Estos derechos son personalísimos, gratuitos y su atención está sometida a plazos.

Según el artículo 43. 1 de la LOPD: "Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

Las infracciones se encuentran tipificadas en el artículo 44 de la LOPD y las sanciones correspondientes a las mismas en el artículo 45 para los ficheros de titularidad privada que se traducirán en multas y en el artículo 46 para los de titularidad pública, en cuyo caso se dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción.

6.3 LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE ORDENADOR

El desarrollo de Internet ha representado un disparo a la línea de flotación de la propiedad intelectual.

Hemos de tener en cuenta que el principio de territorialidad, tan tenazmente defendido por los Estados hoy día, hay veces que no es tan fácil de aplicar, con los problemas que esta cuestión representa.

Vamos aquí a referirnos específicamente a la protección juridica de los programas de ordenador en España.

El legislador español ha Optado en el Texto Refundido por titularlo de Propiedad Intelectual, olvidando viejas disquisiciones que hacían converger en ésta también la propiedad industrial y contemplando un dominio más amplio de aquélla no sólo la de los derechos de autor y nos parece bien, pues éste comprende no sólo los derechos de

autor sino también otros derechos afines en los que los titulares de los derechos no son autores sino, por ejemplo, ejecutantes.

Llegados a este punto podemos definir la propiedad intelectual como aquella "integrada por una serie de derechos de carácter personal y/o patrimonial que atribuyen al autor y a otros titulares la disposición y exploración de sus obras y prestaciones".

"La propiedad intelectual protege las creaciones originales literarias, artísticas o científicas expresadas en cualquier medio. tales como libros. escritos. composiciones musicales, obras dramáticas, coreografías, obras audiovisuales, esculturas, obras pictóricas, planos, maquetas, mapas. fotografías, programas de ordenador y bases de datos. También protege las interpretaciones artísticas, los fonogramas, las grabaciones audiovisuales y las emisiones de radiodifusión."

La protección de las obras se obtiene desde el momento de su creación por este mismo hecho sin que se exija el cumplimiento de ningún requisito formal.

Existe un Registro de la Propiedad Intelectual en el que voluntariamente se pueden registrar las obras y en determinadas circunstancias la inscripción del derecho puede servir de prueba; pero, ahora bien, ha de tenerse en cuenta que el registro es meramente declarativo y no constitutivo de derechos, pues, repetimos, el acto de creación es el que realmente constituye el derecho.

Los derechos que la ley otorga al autor son de dos clases: morales y patrimoniales.

Los derechos morales se describen en el artículo 14 del Texto Refundido de la Ley de Propiedad Intelectual aprobado por Real Decreto Legislativo 1/1996, de 12 de abril (en adelante TRLPI). A los derechos patrimoniales, que son los que más suelen interesar debido a su efecto económico, nos referiremos más ampliamente al hablar de los programas de ordenador.

6.3.1 Titularidad de los derechos (artículo 97 TRLPI)

Según el artículo 97 del TRLPI se considera autor del programa de ordenador a la persona o grupo de personas naturales que lo hayan creado, o a la persona jurídica que sea contemplada Como titular de los derechos.

Se contemplan los siguientes casos:

- **Autor individual**. Persona natural que haya creado el programa.
- **Obra colectiva**. Salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre.
- **Varios autores.** Será propiedad común y corresponderá a todos en la proporción que determinen.
- **Empresario.** Salvo pacto en contrario, si la creación de un programa de ordenador se ha realizado por un trabajador asalariado, en el ejercicio de las funciones que le han sido encomendadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes será exclusivamente del empresario.

Vemos, pues. que los derechos de explotación pueden detentarlos no sólo las personas naturales sino también las personas jurídicas cuando así lo estipula la ley.

6.3.2 Duración de la protección (artículo 98 TRLPI)

Según el artículo 98 del TRILPI la duración de los derechos de explotación de un programa de ordenador será la siguiente:

- **Persona natural.** Toda la vida del autor y setenta años después de su muerte o declaración de fallecimiento.

- **Personas jurídicas.** Setenta años.

Los plazos se computarán desde el día I de enero del año siguiente al de la muerte 0 declaración de fallecimiento del autor 0 al de divulgación lícita de la Obra según proceda.

Los plazos se fijan para que los derechos de explotación pasen a dominio público lo que en el caso de las obras escritas nos parece razonable. pero que en el caso de los programas de ordenador los plazos nos parecen un tanto exagerados y poco prácticos.

6.3.3 Contenido de los derechos de explotación (artículo 99 TRLPI)

Nos remitimos al artículo 99 del TRLPI.Existen una serie de limitaciones a los derechos de explotación que figuran en el artículo 100 del TRILPI.

Es importante saber que al proteger por el derecho de autor un programa de ordenador protegemos no sólo el programa fuerte y el programa objeto sino también toda la documentación que los acompaña, por ejemplo, entre otros, el manual de explotación.

6.4 LOS DELITOS TECNOLÓGICOS

La implantación de las tecnologías de la información en nuestra sociedad ha hecho posible nuevas modalidades de ataques a bienes jurídicos, lo que en un pasado reciente parecía imposible.

La Ley Orgánica 10/1 995, de 23 de noviembre, que aprobó el actual Código penal trata de hacer frente a estas nuevas situaciones.

A continuación, vamos a examinar los más importantes delitos tecnológicos 0 informáticos, denominación que algunos autores no admiten, entendiendo que no se trata de una nueva clase de delitos sino de los ya existentes pero realizados con medios informáticos.

Resulta importante el artículo 26 al admitir dentro del ámbito penal la validez del documento electrónico.

6.4.1 Delitos contra la intimidad

Se viene a sancionar las infracciones que se cometan contra la LOPD, por la proximidad que existe entre el derecho a la protección de datos de carácter personal y el derecho a

la intimidad.

Artículos 197. 198 y 199. Se puede añadir aquí el artículo 200 que protege a las personas jurídicas, aunque éstas no son objeto de la LOPD.

6.4.2 Delitos contra el patrimonio

Artículo 239, A cuyos efectos se consideran llaves falsas las tarjetas de crédito.
Artículo 248. Estafa. Respecto a la estafa, con el antiguo Código Penal algunos jueces venían reconduciendo el fraude informático hacia la figura de la estafa, algo que no compartíamos pues existía el elemento de engaño necesario en la estafa.

Algo de razón debíamos tener puesto que en el nuevo Código Penal se ha añadido un segundo punto al artículo" referido a la estafa que comprende específicamente la estafa informática.

Artículo 256. Defraudación en telecomunicaciones.
Artículo 264. Daños.
Artículos 270, 271 y 272. Propiedad intelectual.
Artículo 273. Propiedad industrial.
Artículo 278, 279 y 280. Secretos empresariales.

6.4.3 Delitos de falsedades

Artículo 386 y 387. Falsificación de monedas y tarjetas de plástico.
Artículos 390, 391 y 392. Falsificación de documentos públicos oficiales y mercantiles.
Artículo 394. Falsificación de despachos telegráficos.
Artículo 395. Falsificación de documento privado.
Artículo 400. Fabricación 0 tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador que permitan la comisión de los delitos anteriores.

6.4.4 Delitos contra las Administraciones Públicas

Artículo 413 y 414. Sustracción, destrucción, inutilización u ocultación de documentos.
Artículo 415. Infidelidad en la custodia de documentos.

6.4.5 Otros delitos y faltas

Artículo 536. Interceptación de comunicaciones.

Somos conscientes de que la selección, en función de un concepto, dc ciertas partes de un todo, especialmente en el campo jurídico, conlleva una gran carga de subjetividad, algo que por supuesto aceptamos y, por tanto, asumimos.

6.5 LA CONTRATACIÓN ELECTRÓNICA

Antes de referirnos a lo que es la contratación electrónica quisiéramos hacer unas

precisiones puesto que debido a que nos debemos someter, como hemos dicho anteriormente, a unos límites espaciales, lógicamente sólo podemos analizar los temas que hemos considerado más importantes o novedosos.

La contratación en el ámbito informático, como en otros casos, presenta dos facetas: la primera, en la que las tecnologías de la información se presentan como objeto del derecho lo que da lugar a los llamados contratos informáticos, inexistentes para algunos autores, aunque no para nosotros, y la segunda en la que las tecnologías de la información son el medio gracias al cual se formalizan y perfeccionan los contratos cuyo objeto puede ser cualquiera, no necesariamente tecnológico.

Una vez dicho esto, a partir de aquí, nos referiremos sólo a la contratación por medios tecnológicos.

El Titulo IV de la Ley 34/2002, de 11 de julio. de Servicios de la Sociedad de la Información y del Comercio Electrónico (en adelante LSSI) regula lo que se ha dado en llamar contratación electrónica. Sin embargo, la rúbrica del citado Título "Contratación por vía electrónica" indica que para el legislador este tipo de contratación se caracteriza solamente por el medio a través del cual una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio.

Los artículos 23 y siguientes de la LSSI recogen las especialidades aplicables a la contratación por vía electrónica si bien el párrafo segundo del artículo 23.1 establece que "los contratos electrónicos se regirán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos. en especial. las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial

La Ley favorece la contratación por vía electrónica al afirmar la validez y eficacia del consentimiento prestado por vía electrónica. declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de "forma escrita" que figura en diversas leyes.

La LSSI prevé también la posible intervención de terceros de confianza, si así lo pactan las partes para que archive las declaraciones de voluntad que integran los contratos electrónicos y consigne la fecha y la hora en que dichas comunicaciones tuvieran lugar. La intervención de estos terceros, no obstante, no podrá alterar ni sustituir las funciones que corresponde realizar a las personas facultadas con arreglo a Derecho para dar fe pública, como es el caso de los notarios,

En cuanto al lugar de celebración del contrato, el artículo 29 de la LSSI establece que los contratos celebrados por via electrónica en los que intervenga como parte un consumidor se presumirán celebrados en el lugar en que éste tenga su residencia habitual mientras que los contratos electrónicos entre empresarios o profesionales, en defecto de pacto entre las partes, se presumirán celebrados en el lugar en que esté establecido el prestador de servicios.

6.6 LA FIRMA ELECTRÓNICA

La Exposición de Motivos de la Ley 59/2003, de 19 de diciembre, de firma electrónica (en adelante LFE) reconoce el compromiso asumido por el legislador en el sentido de actualizar el marco jurídico hasta entonces vigente establecido en el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica que incorporaba al ordenamiento jurídico español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, "mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional.

Una de las novedades de la LFE respecto del Real Decreto Ley 14/1999, de 17 de septiembre, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita.

El artículo 3 de la LEE distingue en este sentido:

- Firma electrónica como conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- Firma electrónica avanzada como firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- Firma electrónica reconocida como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La LEE otorga a la firma electrónica reconocida respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Con carácter general, y sin ánimo de ser exhaustivos, entre las novedades que incluye la LEE, destacan:

- La eliminación del registro de prestadores de servicios de certificación.
- La modificación del concepto de certificación de prestadores de servicios de certificación con el fin de otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación favoreciendo la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.
- La ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología", dado que la prestación de servicios de certificación no está sujeta a autorización previa.
- Establece el régimen aplicable a la actuación de personas jurídicas como firmantes de forma tal que podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la

persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

Por Otro lado, es importante señalar que las Disposiciones Adicionales de la LFE contienen modificaciones de otras normas concretamente: del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social; artículos 10, 38.2, 38.3, 38.4, 43.1 y 43.2 de la Ley 34,2002, de 1 1 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico y articulo 326 de la Ley de Enjuiciamiento Civil.

6.7 EL DNI ELECTRÓNICO

La Exposición de Motivos de la LFE destaca la regulación que la ley contiene respecto del documento nacional de identidad electrónico como "certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica Capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios

En los artículos 15 y 16 ubicados en el Capítulo III del Título ll de la LFE Se fija el marco normativo básico del nuevo documento nacional de identidad electrónico de forma que se concibe como "el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos."

El apartado 2 del artículo 15 establece. "Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo. y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos."

En cumplimiento del apartado primero de la Disposición final segunda de la LFE, el gobierno aprobó el Real Decreto 1553/2005, de 23 de diciembre, que regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

6.8 EL CORREO ELECTRÓNICO

La utilización del correo electrónico se ha consolidado como una de las vías más frecuentes y rápidas de comunicación en todos los órdenes de la sociedad.

Empleado en muchas ocasiones con demasiada ligereza sin tener en cuenta los riesgos que, de cara al cumplimiento de las normas vigentes, puede traer consigo.

Sin perjuicio de que, a través de las listas de direcciones que se envían a varios destinatarios, se puedan llevar a cabo cesiones incontenidas de datos de carácter personal o que a través de los correos electrónicos pueda enviarse información a personas que no son los destinatarios de los mismos, la infracción más frecuente y conocida que se puede llevar a cabo a través de este tipo de herramienta es el envió del spam o correo basura.

La LSSI regula las comunicaciones comerciales por vía electrónica en su Título III. El

artículo 20 establece la información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.

Artículo 20. Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en nombre de la cual se realizan.

   En el Caso en el que tengan lugar a través de correo electrónico u Otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra «publicidad».

2. En los supuestos de ofertas promocionales. como las que incluyan descuentos. premios y regalos, y de concursos o juegos promocionales. previa la correspondiente autorización. se deberá asegurar. además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio. que queden claramente identificados como tales y que las condiciones de acceso y, en su caso. de participación se expresen de forma clara e inequívoca, "

El artículo 21.1 prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otra forma de comunicación electrónica equivalente que no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En el apartado 2 del mismo artículo se establece una excepción a esta prohibición.

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

1. Queda prohibido el envío de comunicaciones publicitarias 0 promocionales por correo electrónico u Otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido deforma licita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

   En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de datos como en cada una de las comunicaciones comerciales que le dirija,

El articulo 22 regula los derechos de los destinatarios de los servicios:

Artículo 22. Derechos de los destinatarios de servicios.

1. El destinatario podrá revocar en cualquier momento el prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

   A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.

   Asimismo. deberán facilitar información accesible por medios electrÓnic0s sobre dichos procedimientos.

2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales. informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, Ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónica, en la medida que resulte estrictamente necesario. para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario."

Es importante incidir en la idea de que el incumplimiento de estos artículos, además de suponer una infracción de la LSSI tipificada como infracción leve 0 grave, y cuya sanción corresponde a la AEPD. la práctica del spam puede suponer el incumplimiento de la legislación sobre protección de datos puesto que la dirección de correo electrónico puede ser considerada como dato de carácter.

Ha sido muy importante en relación con el spam la Sentencia de 17 de mayo de 2007 de la Sala de 10 contencioso-administrativo de la Audiencia Nacional por la que falla contra la resolución del director de la AEPD de fecha 22 de marzo de 2005 en la que se imponía a un particular una multa de 30.001 euros, resolución que se anula dejando sin efecto la sanción impuesta al ordenar que se devuelva al recurrente la cantidad abonada junto con sus intereses.

6.9 LA VIDEOVIGILANCIA

Sin perjuicio de que este tema sea tratado más extensamente en Otro capítulo de esta obra, vamos a dar unas nociones básicas sobre las normas actualmente vigentes sobre la materia.

La única ley sobre utilización de videocámaras es la Ley Orgánica 4/1997. de 4 de agosto, sobre utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos y su reglamento de desarrollo aprobado por Real Decreto 596/1999, de 16 de abril. Sin embargo, constriñe la utilización de videocámaras en función del sujeto (Fuerzas y Cuerpos de Seguridad) y del objeto (grabación de imágenes y sonidos en

lugares públicos, abiertos o cerrados) y su posterior tratamiento con la finalidad de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.

La Disposición adicional novena de esta Ley Orgánica emplazaba al Gobierno para que en un año elaborase la normativa correspondiente para adaptar los principios inspiradores de la ley al ámbito de la seguridad privada. Esta normativa no se ha aprobado y actualmente se encuentra en vigor la Ley 23/ 1992, de 30 de julio, de Seguridad Privada, y el Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre. En el ámbito de la seguridad privada solamente el artículo 120 del Reglamento de Seguridad Privada hace referencia a la utilización de equipos de captación de imágenes en los establecimientos u oficinas de las entidades de crédito donde se custodien fondos o valores.

Por otro lado, y teniendo en cuenta que la imagen es un dato de carácter personal resulta de aplicación a su tratamiento la LOPD y su normativa de desarrollo.

Con la finalidad de aclarar las múltiples dudas que se han generado en cuanto al tratamiento de este tipo de datos de carácter personal la AEPD ha publicado la Instrucción 1/2006. de 8 de noviembre, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras 0 videocámaras y la Agencia de Protección de Datos de la Comunidad de Madrid ha aprobado la Instrucción I de 16 de mayo, sobre el tratamiento de datos personales a través de sistemas de cámaras o videocámaras en el ámbito de los órganos y Administraciones Públicas de la Comunidad de Madrid.

6.10 LEY ESTADOUNIDENSE SARBANES-OXLEY (SOX)

Puede extrañar que en un capítulo en el que se desarrolla el entorno jurídico en el que se mueve la Auditoría de los Sistemas de Información aparezca un punto que dedicamos a una ley de los Estados Unidos de América que lógicamente no está incorporada al ordenamiento jurídico español.

Su inclusión viene dada, como veremos más adelante, por su aplicabilidad no sólo a las sociedades mercantiles estadounidenses sino también a las filiales de aquéllas que residan en la Unión Europea y a las no estadounidenses que coticen en alguno de los mercados de valores de aquel país.

El origen de la aprobación en 2002 de la Ley de Sarbanes-Oxley (SOX) por el Congreso de los Estados Unidos fueron los sucesivos escándalos financieros de empresas norteamericanas.

Esta Ley, obligatoria, como ya se ha indicado, para las sociedades estadounidenses que coticen en Bolsa y sus filiales residentes en la Unión Europea y para las sociedades no estadounidenses que coticen en alguno de los mercados de valores de Estados Unidos. establece que dichas sociedades deben incorporar en su comité de auditoría "procedimientos para la recepción. retención y tratamiento de quejas recibidas por el causante en relación con la contabilidad, controles contables internos o cuestiones de

auditoria: y la presentación confidencial y anónima por parte de los empleados de la persona causante de preocupación en relación con cuestiones contables 0 de auditoria cuestionables.

Especial énfasis se pone en la Ley en garantizar la protección de los empleados de dichas sociedades que presenten pruebas frente a las represalias tomadas contra ellos por sus empleadores por dicho hecho.

Las sociedades que no cumplan esta Ley están sujetas a graves sanciones y multas por parte de las autoridades de las Bolsas norteamericanas.

En la Unión Europea se enfrenta, en cierto modo, la aplicación de esta Ley con las normas europeas sobre protección de datos personales por lo que las Autoridades de Control de la Unión Europea están analizando la cuestión. Prueba de ello es el Dictamen 1/2006 sobre la aplicación de las normas de la UE relativas a la protección de datos a programas internos de denuncia de irregularidades en los campos de la contabilidad, controles contables internos, asuntos de auditoría, lucha contra el soborno. delitos bancarios y financieros, adoptado el I de febrero de 2006 como documento WP117 por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE.

Así mismo el Gabinete Jurídico de la AEPD ha elaborado recientemente el Informe Jurídico 2007-0128 sobre Creación de sistemas de denuncias internas en las empresas (mecanismos de "whistleblowing").

No sería de extrañar que con el tiempo en el ámbito de la Unión Europea se aprobase una ley de estas características dados los escándalos financieros que periódicamente se vienen sucediendo.

6.11 CONCLUSIONES

Como siempre somos partidarios de dejar al amable lector que saque las conclusiones que considere más oportunas de las líneas que preceden, pero, no obstante, vamos a exponer algunas reflexiones a modo de epilogo.

Los hechos tecnológicos se suceden rápidamente sustituyendo 0 modificando en algunas ocasiones a los que venían existiendo y el derecho, como tiene que ser, debe a continuación regular los mismos.

El principio de territorialidad vigente y que ha regido en derecho internacional hasta la fecha, debido a Internet, en muchas ocasiones resulta difícil de aplicar.

La originalidad de algunos nuevos hechos tecnológicos plantea serias dudas al legislador acerca de qué derecho aplicar, lo que hace que muchas directivas de la Unión Europea tengan un plazo de temporalidad para, una vez transcurrido éste, examinar los resultados.

En cualquier caso, este mundo es el que nos ha tocado vivir y por tanto cuyos problemas hemos de afrontar.

6.12 LECTURAS RECOMENDADAS

Davara Rodríguez, Miguel Ángel. Manual de derecho informático. (8ª edición). Aranzadi. Cizur Menor, 2006.

Peso Navarro, Emilio del. La Ley de Protección de Datos. La nueva LORTAD. Diaz de Santos. Madrid, 2000.

Piattini Velthuis, Mario y Hervada Vidal, Fernando (eds). Gobierno de las Tecnologías y los Sistemas de Información. Ra-Ma. Madrid, 2007.

Soler Matutes, Pere (dir.), Piattini Velthuis, Mario e Ilustre Colegio Oficial de Ingenieros de Informática de Cataluña (coor.). Manual de Gestión y Contratación Informática. Aranzadi. Cizur Menor, 2006.

6.13 BIBLIOGRAFÍA

Castells, Manuel. La galaxia Internet. Plaza & Janés. Barcelona, 2001.

Cruz Rivero, Diego. Eficacia formal y probatoria de la firma electrónica. Marcial Pons. Madrid, 2006.

Davara & Davara, Asesores Jurídicos. Facebook sobre comercio electrónico. (Y edición) Aranzadi. Pamplona, 2004.

peso Navarro, Emilio del. Servicios de la Sociedad de la Información.

Comercio electrónico y protección de datos. Diaz de Santos. Madrid, 2003.

Sieber, Ulrich (ed.). Information Technology Crime. Carl Heymanns

Verlag KG. Kóln. Berlin. Bonn, München, 1994.

Varios autores. "Delito cibernético" en Informática y derecho. Revista Iberoamericana de Derecho Informático. N^{O} 27, 28 y 29. UNED. Mérida, 1998.

6.14. CUESTIONES DE REPASO

1. ¿Cuáles son los principios recogidos en la LOPD?
2. ¿Cuáles son los derechos que pueden ejercitar los interesados según la LOPD?
3. ¿Qué tipos de derechos se reconocen a un autor?
4. ¿Cuál es la duración de los derechos de autor cuando se trata de una persona física y a partir de qué fecha se computan?
5. ¿Qué se puede considerar delito tecnológico?
6. ¿Cuál es la diferencia entre contratación informática y contratación electrónica?
7. ¿Qué clases de firma electrónica reconoce el artículo 3 de la LFE?
8. ¿En qué supuestos puede el prestador enviar comunicaciones comerciales u ofertas promocionales según la LSSI?
9. ¿Cuál es la única ley vigente sobre utilización de videocámaras y cuál es su objeto?
10. ¿Qué empresas españolas deben cumplir con la Ley Sarbanes-Oxley?

CUARTA PARTE: CONTROLES DE ACCESO LÓGICOS Y FÍSICOS

Capítulo 7

AUDITORÍA DE LA SEGURIDAD FÍSICA

7.1 INTRODUCCIÓN

El estudio de la seguridad de un Sistema de Información tradicionalmente se suele dividir en dos grandes bloques: Seguridad Lógica y Seguridad Física.

Hoy en día, la línea que separa estos dos bloques es cada día más difusa, debido sobre todo a que los elementos de las salvaguardas técnicas se utilizan tanto para proteger activos de carácter físico como lógico. Por ejemplo: el mismo token puede utilizarse para identificarnos y autenticamos tanto a la entrada de un edificio, como ante un sistema informático. En el primer caso se trata de permitir un acceso físico y en el segundo un acceso lógico.

Para intentar definir el ámbito de la seguridad física, diremos, que comprende todas aquellas medidas de seguridad aplicables a un Sistema de Información, que tratan de proteger a este y a su entorno tanto de las amenazas de carácter físico procedentes de la naturaleza, de los propios medios técnicos y de las personas, como de las amenazas de carácter lógico, cuyas medidas de protección son de carácter físico.

7.2. SEGURIDAD FISICA VS. SEGURIDAD LOGICA

Todas las amenazas a las que está sometido un Sistema de Información, así como las medidas de protección y salvaguarda que se implantan en dicho sistema para garantizar la Seguridad de la Información, se pueden encuadrar en uno de estos dos bloques, por ello se habla de amenazas de carácter lógico o físico, y de medidas de Seguridad Lógica y Seguridad Física.

Las amenazas de tipo lógico suelen comprometer tanto la Confidencialidad, como la Integridad y Disponibilidad de la Información, sin embargo, las amenazas físicas atacan en mayor medida a la Disponibilidad, aunque también existen amenazas de carácter físico sobre la Confidencialidad e Integridad para las que son necesarias implementar medidas de protección y salvaguarda de carácter tísico.

La Seguridad Lógica es la rama de la Seguridad Informática más conocida y a la que generalmente se le otorga mayor importancia, pero hay que tener en cuenta que los grandes incidentes de seguridad, los que ponen en peligro la continuidad del servicio y hasta la existencia de la organización que los sufre, suelen estar comprendidos dentro del ámbito de la Seguridad Física.

Dentro del ámbito de la Seguridad Física, es sobradamente conocido el grave impacto que los desastres naturales tienen sobre las infraestructuras de todo tipo, de las que los sistemas informáticos forman parte, y de las que así mismo dependen para su adecuado funcionamiento.

Sin olvidar que si un ataque lógico a un Sistema de Información puede comprometer su funcionamiento y dejarlo lucra de servicio durante un período de tiempo más o menos largo, un ataque físico puede dejarlo inoperativo para siempre. Teniendo en cuenta además que, para poder realizar un ataque lógico, es necesaria una serie de herramientas y medios técnicos, algunos de ellos con un coste económico importante además de unos conocimientos tecnológicos de cierto nivel; pero que para llevar a cabo un ataque de carácter físico en la mayoría de los casos no suele ser necesario disponer de grandes medios, ni tener unos grandes conocimientos específicos.

Como se ha comprobado, la amenaza más grave a la que está sujeto el hardware es un ataque malintencionado, debido a que existe voluntad de hacer daño y se suele dirigir contra el elemento más débil, habitualmente con menos protección y que más impacto causa en la organización cuando es destruido.

Por ello, las salvaguardas a aplicar ante este tipo de ataques son las mismas que se utilizan en la protección de elementos valiosos de la industria y el comercio: zonas de acceso restringido, vigilantes armados, detectores de intrusos y demás medidas de seguridad tradicionales.

Las cuatro normas básicas de la seguridad física tradicional son: evitar, retrasar, detectar y defender (entendiendo por defender una respuesta activa contra el hecho), siendo estas de aplicación a la protección física de los sistemas de información.

La seguridad física, además de en las cuatro normas tradicionales, debe basarse en el principio de la defensa en profundidad. Para ello, se debe establecer un conjunto escalonado de medidas de seguridad física que garanticen una defensa en profundidad y permitan una respuesta apropiada ante los incidentes.

La primera línea de defensa debe estar diseñada de forma que evite y retrase la materialización de las amenazas, la segunda línea de defensa debe estar formada por medidas de seguridad física que permitan detectar los incidentes de seguridad física e informar de los mismos. Y la tercera línea de defensa debe estar construida de forma que los controles implantados minimicen los impactos en caso de materialización de las amenazas y permitan responder adecuadamente ante los inicidentes de seguridad física.

7.3 COBIT - DS 12 GESTIÓN DEL ENTORNO FÍSICO

Si queremos disponer de una referencia de buenas prácticas en el campo de la auditoría y el control de los Sistemas de Información, podemos utilizar los Objetivos de Control para la Información y la Tecnología relacionada (COBIT ®), elaborados por el IT Governance Institute, bajo el auspicio de ISACA, Information Systems Audit and Control Association. Entre los diferentes controles que contempla, se encuentran los relacionados con la seguridad física.

El dominio Entrega de Servicios y Soporte de la versión 4 de COBlT. contempla los aspectos relativos a la gestión de la segundad y la continuidad de las operaciones e incluye un objetivo de control de alto nivel especifico para la Seguridad Física y del Entorno: el DS 12 Gestión de Entorno Físico.

Este objetivo de control hace hincapié en que para una adecuada protección de las personas y de los elementos que componen un sistema de información son necesarias unas instalaciones bien diseñadas y bien gestionadas.

Los procesos de gestión del entorno físico deben incluir la definición de los requisitos que deben cumplir los edificios y localizaciones donde vayan a residir los elementos de nuestro sistema de información, la selección de locales e instalaciones, así como el diseño de ios procesos necesarios para supervisar los factores ambientales y gestionar el acceso físico a las instalaciones y recursos.

Una gestión adecuada y efectiva del entorno reduce la frecuencia de las interrupciones del funcionamiento habitual del negocio, ocasionadas por daños a los equipos y al personal.

Según COBIT, el objetivo de control de alto nivel DS 12 Gestión de Entorno Físico es un control sobre el proceso de TI (tecnologías de la información), gestión del entorno físico, que satisface el requisito de negocio de TI, proteger los activos de TI y la información del negocio, minimizando el riesgo de una interrupción del servicio.

Este objetivo de control está dirigido a proporcionar y mantener un entorno físico adecuado para proteger los activos de TI contra acceso, daño o robo. Para ello es necesario implementar medidas de seguridad física, así como seleccionar y gestionar las instalaciones donde residen los elementos del sistema de información.

Así mismo, es necesario medir su efectividad, para ello se utilizan los siguientes indicadores:

- Tiempo sin servicio ocasionado por incidentes relacionados con el entorno físico.
- Número de incidentes ocasionados por fallos o vulnerabilidades de seguridad física.
- Frecuencia de [a revisión y evaluación de los riesgos físicos.

El objetivo de control de alto nivel. Gestión del Entorno Físico, se descompone en los cinco objetivos de control detallados que se describen a continuación.

7.3.1 DS 12.1 Selección y diseño de los centros de proceso de datos

La selección y diseño de los centros de procesos de datos y demás instalaciones debe realizarse teniendo en cuenta tanto los riesgos asociados a los desastres naturales como a los provocados por el hombre. También se debe considerar la legislación aplicable, como las leyes y los reglamentos relativos a la seguridad y la salud en el trabajo.

7.3.2 DS12.2 Medidas de seguridad física

Se deben definir e implementar las medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir pero no limitarse al establecimiento de un perímetro de seguridad, de zonas de seguridad, la ubicación de los equipos críticos y de las zonas de carga y descarga. Deben definirse las responsabilidades relativas a los procedimientos de supervisión, informe y resolución de los incidentes de seguridad física.

7.3.3 DSI2.3 Acceso físico

Se deben definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo los accesos en caso de emergencia. El acceso a locales, edificios *y* áreas debe justificarse, autorizarse, registrarse *y* supervisarse. Esto es aplicable a todas las personas que accedan a las instalaciones, incluyendo personal propio, clientes, proveedores, visitantes o cualquier otra persona.

7.3.4 DSI2.4 Protección contra factores ambientales

Se deben diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipos adecuados para la supervisión y control del entorno.

7.3.5 DS12.5 Gestión de las instalaciones

Se deben gestionar las instalaciones, incluyendo los equipos de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos aplicables, los requerimientos técnicos y del negocio, las especificaciones de los proveedores y los requisitos relativos a la seguridad y a la salud en el trabajo.

7.4 ISO 27002:2005 - SEGURIDAD FÍSICA Y DEL ENTORNO

Si hablamos de seguridad de la información la norma ISO 27002:2005, Ja anterior ISO 17799:2005, Buenas Prácticas para la Gestión de la Seguridad de la Información, es una referencia que siempre hemos de tener en cuenta.

A continuación, comentaremos brevemente los controles relativos a Seguridad Física y del Entorno y al Control de Acceso que propone dicha norma y que son aplicables a nuestro caso.

7.4.1. Seguridad Física y del Entorno

Perímetro de Seguridad. - Se deben establecer perímetros de seguridad para proteger las áreas donde se almacenan soportes de información o que albergan instalaciones de proceso de datos.

Controles físicos de entrada. - Las áreas seguras deben contar con controles de entrada adecuados para garantizar que sólo accede a ellas el personal debidamente autorizado.

Seguridad de oficinas, despachos e instalaciones. - Se deben diseñar y aplicar normas y procedimientos de seguridad física para proteger todo tipo de instalaciones.

Protección contra amenazas externas y ambientales. - Se deben diseñar e implementar las medidas de protección contra los daños originados por el fuego, inundación, terremoto, explosión, desórdenes públicos y otras formas de desastre.

Trabajo en áreas seguras. - Se deben diseñar c implementar los procedimientos y medidas de seguridad física aplicables al trabajo en áreas seguras.

Áreas de acceso público, áreas de carga y descarga. - En los puntos de acceso público, como las áreas de carga y descarga y otros puntos donde exista la posibilidad de que se produzca el acceso de personas no autorizadas, se deben extremar los controles y si es posible, aislarlos de las instalaciones de proceso de datos para evitar accesos no autorizados.

Instalación y protección de los equipos. - Los equipos deben ser instalados en áreas seguras y protegidos para reducir los riesgos provenientes de las amenazas del entorno, de los accesos no autorizados y otros tipos de amenazas de carácter físico.

Suministro eléctrico - Se deben establecer medidas de protección contra los cortes de suministro eléctrico y otras interrupciones causadas por fallos en otros tipos de suministros auxiliares. Los equipos deben protegerse de los daños producidos por la falta de calidad del suministro eléctrico.

Seguridad del Cableado. - Tanto los cables de suministro eléctrico como los de comunicaciones, deben protegerse contra la interceptación de la comunicación y el daño físico.

Mantenimiento de Equipos. - Los equipos deben mantenerse de Forma adecuada para asegurar su disponibilidad e integridad.

Seguridad de los equipos Juera de los locales de la Organización. - Deben establecerse medidas de protección de los equipos que se encuentren fuera de las instalaciones de la organización, teniendo en cuenta los riesgos inherentes a la utilización de equipos fuera de las instalaciones.

Seguridad en la reutilización, enajenación o deshechado de equipos. - Todos los componentes de los equipos que contengan medios de almacenamiento deben ser controlados para asegurar que tanto los datos sensibles que contengan como el software que tengan instalado sean eliminados de forma segura antes de su reutilización, enajenación o deshechado.

Salida de las instalaciones. - Los equipos, la información o el software no deben salir de las dependencias de la organización sin una autorización previa.

7.4.2. Control de Acceso

Política de Control de Acceso - Debe establecerse una política de control de acceso, basada en los requisitos de seguridad del negocio, dicha política debe incluir el control de acceso físico.

Gestión de Accesos de Usuarios.- Debe establecerse un procedimiento formal de registro de altas y bajas de usuarios para garantizar el acceso y la revocación de accesos a todos los sistemas y servicios de información, incluyendo el acceso físico.

Gestión de Privilegios.- Deben restringirse y controlarse la asignación y uso de privilegios de acceso.

Revisión de Derechos de acceso de Usuarios.- Se debe establecer una revisión periódica de los derechos de accesos de los usuarios utilizando un procedimiento formal.

Equipo Informático de usuario desatendido.- Se deben establecer medidas de seguridad para poder garantizar que los equipos desatendidos tienen la protección apropiada.

Políticas de limpieza de escritorio y pantalla. - Debe establecerse una política de escritorio limpio de papeles, de medios extraíbles y de pantalla limpia.

Informática móvil y comunicaciones. - Se debe establecer una política de uso y adoptar medidas de seguridad apropiadas contra las amenazas inherentes al uso de equipos informáticos portátiles.

7.5 CSCN DEL MAP - SEGURIDAD FÍSICA

Una de las publicaciones que no se puede obviar cuando se habla de seguridad de la información y las TIC es *Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades (CSCN).* Se trata de una publicación del Ministerio de Administraciones Públicas, en la que se describen una serie de medidas organizativas y técnicas dirigidas a asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas se dividen en CRITERIOS, que se consideran de obligado cumplimiento y en RECOMENDACIONES, que como su nombre indica son recomendaciones que ayudan a alcanzar el nivel de seguridad requerido.

En este caso comentaremos las dos áreas de los CSCN que son de aplicación a la seguridad física de los sistemas de información.

7.5.1. Seguridad Física

7.5.1.1. Criterios

Se debe situar el equipamiento que soporta a la aplicación, así como los soportes de información en áreas seguras y protegidas adecuadamente.

Se deben definir de forma proporcionada las medidas que garanticen la seguridad de los locales a proteger en relación con los requisitos de seguridad de la información que se almacene o procese.

Se deben construir barreras físicas del suelo al techo, para prevenir entradas no autorizadas o contaminación del entorno. Las ventanas y puertas de las áreas seguras

deben estar cerradas y controlarse periódicamente. Las ventanas deben protegerse externamente. Se pueden necesitar barreras adicionales y perimetrales entre áreas con diferentes requisitos de seguridad dentro del perímetro global de seguridad.

Se deben construir las instalaciones de forma discreta y minimizar las indicaciones sobre su propósito, evitando signos obvios (fuera o dentro del edificio) que identifiquen la presencia de las actividades cuya seguridad se desea. No informar al personal que no esté directamente implicado de las actividades que se hacen dentro de las áreas seguras.

No se deben identificar en directorios telefónicos y de los vestíbulos de la organización las localizaciones informáticas (excepto las oficinas y áreas de recepción).

Se deben proteger los locales de amenazas potenciales:

- *Eléctricas*: realización de un proyecto eléctrico para la instalación, que asegure la independencia de las líneas eléctricas de los equipos de las lincas de tuerza del edificio (motores, alumbrado, etc.) del edificio, la seguridad de las personas y de los equipos mediante un adecuado diseño de los cuadros eléctricos y de las protecciones diferenciales, magnetotérmicas y filtros, la disponibilidad mediante sistemas de alimentación ininterrumpida, equipos electrógenos, etc., el correcto estado del sistema de puesta a tierra del edificio, una correcta instalación de la malla de tomas de tierra en el falso suelo, una correcta canalización y protección de los cables, etc. La instalación de un suelo técnico con unas características antiestáticas y conductoras, adecuadas a los equipos y los riesgos asociados a las tareas que se realizan en la sala. La instalación de sistemas de alarmas efectivos ante contingencias.

- *Incendios:* cumplimiento de las normas relativas a protección de incendios, vigilando la señalización, prohibiciones de fumar, no acumulación de papel y la no ocupación de las vías de salida de emergencia. Instalación de sistemas de detección, alarma y extinción de incendios y su revisión periódica. Disponibilidad de armarios ignífugos para el almacenamiento de las copias de respaldo.

- *Climatización:* instalar sistemas de control de la temperatura y de la humedad.

- *Agua:* instalar sistemas de detección y evacuación de agua. Elegir ubicación sin canalizaciones cercanas de agua.

- *Interferencias:* evitar interferencias electromagnéticas, como las provenientes de los dispositivos móviles, cebadores de los fluorescentes, etc.

- *Agentes químicos*: considerar el uso de protecciones especiales para equipamientos situados en ambientes particularmente agresivos.

- *Otros:* elegir la ubicación evitando las vibraciones excesivas. Control del polvo mediante limpieza periódica y el uso de pinturas especiales para el suelo de la sala que evite su acumulación.

Se deben documentar debidamente los procedimientos de emergencia y revisar esta

documentación de forma periódica.

Se debe formar al personal en el funcionamiento de todos los sistemas instalados, realizando simulaciones de contingencias.

Se deben implantar medidas para proteger los cables de lineas de datos contra escuchas no autorizadas, contra daños (por ejemplo, evitando rutas a través de áreas públicas o fácilmente accesibles) o interferencias (por ejemplo, evitando recorridos paralelos y cercanos a líneas eléctricas), instalar las líneas de suministro y telecomunicaciones para servicios de los sistemas de información en instalaciones comunes, subterráneas cuando sea posible, o tener medidas alternativas de protección adecuada.

Se deben ubicar los terminales que manejen información y datos sensibles en lugares donde se reduzca el riesgo de que aquellos estén a la vista.

Se deben almacenar los materiales peligrosos y/o combustibles a una distancia de seguridad del emplazamiento de los ordenadores. Por ejemplo, los suministros informáticos como el papel no se deben almacenar en la sala de ordenadores (hasta que se necesiten). Inspeccionar el material entrante, para evitar amenazas potenciales, antes de llevarlo al punto de uso o almacenamiento.

Se debe ubicar el equipamiento alternativo y copias de respaldo en sitios diferentes y a una distancia conveniente de seguridad. Estas copias de respaldo se almacenarán en armarios ignífugos.

Se debe controlar la entrada a las áreas que se hayan definido como áreas a ser protegidas, permitiendo el acceso exclusivamente al personal autorizado. Autorizar la entrada a es las áreas sólo para propósitos específicos, controlando los accesos, registrando los dalos y horas de entrada y salida. Obligar a todo el personal a que lleve una identificación visible dentro del área segura y que observe e informe de la presencia de personal extraño al área. En éstas se deben prohibir los trabajos no autorizados en solitario para evitar la oportunidad de acción maliciosa. Cerrar la puerta externa del área, cuando la interna esté abierta.

Se debe restringir el acceso a las áreas seguras del personal de los proveedores o de mantenimiento a los casos en que sea requerido y autorizado. Aun con acceso autorizado deben restringirse sus accesos y controlarse sus actividades (especialmente en zonas de datos sensibles).

Se deben definir normas y controles relativos a la posible salida/entrada física de soportes de información (impresos, cintas y disquetes, CD, etc.), así como de los responsables de cada operación.

7.5.1.2. RECOMENDACIONES

En relación con la adecuación de locales:

- Separar las áreas de carga y descarga de material de las áreas a proteger. En caso de que esto no sea posible, se deberán establecer los controles adecuados para

impedir accesos no autorizados.

- Restringir los accesos al área de carga y descarga desde fuera del edificio, al personal autorizado y debidamente identificado.

En relación con la instalación de líneas de telecomunicaciones:

- Considerar medidas adicionales para sistemas sensibles o críticos, como:
    - Instalación de conductos blindados, salas cerradas, etc.
    - Uso de rutas o medios de transmisión alternativos.

En relación con la ubicación de equipamiento, materiales y copias de respaldo:

- Situar en áreas seguras los equipos a proteger donde se minimicen los accesos innecesarios a las áreas de trabajo, distanciadas de las zonas de acceso público y de las zonas con aproximación directa de vehículos públicos.

- Definir perímetros de seguridad con las correspondientes barreras y controles de entrada. Su protección física debe impedir accesos no autorizados, danos y cualquier otro tipo de interferencias.

7.5.2. Protección de Soportes de Información

7.5.2.1. Criterios

Se deben desarrollar y aplicar procedimientos de seguridad que contemplen la autenticidad, confidencialidad, integridad y disponibilidad, el tratamiento de datos de carácter personal, la gestión de soportes removi bles, la eliminación y destrucción de soportes y la documentación del sistema de conservación.

Se debe elegir un lugar de almacenamiento adecuado para los soportes de información.

Para ficheros a los que haya que aplicar medidas de nivel alto, se debe recurrir a dos copias distintas, una de las cuales debe guardarse en una ubicación diferente de donde se encuentren los equipos informáticos que las tratan.

Se debe mantener un registro de entrada y salida de los soportes de información. Permitirá conocer: el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada. Cabe recoger así mismo el número de serie del soporte y marca de clasificación.

Verificar la definición y correcta aplicación de las medidas de protección de los soportes de información.

Se deben incluir entre las prácticas de protección de tos soportes de información medidas básicas como las siguientes, dentro y fuera del horario normal de trabajo, para evitar su pérdida o destrucción:

- Los documentos, disquetes y otros soportes de información deben guardarse en armarios cuando no se usen y especialmente, fuera del horario normal de trabajo.

- La información crítica o sensible debe encerrarse bajo llave cuando no se requiera especialmente o la oficina esté vacía.

- Los ordenadores personales y los terminales deben estar protegidos por llave, contraseñas u otras salvaguardas cuando no se usen.

Se debe verificar que los usuarios cumplen las recomendaciones relativas a que los equipos no atendidos queden convenientemente protegidos.

El borrado de los datos debe realizarse mediante mecanismos adecuados, como por ejemplo, los basados en ciclos de reescritura de los ficheros. El procedimiento de borrado tendrá en cuenta la naturaleza de los datos y el riesgo aparejado a su desvelamiento.

Recomendaciones:

- Proteger la entrada y salida de correo, así como los puntos de fax desatendidos.

- Considerar que la denominación del nivel de seguridad aplicable aparezca señalada de forma inequívoca en todos sus soportes:

    - Reflejar el nivel de seguridad aplicable en todas y cada una de las páginas de los impresos, incluyendo la carátula; opcionalmente, el nivel de seguridad puede figurar en la cabecera o en el pie de página, siempre que resulte fácilmente legible.

    - Reflejar el nivel de seguridad aplicable en todas y cada una de las pantallas que aparezcan en los terminales o puestos del usuario, o estar pennanentemente en la cabecera de la pantalla.

    - Etiquetar cada soporte electrónico transportable (cintas, cartuchos, disqueles, etc.) con el máximo nivel de seguridad de la información que contenga.

Si la información se envía al exterior o por correo externo a la organización, el sobre cerrado y marcado con el citado nivel de seguridad deberá introducirse en un contenedor NO marcado.

7.6 CONTROLES DE SEGURIDAD FÍSICA

A la hora de diseñar e implantar un plan de Seguridad Física, es necesario realizar un análisis de riesgos, para ello determina remos las amenazas existentes y calcularemos el nivel de riesgo intrínseco al que estamos expuestos, e implantaremos las salvaguardas necesarias para alcanzar el nivel de riesgo asumido por la organización.

Para determinar qué salvaguardas, controles debemos implantar, podemos utilizar como referencia los controles de alto nivel referidos a la Seguridad Física propuestos

tanto por ISACA, como por ISO y por el MAP, y que hemos citado en los apartados anteriores. Este es el momento adecuado para definir los procedimientos y medidas técnicas necesarios para implantar los controles detallados correspondientes.

A continuación, expondremos cómo desarrollar un par de controles de alto nivel en sus correspondientes controles detallados, para que sirvan de ejemplo de cómo desarrollar el resto de controles de alto nivel que es necesario implantar para garantizar un adecuado nivel de Seguridad Física.

7.6.1 Perímetro de seguridad física

Para implantar este control de alto nivel, la existencia de un perímetro definido de seguridad física, debemos detallar una serie de controles de bajo nivel organizados por capas.

La existencia de un perímetro de seguridad física implica la necesidad de unas medidas de protección de perímetro: el acceso al interior del perímetro debe realizarse a través de un área vigilada, con una clara separación de nuestro perímetro de las áreas que no se encuentren bajo nuestra responsabilidad y sean gestionadas por terceros.

Desarrollo del control:

- Perímetro de seguridad física:
    - Protección del perímetro:
        - Perímetro claramente definido con una valla, muro o similar.
        - Construcción resistente.
        - Puertas de acceso:
            - Puertas de acceso reforzadas.
            - Puertas de acceso blindadas.
            - Puertas de acceso acorazadas.
            - Mínimo número de entradas.
            - Ventanas:
                - Ventanas de fácil acceso con cristales blindados.
                - Ventanas de fácil acceso con barrotes o rejas.
                - Ventanas de fácil acceso con barrotes o rejas *y* detectores de rotura/apertura.
    - Cristales opacos.
    - Protección de conductos y aberturas (falso tedio, conductos de aire, etc.).
    - Sistema de detección de intrusión perímetra).
    - Sistema de Circuito Cerrado de TV.
- Acceso a través de un área de recepción.
- Separación de áreas gestionadas por terceros.

7.6.2. Control de entrada

Para implantar un control de entrada adecuado, hay que tener presente que es

necesario desplegar una serie de controles detallados que garanticen un adecuado control de los accesos físicos a las instalaciones, como por ejemplo, una gestión del cierre de oficinas y locales, lo que implica la implantación de un control sobre la custodia de las llaves de las mismas.

Desarrollo del control:

Control de los accesos físicos.

- Control de los accesos:
- Procedimiento de control de accesos
- Verificación previa de las autorizaciones de acceso del personal.
- Registro de los accesos.
- Revisión periódica del registro de accesos.
- Investigación de cualquier sospecha o intento de acceso tísico no autorizado.
- Sistema automático de control de accesos:
  - Alimentación redundante.
  - Mecanismo de identificación:
    - Basado en PIN o token.
    - Basado en token y PIN.
    - Basado en biometría.
    - Basado en biometría y token.
- Revisión y mantenimiento periódicos.

Sistema de Detección de Intrusión centralizado:

- Instalación por empresa autorizada.
- Alimentación redundante.
- Atendido por personal:
  - Atendido por personal de seguridad durante el horario laboral y conectado con la central receptora de alarmas fuera de dicho horario.
  - Permanentemente atendido por el personal de seguridad.
- Protección contra sabotajes.
- Verificación periódica del funcionamiento.
- Mantenimiento periódico.

- Las salidas y procedimientos de emergencia garantizan que solamente el personal autorizado puede acceder a las instalaciones.
- Control de las visitas.
  - Es necesaria una autorización previa para el acceso de visitas, persona] de mantenimiento o de empresas de servicios.
  - Comprobación de la identidad de las visitas.
  - Registro de entrada/salida.
  - Supervisión y escolta de movimientos y actividades de los visitantes.
  - Revisión periódica del registro de visitas.
- Pases o identificadores:
  - Es obligatorio el uso de identificadores en el interior del recinto.
  - Procedimiento para la emisión, control, registro, baja y cancelación de los identificadores.

    - Empleo de diferentes tipos de identificadores según el tipo de personal y de área a la que accedan.
    - Diseño difícil de falsificar.
    - Deben incluir fotografía de la persona a la que se emiten.
    - Deben permitir reconocer visualmente el tipo de áreas a las que puede acceder su portador.
    - No contendrán datos que permitan, en caso de pérdida, obtener información acerca de su finalidad.
- Accesos cerrados fuera de las horas de trabajo.
- Los locales y oficinas se cerrarán y controlarán periódicamente cuando estén vacíos.
- Control de llaves, combinaciones o dispositivos de seguridad:
    - Inventario:
        - Registro de llaves.
        - Registro de combinaciones de acceso.
        - Identificación del responsable.
        - Revisión periódica del inventario.
    - Las áreas de seguridad dispondrán de llave, combinación o dispositivo de seguridad para permitir el acceso a las mismas.
    - Solamente serán utilizados por el personal autorizado.
    - Se custodiarán de forma segura, incluyendo los duplicados.
    - Las llaves se cambiarán cuando se hayan comprometido o exista sospecha de ello.
    - Las combinaciones se cambiarán o modificarán cuando hayan sido comprometidas o exista sospecha de ello.
    - Las combinaciones se cambian o modifican cuando haya cambios de personal que hayan tenido acceso a las mismas.
    - Las combinaciones se cambian o modifican al menos cada seis meses.
    - Se realizan revisiones periódicas del control de llaves, combinaciones o dispositivos de seguridad.

7.7 PLANIFICACIÓN Y EJECUCIÓN DE LA AUDITORÍA DE LA SEGURIDAD FÍSICA

La Auditoria de la Seguridad Física es una de las partes parte en las que se puede dividir la Auditoría de Sistemas y, por tanto, en la planificación y ejecución

de la misma son de aplicación los mismos principios y procedimientos que en cualquier otro tipo de auditoría. Igualmente, las herramientas que se utilizan son las habituales en los procesos de auditoría.

Las dos diferencias apreciables que podemos señalar son: la primera, que a diferencia de otros tipos de auditoría, estamos auditando algo físico, algo material que podemos ver y tocar, lo que facilita la obtención y documentación de las evidencias. La segunda, que los controles a auditar son complejos y pertenecen a diferentes áreas de conocimientos, la mayoría fuera del campo habitual de los informáticos, siendo en algunos casos más propios de arquitectos y de ingenieros industriales. Por ello, es necesario que para poder realizar este tipo de auditoría el auditor disponga de una formación multidisciplinar básica y de la colaboración de expertos en las diferentes

ramas o materias implicadas en los controles de seguridad física.

Con una formación multidisciplinar básica que le permita verificar y comprender el funcionamiento de los controles de seguridad física, el auditor puede afrontar con éxito la primera parte de una auditoría de seguridad física, la obtención de evidencias con la utilización de entrevistas *y* cuestionarios, recurriendo a la colaboración de expertos en las materias concretas cuando considere que es necesario verificar en profundidad un control determinado.

Como las entrevistas son herramientas utilizadas en todos los tipos de auditorías y ya han sido tratadas en otros capítulos, no es necesario profundizar en su utilización, en cambio, si que a continuación se incluye un cuestionario o lista de comprobación de los utilizados en la realización de una auditoria de seguridad física.

7.7.1 Cuestionario de Seguridad Física

El cuestionario que se incluye a continuación únicamente es un ejemplo de cómo se puede construir una batería de cuestionarios para obtener evidencias del grado de implantación de los controles de seguridad física en un organización.

En este caso, el criterio que se ha seguido a la hora de agrupar tos controles es el origen de la amenaza o activo amenazado, y todo aquel que no puede ser agrupado por este criterio se ha incluido en un grupo genérico.

Otra alternativa puede ser agrupar los controles tal como lo hacen las normas y estándares a los que se ha hecho referencia anteriormente, por ejemplo el cuestionario podría estar agrupado según la organización que propone la ISO- 27002:

- Seguridad Física y del Entorno:
    - Perímetro de Seguridad.
    - Controles físicos de entrada.
    - Seguridad de oficinas, despachos e instalaciones.
    - Protección contra amenazas externas y ambientales.
    - Trabajo en áreas seguras.
    - Áreas de acceso público, áreas de carga y descarga.
    - Instalación y protección de los equipos.
    - Suministro eléctrico.
    - Seguridad del Cableado.
    - Mantenimiento de Equipos.
    - Seguridad de los equipos fuera de los locales de la Organización.
    - Seguridad en la reutilización, enajenación o desechado de equipos.
    - Salida de las instalaciones.
- Control de Acceso:
    - Política de Control de Acceso.
    - Gestión de Accesos de Usuarios.
    - Gestión de Privilegios.
    - Revisión de Derechos de acceso de Usuarios.
    - Equipo Informático de usuario desatendido.

- Políticas de limpieza de escritorio y pantalla.
- Informática móvil y comunicaciones.

Como se ha indicado anteriormente, el cuestionario que se incluye como ejemplo no es exhaustivo» no se contemplan en él todos los posibles controles de seguridad física que pueden ser necesarios en una organización, únicamente debe emplearse como base para elaborar un cuestionario apropiado para el proyecto de auditoria física concreto en el que se vaya a trabajar

CUESTIONARIO DE SEGURIDAD FISICA

PROCEDIMIENTOS GENERALES

Control Estado Observaciones:

¿Existe una política de seguridad física en la empresa y está actualizada?
¿Existen y se difunden los planes de contingencia / emergencia?
¿Existe un registro de todos los incidentes de seguridad y están clasificados según su gravedad?
¿Se dan conferencias sobre Seguridad Física a todos los empleados al incorporase al trabajo y de forma periódica?
En los contratos de comunicaciones, ¿están claramente reflejados los parámetros que definen la calidad de servicio, como ancho de banda, CIR, tiempo de respuesta de averías, etc.?
¿Se ha hecho un análisis de riesgos de la Seguridad Física?
¿Tiene todo el personal disponible un listado con los números de teléfono más importantes en caso de emergencia?
¿Se realizan simulacros *f* ejercicios en caso de emergencia
¿Tiene la empresa contratados seguros generales?
¿Tiene la empresa contratados seguros específicos de las tecnologías de la Información?
¿Tiene la empresa un seguro específico de responsabilidad civil?
¿Existe un contrato / seguro que garantice la continuidad del negocio en caso de emergencia?
¿Existen planos sobre las rutas de emergencia?
¿Están bien señalizadas las nitas y salidas de emergencia?
¿La ubicación del CPD está estudiada y documentada?
¿Se tía evaluado el riesgo del edificio y zonas aledañas?
¿Existe un estudio de las condiciones estructurales del edificio (Tipo y espesor de paredes, vigas, suelos y techos)?
¿Existen planos de todas las conducciones y están actualizados (¿climatización? agua, eléctrica, ¿comunicaciones...)?
¿Tiene el edificio escaleras de emergencia?
¿Cuenta el edificio con pararrayos y respetan la normativa vigente?
¿Las salas de ordenadores están alejadas y aisladas de los ruidos y las vibraciones?
¿El tiempo de respuesta de los servicios de emergencia (¿bomberos, ambulancia, policía, etc.} es inferior a 15 minutos?

¿Existe un sistema de climatización adecuado?
¿Existe un sistema de climatización de emergencia?
¿Hay un sistema de vigilancia de la instalación, de climatización y de medida de las características ambientales (humedad, temperatura, partículas en suspensión...)?
¿Se realiza un mantenimiento adecuado del sistema de climatización (inspecciones, cambio de filtros, limpieza de conductos...)?

CONTROL DE ACCESO

Control Estado Observaciones
¿Se ha realizado un estudio de riesgo de intrusión en el edificio?
¿Se ha realizado un análisis de riesgos de acceso al CPD?
¿El CPD está completamente aislado del resto del edificio y sus accesos controlados?
¿Existe un Circuito cerrado de televisión que controle el acceso al CPD y las puertas de emergencia?
¿Existe un registro escrito o impreso de todos los accesos a todas las salas de equipos informáticos?
¿Existe un sistema de control de acceso biométrico?
¿Todas las personas con acceso autorizado tienen una tarjeta de identificación y están controlados?
¿Todo el personal, ajeno o no a la empresa, exhibe de forma clara la tarjeta de identificación?
¿Se utiliza un sistema de control de acceso automático para el acceso al CPD?
¿El acceso al CPD está auditado, tanto para la entrada como para la salida?
¿Existen procedimientos específicos de control de acceso para el personal ajeno a la empresa?
¿Existe una vigilancia exterior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?
¿Existe una vigilancia interior por medio de detectores de intrusión, conectado a un puesto permanente de vigilancia?
¿Todas las salidas de emergencia están equipadas con un dispositivo de control, unido a un puesto permanente üe vigilancia que alerte de su apertura?
¿Las oficinas se cierran con llave y se verifica su cierre al terminar la jomada laboral?
¿Se aplica en la empresa la política de mesas vacías?
¿Se ha verificado la resistencia de los muros del edificio ante un intento de intrusión?
¿Se ha verificado la resistencia de las puertas (calidad de los marcos, resistencia de la puerta, calidad de los cerrojos y cerraduras,..)?
¿Se ha verificado la resistencia de las ventanas?
¿Las ventanas de las plantas bajas disponen de rejas o barrotes y se ha verificado su resistencia?
¿Se necesita un permiso expreso para acceder al CPD?
¿Se notifican al CPD con suficiente antelación las visitas previstas?
¿Hay un control y archivo diarios de las grabaciones del sistema de vigilancia?

¿Existe un servicio de vigilantes de seguridad?
¿Existe un procedimiento de rondas y de verificación de la seguridad física?
¿Existe un procedimiento de recepción de materiales que garanticen su inspección antes de su traslado al interior del edificio?
¿Existe un control de la entrada y salida de material?
¿Existe un sistema de detección de metales?
¿Existe un procedimiento específico de control de acceso del personal de limpieza?

INCENDIO

Control Estado Observaciones
¿Se ha realizado un estudio de los riesgos de incendio que cubra tanto la prevención como la protección?
¿Los tabiques *y* revestimientos de muros, techos y suelos están fabricados con materiales ignífugos?
¿El mobiliario del edificio del CPDes ignífugo?
¿Existe un sistema automático de detección de incendios y está conectado a una central de alarmas?
¿Los conductos de aire acondicionado / ventilación están equipados con válvulas automáticas contra incendios?
¿Se activa automáticamente el sistema de corte de energía eléctrica tras la detección de un incendio?
¿Hay barreras como puertas antifuego y/o cortinas antihumos en los lugares susceptibles de ser utilizadas?
¿Las puertas cortafuegos se cierran automáticamente al saltar la alarma?
¿Existe una instalación fija de contra incendios en el CPD?
¿Existe un suministro adecuado de agua para los sistemas de extinción de incendios?
¿La instalación de detección automática de incendios está compuesta por al menos dos tipos de detectores (por ejemplo; detectores de humo iónicos y ópticos)?
¿Existe un indicador luminoso y sonoro fuera del CPD cuando el sistema contra incendios se dispara?
¿Estas instalaciones son revisadas periódicamente, conforme a la reglamentación y tienen un mantenimiento adecuado?
¿El número y distribución de dispositivos de alarma contra incendios es el adecuado?
¿Las instalaciones de extinción automática están realizadas según la normativa vigente y están certificadas como tales?
¿Las instalaciones de extinción automática se verifican periódicamente de acuerdo con la normativa» y su mantenimiento se realiza regularmente?
Cuando las instalaciones de extinción automática se quedan fuera de servicio, ¿se señaliza automáticamente en un puesto permanente de vigilancia ocupado por dos personas como mínimo?
¿Existe una instalación de extintores portátiles en el conjunto de los locales informáticos y el equipamiento del entorno?
¿La instalación de extintores portátiles cumple la normativa vigente?

¿Existen indicaciones claramente visibles acerca de las condiciones de uso de los extintores?
¿Los extintores portátiles se verifican periódicamente de acuerdo con la normativa y su mantenimiento se realiza adecuadamente?
¿Se utilizan sólo papeleras metálicas en el edificio *y* papeleras ignifugas con sus correspondientes lapas en las salas de ordenadores?
¿La cantidad de papel almacenada en las salas de impresión es inferior a las necesidades de un día de producción?
Los productos diversos de mantenimiento, fácilmente inflamables, ¿se almacenan fuera del CPD?
¿Los documentos o soportes informáticos de interés para la empresa se guardan en armarios ignífugos?
¿Está prohibido fumar en el CPD *y* se respeta la prohibición?
¿Se efectúa una limpieza periódica de los espacios ocultos {bajo el falso suelo, escaleras, etc.,)?
¿Se evita la acumulación de material innecesario en el CPD?
¿Se utilizan contenedores de basura resistentes al fuego?

AGUA

Control Estado Observaciones

Los problemas relacionados con el agua (lluvia, goteras, agua a presión de dispositivos contra incendios, inundaciones..,), ¿han sido tratados adecuadamente (filtración, drenaje. sifones, sumideros,.,)?
¿Se ha hecho un estudio acerca de la posibilidad de inundaciones en la zona?
¿El techo de la sala donde se encuentran los equipos informáticos es impermeable?
¿Existe un sistema automático de detección de fugas de agua (en los locales superiores al CPD?
¿Existen planos actualizados con la situación de todas las tuberías (¿agua potable, desagües, aire acondicionado}?
¿Existe un sistema de llaves de paso, así como planos claros, actualizados y fácilmente disponibles de las canalizaciones?
¿Existe un sistema de drenaje adecuado en falso suelo y en salas adyacentes al CPD?
¿Hay instaladas bombas de achique por si fueran necesarias?
¿Se realiza una revisión periódica del estado de las tuberías, llaves de paso y canalizaciones?
¿Existen detectores de humedad / agua en el falso suelo?
¿Están los sistemas de detección conectados con un puesto permanente de vigilancia con al menos dos personas?
¿Se revisan periódicamente los detectores?
¿Todo el sistema de cableado está protegido contra inundaciones / humedad?
¿Hay instaladas bombas de achique como mecanismo de emergencia en caso de inundación?

SUMINISTRO ELÉCTRICO

Control Estado Observaciones

¿Existe un sistema de vigilancia de la calidad y continuidad del suministro eléctrico?
¿El suministro eléctrico es redundante (dos compañías» dos líneas de entrada diferentes...)?
¿Existe un sistema de alimentación ininterrumpida?
¿El Tipo de SAI y el mantenimiento del SAI es adecuado (inspecciones, pruebas, revisión de baterías,..)?
¿Qué autonomía proporciona el SAI (tiempo)?
¿Existe un sistema autónomo de generación de energía eléctrica?
La capacidad de generación de estos grupos electrógenos, ¿es suficiente para garantizar la segundad de los edificios *y* el funcionamiento de los equipos informáticos?
¿Se realizan pruebas periódicas de las instalaciones de los grupos electrógenos?
¿Los paneles de control de energía eléctrica están cerrados con llave?
¿La instalación eléctrica del edificio cumple con la normativa vigente?
¿Se realizan inspecciones periódicas de todas las instalaciones de suministro eléctrico?
¿Existen elementos de protección contra sobretensión?
¿Existe un dispositivo de corte manual de energía para emergencias (machete de corte)?
¿Se verifica su funcionamiento?
¿Se encuentran los interruptores de emergencia ubicados cerca de las salidas de emergencia?
¿Está restringido el acceso a los cuadros de alimentación?
¿Cumple el edificio la normativa vigente en cuanto a la instalación eléctrica?
¿Están claramente indicados los locales o puntos de riesgo de descarga eléctrica?
¿Está el personal instruido *y* existen carteles claramente visibles sobre las acciones *a* tomar en caso de descarga eléctrica?
¿Tienen los equipos informáticos placas para que el personal se descargue de la electricidad estática?

COMUNICACIONES

Control Estado Observaciones

¿Existen sistemas de comunicación alternativos en caso de avería o fallo?
¿Se dispone de dos proveedores de comunicaciones, o en su detecto de un único proveedor con dos puntos de acceso distintos *y* que recorran distintos caminos?
En los contratos de comunicaciones, ¿están claramente reflejados los parámetros que definen Ja calidad de servicio, como ancho de banda, CIR, tiempo de respuesta de averías, etc.?
¿Existe algún plano de la instalación del cableado y sistemas de comunicaciones en el edificio?
¿Se realizan pruebas periódicas para garantizar la calidad de tas líneas y

sistemas de comunicación?
El cableado de comunicaciones, ¿es fácilmente accesible para las labores de mantenimiento?
El personal de mantenimiento* ¿es custodiado mientras realiza sus labores?
Los paneles de control de las comunicaciones, ¿son revisados periódicamente?
El cableado, ¿está protegido frente a accesos no autorizados, sabotaje, interceptación, etc.?
Los equipos de comunicaciones, ¿se encuentran en un lugar de acceso restringido?
¿El cableado de comunicaciones está separado de la instalación eléctrica?
¿Existe alguna protección física para los principales cables de conexión con el proveedor de comunicaciones?
¿Se ha realizado un estudio sobre la problemática TEMPEST?

HARDWARE/SOFTWARE

Centro Estado Observaciones

¿Existe un plan establecido para el mantenimiento y la protección del hardware y de los soportes de almacenamiento de la información?
¿Existe un control de configuración del hardware y del software?
¿Existe un plan de mantenimiento del hardware?
¿Existe un registro de la entrada y salida del hardware?
¿Existe algún procedimiento físico de identificación del hardware (grabado con el logotipo de la empresa?
¿Se registran y documentan todos los fallos software que se detectan?
¿Existe algún procedimiento o norma de registro y custodia de los soportes?
¿Es necesaria una autorización para permitir la salida de soportes de su lugar de almacenamiento?
¿Existen mecanismos para verificar la integridad de los datos almacenados en los soportes?
¿Existe algún procedimiento de etiquetado de soportes[1]?
¿Se respetan los tiempos de vida medios de los soportes y las condiciones de almacenamiento de los mismos?
¿Se siguen los consejos del fabricante en cuanto a condiciones de almacenamiento de los soportes?
¿Existen al menos dos copias de software de aplicación y de base, almacenadas en lugares distintos al de su utilización (al menos una de las copias) para el caso de que se tenga que realizar una nueva instalación?
La adquisición de los soportes, ¿se realiza en diferentes lotes?
Los sopones, ¿se encuentran almacenados en un lugar lo suficientemente alejado del CPD?
¿Se procede a un borrado seguro de los soportes antes de ser re utilizados?
¿Existen máquinas adecuadas de destrucción de soportes magnéticos?

7.8 CONCLUSIONES

La seguridad física y su auditoría son imprescindibles para poder garantizar la

confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.

Para la ejecución de un ataque físico contra la información y los sistemas que la almacenan procesan o trasmiten, no son necesarios grandes conocimientos técnicos ni grandes inversiones, lo único necesario es la voluntad de hacer daño y la ocasión para intentarlo.

Los fenómenos de la naturaleza (terremotos, inundaciones, tormentas., etc.) y sus efectos y representan una de las mayores amenazas tísicas a las que están expuestos los sistemas de información.

Lo mismo que en otras áreas de la auditoría de sistemas, normas como la ISO-27002 y publicaciones como COBIT de ISACA y los Criterios de Seguridad, Conservación y Normalización del MAP son referencias básicas a tener en cuenta a la hora de planificar tanto la seguridad física de los sistemas de información como su auditoría.

La auditoria de la seguridad física no es más que una parte de la auditoria de sistemas de información, con una serie de características específicas, pero aun así, le son aplicables las buenas prácticas y procedimientos generales de la auditoría de sistemas.

Para afrontar con éxito una auditoria de la seguridad física, el auditor necesita una formación multidisciplinar básica que le permita verificar y comprender el funcionamiento de los controles de seguridad física, y contar con la ayuda y soporte de expertos en las materias concretas, para poder auditar en profundidad aspectos técnicos de los controles, por ejemplo, de un ingeniero eléctrico, para todo lo relativo a la instalación y suministro de energía eléctrica.

7.9 LECTURAS RECOMENDADAS

Security Guide TSB/SG-25, *Cuide To The Preparation Of Physical Security Briefs*, Roy al Canadian Mounted Pólice, Technical Security Branch.

Gukle tu Minimizing Computer Theft, Information Technology Security Branch, Royal Canadian Mounted Pólice.

Information Technology Security Standard and fhe Tech nica! Security Standardfor Information Technology (TSSIT), *Royal Canadian Mounted Pólice*

An Introduction to Computer Security; The NfST Handbook. Special Publication 800-12 National Inslitutc of Standards and Technology U.S. Department of Commerce.

CAPITULO 8

LA AUDITORÍA DE LA DIRECCIÓN DE INFORMÁTICA

8.1 INTRODUCCIÓN

Siempre se ha dicho que una organización es un reflejo de las características de su dirección. Los modos y maneras de actuar de aquella están influencias por la filosofía y la personalidad de la segunda.

Obviamente, los departamentos informáticos no son excepción. Aunque puede argumentarse con razón que, a su vez, estos departamentos están integrados en organizaciones mayores y que por tanto son destinatarios de un sinfín de estímulos de las mismas, qué duda cabe que, dado el habito tecnológico tan particular, la principal influencia de dichos departamentos reciben viene inducida desde la propia dirección de informática. En cualquier caso, es a ello que se enfoca el capítulo: a la auditoria de la Dirección, entendida como gestión (en el resto del capítulo se intercambiaran los dos términos) de la informática.

Las enormes sumas que las empresas dedican a las tecnologías de la información en un conocimiento del que no se vislumbra el final y la absoluta dependencia que las mismas tienen el uso correcto de dicha tecnología hacen muy necesaria una evaluación independiente de la función que la gestiona. Ello constituye, de hecho, la razón principal de este libro. La dirección de informática no debe quedar afuera: es una pieza clave el engranaje.

Sin entrar en discusiones profundas sobre el alcance y significado detrás del verbo dirigir (no es el objetivo de este libro y existen multitud de plumas más preparadas que la mía para disertar adecuadamente sobre este aparto), de una manera general, se podría decir que algunos de las actividades básicas de todo proceso de direcciones son.

- Planificar
- Organizar
- Coordinar
- Controlar

8.2 PLANIFICAR

En grandes líneas, se trata de prever la utilización de las tecnologías de la información

en la empresa. Dicha previsión, además de estar en la mente del ejecutivo, suele venir plasmada en documentos llamados planes (y es bueno y recomendable que así sea; en caso contrario, estaríamos ante un primer punto de atención para el auditor: no sería lógico que la previsible evolución futura de la informática en la empresa estuviera únicamente en la mente n de su primer ejecutivo) Los documentos llamados planes demuestran, además, varias cosa:

- Que se ha reflexionado sobre el objetivo del documento y. por tanto, la existido una actividad consciente de consideraciones del futuro, de análisis de alternativas y de evaluaciones riesgos.
- Sirven para marcar un camino, poner objetivos, tareas, plazos y responsables.
- Son muy útiles como elemento de referencia para medir el avance de las organizaciones los diseños.
- Y aunque su implantación en la práctica acabe difiriendo del documento papel original, los participantes serán conscientes de las diferencias y de su justificación y, además, para el próximo ejercicio de planificación, estarán, quizás, mas curtidos, lo que redundara en una mejora general del proceso.

Existen varios tipos de planes informáticos. El principal, y origen de todos los demás, es el que marca el camino general de evolución de la informática empresarial y que llamaremos aquí: el plan estratégico de Sistemas de Información.

8.2.1 Plan Estratégico de Sistemas de Información

Es el marco básico de actuación de los Sistemas de información en la empresa. Debe asegurar el alineamiento de los mismos con los objetivos de negocio de la propia empresa.

Desgraciadamente, la transformación de dichos objetivos de negocio en objetivos informáticos no siempre una tarea fácil. Mucho se ha escrito sobre el contenido y las ventajas e inconvenientes de las diversas metodológicas de realización de este tipo de planes. No se trata en estos breves apuntes de terciar en dicha polémica. El lector encontrara abundante bibliografía sobre la materia. El auditor deberá evaluar si tales metodológicas se están utilizando, como se están utilizando y/o, en caso contrario, si pueden ser utilidad para su empresa.

Estrictamente hablando, estos planes no son de la responsabilidad exclusiva de la Dirección de Informática. Su aprobación final de incumbencia de otros estamentos de la empresa: Comité de informática (ver más abajo) e incluso en último término de la Dirección General. Sin embargo, la Dirección de Informática debe ser permanente impulsor de unja planificación de Sistemas de Información adecuada y a tiempo.

Aunque se suele definir la vigencia de un plan estratégico como de 3 a 4 años, de hecho tal plazo es muy dependiente del entorno en el que se mueve la empresa, Hay muchos factores que incluyen: la cultura empresarial, el sector en el que el uso adecuado de la tecnología informática es un factor estratégico el sector financiero o el de las telecomunicaciones, por ejemplo, las actividades que realice la competencia, etc. Cada empresa tiene su equilibrio natural y el auditor deberá evaluar sin los plazos en uso su

empresa son los adecuados.

En cualquier caso, independiente d la metodología, los plazos y las acciones concretas llevadas a cabo, debe existir un proceso, con participación activa de los usuarios (aspecto clave), que regularmente elabore planes estratégicos de Sistemas de Informática largo plazo, cualquiera que sea ese largo, y el auditor deberá evaluar su adecuación.

Guía de auditoria

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

Entre otros aspectos, deberá evaluar si:

- Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa, se establecen mecanismos de sincronización entre sus grandes hitos y los proyectos informáticos asociados y se tienen en cuenta aspectos como cambios, organizativos entorno legislativo, evolución tecnológico, organización informática, recursos, etc., Y sus impactos están adecuadamente escogidos en el Plan Estratégico de sistemas de información igualmente, el auditor deberá evaluar si se presta adecuada consideración a nuevas tecnologías informáticas, siempre desde el punto de vista de su contribución a los fines de la empresa y no como experimentación tecnológica.
- Las tareas y actividades presentes en el Plan tiene la correspondiente y adecuada asignación de recursos para poder llevarlas a cabo. Así mismo, si tienen plazos de consecución realistas en función de la situación actual de la empresa, de la organización informática, del estado de la tecnología, de experiencias pasadas, etc.

Entre las acciones a realizar, se puede describir:

- Lectura de actas de sesiones del Comité de Informática dedicadas a la planificación estratégica.
- Identificación y lectura de los documentos intermedios prescritos por la metodología de planificación.
- Lectura y comprensión detallada del plan e identificación de las consideraciones incluidas en el mismo sobre los objetivos empresariales, cambios organizativos, evolución tecnológica, plazos y niveles de recursos, etc.
- Realización de entrevistas al Director de Informática y otros miembros del Comité de Informática participantes en el proceso de elaboración del Plan Estratégico.
- Igualmente realización de entrevistas a representantes de los usuarios con el fin de evaluar su grado de participación y sintonía con el contenido del Plan. Este es un Aspecto esencial. A lo largo de la historia de la informática ha habido épocas en las que los informáticos se arrogaban demasiados privilegios de decisión sobre las necesidades de los usuarios y aunque ahora estos modos y maneras ya

han caído en desuso, el auditor debe estar siempre vigilante para comprobar que el punto de vista de los usuarios es ampliamente tenido en cuenta.
- Identificación y comprensión de los mecanismos existentes de seguimiento y actualización del plan y de su relación con la evolución de la empresa.

8.2.2 Otros planes relacionados

Como se ha comentado más arriba, normalmente, deben existir otros planes informáticos, todos ellos nacidos al amparo del Plan Estratégico. Entre otros, los más habituales suelen ser (con nombres más o menos similares):

- Plan operativo anual
- Pla de dirección tecnológica
- Plan de arquitectura de la información
- Plan de recuperación ante desastres

Algunos de ellos (Plan tecnológico, Plan de arquitectura) aparecen a veces integrados en el propio Plan Estratégicos. En este capítulo se trataran solo dos de estos planes, los más comunes que, además, siempre tienen vida propia: Plan operativo anual y Plan de recuperación.

Plan operativo anual

El plan operativo se establece al comienzo de cada ejercicio (año, normalmente) y es el que marca las pautas a seguir durante el mismo. Suele coincidir en el tiempo con el proceso de presupuestario general de la empresa para el año siguiente, debe estar, obviamente, alineado con el Plan Estratégico y es también una ocasión propicia para evaluar si los objetivos marcados en este siguen siendo válidos y coherentes. Así mismo, debe estar precedido de una recogida de necesidades de los usuarios (actividad esencial una vez más).

El plan operativo de Sistemas de Información describe las actividades a realizar durante el siguiente natural. En otros aspectos, debe señalar los sistemas de información a desarrollar, los cambios tecnológicos previos, los recursos y los plazos necesarios, los costes anticipados, los responsables, etc.

El auditor deberá evaluar la existencia del Plan y su nivel de Calidad. Deberá estudiar1 su alineamiento con el Plan Estratégico, su grado de atención a las necesidades de los usuarios, sus previsiones de los recursos necesarios para llevar a cabo el Plan, etc. Deberá analizar si los plazos descritos son realistas teniendo en cuenta, entre otras cosas, las experiencias anteriores en la empresa, etc.

Plan de recuperación ante desastres

Una instalación informática puede verse afectada por desastres de variada naturaleza: incendio, inundación, fallo de algún componente critico de hardware, roco, sabotajes, acto de terrorismo, etc. Que tenga como consecuencia inmediata la disponibilidad de un servicio informático adecuado. La dirección debe prever esta posibilidad y, por tanto, planificar para hacer frente.

Estrictamente hablando, la responsabilidad de hacer frente a su riesgo es la dirección General de la empresa y ello por las siguientes razones al menos:

- Porque lo que se trata de proteger con un plan de este tipo es la actividad de la empresa, no solo la actividad de los sistemas de información.
- Porque se necesita la colaboración del resto de la empresa para plasmar y crear un plan (un documento, no se olvide) creíble y que sea útil para el objetivo de proteger de la empresa, y no hay nadie mejor que los propios departamentos empresariales involucrados en el día a día para conocer que necesitan y como deben operar en ausencia de servicio
- Porque las necesidades presupuestarias derivadas de un plan de este tipo son muy importantes y están, en general, fuera del alcance de la aprobación directa de la Dirección de Informática.

La dirección de Informática debe actuar como impulsor, catalizador, impulsor de este plan. En otro capítulo de este libro, se cubren los aspectos relativos a la auditoria de un plan de recuperación ante desastre.

8.3 ORGANIZAR Y COORDINAR

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

8.3.1 Comité de Informática

Una de las acusaciones mas comúnmente lanzadas contra la informática y de los informáticos es la falta de comunicación y entendimiento que se establece entre el departamento de informática en la empresa y el resto de la misma. El comité de Informática es el primer lugar de encuentro dentro de la empresa de los informáticos y sus usuarios: es el lugar en el que se debaten los grandes asuntos de la informática que afectan a toda la empresa y permite a los usuarios conocer las necesidades del conjunto de la organización no solo las del área y participar en la fijación de prioridades. Se evitan así acusaciones de favoritismo entre unas áreas usuarios y otras en relación al trato recibido de informática y, en definitiva, se atiende a la mejor utilización de los recursos informáticos, tradicionalmente escasos.

Si bien estrictamente el nombramiento, la fijación de funciones, etc. del Comité de Informática no son responsabilidades directas de la Dirección de Informática, si no de le Dirección General fundamentalmente. la Dirección de Informática se ha de convertir en el principal impulsor de la existencia de dicho Comité.

Aunque no existe regla fija, el Comité debería estar formado por pocas personas y presidido por el director más senior, dentro de la empresa, responsable en último término de las tecnologías de la información, posición que puede coincidir o no con el propio Director de Informática, Éste debería actuar como secretario del Comité y las grandes áreas usuarias deberían estar representadas a] nivel de sus directores más senior, Así mismo, el director de Auditorio Interna debería ser miembro del Comité. (otras personas de la organización también pueden integrarse en el Comité como miembros temporales cuando se traten asuntos de su incumbencia o de su especialidad.

Se ha escrito mucho sobre las funciones que debe realizar un Comité de Informática y parece existir un cierto consenso en, al menos, los siguientes aspectos:

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

Guía de auditoria

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

Para ello, deberá conocer, en primer lugar, las funciones encomendadas al Comité. En este punto, difieren las acciones concretas que el auditor deberá emprender ya que dependerán, en gran manera, del grado de formalización imperante en la empresa. En unos casos, existirá una normativa interna explicando Los objetivos. responsabilidades. componentes, etc. del Comité y en otros no existirá nada de eso y no habrá 111.ÉIS que reuniones informales y no periódicas del mismo.

Entre las acciones a realizar, figuran:

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

Una vez establecida la existencia del Comité de informática, habrá que evaluar la adecuación de las funciones que realiza, Para ello, el auditor, mediante un conjunto de entrevistas. lecturas de documentación interna del Comité. etc., deberá establecer un juicio sobre la validez, adecuación. ele, de las actuaciones del Comité. Uno de los aspectos fundamentales que deberá revisar es lo que hace referencia a la presencia y participación electiva de las áreas usuarias (aspecto esencial, tina vez más.

Entre las acciones a realizar, figuran:

- Lectura de las actas del Comité y entrevistas a los miembros del mismo, con especial incidencia en los representantes de los usuarios para comprobar que:

- el Comité cumple efectivamente con las funciones enunciadas más arriba,
- los acuerdos son tornados correctamente y los puntos de vista de los representantes de les usuarios son tenidos en cuenta.

8.3.2 Posición del departamento de Informática en la empresa

El segundo aspecto importante a tener en cuenta a la hora de evaluar el papel de la informática en la empresa es la ubicación del Departamento de Informática en la estructura organizativa general de la misma. El Departamento deberla estar suficientemente alto en la jerarquía y contar con masa crítica suficiente para disponer de autoridad e independencia frente a los departamentos usuarios.

Tradicionalmente, la informatización en las empresas comenzó por e] departamento financiero o de administración y, por tanto, el esquema tradicional era encontrar al departamento de informática integrado dentro del mismo_ Hoy en dio, la informática da soporte a un conjunto mucho mayor de áreas empresariales y. por ello, coda *%ei* es más habitual encontrar a departamentos de informática dependiendo directamente de Dirección General. Siempre que el departamento de informática esté integrado en algún departamento usuario, pueden surgir dudas razonables sobre su ecuanimidad a la hora de atender las peticiones del reste de departamentos de la empresa.

Además, empieza ya a ser bastante habitual que el director de Informática sea miembro de derecho del Comité de Dirección u árgano semejante, aunque esta situación depende mucho del sector de actividad: cuanto más estratégicas son las tecnologías de la información para la empresa. mayor es la necesidad de contar con su representante en el máximo órgano decisorio de la organización.

Una vez más, estrictamente hablando, la posición del Departamento de Informática a no es de la incumbencia de su Dirección sino de pitos estamentos empresariales. probablemente.

la Dirección General. Sin embargo. se trae a colación en este capítulo, porque el auditor debe evaluar si las necesidades de los diferentes departamentos de la empresa son tratadas equitativamente por Informática y no existe un sesgo demasiado alto hacia un departamento o departamentos concretos de la misma. Si este último ocurriera, una de las primeras razones para ello puede ser la ubicación incorrecta de dicho Departamento.

Guía de auditoria

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

independencia y atención del Departamento de Informática.

8.3.3 Descripción de funciones y responsabilidades del Departamento de Informática.

Segregación de funciones

Es necesario que las grandes unidades organizativas dentro del Departamento de Informática tengan sus funciones descritas y sus responsabilidades claramente delimitadas y documentadas Igualmente, es necesario que este conocimiento se extienda a todo el personal perteneciente a Informática: todos ellos deben conocer sus funciones y responsabilidades en relación con los sistemas de información. Y todo ello es una labor que compete. en gran medida. a le Dirección de informática.

Por otro lado, es de lodo punto esencial para tener un entorno controlado que exista una segregación de funciones, La filosofía básica que *debe* orientar esta separación de papeles es impedir que un solo individuo tenga actividades incompatibles en un proceso critico (por ejemplo, un programador que pueda modificar una aplicación. probarla y traspasarla al entorno de producción; o un responsable de seguridad que pueda autorizar a Los usuarios para al: ceder al sistema informático y además darles de alta en ese mismo sistema), Además. se debería asegurar que el personal de Informática actúa únicamente dentro de la descripción de las funciones existente para su puesto de trabajo concreto.

En particular, se debería asegurar la segregación entre las funciones de desarrollo de sistemas de información y la de producción o explotación y entre estos dos y los departamentos de usuarios (los informáticos no deben sustituir nunca a los usuarios. por ejemplo. alterando datos directamente en los ficheros informáticos sin mediar aprobación previa de los usuarios pertinentes). Además, es aconsejable que *la* función de administración de la seguridad esté cierne/lente sepan¯ida de la de producción, incluso que no dependa de. la Dirección de Informática (por segregación de funciones exclusivamente: esta última organización jerárquica puede tener otras complicaciones cuyas consideraciones están fuera del objetivo de este capítulo).

Aseguramiento de Calidad

La calidad de los servicios ofrecidos por el Departamento de Informática debe estar asegurada mediante el establecimiento de una función organizativa de Aseguramiento de la Calidad. Hoy en día. se asiste en las organizaciones informáticas evolucionadas, cada vez más, a la aparición de esta función de control de calidad de los servicios informáticos, a imagen y semejanza de las organizaciones en el mundo industrial, Esta función de control ha de ser independiente de la actividad diaria del departamento y ha de depender directamente de La Dirección de Informática.

Es muy importante que esta función. de relativa nueva aparición en el mundo de las organizaciones informáticas, tenga el total respaldo de la Dirección y percibido así por el resto del Departamento.

Guía de auditorio

No es propósito de este capítulo describir les funciones de un departamento de informática. Ello se describe en otros capítulos de este libro, además de que existe: una amplísima bibliografía sobre la materia. El aspecto fundamental que queremos resaltar aquí es que el auditor deberá comprobar que las descripciones están documentadas y son actuales y que las unidades organizativas informáticas Las conocen y comprenden y desarrollan su labor de acuerdo a las mismas.

Entre las tareas de autor que el auditor podrá realizar. figuran.

- Examen del organigrama del Departamento de Informática e identificaban de las grandes unidades organizativas.
- Revisión de la documentación existente para conocer la descripción de las funciones y responsabilidades.
- Realización de entrevistas a los directores de cada una de las grandes unidades, organizativas para determinar su conocimiento de las responsabilidades de su unidad y que éstas responden a las descripciones existentes en la documentación correspondiente y a actuación en el din a día operativo.
- Examen de las descripciones de las funciones para evaluar si existe adecuada segregación de funciones, incluyendo la separación entre desarrollo de sistemas de información, producción y departamentos usuarios. Igualmente, será menester evaluar la independencia de la función de seguridad.
- Observación de las actividades del personal del Departamento para analizar, en la práctica, las funciones realizadas, la segregación entre las mismas y el grado de cumplimiento con la documentación analizada.

Aseguramiento de la Calidad

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

Entre las acciones a llevar a cabo, se pueden considerar,

- Conocimiento de la posición de la Función en el organigrama del
- Departamento de Informática.
- Análisis del grado de cumplimiento de las actividades del Departamento una relación a las políticas, estándares y procedimientos existentes tamo generales

del Departamento, cornos específicos de sus funciones organizativos. De particular importancia es el grado de cumplimiento de la metodología del ciclo de vida de los sistemas de información, de los procedimientos que gobiernan la explotación del ordenador y de la investigación de la calidad de los datos que se envían a los usuarios.

- Revisión de algunos informes emitidos por la Función con el fin de evaluar si su estructura y contenido son adecuados. Analizar la existencia de acciones de seguimiento basadas en dichos informes.

8.3.3.1 ESTANADARES DE FUNCIONAMIENTO Y PROCEDIMIENTOS. DESCRIPCION DE LOS PUESTOS DE TRABAJO

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

De particular importancia son los aspectos relacionados con la adquisición de equipos o material para el Departamento, con el diseño y el desarrollo/modificación de sistemas de información, con la producción o explotación y con la administración de la seguridad.

Además, dichos estándares y procedimientos deberían estar documentados, actualizados y ser comunicados adecuadamente a lodos los departamentos afectados, La Dirección de informática debe promover la adopción de estándares y procedimientos y dar ejemplo de su uso.

Por otro lado, deben existir documentadas descripciones de los puestos de trabajo dentro de Informática delimitando claramente la autoridad y responsabilidad en cada caso. Las descripciones deberían incluir los conocimientos técnicos y/o experiencia necesarios para cada puesto de trabajo.

Gula de auditorio

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

Entre las acciones a realizar, se pueden citar,

- Evaluación del proceso por el que los estándares, procedimientos y

  puestos de trabajo son desarrollados, aprobados, distribuidos y actualizados.

- Revisión de los estándares y procedimientos existentes para evaluar si transmiten y promueven en una filosofía adecuada de control. Evaluación de su adecuación, grado de actualización y nivel de cobertura de las actividades informáticas y de las relaciones con los departamentos usuarios.

- Revisión de las descripciones de los puestos de trabajo para evaluar si reflejan las actividades realizadas en la práctica.

8.3.3.2 GESTION DE RECURSOS HUMANOS: SELECCIÓN, EVALUACIONDEL DESEMPEÑO, FORMACION, PROMOCION, FINALIZACION

La gestión de los recursos humanos es uno de los elementos críticas en la estructura general informática. como en cualquier organización de personas. La calidad de los recursos humanos influye directamente en la calidad de los sistemas de información producidos, mantenidos y operados por el Departamento de informática. Además, parte de los recursos humanos necesarios en tusa instalación informática son grandes expertos técnicos, Seleccionarlos, mantenerlos y motivarlos adecuadamente puede ser crucial para la buena marcha de lo informática y su papel en la empresa.

Gula de auditoria

Entre otros aspectos, el auditor deberá evaluar que:

- La selección de personal se basa en criterios objetivos y tiene en cuenta la formación experiencia y niveles de responsabilidad anteriores.
- El desempeño de cada empleado se evalúa regularmente en base en estándares establecidos y responsabilidades específicas del puesto de trabajo. Que los objetivos a alcanzar por cada empleado y Los criterios bajo los que va a ser evaluado son conocidos por cada empleado en base a un ciclo periódico (anual, normalmente) de evaluación.
- Existen procesos para determinar las, necesidades de formación de los empleados en base a su experiencia. puesto de trabajo, responsabilidad y desarrolla futuro personal y tecnológico de la instalación Se planifica la cobertura ordenada de estas necesidades y se lleva a la práctica.
- Existen procesos para la promoción del personal que tienen en cuenta se desempeñó procesional.
- Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los. contratos laborales no afectan a los controles internos y a la seguridad informática.

Adiarás. el auditor deberá evaluar que todos los aspectos anteriores están en línea con las políticas y procedimientos de la empresa.

Entre las acciones a realizar, se pueden citar

- Conocimiento y evaluación de los procesos utilizados para cubrir vacantes en el Departamento de Informática bien sea por promoción interna, búsqueda directa de personal externo, utilización de empresas de selección de personal o de trabajo temporal.
- Análisis de las cifras de rotación de personal, niveles de absentismo laboral y estadísticas de proyectos terminados fuera de presupuesto y de plazo. Si los números son anormales (muy altos), podría constituir una señal de falta de

liderazgo por parle de la Dirección de Informática de motivación por parte del personal.

- Realización de entrevistas al personal del Departamento paro determinar su conocimiento de las responsabilidades asociadas a su puesto de trabajo, si los procesos de evaluación han seguido las paulas mareadas en la política general de la empresa, si los empleados conocían los estándares de desempeño, sus objetivos particulares y los criterios que se iban a seguir en su evaluación y si los resultados de sus evaluaciones de desempeño les han sido comunicados de una manera acorde con los procedimientos establecidos,
- Revisión del calendario de cursos, descripciones de los mismos, métodos y técnicas de enseñanza. para determinar que los cursos son consistentes con los conocimientos. experiencia, responsabilidades, etc. asignadas al personal y con la estrategia tecnológica marcada parte los sistemas de información de la empresa,
- Revisión de los procedimientos para la finalización de contratos. Evaluar si dichos procedimientos prevén que los identificadores de usuario, contraseñas y otros dispositivos necesarios para tener acceso a los locales y sistemas informáticos son cancelados, desuellos, etc. con efectividad inmediata tras la finalización del contrato de un empleado.

Comunicación

Es necesario que exista una comunicación efectiva y eficiente entre la Dirección de informática y el resto del personal del Departamento. Entre los aspectos que son importantes hacer llegar se encuentran: actitud de servicio hacia las usuarios y resto de la empresa. actitud positiva hacia los controles. integridad. ética, cumplimiento de la normativa interna -entre otras, la de seguridad informática-. compromiso) con la calidad, cte.

Cuila de auditoria

EJ auditor deberá evaluar las características de la comunicación entre la Dirección y el personal de Informática. Para ello se podrá servir de tareas formales come las descritas hasta ahora y de otras, por ejemplo, a través de entrevistas informales con el personal del Departamento.

8.3.3.3 GESTIÓN ECONÓMICA

Este apartado de las responsabilidades de la Dirección de Informática tiene varias facetas: presupuestario, adquisición de bienes y servicios y medida y reparto de costes,

Presupuestario

Como lodo departamento de la empresa, el de informática debe tener un presupuesto económico, normalmente en base anual. Los criterios sobre cuáles deben ser los componentes del mismo varean grandemente. Un ejemplo típico son los costes de las comunicaciones: en unos casos es el propio Departamento quien Las administra y, en otros casos, puede ocurrir que la politiza de la empresa indigne que sean pagados por los departamentos usuarios_ En Loro ejemplo, también puede ocurrir que los terminales

(pantallas e impresoras) sean costeados por los usuarios en vez de serio por Informática. Sea cual sea la política seguida en la empresa, el Departamento de Informática debe seguirla para elaborar su presupuesto anual.

No vamos a entrar aquí en los diversos métodos existentes de presupuestación, pero el auditor deberá juzgar si son apropiados. Lo que si deberla darse en todo proceso de presupuestación de un Departamento de Informática es una previa petición de necesidades. a les departamentos usuarios (aspecto, como ya se ha señalado 'varias veces en este capítulo, esencial. Adicionalmente, el Departamento tendrá sus propias necesidades: enrabio o ampliación de los ordenadores o de los discos, de elementos de seguridad, de equipamiento auxiliar (aire acondicionado, sistemas de alimentación ininterrumpida…}, instalación de un robot manejador de cartuchos, de una unidad de comunicaciones, etc.. que se deberán integrar en el presupuesto, Lo más lógica es elaborar al mismo tiempo el presupuesto económico y el Plan operativo anual.

Guía de auditoria

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

Adquisición de bienes y servirlos

Los procedimientos que el Departamento de Informática siga para adquirir los bienes y servicios descritos en su plan operativo anual y/o que se demuestren necesarias a lo largo del ejercicio han de estar documentados y alineados coa los procedimientos de compras del resto de la empresa. Aquí, la variedad es infinita con lo que es imposible dar reglas fijas.

Guía de auditoria

Una auditoria de esta área no debe diferenciarse de una auditoria tradicional del procese de compras de cualquier otra área de la empresa, con lo que el auditor deberá seguir básicamente las directrices y programas de trabajo de auditoria elaborados para este proceso.

Medida y reparto de costes

La Dirección de Informática debe en lodo momento gestionar los costes asociados con la utilización de los recursos informáticos, humanos y tecnológicos. Y ello, obviamente, exige medirlos.

Un aspecto muy relacionado es el reparto de los costes del Departamento entre los usuarios. Esta medida no está implantada en todas las empresas y, además, tiene sus ventajas e inconvenientes que, también, se encuentran fuera del alcance de este capítulo. Normalmente. la existencia o ausencia de un sistema de este tipo suele estar muy asociada a la propia cultura de la empresa, En cualquier caso, es cierto que, de estar presente, se da en general, con mayor frecuencia, en grandes organizaciones con

importantes departamentos de informática, No es habitual encontrar un sistema de reparto de costes informáticos en empresas de tamaño mediano o pequeño.

Guía de auditoria

El reparte de costes suele ser un tema delicado. En realidad, los asuntos espinosos suelen ser el llamado precio de transferencia, o sea el coste interno que el Departamento de Informática repercute a los departamentos usuarios por los servicios les presta, así como los componentes de coste incluidos en dicha facturación interna, no siempre inteligibles para las unidades de negocio.

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

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

- Realización de entrevistas a la dirección de los departamentos usuarios para evaluar su grado de comprensión de los componentes. de coste utilizados en la fórmula de cálculo del precio de transferencia.
- Análisis de los conceptos y criterios con los que está calculado el precio de transferencia para evaluar su ecuanimidad y consistencia, y acudir al mercado externo y a ofertas de centros de proceso de dalos independientes para comprarlas cori dichos costes internos,
- Conocimiento de los diversos sistemas existentes en el Departamento para recoger y registrar la actividad del mismo (consumo de recursos de máquina, número de líneas impresas, horas de programación, de help-desk, etc..), para procesarla con el fin de obtener la información de costes y presentarla de una manera apropiada.

Seguros

La Dirección de Informática debe tomar las medidas necesarias con el fin de tener suficiente cobertura de seguros para los sistemas informáticos, Aquí se incluyen no solo las coberturas más tradicionales COMO la de los equipos (el hardware) o la de infidelidad de los empleados, sino también otro tipo de coberturas normalmente más asociadas a la repentina interrupción del servicio informático per causa de algún desastre. Estas coberturas amparan riesgos tules como la posible pérdida de negocio derivada de dicha interrupción, los costes asociados a tener que ofrecer servicio informático desde un lugar alternativo al estar indisponible el sitio primario, los costes asociados a la regeneración de datos por pérdida o inutilización de los datos originales, ele.

GUIA DE AUDITORIO

El auditor deberá estudiar las pólizas de seguros y evaluar La cobertura existente, analizando si la empresa está suficientemente cubierta o existen huecos en dicha cobertura, Por ejemplo. algunas pólizas solo cubren el remplazo del equipo, pero no los otros costes mencionados, etc.

8.4 CONTROLAR

La tarea de dirigir no puede considerare completa sin esta faceta que Forma parte indisoluble de tal responsabilidad,

8.4.1 Control y Seguimiento

Un aspecto común a todo lo que se ha dicho hasta el momento es la obligación que la Dirección tiene de controlar y efectuar un seguimiento permanente de La actividad del Departamento. Se ha de vigilar la elaboración de los planes estratégico y operativo y de los proyectos que los desarrollan, La ejecución del presupuesto, la cartera de peticiones de usuario pendientes, la evolución de los costes. los planes de formación, la evolución de la carga del ordenador y de los otros recursos (espacio en disco, comunicaciones, capacidad de las impresoras..._), etc.

En esta labor, es muy conveniente que existan estándares de rendimiento con los que comparar la actividad del Departamento. Una de las técnicas que más se utiliza para ello y para gobernar las relaciones entre el Departamento de Informática y los usuarios son los llamados Acuerdos del Nivel de Servicio (ANS, también llamados Servicie Level Agreemnts o SLA por su nombre en inglés).

Los ANS constituyen documentos que reflejan acuerdos entre dos partes, Departamento de informática y usuarios, en los que quedan descritos los servicios que aquél presta a los últimos y los indicadores que sirven para medirlos. A Galileo Galilei se le atribuye una frase que viene muy a colación en este apanado: "Mide todo lo que puedas medir y lo que no sea, hazlo medible” Y este es el espíritu detrás de los ANS. Entre sus ventajas, se pueden mencionar.

- Permiten objetivar las relaciones entre el Departamento de Informática y los usuarios de tal manera que una parte conoce qué servicios tiene que suministrar y la otra qué servicios y en qué forma debe esperar recibir.
- Existen mecanismos claros de medida del nivel de cumplimiento de dichos servicios.
- Los ANS son aplicables a las diversas facetas de la producción del Departamento hacia los usuarios y son un documento vivo suele tener una validez anual.

Guía de auditoria

Entre las acciones a realizar, se puede mencionar:

Conocimiento y análisis de los procesos existentes en el Departamento para llevar a cabo el seguimiento y control. Evaluación de la periodicidad de los mismos. Analizar igualmente los procesos de Re presupuestación económica, si existen, y las consideraciones que se tiene en cuenta.

Revisión de planes. Proyectos, presupuestos de años anteriores y del actual para comprobar que son estudiados, que se analizan las desviaciones y que se toman las medidas correctoras necesarias.

Conocimiento y análisis de los procesos existentes para la negociación de los ANS y acuerdo con los usuarios. El auditor no debe evaluar tanto el contenido de los ANS sino más bien que existen, que cumplen su papel de mejora de las relaciones Informática-usuarios, tiene la oportunidad de participar y su opinión es tenida en cuenta, que hay implantados mecanismos para su denuncia y renegación en su caso etc.

8.4.2 Cumplimiento de la normativa legal

La dirección de Informática debe controlar que la realización de sus actividades se lleva a cabo dentro del respeto a la normativa legal aplicable. En particular, se consideran fundamentales los relativos a la seguridad e higiene en el trabajo, normativa laboral y sindica, protección de datos personales, propiedad intelectual del software, requisitos definidos en la cobertura de seguros, prevención de riesgos laborales, etc. Así como normativa emitida por órganos reguladores sectoriales.

Así mismo, deben existir procedimientos para vigilar e identificar permanente la legislación aplicable.

Guía de auditoria

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

Para ello, deberá, en primer lugar, entrevistarse con la Asesoría Jurídica de la empresa, la Dirección de Recursos Humanos y la Dirección de Informática con el fin de conocer dicha normativa, todo ello independiente de su responsabilidad de conocer el entorno legislativo aplicable a su empresa que, como auditor, le obliga.

A continuación, evaluara el cumplimiento de las normas, en particular, en los aspectos más críticos mencionados mas arriba. Si el auditor no es un técnico en los distintos aspectos legales, deberá buscar asesoramiento adecuado, interno a la empresa o externo.

8.5 CONCLUCIONES

La auditoría de Dirección de Informática es una tarea difícil. Sin embargo, la contribución que dicha Dirección de Informática realiza (o debe realizar) al ambiente de control de las operaciones informáticas de una empresa es esencial. Desde punto de vista de auditoria, la calidad del marco de controles impulsado e inesperado por la Dirección Informática tiene una gran influencia sobre el probable comportamiento de los sistemas de información. Por parte del auditor, se necesitan capacidades de evaluar la gestión más capacidades técnicas muy profundas.

8.6 LECTURAS RECOMENDADAS

Control de objectives for Information and reeled Technology version 4.1, IT Governance Institute 2007. La serie de publicaciones emitidas alrededor del COBIT constituyen una amplísima fuente de documentación y referencia para el auditor informático.

8.7 CUESTIONES DE REPASO

1. Descríbanse las actividades a realizar por un auditor para evaluar un plan estratégico de sistemas de información.
2. Descríbanse las funciones de un comité de informática. Elabórese una lista con las funciones empresariales que deberían estar representadas en dicho comité. ¿Qué objetivo tiene para los usuarios su presencia en el comité?
3. Descríbanse las ventajas de tener procedimientos. Elaborase un guion de lo que podrían ser procedimientos de: a) diseño de sistemas, b) programación.
4. ¿Qué evidencias deberá buscar el auditor para poder evaluar si las necesidades de los usuarios son adecuadamente tenidas en cuenta?
5. Identifíquense las actividades incompatibles desde un punto de vista de control en un departamento de informática. Razónese.
6. ¿Qué ventajas de control aporta la existencia de la función de aseguramiento de la calidad?
7. Descríbase los objetivos del control a ser evaluados por el auditor en el apartado de gestión de recursos s humanos.
8. ¿Qué tareas debe hacer un auditor para evaluar el plan de formación del QUINTA PARTEdepartamento de informática? ¿Como puede juzgar si dicho plan está acorde con los objetivos de la empresa?
9. Relaciónense las actividades a realizar por un auditor para la evaluación del precio de transferencia de reparto de costes entre el departamento de informática y los usuarios.
10. Descríbase un programa de trabajo para evaluar acuerdos de nivel de servicio para el área de desarrollo y programación, identifique si los principales conceptos de servicio que deberían contener a n ANS, así como los indicadores de media parientes.

QUINTA PARTE: SEGURIDAD EN LOS SISTEMAS DE BASES DE DATOS

Capítulo 9

AUDITORÍA DE BASES DE DATOS

9.1 INTRODUCCIÓN

La gran difusión de los Sistemas de Gestión de Rases de Datos (SGBD), junto con la consagración de los datos corno Orlo de los recursos fundamentales de las empresas, han hecho que los temas relativos a su control interno y auditoria cobren, cada día, mayor interés. De hecho, las bases de datos se han convertido en el corazón de los sistemas de información de las organizaciones. que cada día más dependen del buco Funcionamiento de éstos para su supervivencia.

Además de por su importancia económica y empresarial, la auditoría de bases de datos ha sufrido un gran impulso en Espacia, a partir de la entrada en vigor de la Ley Orgánica 5/1992 de 29 de octubre de Regulación del Tratamiento Automatizado de Datos de carácter personal (conocida como LORTAD) y del Reglamento correspondiente, así corno de su sucesora la Ley Orgánica 15/1999, de 13 de diciembre de Protección de los Datos de Carácter Personal (conocida por LOPD) que traspone la Directiva 95416/CE, de 24 de octubre, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

Además, el control interno y la auditoria de bases de datos resultan fundamentales para el control y la auditoria de las aplicaciones que acceden a las mismas, y para proporcionar confianza sobre lodo del sistema de información. De hecho, el ITGI (Information Technology Governante Instinde) en el CobiT destaca, entre los recursos principales de TI, dos que están muy estrechamente relacionados con los sistemas de bases de datos:

De hecho, el ITGI (Information Technology Governante Instinde) en el CobiT destaca, entre los recursos principales de TI, dos que están muy estrechamente relacionados con los sistemas de bases de datos:

- La información, definida en el COBIT como "los datos en todos sus. formatos, de entrada. procesados o de salida de los sistemas de información sea cual sea la manera en que san usados por la organización",
- La infraestructura, es decir, la tecnología e instalaciones. incluyendo el sistema de gestión de bases de datos.

9.2 METODOLOGÍA PARA LA AUDITORIA DE BASE DE DATOS

Siguiendo la metodología de auditoria propuesta por la ISA CA, se empezaría fijando los objetivos de control que minimizan los riesgos potenciales a los que está sometido el

entorno de bases de datos.

Considerando estos riesgos, se podría definir por ejemplo el siguiente:

Objetivo de Control:

El SGBD deberá preservar la confidencialidad de la base de datos.

Una vez establecidos los objetivos de control, se especifican las técnicas especificas correspondientes a dichos objetivos, por ejemplo:

Técnica de Control:

Se deberán establecer los «pos de usuarios, perfiles y privilegios necesarios para controlar el acceso u la base de datos.

Un objetivo de control puede llevar asociadas varias chicas que permiten cubrirlo en su totalidad. Estas técnicas pueden ser preventivas (corno la arriba mencionada), defectivas (corno, por ejemplo, monitorizar los accesos a la BD) o correctivas (por ejemplo, una copia de respaldo -backup).

En caso de que los controles existan, se diseñan unas pruebas (denominadas pruebas de cumplimiento) que permiten verificar la consistencia de los mismos, por ejemplo:

Prueba de cumplimiento:

Listar los privilegias y perfiles existentes en el SGBD.

Si estas prueban detectan inconsistencias en los controles, o bien, si los controles no existen, se pasa a diseñar otro tipo de pruebas -denominadas pruebas sustantivas- que permitan dimensionar el impacto de estas deficiencias.

Prueba sustantiva:

Comprobar si la información ha sido corrompida comparándola con otra Mente. o revisando los documentos de entrada de datos y las transacciones que se han ejecutado.

Una vez valorados los resultados de las pruebas se obtienen unas conclusiones que serán comentadas y discutidas con los responsables directos de las áreas afectadas con el fin de corroborar los resultados, Por último, el auditor deberá emitir una serie de comentarios donde se describa la situación, el riesgo existente, la deficiencia a solucionar y, en su caso, sugerirá la posible solución.

Como resultado de la auditoria. se presentará un informe final en el que se expongan las conclusiones más importantes a las que se ha llegado, así corno el alcance que ha tenido la auditoria.

Esta será la técnica a utilizar para auditor el entorno general de un sistema de bases de datos, tanto en su desarrollo como durante la explotación.

9.3 RECOMENDACIONES DE LOS COBIT PARA AUDITORIA DE BASE DE DATOS

En COBIT los principales objetivos de control relacionados con las bases de datos son los siguientes (ITGI, 2007a):

- P02 Definir la Arquitectura de información
- P02,1 Modelo Corporativo de Arquitectura de Información
- P02.2 Diccionario de Datos Corporativo y Reglas de Sintaxis de Datos
- P023 Esquema de Clasificación de Datos
- P02,4 Gestión de Integridad
- DS 11 Gestionar Datos
    - DS 11.1 Requisitos de Negocio para la Gestión de Datos
    - DS 11.2 Planes de Almacenamiento y Retención de Datos
    - DS 1 13 Sistema de Gestión de Bibliotecas de Medios
    - D511.4 Eliminación de Datos
    - DS 1 1.5 Copia de Respaldo y Restauración
    - DS 11.6 Requisitos de Seguridad para Gestión de Datos

Para estos objetivos de control se definen diferentes objetivos y métricas. Así, por ejemplo, para el DS1 1 se establecen los siguientes:

- Objetivos de las tecnologías de la información: optimizar la utilización de la información, asegurar que la información crítica y confidencial es inaccesible para aquellos que no deben tener acceso a la misma y asegurar la conformidad de las tecnologías de la información con las leyes, regulaciones y contratos, Para estos objetivos se proponen algunas métricas como: el número de ocurrencias de incapacidad para recuperar datos críticos para los procesos de negocio, el porcentaje de satisfacción del usuario con la disponibilidad de los datos y el número de incidentes de no conformidad con las leyes debido a cuestiones de gestión de almacenamiento.
- Objetivos de los procesos: mantener la compleción, exactitud, valide, y accesibilidad de los datos almacenadas; asegurar los datos durante la entrega de medios, gestionar efectivamente el almacenamiento de los medios. Para estos objetivos se proponen como métricas: el porcentaje de restauraciones de datos exitosas, el número de incidentes en los que se recuperan datos sensibles después de disponer de los medios y el isómero de caldas de sistemas o incidentes de integridad de dates causados.
- Objetivos de las actividades: realizar copias de respaldo y pruebas de restauración, gestionar almacenamiento de datos consiste y olvide. asegurar la disposición de

dalos y equipos. Algunas métricas son: la frecuencia de pruebas de copias de respaldo de los medios y el tiempo medio de restauración de datos.

En ITGI (2007h1 se definen para cada objetivo de control los drivers de valor y riesgo, y las pruebas de diseño del control correspondientes. Así, en el caso del DS11.6 de Requisitos de Seguridad para Gestión de Datos se proponen los siguientes:

- Drivers de valor: información sensible asegurada y protegida apropiadamente, capacidad de ver o alterar la información disponible a los usuarios autorizados, compleción y exactitud de datos transmitidos.
- Drivers de riesgo: datos sensibles mal utilizados o destruidos, accesos a datos 110 autorizados, falta de compleción e inexactitud de datos transmitidos, datos alterados por usuarios no autorizados
- Pruebas de diseño del control: preguntando y confirmando que:
- Se dispone de un proceso que identifica datos sensibles y aborda las necesidades organizativas relativas a la confidencialidad de los datos, conformidad con las leyes y regulaciones aplicables, y que se ha acordado [a clasificación de los datos con los propietarios de los procesos de negocio.
- Se define e implementa una política para proteger datos y mensajes sensibles de accesos no autorizados y transmisiones y transportes incorrectos, incluyendo: cifrado, código de autenticación de mensajes, totales hask etc.
- Se han establecido requisitos para el acceso físico y lógico a salidas de datos y se define y se tiene en cuenta la confidencialidad de la salida.
- Se han establecido reglas y procedimientos para el acceso por parte de los usuarios finales a las salidas de datos y para la gestión y realización de copias, de respaldo de datos sensibles.

9.4 OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS

A continuación, expondremos algunos objetivos y técnicas de control más específicos a tener en cuerna a lo largo del ciclo de vida de una base de datos, véase figura 9.1. que abarca desde el estudio previo hasta su explotación.

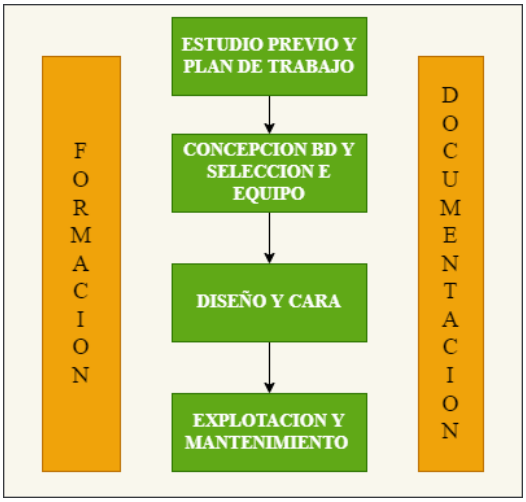

Figura 9.1, Cielo de vida de una base de datos

9.4.1 ESTUDIO PREVIO Y PLAN DE TRABAJO

En esta primera fase, es muy importante elaborar un estudio tecnológico de viabilidad en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto acompañados de un análisis coste-beneficio para cada una de las opciones. Se debe considerar entre estas alternativas la posibilidad de no llevar a cabo el proyecto (no siempre está justificada la implantación de un sistema de bases de datos) así como la disyuntiva unirle desarrollar y comprar (en la práctica, a veces nos encontramos que se ha desarrollado una aplicación que ya existía en el mercado, cuya compra hubiese supuesto un riesgo menor, asegurándonos incluso una mayor calidad a un precio inferior). Desafortunadamente, en bastantes organizaciones, este estudio de viabilidad no se lleva a cabo con el rigor necesario, con lo que a medida que se van desarrollando, los sistemas demuestran, a veces, ser poco rentables.

El auditor debe comprobar también que la alta dirección revisa los informes de los estudios de viabilidad y que es la que decide seguir adelante o no con el proyecto. Esto es fundamental porque los técnicos han de tener C11 cuenta que si no existe una decidida voluntad de la organización en su conjunto, impulsada por los directivos, aumenta considerablemente el riesgo de fracasar en la implantación del sistema.

Es importante destacar la necesidad de llevar a cabo una gestión de riesgos (valoración, identificación, medida, plan de acción y aceptación), que es objeto de atención, afortunadamente, de un número cada día mayor de organizaciones.

En caso de que se decida llevar a cabo el proyecto es fundamental que se establezca un plan director. debiendo el auditor verificar que efectivamente dicho plan se emplea para el seguimiento y gestión del proyecto, y que cumple con los procedimientos generales de gestión de proyectos que tenga aprobados la organización.

Otro aspecto muy importante en esta fase es la aprobación de la estructura orgánica no sólo del proyecto en particular, sino también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos: recordemos que. par-a que un entorno de base de datos funcione debidamente, esta unidad es imprescindible. En ITGI (2006) se contemplan diferentes roles relacionados con la Gestión de Datos (DS I I) que se reflejan en la tabla 13.1.

A la llora de detallar las responsabilidades de estas funciones hay que tener en cuenta uno de los principios fundamentales del control interno: la separación de funciones (véase en la tabla 13,1).

Se recomienda una separación de funciones entre:

- el personal de desarrollo de sistemas y el de explotación
- explotación y control de datos

- administración de bases de datos y desarrollo

Funciones Actividades	Trasladar los requisitos de almacenamiento y retención de datos en procedimientos	Definir, mantener e implementar procedimientos para gestionar la biblioteca de medios	Definir, mantener e implementar procedimientos para disponer de forma segura de los medios y	Realizar capias de respaldo	Definir, mantener e implementar procedimientos para restauración de datos
CIO	A	A	A	A	A
Propietario del proceso de negocio	1		C		C
Director de operaciones	C	R	R	R	R
Arq. jefe	R	C			C
Dir. De Desarrollo		C			C
Dir. De Adm.		1	1		
Cumplimiento Auditoria de Seguridad	C	C	C		1

Tabla 13.1. Roles relacionados con la Gestión de Datos (ITGI. 2006)

R = responsables A ="Accountable", C = Consultado, I = Informado

Debería existir también una separación de funciones entre el administrador de la seguridad y el administrador de la base de datos. Esto no quiere decir que estas tareas tengan forzosamente que desempeñarlas personas distintas no que no sería viable en muchas pequeñas y medianas empresas) pero sí que es un aspecto importante de control a considerar, por lo que en caso de que no pueda lograrse la separación de funciones, deberán establecerse controles compensatorios o alternativos. como. por ejemplo, una mayor atención de la dirección y la comprobación por parte de algún Usuaria del contenido y de las salidas más importantes producidas a partir de la BD.

9.4.2 Concepción de la Base de datos y selección del equipo

En esta fase se empieza a diseñar la base de datos, por lo que deben utilizarse los modelos y las técnicas definidos en la metodología de desarrollo de sistemas de la empresa, véase por ejemplo Piattini et al. (2003).

La metodología de diseño debería también emplearse para especificar los documentos fuentes. los mecanismos de control. las características de seguridad y las pistas de auditorio a incluir en el sistema, estos últimos aspectos generalmente se descuidan. lo que produce mayores costes y problemas cuando se quieren incorporar una vez concluida la implementación de la base de dalos y la programación de las aplicaciones.

El auditor debe por tamo, en primer lugar, analizar la metodología de diseño con el fin

de determinar si es o no aceptable. y luego comprobar su correcta utilización. Como mínimo una metodología de diseño de BE) debería contemplar dos fases de diseño: lógico y físico, aunque la mayoría de las empleadas en la actualidad contempla tres fases; además de las dos anteriores, una fase previa de diseño conceptual que sería abordada en este momento del ciclo de vida de la base de datos; véase. por ejemplo, Piattini etc. al. (2006b),

En cuanto a la selección del equipo, en case de que la empresa no disponga ya de uno, deberá realizarse utilizando un procedimiento riguroso, en el que se consideren, por un lado, las necesidades de la empresa (debidamente ponderadas) y, por otro. las prestaciones que ofrecen los distintos SGBD candidatos (puntuados de manera oportuna). Además, se debe tener en cuenta el impacto que el nuevo software tiene en el sistema y, especialmente. en su seguridad.

9.4.3 Diseño y carga

En esta fase se llevarán a cabo los diseños lógico y físico de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente, determinando si la definición de los datos contempla además de su estructura. las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad. El auditor tendrá que tomar una muestra de ciertos elementos (tablas. vistas, índices) y comprobar que su definición es completa, que ha sido aprobada por el usuario y que el administrador de la base de datos participó en su establecimiento.

Una vez diseñada la DI), se procederá a su carga, ya sea migrando datos de un soporte magnético o introduciéndoos manualmente, Las migraciones o conversiones de sistemas, como el paso de un sistema de ficheros a orto de bases de datos, o de un tipo de SGBD (de jerárquico a relacional) entrañan un riesgo muy importante por lo que deberán estar claramente planificadas para evitar pérdida de información y la transmisión al nuevo sistema de datos erróneos. También se deberán realizar pruebas en paralelo. verificando que la decisión real de dar por terminada la prueba en paralelo se atenía a los criterios establecidos por la dirección y que se haya aplicado un control estricto de la corrección de errores detectados en esta fase.

Por lo que respecta a la entrada manual de datos, hay que establecer un conjunto de controles que aseguren la integridad de los mismos, a este respecto. cabe destacar que las declaraciones escritas de procedimientos de la organización referentes a la entrega de datos a ser procesados deben asegurar que los datos se autorizan. recopilan. preparan, ~miren. y se comprueba su integridad. de forma apropiada.

También es aconsejable que los procedimientos y el diseño de los documentos fuentes minimicen los errores y las omisiones, así como el establecimiento de unos procedimientos de autorización de datos.

Un aspecto muy importante es el tratamiento de datos de entrada erróneos, para los que deben cuidarse con atención los procedimientos de re introducción de forma que no disminuyan los controles, a este respecto lo ideal es que los datos se validen y corrijan tan cerca del punto de origen como sea posible.

Corno sabemos. no toda la semántica de los datos puede siempre almacenarse en el esquema de la base de datos, por lo que hay parte de esta semántica que se ve obligado a residir en los programas. Será necesario, por tanto. comprobar que los programas implementan de forma adecuada esta integridad.

9.4.4 Explotación y mantenimiento

Una vez realizadas las pruebas de aceptación, con la participación de los usuarios, el sistema se pondrá (mediante las correspondientes autorizaciones y siguiendo los procedimientos establecidos para ello) en explotación.

En esta fase, se debe comprobar que se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas sólo se modifica mediante la autorización adecuada.

Sería conveniente también que el auditor pudiera llevar a cabo una auditoria sobre el rendimiento del sistema de BD, comprobando si se lleva a cabo un proceso de ajuste (tuning) y optimización adecuados, que no sólo consiste en el re diseño físico o lógico de la BD. sino que también abarca cienos parámetros del SO, e incluso la lamia en que acceden las transacciones a la BD.

9.4.5 Revisión post-implantacion

Aunque en bastantes organizaciones no se lleva a cabo, por falta de tiempo y recursos, se debería establecer el desarrollo de un plan para efectuar MILI revisión post-implantación de todo sistema nuevo o modificado. con el fin de evaluar si:

- Se han conseguido los resultados esperados, se satisfacen las necesidades de los usuarios, los costes y beneficios coinciden con los previstos.

9.4.6 Otros procesos auxiliares

A lo largo de todo el ciclo de vida de la base de dalos se deberá controlar la formación que precisan tanto los usuarios informáticos (administrador, analistas, programadores. cte.) como los no informáticos: ya que la formación es tina de las claves para minimizar el riesgo en la implantación de una base de datos.

Esta formación no se puede basar simplemente en cursos sobre el producto que se está instalando, sino que suele ser precisa una formación de base, que resulta imprescindible cuando se pasa de trabajar de un entorno de ficheros orientado al proceso a un entorno de bases de damos, por lo que supone un "cambio filosófico". lo mismo puede decirse si se cambia de tipo de SGBD (por ejemplo, de relacional a orientado a objetos o semiestructurado),

Hay que tener en cuenta que usuarios poco formados constituyen uno de los riesgos más importantes de un sistema. Esta formación no debería limitarse al área de las bases de datos, sino que tendría que ser complementada con formación relativa a los conceptos de control y seguridad.

Además, el auditor tendrá que revisar la documentación que se produce a lo largo de todo el proceso, para verificar si es suficiente y si se ajusta a los estandartes establecidos por la metodología adoptada en la empresa,

A este respecto resulta muy importante que se haya llevado a cabo un aseguramiento de calidad; lo ideal seria que en la propia empresa existiera un grupo de calidad que se encargara, entre otras cosas, de asegurar la calidad Lie los distritos e implantaciones de bases de datos (Piattini et al., 2006a). Es cieno que existen pocas "medidas de calidad para una base de datos, de todas maneras, hay algunas técnicas bastante difundidas que se pueden aplicar para asegurar su calidad (véase Piattini et al., 2002).

9.5 AUDITORIA Y CONTROL INTERNO EN UN ENTORNO DE BASE DE DATOS

Cuando el auditor se encuentra el sistema en explotación, deberá estudiar el SGBD y su entorno_ El gran problema de las bases de datos es que su entorno cada vez es más complejo y no puede limitarse serlo al propio SGBD. En la figura 13.2, se muestra un posible entorno de bases de datos, en el que aparecen los elementos más usuales,

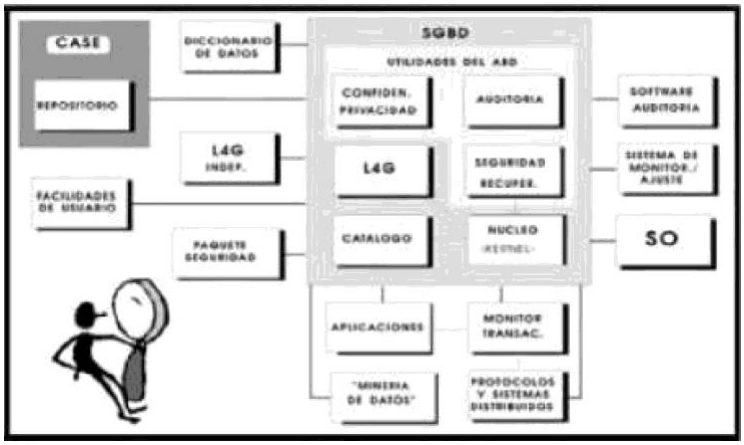

Figura 13.2. Entorno de ha ve de datos

9.5.1 Sistema de Gestión de Base de Datos (SGBD)

Entre los componentes del SGBD podemos destacar el núcleo (kernel), el catálogo (componente fundamental para asegurar la seguridad de la base de datos), las utilidades para el administrador de la base de datos (entre las que se suelen encontrar algunas para crear usuarios, conceder privilegios y resolver otras cuestiones relativas a la confidencialidad); las que se encargan de la recuperación de la BD: re arranque, copias de respaldo, ficheros diarios (log), etc., y algunas funciones de auditoría, y los lenguajes de cuarta generación (L4G) que incorpora el propio SGBD.

En cuanto a las funciones de auditoría que ofrece el propio sistema, prácticamente todos los productos del mercado permiten registrar ciertas operaciones realizadas sobre la base de datos en un fichero (o en un conjunto de tablas) de pistas de auditoria (audit, trail),

El auditor deberá revisar, por tanto, la utilización de todas las herramientas que ofrece el propio SGBD y las políticas y procedimientos que sobre su utilización haya definido el

administrador, para valorar si son suficientes o si deben Ser mejorados.

9.5.2 Software de auditoria

Son paquetes que pueden explicarse para facilitar la labor del auditor, en cuanto a la extracción de datos de la base, el seguimiento de las transacciones, datos de prueba, etc. ahí también productos muy interesantes que permiten cuadrar datos de diferentes entornes, permitiendo realizar una verdadera ¯auditoria del dato".

9.5.3 Sistema de monitorización y ajuste (tuning)

Este tipo de sistemas complementan las facilidades ofrecidas por el propio SGBD, ofreciendo mayor información para optimizar el sistema, llegando a ser en determinadas ocasiones verdaderos sistemas expertas que proporcionan la estructura óptima de la base de datos y de ciertos parámetros del SGBD y del SO.

La optimización de la base de datos, corno ya hemos señalado, es fundamental puesto que si actúa en un entorno concurrente puede degradarse fácilmente el nivel de servicio que haya podido establecerse con los usuarios.

9.5.4 Sistema operativo (S)

El SO es una pieza clave del entorno, puesto que el SGBD se apoyará, en mayor o menor medida, en los servicios que le ofrezca el SO en cuanto a control de memoria, gestión de áreas de almacenamiento intermedio (buffers), manejo de errores, control de CONFIDENCIALIDAD, mecanismos de interbloqueo, etc. desafortunadamente. el auditor informático tiene serias dificultades para controlar de manera rigurosa el interfaz entre el SGBD y el SO, debido a que, en parte, constituye información reservada de los fabricantes de los productos, además de requerir unos conocimientos excepcionales, que entran en el campo de la técnica de sistemas.

9.5.5 Monitor de transacciones

Algunos autores lo incluyen dentro del propio SGBD, pero que. actualmente, puede considerarse un elemento más del entorno, con responsabilidades de seguridad y, sobre todo, de rendimiento.

9.5.6 Protocolos y Sistema Distribuidos

Cada vez más se está accediendo a las bases de datos a tras de de redes, con lo que el riesgo de violación de la confidencialidad e integridad se acentúa,

También las bases de datos distribuidas pueden presentan graves riesgos de seguridad.

9.5.7 Paquetes de seguridad

Existen en el mercado varios productos que permiten la implantación efectiva de una política de seguridad. puesto que centralizan el control de accesos, le definición de privilegios, perfiles de usuario, etc. Un grave inconveniente de este tipo de software es

que a veces no se encuentra bien integrado con el SG111), pudiendo resultar poco útil su implantación si los usuarios pueden "saltarse- los controles a través del propio SGBD,

9.5.8 Diccionario de datos

Los diccionarios de datos se pueden auditar de manera análoga a las bases de datos (puesto que son bases de "Metadatos-); las diferencias entre unos y otros residen principalmente en que un fallo en una base de datos puede atentar contra la integridad de los datos y producir un mayor riesgo financiero. mientras que un fallo en un diccionario (o repositorio) suele llevar consigo una pérdida de integridad de los procesos; siendo más peligrosos los fallos en los diccionarios puesto que pueden introducir errores de forma repetitiva a lo largo del tiempo.

9.5.9 Herramientas CASE (Computer Aided System/Software Engineering) /IPSE (Integrated Project Support Environments)

Estas herramientas, corno soporte al diseño y concepción ele sistemas de información, suelen llevar incorporado un diccionario de datos (o repositorio) más amplio que los mencionados anteriormente en los que se almacenan además de información sobre datos, programas, usuarios, etc., los diagramas, 'matrices y grifos de ayuda al diseño. Constituyera una herramienta clave para que el auditor pueda revisar el diseño de la base de datos, comprobar si se ha empleado correctamente la metodología y asegurar un nivel mínimo de calidad.

9.5.10 Lenguajes de Cuarta Generación (L4G) independientes

Además de las herramientas que ofrezca el propio SGBD, el auditor se puede encontrar con una amplia gama de generadores de aplicaciones, de formas. de informes, etc. que actúan sobre la base de datos y que, por tanto_ también son un elemento importante a considerar en el entorno del SGBD.

En efecto, uno de los peligros más graves de los 1.40 es que no se apliquen controles con el mismo rigor que a los programas desarrollados con lenguajes de tercera generación. Esto puede debersen parte, a un inadecuado interfaz entre el L4G y el paquete de seguridad y de la falta de código fuente en el sentido tradicional, que hacen más difícil de esta manera el control de cambios en las aplicaciones.

Otros problemas asociados a los 61G, y con los que nos encontramos Frecuentemente, pueden ser su ineficiencia y elevado consumo de recursos, las limitaciones que, en ocasiones, imponen al programador, los cambios que pueden suponer en la metodología de desarrollo, etc.

El auditor deberá estudiar los controles disponibles en los L4G utilizados en la empresa, analizando con atención si permiten construir procedimientos de control y auditoria dentro de las aplicaciones y, en caso negativo, recomendar su construcción utilizando lenguajes de tercera generación.

9.5.11 Facilidades de usuario

Con la aparición de interfaces gráficos amistosos (con menús, ratón, ventanas, etc.) se ha desarrollado toda una serie de herramientas que permiten al usuario final acceder a los datos sin tener que conocer la sintaxis de los lenguajes del SGBD. El auditor deberá investigar las medidas de seguridad que ofrecen estas herramientas y bajo qué condiciones han sido instaladas: las herramientas de este tipo deberían "proteger al usuario de sus propios errores".

En este apartado podemos incluir también las diferentes facilidades que ofrecen algunos SGBD que permiten su conexión con paquetes ofimáticos (por ejemplo, hojas de cálculo), que pueden acceder a la base de datos e incluso actualizarla. En caso el auditor debe prestar especial atención a los procedimientos de carga y descarga (uploading/downfoading) de datos de la base a/desde los paquetes ofimáticos, comprobando, por ejemplo, si se puede actualizar la base de datos desde cualquiera de éstos o si la descarga se realiza con datos correctamente actualizados ("descarga de los datos correctos en el momento correcto").

9.5.12 Herramientas de “minería de datos”

En los últimos años ha explosionado el fenómeno de los almacenes de datos "datawarehouse" y las herramientas para la explotación o "minería" de datos ("datamining"), Estas herramientas ofrecen soporte a la tonta de decisiones., sobre datos de calidad integrados en el almacén de datos, debiéndose controlar ha política de refresco y carga de los datos en el almacén a partir de las bases de datos operacionales existentes, así corno la existencia de mecanismos de retroalimentación (feedback), que modifican las bases de datos operacionales a partir de los datos del almacén.

9.5.13 Aplicaciones

El auditor deberá controlar que las aplicaciones no atentan contra la integridad de los datos de la base,

9.6 TÉCNICAS PARA EL CONTROL DE BASES DE DATOS EN UN ENTORNO COMPLEJO

Como hemos visto en el epígrafe anterior existen muchos elementos del entorno del SGBD que influyen en la seguridad e integridad de los datos, en los que cada uno se apoya en la operación correcta y predecible de otros. Como se destaca en Clark el al. (1994), el efecto de todo esto es "debilitar la seguridad global del sistema, reduciendo la fiabilidad e introduciendo un conjunto de controles des coordinados ti, solapados, d' Alíes das gestionar". Esta situación se acentúa aún más si los diferentes componentes provienen de distintos fabricantes que se adaptan a estándares muchas veces contrapuestos.

La dirección de la empresa tiene, por tanto, tina responsabilidad fundamental en lo que se refiere a la coordinación de los distintos elementos y a la aplicación consistente de los

controles de seguridad. Para llevar a cabo esta labor se deben fijar claramente las responsabilidades sobre los diferentes componentes, utilizar informes de excepción efectivos que permitan monitorizar los controles, establecer procedimientos adecuados, implantar una gestión rigurosa do la configuración del sistema, etc.

Cuando el auditor se enfrenta a un entorno de este tipo, puede emplear, entre otras, dos técnicas de control: Matrices de control, que sirven para identificar los conjuntos de datos del SI junto con los controles de seguridad o integridad implementados sobre los mismos. y Análisis de los caminos de acceso, en los que se documentan el flujo, almacenamiento y procesamiento de los datos en todas las fases por las que pasan desde el mismo momento en que se introducen, identificando los componentes da sistema que atraviesan (tanto hardware corno software) y los controles asociados.

Con este marco, el auditor puede identificar las debilidades que expongan los datos a riesgos de integridad, confidencialidad y seguridad, los distintos interfaces entre componentes y la compleción de los controles.

En la práctica se suelen utilizar conjuntamente ambas técnicas, si bien la del análisis de caminos de acceso requiere unos mayores conocimientos técnicos y se emplea en sistemas más complejos.

9.7 CONCLUSIONES

Corno señala Brathwaite (1985). "la tecnología de bases de datos ha afectada al papel del auditor interno más que a cualquier otro individuo". Esto se debe, como hemos visto, no sólo a la complejidad de la propia tecnología de bases de datos, sino también a que el entorno del SGBD ha ido creciendo de manera extraordinaria en los últimos años, por lo que requiere personal especializado,

El gran número de componentes que forman dicho entorno y sus interfaces hacen necesario que. antes de empezar una revisión de control interno. el auditor deba examinar el entorno en el que el SGBD opera. que está compuesto como hemos visto, por el personal de la empresa (dirección, informáticos y usuarios finales), hardware, software. etc.

El auditor debe verificar que todos estos componentes trabajan conjunta y coordinadamente para asegurar que los sistemas de bases de datos continúan cumpliendo los objetivos de la empresa y que se encuentran controlados de manera efectiva,

Por lo que respecta al futuro de esta área, con la aparición de nuevos tipos de bases de datos, como las activas, orientadas a objetos, temporales, multimedia, multidimensionales, etc., véase Piattini y Díaz (2000), y la creciente distribución de los datos (bases de datos federadas, multibase de datos, Web, bases de datos móviles. etc.), aparecen nuevos riesgos de interés para el auditor como, por ejemplo, en el área de seguridad, o en las metodologías de desarrollo.

Desafortunadamente, como nos enseña la experiencia, los sistemas aumentan su complejidad y alcance con mayor rapidez que los procedimientos y técnicas para

controlarlos.

Por último, queremos destacar la importancia cada día mayor de una disciplina más amplia que la de bases de datos: la de Gestión de Recursos de Información (o en sus siglas inglesas. IRM, Información Rezurce Management). que nace precisamente con la vocación integradora necesaria para lograr convertir los datos en el activo más importante de las empresas; lo que Ilesa consigo que las medidas de control y auditoria pasen a un primer plano dentro de las actividades de las empresas; y que se alineen con las estrategias de las mismas y con el gobierno de sus tecnologías y sistemas de información (Piattini y Herbada, 2007).

9.8 LECTURAS RECOMENDADAS

Pianini, M.. Marcos. E., Calero. U. y Vela. B. (2006). Tecnólogo y diseño de bases de datos. Madrid, Ra-Ma.

En este libro se exponen los fundamentos de la tecnología de bases de datos (desde los sistemas jerárquicos y relocitmoles basta los objeto-relacionales, semis estructurados y multidimensionales), así en diferentes técnicas para su desafío,

Notan. R.B. (2005). Implementing D'alabase Security and Audititig: Includes Eramples for Oracle. SQL Server. DB2 UDB. Svbase. Elsevicr.

En este libro se presentan métodos y técnicas para proporcionar seguridad y auditoria en bases de datos. Se presentan diversos ejemplos de vulnerabilidades y ataques en los unamos más difundidos de bases de datos como Oracle, SOL Server y DB2.

!MI (2004). Oracle Database Security. Audi(and Control Fu:tures, 1T (Josemance Instituie.

El ITU presenta en esta obra las principales características de control. seguridad y auditoría en el entorno de bases de datos Oracle.

9.9 BIBLIOGRAFÍA

K.S_ (1985). Dora Administrailow Seiected Topics of Data Control. New York, EEL1111, John Wiley c Sons.

elark, R. el al. (cd.) (1991). 77w Securit•, Audi, and Control o' D'alabases. Avebury Technical, Aldershot, Gran Bretaña.

1TGI (2007a). COBIT 4.1, Framework, Control Objectives. Management Grridelines, Aforado, MocieLs. IT Csovemance Instituto, EEUU.

iTGI (2007b). IT Assurance Guide: Using COB/T. IT Cioventance Institutc, EEUU.

Piattini, M. y Díaz, O. (2000). Advanced D'alabases Technology and Design. Artech House. Londres

M., Calero, C. y Genero, M. (eds.) (2002). informatian and databose Kluwer Academie Publishers, Nomen, EEUU.

M., Calvo Manzano. J.. Cervera, J. y Fernández, L. (2103). Análisis y Diseño de Aplicaciones informáticas de Gestión. Una perspectiva de Ingeniería del Software. lita- a. Madrid.

Piattini, M., Caballero, 1. y García, F. (2006a). Calidad de los Sistemas. Informáticos., Ra-Ma, Madrid.

Piattini, M., Mareos, E., Calero, C. y Vela. B. (2006b). Tecnologia 'diseño de bases de dalos. Madrid. Ra-Ma.

SEXTA PARTE: SEGURIDAD DE REDES Y SISTEMAS DISTRIBUIDOS

Capítulo 10.

AUDITORÍA DE REDES

10.1 TERMINOLOGÍA DE REDES

Para poder auditar redes, lo primero y fundamental cs utilizar el mismo vocabulario (más bien jerga) que los expertos en comunicaciones que las manejan. Debido a la constante evolución en este campo, un primer punto de referencia es poder referirse a un modelo comúnmente aceptable. El modelo común de referencia, adoptado por ISO (International Standards Organiz.ation) se denomina Modelo OSI (Open Systems Interconection), y consta de siete capas, que se condensan en cuatro en el modelo TCP/IP equivalente.

La potencia del modelo 051 proviene de que cada capa no tiene que preocuparse de qué es lo que hagan las capas superiores ni las inferiores; cada capa se comunica con su igual en el interlocutor, con un protocolo de comunicaciones específico. Entre cada par de capa N y capa N- I está perfectamente definido el paso de la información, que se produce dentro de la misma máquina, con métodos clásicos de programación en local. Por tanto, cada capa tiene unos métodos prefijados para comunicarse con las inmediatamente inferior y superior

Para establecer una comunicación, la información desciende a través de la pila formada por las siete capas, atraviesa el medio físico y asciende a través de las siete capas en la pila de destino. Dependiendo de la cantidad de saltos que la información tenga que dar entre origen y destino, la información puede subir y bajar varas veces en los intermedios. Normalmente a la capa de enlace o red.

(Véase en la tabla 10.1)

CAPA	MODELO OSI	Modelo TCP/IP
7 Aplicación	Es donde la aplicación que necesita transferir información enlaza con el sistema de comunicaciones. La interfaz con el usuario, bien sea un programático – interfaz de programa de aplicación (API)- o humano – interfaz gráfico de usuario de usuario (GUI) – u otros tipos, NO es parte del modelo OSI.	Aplicaciones de uso específico, como protocolo de transferencia de ficheros FTP, Protocolo de transferencia de correos sencillos SMTP, Protocolo de transferencia de hipertexto http, Ídem mas criptografía HTTP, Sistema de nombres de dominio DNS, Protocolo de aplicación orientada a servicios SOAP, Procedimiento de llamada remota RPC, etc.
6 Presentación	Define el formato de los datos que se van a presentar a la aplicación. Por ejemplo: XML, HTML, ASCII, Unicode, etc. Los estándares que definen la sintaxis y semántica de los mensajes (como XBRL) están este nivel.	

5 Sesión	Establece los procedimientos de aperturas y cierres de sesión de comunicaciones, así como la información de la sesión en curso. Por ejemplo: capa de transporte segura (TLS/SSL, entre http y TCP)		
4 Transporte	Comprueba la integridad de los datos transmitidos (que no ha habido perdidas ni alteración de datos)	Protocolo de control de transferencia TCP. Pone los paquetes IP de cada mensaje en orden y comprueba que todos se transmitan y reciban.	
3 RED	Selecciona y establece la ruta de comunicación entre el emisor y el receptor, que pueden pertenecer a redes distintas, mediante el envió de paquetes de información. Un encaminador (router) interconectada redes, gestionándola dirección de red (típicamente IP). Una pasarela (Gateway) interconecta redes de distinto tipo (como AppleTalk con TCP/IP, cambiando los formatos).	Protocolo internet IP. Los datos se envían en diagramas independientes (sin sesión), conteniendo la dirección IP de emisor y receptor, en base al mejor esfuerzo (sin garantía), mediante conmutación de paquetes, saltando un numero de máximo de veces entre conmutadores o encaminadores, IP sec es IP mas criptografía.	
2 ENLACE	Transforma los paquetes de información en tramas adaptadas a los dispositivos físicos. Controla el flujo de tramas y el direccionamiento físico en un segmento de red, comúnmente a través de la identificación unica de seis bytes MAC que tiene cada tarjeta de red. Los segmentos se pueden interconectar, usando la dirección MAC, mediante conmutador (switch, entre varios segmentos) o	Ethernet (802,3), Wifi (802.11), PPP(protocolo punto a punto – línea entre dos puntos), ATM (modo de transferencia asíncrono), MPLS (conmutación por etiquetas multiprotocolo- básicamente grandes rutas prefijadas para trafico IP	
1 FISICO	Transforma la información en señales físicas adaptadas al medio de comunicación: par trenzado, cable coaxial, radio, fibra óptica, etc. El equipo se conecta mediante tarjeta de interfaz de red (NIC) específica para el medio (10BASET-RJ45, inalámbrica 802.1). Varios medios del mismo tipo se pueden conectar mediante repetidores físicos de señal (hubs, en desuso).		

Tabla 10.1. Modelo OSI

De esta manera. se aíslan los protocolos que se utilizan en unas capas con los protocolos que se utilizan en otras. Por ejemplo, es posible transmitir trafico TCP/IP (capas superiores), a través de Ethernet o Wifi indistintamente (capas inferiores), gracias a esta independencia entre capas. Este método de especificar a qué capas corresponde cada

protocolo de comunicaciones resulta muy útil a efectos didácticos, pues rápidamente se tiene una visión del alcance y utilidad del protocolo o elemento de comunicaciones en cuestión.

Como regla mnemónica para recordar fácilmente el orden de las siete capas OSI, suele utilizarse la frase "Formemos Esta Red y Todos Seremos Pronto Amigos" (Físico. Enlace. Red. Transpone. Sesión. Presentación y Aplicación).

En los niveles inferiores, habitualmente hasta el nivel tres, es donde se definen las redes LAN (Local Ama Network). MAN (Metropolitan Área Network) y WAN (Wide Área Network). Las funcionalidades de estas tres tipos de redes son similares, variando fundamentalmente la distancia que son capaces de salvar entre el emisor y el receptor (LAN: dentro de un edificio. MAN: dentro de un campus o zona urbana. WAN: cualquier distancia), siendo normalmente la velocidad inversamente proporcional a la distancia.

La red LAN más extendida, Ethernet, está basada en que cada emisor envié, cuando desea, una trama (paquete básico de data) al medio físico, sabiendo que todos los destinatarios están permanentemente en escucha. Justo antes de enviar, el emisor se pone a la escucha, y si no hay tráfico, procede directamente al envió. Si al escuchar detecta que otro emisor está enviando, espera un tiempo aleatorio antes de volverse a poner a la escucha. Según crece el tráfico, se incrementa la probabilidad de que dos emisores hayan escuchado que el medio está libre, y se pongan a transmitir simultáneamente. En ese caso, se habrá producido una colisión y los tramos enviados se destruirán mutuamente, creándose una alteración que es percibida físicamente como colisión de tramas. Cada emisor procede entonces a dar la trama como no enviada y a esperar un tiempo aleatorio antes de ponerse de nuevo a escuchar, exactamente igual que cuando el medio estaba ocupado. Las tecnologías de Ethernet (10 megabits por segundo - Mbps). Fast Ethernet (100 Mbps) y Giga Ethernet (1.000 Mbps) se basan en el mismo principio, incrementando sucesivamente la velocidad de transmisión. En vez de tender un único cable que recorra todos los equipos del segmento Ethernet, se suele tender un cable por equipo, y conectar los cables en armarios de encaminadores, que seleccionan para cada cable sólo el tráfico que va dirigido específicamente a su equipo, lo que reduce las colisiones.

Una red interna TCP/IP se conecta al exterior normalmente mediante Línea de Abonado Digital Asimétrica ADSL (velocidad de Mbits/segundo) o mediante línea punto a punto de alta velocidad (como T1) a un Punto de Presencia (PoP) de Proveedor de Servicios Internes (ISP), que a su vez conectan sus redes entre sí en diversos Puntos Neutros (IXP). De los que en España existen cuatro a la fecha.

10.2 VULNERABILIDADES EN REDES

Todos los sistemas de comunicación, desde el punto de vista de auditoria, presentan en general una problemática común: la información transita por, y es accesible desde, lugares típicamente alejados de las personas responsables. Esto presupone un compromiso en la seguridad, ya que no existen procedimientos físicos para garantizar la inviolabilidad de la información. Y un compromiso en la disponibilidad, pues un fallo en comunicaciones impide dar el servicio.

10.3 VULNERABILIDAD EN CAPAS FÍSICA, ENLACES Y RED

En la red física de comunicaciones, por causas propias de la tecnología, pueden producirse básicamente tres tipos de incidencias:

1 Alteración de bits. Por error en los medios de transmisión, una trama puede sufrir variación en parte de su contenido. Los protocolos de comunicación (usualmente capas I a 3) sufijan cada trama trasmitida con un código de redundancia cíclico (CRC). que detecta cualquier error.

2 Alteración de secuencia. El orden en el que se envían y se reciben las tramas no coincide, pues se han adelantado unos a otros. La capa de transporte, en último extremo, reordenaría la información.

3 Ausencia de paquetes. Por sobrecarga, direccionamiento o error en el medio, las tramas pueden desaparecer en el camino del emisor al receptor. La capa de transporte, en último extremo detectaría la ausencia.

Por causas dolosas, y teniendo en cuenta que es físicamente posible interceptar la información, los tres mayores riesgos a atajar son:

1 Indagación. Un paquete puede ser leído por un tercero, obteniendo la información que contenga.

2 Suplantación. Un tercero puede introducir un paquete espurio que el receptor cree proveniente del emisor legítimo.

3 Modificación. Un tercero puede alterar el contenido de un paquete.

Para este tipo de actuaciones dolosas, la única medida prácticamente efectiva en redes MAN y WAN (cuando la información sale del edificio) es la criptografía. En redes LAN suelen utilizarse más bien medidas de control de acceso al edificio y al cableado, ya que la criptografía todavía sólo es práctica en casos concretos para redes locales.

Dada la proliferación de equipos que precisan comunicación de datos dentro de los edificios, es muy habitual plantearse sistemas de tableado integral, en vez de tender un cable en cada ocasión. Esto es prácticamente un requisito en edificios con cieno volumen de usuarios. Los sistemas de tableado suelen planearse según su ámbito geográfico. En cada planta o zona se tienden cables desde un armario distribuidor a cada uno de los potenciales puestos. Este tableado se denomina habitualmente de -planta" Estos armarios están conectados, a su vez, entre si y con las salas de ordenadores, denominándose a estas conexiones cableado -troncal". Desde las salas de ordenadores parten las líneas hacia los transportistas de datos (Telefónicas o PTT), saliendo los cables al exterior del edificio en lo que se denomina cableado de "ruta". El cableado troncal y el de ruta cada vez más frecuentemente se tiende mediante fibras ópticas, que son muy difíciles de interceptar, ya que apenas provocan radiación electromagnética, y la conexión física a una fibra óptica requiere una tecnología delicada y compleja. El cableado de planta suele ser de cobre (y ondas), por lo que es factible la escucha ("pinchazo"), difícil de detectar.

Dentro de las redes locales, el mayor peligro físico es que alguien instale una

"escucha" no autorizada. Al viajar en claro la información dentro de la red local, es imprescindible tener una organización que controle el acceso físico. El método más sencillo es instalar un equipo no autorizado (por ejemplo: en un armarios de cables) y darle acceso a la red. Dentro de cualquier instalación de cieno tamaño son de uso habitual los equipos de escucha, bien sean éstos físicos ("sniffer-) o lógicos ('trapeadores"), por lo que su uso legítimo ha de estar controlado y no devenir en actividad espuria.

En el propio puesto de trabajo puede haber peligros, como grabar/retransmitir la imagen que se ve en la pantalla, teclados que guardan memoria del orden en que se han pulsado las teclas, o simplemente que las contraseñas estén escritas en papeles a la vista. Las contraseñas de usuario son un punto especialmente crítico en los canales de comunicaciones. Mientras que en un sistema de almacenamiento las contraseñas suelen guardarse cifradas, no siempre los terminales u ordenadores personales son capaces de cifrar la contraseña cuando se envía al servidor (por ejemplo: página Web HTTP). Por tanto, alguien que intercepte la información, puede hacerse con las contraseñas en claro. Además, dado que las carátulas iniciales, donde se teclea la contraseña, son siempre las mismas, se facilita la labor de los agentes de interceptación, pues proporcionan un patrón del paquete de información donde viaja la contraseña a interceptar.

10.4 VULNERABILIDAD EN EL TRANSPORTE

El Protocolo de Control de transferencia/Protocolo Internet TCP/IP fue diseñado originalmente en los años 70, para sobrevivir inclusive a ataques nucleares contra los EEUU e impulsado desde el ámbito académico. La enorme versatilidad de este protocolo y su aceptación generalizada le han convertido en el paradigma de protocolo abierto, siendo la base de interconexión de redes que forman la Internet. Fa el protocolo que se ha impuesto. por derecho propio, como gran unificador de todos las redes de comunicaciones. Y sobre clásicos los modelos de red jerárquicos, ofrece una mayor resilencia (recuperación ante fallos).

Al ser los sistemas de comunicaciones, procesos "sin historia", donde no se almacenan permanentemente datos de ningún tipo, los sistemas de recuperación se ven especialmente beneficiados por esta característica. Si una sesión cae, una vez que se vuelve a establecer la sesión, el incidente queda solucionado. Es responsabilidad de la aplicación volver a reinicializar si **la** interrupción se produjo en mitad de una unidad de proceso. Por ejemplo, si la interrupción de la sesión se ha producido a mitad de una transferencia de fichero, será misión de la aplicación, cuando la sesión se reanude, determinar si vuelve a comenzar la transmisión del fichero desde el principio o si reutiliza la parte que ya se ha transmitido. Si es una persona quien ha sufrido el incidente, cuando se reanude la sesión deberá volver a identificarse con su nombre de usuario y contraseña, comprobando hasta qué punto la aplicación en la que estaba operando recogió los últimos datos que introdujeron.

Esta restricción fundamental, de que los sistemas de comunicaciones no almacenen datos, permite una mayor facilidad a la hora de duplicar equipamiento. Dado que una vez cerrada la sesión no queda ninguna información a retener (salvo obviamente estadísticas y pistas de auditoria), la sesión, al reanudarse, puede utilizar la misma o diferente ruta. Si existen diversos nodos y diversos enlaces entre ellos, la caída de un

nodo sólo ha de significar como máximo la interrupción de las sesiones que por él transiten, que se podrán reiniciar a través de los restantes nodos. Por ello, es una norma generalmente aceptada, al menos en redes de cierto tamaño, tener nades y enlaces replicados para prevenir situaciones de contingencia.

Una vez más, el protocolo TCP/IP demuestra en este caso su utilidad. Al haber sido este protocolo diseñado para encontrar rutas remanentes, inclusive ante caídas masivas, está especialmente bien orientado para facilitar la reestructuración de una red ante fallos de parte de sus componentes, sean éstos líneas, nodos o cualquier otro tipo de equipamiento. Los equipos de red manejan prioritariamente Tráfico TCP/IP y poseen facilidades añadidas de gestión de sobrecargas. rutas alternativas, tratamientos de contingencias, y todo tipo de situaciones que acontecen en una red en funcionamiento. La pregunta clave en auditoria es saber si esas facilidades se usan: si sc han estudiado en el diseño de red, si están documentadas, si se han puesto en práctica. y si se prueban regularmente.

10.5 REDES INTERNAS Y EXTERNAS

La primen y más importante regla en redes de comunicaciones es tener claramente establecido el perímetro de seguridad, que arda la red interna del exterior. hay tres zonas que han de estar perfectamente delimitadas:

- Intranet: es la red interna. privada y segura. de una empresa. utilice o no medios de transporte de terceros.

- Zona Desmilitarizada DMZ: es perímetro de seguridad que conecta la red interna a una red externa (como Interna), a dejando pasar sólo el tráfico legítimo.

- Internet: es la red de redes. "metared" a donde se conecta cualquier red que se desee abrir al exterior, de alcance mundial, pública e insegura, donde puede comunicar cualquier pareja o conjunto de interlocutores, dotada además de todo tipo de servicios de valor añadido.

Las políticas de protección oscilan entre *paranoicas y promiscuas,* pasando por todo tipo de gamas intermedias. Dícese de la política paranoica cuando absolutamente todo está prohibido, requiriéndose una autorización específica para cada servicio en concreto entre cada par de interlocutores concretos. Dícese de política promiscua cuando todo está autorizado, identificándose específicamente aquellos servicios concretos entre parejas concretas de interlocutores que se prohíben. Lo más habitual es autorizar específicamente servicios (por ejemplo correo electrónico) para cienos tipos genéricos de usuarios (por ejemplo a todos) otros servicios (por ejemplo terminal virtual) a ciertos usuarios especificas (por ejemplo servidor de terminales virtuales) y el resto no autorizarlo.

El mayor peligro que representa un acceso TCP/IP no autorizado viene dado precisamente por la mayor virtud del TCP/IP: su amplia disponibilidad de utilidades. Usualmente, cada utilidad tiene asociado un número, denominado "puerto" TCP/IP. Dada la estandarización de las utilidades TCP/1P, es muy común que cada máquina con acceso TCP/IP venga con los puertos abiertos, que a su vez son utilidades listas pan

funcionar, como transmisores de ficheros, servidores de correo, terminales virtuales, y todo tipo de servicios de utilidad. Una ausencia de protección significaría que un tercero puede utilizar estas utilidades normalizadas. de común existencia con cualquier máquina, en beneficio propio.

Un dispositivo específicamente dedicado a la protección de una Intranet ante Internet, es el cortafuego (firewall). Esta es una máquina delicada en exclusiva a leer cada paquete que entra o sale de una red, para permitir o impedir su paso. Esta autorización o rechazo está basada en unas tablas que identifican para cada pareja de interlocutores (bien sea tusado en el tipo de interlocutor o inclusive en su identificación individual) los tipos de servicios que pueden ser establecidos. El cortafuego ha de ser capaz de interpretar la información de las diferentes capas, y aplicar todo tipo de reglas. Por ejemplo, sólo ciertas direcciones IP internas se podrían conectar con el exterior, no se permitiría usar TSL/SSL (cifrado de sesión), y las aplicaciones admisibles sólo serían HTPP y FTP, estando prohibido cualquier otro uso.

En la capa de red, el número de direcciones IP (en la versión actual. IPv4) es limitado, por lo que no se puede asignar una dirección IP específica a cada equipo. El ISP es quien proporciona direcciones IP en Internet. pero la definición de direcciones IP dentro de la Intranet es responsabilidad de cada empresa. Por tanto se necesitan encaminadores que hagan la traducción de direcciones IP, mediante un traductor de direcciones de red NAT.

En la capa de aplicación, es muy útil el apoderado (proxy) que da servicio a cada petición que le llegue pasándosela a un servidor final, que queda así protegido de accesos directos del cliente. En caso de intrusión, el apoderado queda comprometido, pero el servidor real sigue a salvo. Una pasarela de aplicación (Gateway) puede hacer la misma función de aislamiento en casos específicos.

Para construir una zona desmilitarizada segura. existen diversas configuraciones, donde se pueden incluir encaminadores, cortafuegos, apoderados, bastiones (ordenadores con una única función y punto único de entrada y salida), tarros de miel (honeypot, servidores simulados para atraer intrusos) y demás parafernalia, a veces copiada de la jerga militar. (Véase en la figura 16.1).

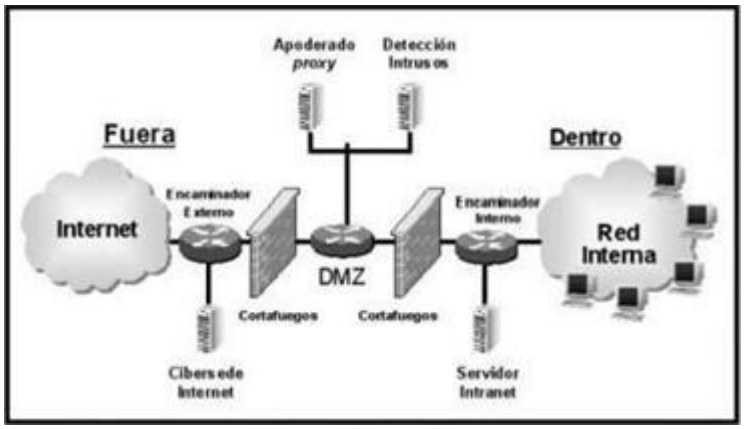

Figura 10.1. Configuración para zona desmilitarizada

Para proteger la red interna Intranet del exterior suele utilizarse el esquema

expuesto, o variaciones del mismo. Se parte de la base la información que viaja entre la Intranet y el exterior ha de atravesar la zona desmilitarizada, pasando por dos cortafuegos. Un cortafuegos protege los accesos desde el exterior hacia la zona desmilitarizada y el otro protege los accesos desde la zona desmilitarizada hacia la Intranet. Si el cortafuego exterior resultare comprometido, todavía quedaría el cortafuego interior. Un ataque de Denegación de Servicio DoS, saturando el cortafuego externo de mensajes, no pone en peligro al cortafuego interno.

En la zona desmilitarizada se instalan aquellos servicios que hayan de ser accedidos desde el exterior y desde el interior, por ejemplo, un bastión proxy accede a un servidor Internet, recuperando la información que haya solicitado un usuario interno y almacenándola para que pueda ser recuperada desde la Intranet. De esta manera se evita una conexión directa desde una máquina interna (Intranet), a un servidor externo (Internet) o viceversa. El objetivo es evitar establecer sesiones directas entre un ordenador interno y uno externo, desde donde se le pueda infectar. Los cortafuegos impedirán que se establezcan conexiones dentro-fuera, salvo aquellas que específicamente se determinen. El cortafuegos externo cuidará de que rolo atraviese tráfico autorizado entre el exterior y el bastión, y el cortafuegos interno hará lo propio con el tráfico entre el bastión y la red interna. Un detector de intrusos (como Snort) en la zona desmilitarizada, en conjunción con un -tarro de miel- para atraer intrusos (como honeyd, ambos de código abierto), pueden ayudar a detectar la presencia de huéspedes no invitados.

Este esquema de protección puede ser simplificado, a costa de disminuir funcionalidades y solidez prescindiendo en primer lugar del encaminador interno (quedaría un encaminador con tres patas: interna, externa y DMZ), y en segundo lugar del bastión. Abrir al exterior, sin protección, una red interna queda fuera de cualquier buena práctica informática.

Pan conectar varias dependencias de una empresa distantes entre si, usuarios móviles de la empresa, o ciertas aplicaciones de distintas empresas asociadas, se utiliza el concepto Extranet, que se suele poner en práctica mediante una Red Privada Virtual VPN, que permite la extensión de una red local sobre una red pública o insegura, como por ejemplo Internet. Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación (¿quién está del otro lado?: privilegios de acceso según usuario y equipo), la integridad I los datos no se han alterado) y la confidencialidad (cifrar los datos para que ningún tercero los pueda leer). Un peligro a considerar es "el hombre en el medio", donde un intruso se coloca con el canal de comunicaciones, retransmitiendo a cada extremo la información proveniente del otro lado, y pudiendo suplantar la identidad de ambos extremos. Muchos cortafuegos tienen prestaciones VPN, que se les pueden añadir mediante software adecuado a los equipos remotos (véase figura 10.2).

El peligro más clásico es que un extraño se introduzca desde el exterior hacia la red interna. Dado que las técnicas para saltar los procedimientos de seguridad son públicas, y están accesibles en Internet, una primen preocupación debiera ser, periódica, controlada y preventivamente, poner a prueba los

procedimientos de seguridad, antes de que un extraño lo haga.

Para comprobar los controles de acceso desde el exterior, ni como las vulnerabilidades en la red interna, cortafuegos, servidores, etc., existen programas específicos que facilitan esta tarea, como Nessus, SAFEsuite, Satan, Nmap, Cops, u otros (algunos son gratuitos), comprobando las vulnerabilidades ya conocidas. Las nuevas versiones de estos programas. que aparecen regularmente, incluyen comprobaciones de las nuevas debilidades detectadas. Como en el caso de los antivirus, se deben tener estos programas actualizados a fecha reciente.

Un ataque básico es conseguir la identificación de un usuario. Para ello pueden utilizarse técnicas de indagación, leyendo el tráfico hasta encontrar nombres de usuario y contraseñas, poner a prueba la buena fe de los usuarios mandándole un mensaje basado en ingeniería social (phishing) del tipo "soy su administrador, por favor dígame su contraseña" o directamente intentar encontrar identificaciones habituales de usuarios ("prueba", "test", "master"...) que ya vienen por defecto en muchos sistemas. Véase en la figura 10.2.

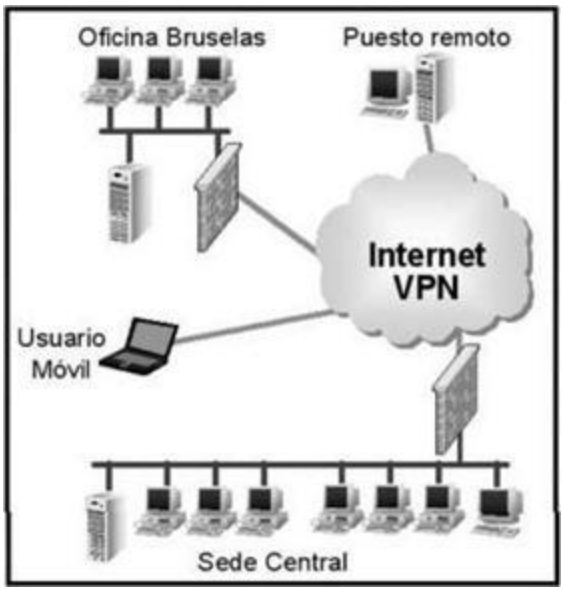

Figura 10.2. UPN

Aunque los ficheros de contraseñas están cifrados, utilizando habitualmente como clave de cifrado de cada contraseña la propia contraseña, los métodos y algoritmos de cifrado son públicos. Existen programas que son capaces de probar miles de contraseñas usuales ya cifradas para ser si corresponden con alguna del fichero de contraseñas cifradas. Los programas de ruptura de clases como Crack o John the Ripper son públicos y muy rápidos para claves cortas. Por ello es fundamental evitar que los ficheros con las contraseñas cifradas caigan en manos de terceros.

Una buena práctica es la defensa en profundidad, segmentando la red interna, y poniendo cortafuegos adicionales a segmentos con ordenadores especialmente sensibles. Por ejemplo el cortafuegos sólo dejarla pasar tráfico LDAP (Protocolo Ligero de Acceso a Directorio) hacia el servidor de directorio

de usuarios, o autoritaria solo desde ciertas direcciones acceso al servidor con la aplicación de nómina. Es una buena práctica centralizar el registro de sucesos (log), donde quedan útiles pistas de auditoria, con un servidor protegido detrás de un cortafuegos especifico, pues de esta manen Sea más difícil borrar las huellas.

Siempre es importante tener un monitor de servicios de red que alerte sobre comportamientos anómalos, que pueden ser indicativos de problemas o ataques, como Nagios.

En los sistemas distribuidos, se suele utilizar la técnica de "confianza entre nodos", de manera que si un usuario está autorizado para el nodo A, y solicita desde el nodo A un servicio al nodo B, como el nodo B "confía" que el nodo A ya ha hecho la autenticación del usuario, el nodo B admite la petición del usuario sin exigirle la de nuevo la contraseña. Un intruso que sea capaz de entrar con un nodo, podría entrar en todos los nodos que "confiera" en el nodo ya accedido.

También aparece diverso código malicioso (malware), como "gusanos" -mensajes de correo electrónico que se reproducen y acaban por colapsar la red, "caballos de Troya" -programas aparentemente "inocuos" que llevan código escondido-, virus -que se autocopian de un programa/documento "infectado" a otros programas/documentos "limpios"-, "Nenas falsas" -accesos que muchas veces se dejan de la etapa de instalación/depuración de los sistemas-. Todo ello es un riesgo de que el atacante, valiéndose de este código malicioso, especialmente si utiliza técnicas de código móvil (que se trasmite en la red y se ejecuta al otro extremo), pueda llegar a tomar control del equipo.

10.6 AUDITANDO A LA ORGANIZACIÓN

Cada vez más y más las comunicaciones están tomando un papel determinante en el tratamiento de datos, cumpliéndose el lema el ordenador es la red. La telemática (informática más comunicaciones) no es un juguete tecnológico, es un función clave en la empresa, que tiene un sentido. La regla de oro más sencilla y menos seguida se puede expresar muy fácilmente:

Si no se sabe qué se defiende y porqué, no se puede defender.

El cómo es consecuencia de qué y el para qué. La política de seguridad, en el área de comunicaciones, ha de estar escrita, aprobada formalmente, actualizada. Entendible, entendida y seguida. Los mecanismos concretos de seguridad van a proteger de los riesgos previsibles a un coste asumible: la seguridad nunca es absoluta. Procedimientos y mecanismos han de estar documentados y verificados: las personas cometemos errores. Estar vigilante para detectar problemas o intrusiones es tener media batalla ganada. Todo esto no es gratis, así que la seguridad debe ser un facilitador de los objetivos de la empresa; en caso de conflicto es la seguridad la que suele perder.

No siempre esta implicación con los objetivos corporativos queda adecuadamente reflejada dentro de la estructura organizativa del

Departamento de Informática, especialmente en organizaciones de tipo "tradicional", donde la adaptación a los cambios no se produce inmediatamente. Mientras que comúnmente el directivo informático tiene amplios conocimientos de proceso de datos, sus habilidades y cualificaciones en temas de comunicaciones le pueden parecer menos críticas, por lo que hay que comprobar la existencia de un adecuado anclaje del área de comunicaciones en el esquema organizativo. Por su parte, los informáticos a cargo de las comunicaciones suelen auto considerarse exclusivamente técnicos, obviando considerar las implicaciones de su tarea en los objetivos de la empresa. Todos estos factores convergen en recomendar que la auditoria de comunicaciones se practique con la frecuencia y profundidad equivalentes a las de otras áreas del proceso de datos.

La organización a cargo de la red, para que dar un buen servicio, debe tener una estructura y unos procedimientos a seguir que le utilizar las mejores prácticas de la industria en el soporte y provisión de servicios. El modelo ITIL (Biblioteca de Infraestructura de Tecnología de la Información) se ha venido desarrollando desde los ochenta precisamente para orientado al concepto de ciclo de vida del servicio de la TI. Está estructurado en cinco áreas que corresponden a:

1. Estrategia de Servicio: planificación de estrategia y del valor. Responsabilidades y roles. Enlace entre negocio y estrategia informática. Puesta en marcha de estrategias de servicio. Riesgos y factores críticos de éxito.
2. Diseño del servicio: objetivos del diseño del servicio. Selección de modelo. Análisis de riesgos. Puesta en marcha. Coste, Medición y control
3. Transición en el Servicio: gestión del cambio cultural y organizativo. Gestión del conocimiento. Sistemas de gestión del conocimiento. Métodos, prácticas y herramientas. Medición y control.
4. Operación del Servicio: gestión de aplicaciones. Gestión del cambio. Gestión de operaciones. Control de procesos y funciones. Prácticas escalables, Medición y control.
5. Mejora Continua del Servicio: mejoras impulsadas por negocio y por tecnología. Justificación. Mejoras de gestión, financieras y de organización. Métodos, prácticas y herramientas. Mejores prácticas de empresa.

Se puede utilizar ITIL o cualquier otro modelo, pero hay que utilizar alguno. El ITIL tiene la ventaja que está siendo adoptado por multitud de organizaciones, especialmente de cierto tamaño. Su desventaja es que quizá sea un poco arduo para pequeñas organizaciones, aunque siempre se puede empezar por algo concreto, como la Operación del Servicio, c ir avanzando.

Por tanto, el primer punto de una auditoria es determinar que la función de gestión de redes y comunicaciones esté claramente definida y gestionada, debiendo ser responsable, en general, de las siguientes tareas:

- Gestión de la red, inventario de equipamiento y normativa de conectividad.

- Vigilancia de las comunicaciones, registro y resolución de problemas.
    - Participación activa en la estrategia de proceso de datos, fijación de estándares de comunicaciones a usarse en el desarrollo de aplicaciones y es evaluación de necesidades en comunicaciones.
    - Mantener la documentación de la red al día.
    - Revisión de costes y su asignación, de proveedores y servicios de transponer, y selección de equipamiento.

Como objetivos de control, se debe reseñar la existencia de:

- Una política de seguridad escrita. entendida y ejecutada.
- Un área de comunicaciones responsable de seguir procedimientos operativos documentados.
- Procedimientos y registros de inventarios y cambios.
- Segregación de tareas y de funciones de control de la red.
- Separación de entornes de desarrollo. pruebas y producción.
- Procedimientos para vigilar cl uso de la red de comunicaciones, realizar ajustes para mejorar el rendimiento, registrar y resolver cualquier problema. y controlar costes y proveedores.
- Procedimientos de seguridad y control de intrusiones en la red.
- Participación activa del área de comunicaciones en el diseño de las nuevas aplicaciones on line para asegurar que se sigue la normativa de comunicaciones. se planifica la capacidad requerida. y se acepta su puesta en marcha.

10.7 AUDITANDO LA RED FÍSICA

En una primera división. se establecen distintos riesgos para los datos que circulan dentro del edificio, de aquellos que viajan por el exterior. Por tanto ha de auditarse hasta qué punto las instalaciones físicas del edificio ofrecen garantía, y se han estudiado las vulnerabilidades existentes.

En general, muchas veces se parte del supuesto de que si no existe acceso físico desde el exterior a la red interna de una empresa, las comunicaciones internas quedan a salvo. Debe comprobarse que efectivamente se han indagado los posibles accesos físicos provenientes del exterior, para evitar estos accesos. Debe también comprobarse que desde el interior del edificio no se intercepta físicamente el cableado (“pinchazo").

En caso de desastre, bien sea total o parcial, ha de poder comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar. Ya que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencias deben tener prevista la recuperación en comunicaciones.

Ha de tenerse en cuenta que la red física es un punto claro de contacto entre el área de comunicaciones y el mantenimiento general de edificios, que es quien suele aportar electricistas y personal profesional para el tendido físico de cables y su mantenimiento.

Como objetivos de control, se debe reseñar la existencia de:

- Áreas seguras para los equipos de comunicaciones, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicaciones.
- Mantenimiento y gestión de equipos de red.
- Controles de utilización de los equipos de pruebas en comunicaciones.
- Atención específica a la recuperación de los sistemas de comunicación de datos, en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen salidas directas al exterior, para prevenir accesos no autorizados.

10.8 AUDITANDO LA RED LÓGICA

Cada vez más se tiende a que un equipo pueda comunicarse con cualquier otro equipo, de manera que sea la red de comunicaciones el substrato común que les une, Leído a la inversa, la red hace que un equipo pueda ilegítimamente acceder **a cualquier otro,** incluyendo al tráfico que circule hacia cualquier equipo de la red. Y todo ello por métodos exclusivamente lógicos, sin necesidad de instalar físicamente ningún dispositivo. Simplemente, si un equipo, por cualquier circunstancia se pusiera a enviar indiscriminadamente mensajes, podría ser capaz de inundar la red completa, y por tanto al resto de los equipos de la instalación.

La regla de oro es segmentar la red, de manera que problemas en un segmento no tengan por qué afectar a toda la instalación. Una intrusión se puede contener mejor si el acceso a un punto no implica el acceso a todo. Y la peor amenaza suele venir desde dentro. La segmentación ayuda a detectar mal uso interno, y limitar el acceso ilegitimo conseguido mediante herramientas legitimas. El ejemplo más simple puede ser en encaminador WiFi no cifrado pan visitantes y pruebas, que obviamente debe estar directamente conectado al exterior, y nunca a la red interna. Una política de "lo que no está expresamente permitido es que está prohibido" ayuda a disipar dudas.

Es necesario vigilar la red, revisar los errores o situaciones anómalas que se producen, y tener establecidos los procedimientos para detectar y aislar equipos en situación anómala. En general, si se quiere que la información que viaja por la red no pueda ser espiada, la única solución a efectos prácticos es el cifrado.

Como objetivos de control, se debe reseñar la existencia de:

- Política documentada de uso de servicios de red.
- Autenticación de usuario obligatoria, para limitar y detectar cualquier intento de acceso no autorizado a la red de comunicaciones.
- Autenticación de equipase., para limitar y detectar cualquier intento de conectar un equipo no autorizado a la red de comunicaciones.
- Las funcionalidades para uso remoto de equipos como puertos abiertos u operación remota han de estar desactivadas.
- Segregación de redes, para incrementar puntos de control y posibilitar la defensa en profundidad.
- Controles de privilegios de usuario de conexión a la red.

- Control de flujos de información, encaminamiento y redundancia.
- Registro de la actividad de la red, para ayudar a reconstruir incidencias y detectar accesos no autorizados.

10.9 CONCLUSIONES

La Auditoria de Redes no es distinta a ninguna otra Auditoria: hay que tener nociones de la tecnología aplicable, determinar los objetivos die auditoria (dependientes de los objetivos empresariales y los riesgos a mitigar) y comprobar si la organización a cargo de las comunicaciones comprende su papel está en posición de desempeñarlo y lo desempeña efectivamente.

Quizá la Auditoria de Redes sea un tanto más peculiar por la complejidad tecnológica intrínseca a las redes, y sobre todo por el factor de desaparición de la distancia física. Implícitamente, durante siglos se ha confiado en barreras y separaciones físicas. En el mundo de las redes es exactamente lo mismo, pero son barreras y separaciones virtuales, que ya no se observan físicamente, pero que hay que comprobar que estén ahí, y que estén en buen estado. Cualquier persona, desde cualquier lugar del mundo, *por* cualquier tipo de motivación, podría introducirse si la barrera no existiera. Y aunque la motivación fuera lúdica, el daño podría ser muy real.

La segmentación de la red, la segregación de funciones y la separación de entornos son los tres factores clave. Corno lima de control a utilizar, hay muchas y muy buenas, así que no es necesario inventar otras nuevas. La lista de preparación para el examen CISA es un clásico, lo que k da a la vez su mayor valor (aceptada por todos) y su mayor desventaja (no siempre está al día). En general, el método más sencillo es pedir la documentación aplicable, revisar el manual de fabricante, y comprobar que son coherentes, actualizadas, y se siguen.

10.10 LECTURAS RECOMENDADAS

TANENBAUM, A. (Varias ediciones): *Redes de ordenadores.* Prentice Hall. Es el libro de referencia, por antonomasia, en comunicaciones

UMUIART, A. (2007): *Seguridad de redes.* Amaya. Claras explicaciones prácticas de 125 de los mejores trucos de seguridad en redes.

LAYTON, T. (2007): *Information security.* Auerbach. Una clara y sólida evaluación de riesgos según ISO 17799

10.11 BIBLIOGRAFÍA

CERT. *Computer Emergency Response Team.* Carnegie Mellon University – www.cer.org

CERT España. *Equipo de Respuesta ante Emergencias Informáticas- www.inteco.es*

CSRC. *Computer Security Resource Center.* Instituto Nacional de Estándares y Tecnología EE.UU. http://csrc.nist.gov

Darlington. R. (editor): *Manual de Información Técnica para la Preparación al Examen CISA.* ISACA.

ISO/IEC 17799:2005 Information technology, Security techniques, Code of practico for infomiation security management.

ISO/IEC 18028-5:2006 Information technology, Security techniques, IT network security: Part 5: Securing communications across networks using virtual private networks.

ISO/IEC 150/IEC 18028-1:2006 Information technology, Security techniques, IT mimad(security: Part. 1: Network security management.

ITIL (2007) OCG (Editor) *Lifecycle Publication Suite.* TSO.

Derksen B. et al. (2004) *TCP/IP model*

hup://en.wikipedia.org/wiki/TCP/IP_model.

Krutz, D. y Vines, R. (2001): The *CISSP prep pide* Wiley.

Wadlow, T (2090): The process of Neiwork Security. Addison Wesley.

10.12 CUESTIONES DE REPASO

1. ¿Cuál es el nivel OSI dcl lenguaje XML?
2. ¿Cuáles son las características de un servidor para ser considerado un bastión?
3. ¿Por qué conviene segmentar la Intranet?
4. ¿Dónde almacena la red de comunicaciones el tráfico cursado en una sesión interrumpida?
5. ¿Cuál es el modelo habitual para aprovechar canales externos inseguros en comunicaciones entre distintos puntos de una empresa?
6. Siglas de un protocolo de Directorio de Usuarios muy extendido.
7. ¿Qué es un DOS?
8. ¿Cómo se denomina *engaño basado en ingeniería socia!* en inglés?
9. Equipo prácticamente imprescindible para construir una zona desmitalirizada
10. Modelo de Gestión de Servicio muy extendido.

Capítulo 11

AUDITORÍA DE INTERNET

11.1 INTRODUCCIÓN

El título de este trabajo puede sugerir muy diferentes contenidos a distintos lectores ya que, si al de por si amplio mundo de la auditoria informática le añadimos la palabra Internet, tenemos, prácticamente, un área de estudio prácticamente ilimitada. Por ello, la bibliografía y los trabajos sobre estos temas son muy numerosos y algunos de dios se mencionan en las lecturas recomendadas del Final del capítulo.

No obstante, si incluimos en la ecuación de la auditoria de Internet otro término, el de la privacidad o la protección de datos personales, obtenemos un nuevo enfoque, una nueva perspectiva que no ha sido abordada de manera tan amplia,, existiendo menos material sobre la misma.

Además, la importancia de la introducción de mecanismos de control y revisión de los mismos en este campo alcanza cada vez mayor importancia. No en vano venimos hablando desde hace ya bastante tiempo de la Sociedad de la Información, la Administración electrónica o el comercio electrónico lo que, en términos prácticos, significa que cada vez hay una mayor presencia de las organizaciones en Internet.

Pero no se trata sólo de un incremento cuantitativo sino también, y muy especialmente en los últimos años, de una gran ampliación cualitativa de los servicios que ofrecen las empresas y las Administraciones Públicas. Hemos pasado de un mundo en el que las organizaciones utilizaban Internet fundamentalmente para dar información de sus actividades, productos y servicios a otro completamente distinto en el que se pueden realizar muchos trámites administrativos mediante medios telemáticos —la declaración del Impuesto Sobre la Renta de las Personas Físicas sería el ejemplo paradigmático en España pero hoy en día existen muchos más- y es posible la oferta y prestación de múltiples servicios y la compra de infinidad de productos a través de Internet, siendo la banca electrónica y las subastas on-line dos meros ejemplos de este proceso.

Este nuevo escenario ha introducido un drástico cambio en la forma en que las personas se relacionan con las distintas organizaciones a través de Internet. En el pasado, la mayoría de las acciones de las personas se realizaban de forma anónima o prácticamente anónima puesto que para el mero acceso a la información no es necesario ningún tipo de identificación. Pero desde el momento en que realizamos operaciones en las cuales están implicados intercambios económicos y financieros o nos personamos delante de las Administraciones Públicas realizando solicitudes de cualquier tipo o interviniendo en procedimientos administrativos, la obligación de identificar correctamente a las personas es indispensable y, desde ese mismo momento, las organizaciones comienzan a tratar datos de carácter personal y están sujetas al cumplimiento de las normas que regulan el ejercicio y el debido respeto a este derecho fundamental reconocido en España y en la Unión Europea y regulado, esencialmente, por la Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos(151), la Directiva 2002/5810E, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[162] (Directiva sobre la privacidad y las comunicaciones electrónicas [163], la Ley Orgánica 15/1999, de 13 de diciembre. de Protección de Datos de Carácter Personal (LOPD) [164] y sus normas de desarrollo, la Ley 3212003, de 3 de noviembre, General de Telecomunicaciones[165]y la Ley 34/2002[166], de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSS1) [167]

Por lo tanto, el incumplimiento de estas normas lleva aparejado una serie de importantes riesgos para las organizaciones, tanto en términos económicos debido a las importantes sanciones que la ley establece para las infracciones a la misma corno en pérdida de imagen y confianza por parte de los consumidores, clientes y ciudadanos-

Así pues, huy en dia es indispensable integrar la auditoria del cumplimiento de las normas de protección de datos en el ámbito de lo que constituye probablemente el canal de mayor exposición pública de una organización en su relación con las personas ajenas a la misma. Y este control debe obligatoriamente enfocarse desde dos perspectivas distintas: legal y tecnológica, ya que ambos aspectos confluyen en la implantación de políticas de tratamiento de la información respetuosas con las leyes y los derechos de las personas.

La protección de datos personales se plasma en un conjunto de principios y derechos recogidos en la legislación vigente que es necesario conocer con cierta profundidad y plantearse seriamente su aplicación práctica ya que su aparente sencillez es engañosa: en muchas ocasiones resulta sumamente complejo y plantea dificultades importantes el conjugar la consecución de los legítimos objetivos comerciales, estratégicos o administrativos de una gran organización con el debido respeto a la normativa de protección de datos personales. O, dicho de otro modo, el tratamiento de datos personales en las condiciones marcadas per la ley puede requerir cambios organizativos en !as entidades públicas y privadas así como inversiones en recursos de distinto tipo[m].

11.2 PRINCIPIOS Y DERECHOS DE PROTECCIÓN DE DATOS

En este apartado se repasarán las principales obligaciones que la ley de protección de datos impone a las distintas organizaciones y, en especial, respecto de los servicios y actividades que las mismas prestan o llevan a cabo a través de Internet. Pero antes de comenzar este repaso, es necesario clarificar dos importantes conceptos: el de dato de carácter personal y el de tratamiento de datos personales,

Siguiendo la definición *de* la LOPD, se consideran dato de carácter personal cualquier información concerniente a personas físicas identificadas o identificables, Si la primera cláusula de la definición es obvia (si tomarnos datos de alguien cuya identidad ya conocemos en el momento de la recogida o tratamiento posterior de la información es evidente que estamos en presencia de datos personales) para ver el alcance del concepto de identificabilidad es necesario realizar alguna reflexión adicional.

En efecto, ya que la LOPD carece de una exposición de motivos que pueda ayudarnos a interpretar la voluntad del legislador, hemos de acudir al Considerando 26 de la Directiva

de Protección de Datos en el que se detalla que Y...) *que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado",*

A este respecto vemos que la posibilidad de identificación *se* deriva a un concepto indeterminado con el de "medios razonables" que deberá ser interpretado por cada responsable y tener en cuenta que los mismos no sólo hacen referencia a las posibilidades del responsable sino de otras personas, No obstante, es necesario poner de manifiesto que los criterios utilizados por las autoridades de control son bastante restrictivos a la hora *de* interpretar que un esfuerzo no *es* razonable: habría que presentar evidencias serias y fundadas de que realmente los medios que habría que utilizar para identificar a la persona o personas de que *se* trate son realmente desproporcionados, ya que no debemos olvidar que estamos en presencia de un derecho fundamental de las personas que no puede ser evadido con consideraciones de mero interés económico,

Por poner un ejemplo clasificador, la obtención de la identificación del abonado que está detrás de la dirección IP que ha accedido a una determinada página web en ningún caso puede suponer un esfuerzo desproporcionado para el proveedor de acceso a Internet ya que tiene registrada a quién corresponde la dirección IP utilizada si hay una asignación estática o, en caso de utilizar asignaciones dinámicas, puede en todo momento conocer a quién se le asignó la misma en un instante determinado.

En relación con el concepto de tratamiento de datos personales, la LOPD lo define como las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias, definición que tampoco requiere grandes comentarios o análisis posteriores.

11.2.1 Notificación de los tratamientos

En primer lugar, la LOPD establece que todo fichero o tratamiento de datos personales debe ser notificado a la Agencia Española de Protección de Datos (AEPD) para su inscripción en el Registro General de Protección de Datos. En el caso de aquellas comunidades autónomas que hayan creado su propia autoridad de control en esta inateria'7°, los ficheros de titularidad pública de su ámbito de competencia se notificarán a las mismas que, una vez inscritos en sus propios registros, procederán a comunicarlos a la Agencia española.

En el caso de los tratamientos a través de Internet, habrá que comprobar si los ficheros o tratamientos que se han declarado cubren todas las actividades y servicios de este ámbito, teniendo en cuenta que es una doctrina consolidada por parte de las autoridades de protección de datos que informaciones tales como las direcciones 1P o las direcciones de correo electrónico se consideran datos de carácter personal, por lo que habrá de asegurarse, por ejemplo, que los distintos los de acceso y navegación o las direcciones de correo electrónico están contempladas en los ficheros inscritos en la

AEPD y, si ello no fuera así, proceder a su notificación, bien por la declaración de nuevos tratamientos, bien por la modificación de los ya inscritos para adaptarlos a esta realidad.

El concepto de fichero en la legislación de protección de datos no se corresponde con el concepto de fichero informático. De hecho, La Directiva de Protección de Dates sólo define el concepto de fichero manual, refiriéndose en todo momento a tratamientos de datos personales y no ficheros. De acuerdo con la ley española, un fichero es "todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento organización y acceso", lo que puede perfectamente referirse desde un simple fichero plano a una gran base de datos que soporte todo un sistema de información, en general , en este texto se utilizara el concepto fichero en sus términos más amplios.

Una vez que todos los tratamientos hayan sido inscritos en la autoridad de protección de datos correspondiente, se pueden mostrar en nuestro sitio web los códigos de inscripción otorgados a cada uno de ellos en los lugares en los que se recoge o utiliza información relativa a los mismos y en la política de privacidad, siguiendo las pautas que se tratan más adelante en el apartado de información al interesado.

Este en sentido, resulta sumamente recomendable la consulta periódica de los sitios web de la autoridad de protección de dalos competente: la Agencia Española de Protección de Datos (www.agpd.es) para los Tratamientos del sector privado, de La Administración General del Estado y de las Administraciones Autonómicas y Locales allí donde no exista una agencia autonómica de protección de datos y, en estos momentos, las agencias autonómicas de Madrid (www.apdcm.es), Cataluña (www.apdcat.net) y del País Vasco (voryw.avpd.es) para los Administraciones Autonómicas y locales de **su** ámbito territorial.

También y de forma creciente, cada vez es más habitual que las organizaciones mantengan activas herramientas de comunicación interactiva con sus clientes para permitirles expresar sus opiniones o darles soporte técnico. En concreto, la utilización de blogs y de chats para estos propósitos está muy difundida por lo que también habrá que tener en cuenta que, en muchos casos, en los mismos se procesan datos personales por lo que estos tratamientos habrán de ser notificados a las autoridades de control. De igual forma, tecnologías emergentes de redifusión de contenidos como RSS también pueden suponer el tratamiento de datos personales y, por ello, deberán ser también tenidas en consideración,

Una vez llevada a cabo la notificación inicial, habrá que mantenerla actualizada de tal forma que los cambios que afecten, por ejemplo, a los datos recogidos, a la finalidad con que los mismos se tratan, a los datos del responsable de los mismos —por ejemplo, un cambio de dirección- o a la forma del ejercicio de los derechos de los ciudadanos, se notifiquen a la agencia de protección de datos competente por lo que habrán de establecerse los procedimientos adecuados para detectar que se han producido dichas modificaciones y poner en marcha los mecanismos adecuados de notificación.

11.2.2 Encargo de tratamientos

Un aspecto particularmente interesante de los tratamientos de datos personales

en Internet, aunque no se circunscribe en modo alguno a esta área, son las subcontrataciones de diversas clases de servicios, incluyendo el webhosting o el outsourcing de todos los sistemas informáticos. También se pueden subcontratar diversos servicios de recogida o tratamiento de datos, siendo un ejemplo particularmente interesante la medición de audiencias y los servicios de valor añadido asociados a las mismas, como la construcción de perfiles en base a los datos de diversos sitios web cuya medición de audiencias es gestionada por la misma compañía.

En estos casos se ha de ser particularmente cuidadoso a la hora de cumplir con los requisitos legales establecidos en la LOPD y que se pueden resumir diciendo que es necesaria la celebración de un contrato con el suministrador del servicio (encargado de tratamiento según la terminología de protección de datos) en el que se detallen las tareas que el mismo va a realizar y las finalidades de las mismas así como las medidas de seguridad que debe adoptar, el compromiso de no utilizar los datos personales para ninguna otra finalidad y la devolución o destrucción de los mismos a la finalización del contrato.

En este sentido, hay que señalar que habitualmente las organizaciones firman continuamente contratos de servicios con distintas entidades detallando multitud de aspectos de la relación entre las mismas pero, en muchos casos, estos contratos carecen de las necesarias cláusulas de salvaguardia en términos de protección de datos lo que supone un riesgo importante si se produce una actuación inspectora o de investigación de la autoridad de protección de datos competente, ya sea de oficio o por la existencia de una denuncia.

Por ello, estos aspectos deben de preverse cuando se vaya a establecer cualquier tipo de relación de prestación de servicios. Sería aconsejable introducir cláusulas tipo en los modelos de contrato que habitualmente se utilicen para asegurarse que se tienen en cuenta a la hora de redactar nuevos contratos, Cada vez que se firme un nuevo contrato, habrá que considerar si la cláusula estándar se adapta al servicio que estamos contratando y, en caso contrario, adaptarla a la realidad de cada momento.

11.2.3 Legitimación de los tratamientos

Un aspecto crucial y del que depende en gran medida el cumplimiento de las previsiones legales en materia de protección de datos es la habilitación legal para el tratamiento de los datos personales o, lo que es lo mismo, las previsiones en materia de legitimación de los tratamientos.

En la legislación española el mecanismo primordial para que un tratamiento de datos personales sea legítimo es contar con el consentimiento del afectado, Este consentimiento es una manifestación de voluntad libre, específica, inequívoca e informada mediante la cual e] interesado consiente el tratamiento de datos personales que le conciernen, lo que supone el cumplimiento de una serie de requisitos que no son en modo alguno triviales, destacando entre ellos el que ha de ser libre —lo que implica que debe existir la posibilidad de no prestarlo- y, sobre todo, informado en los términos que la ley establece y que consideraremos más adelante,

Pero el que el consentimiento sea el mecanismo privilegiado de legitimación previsto en la LOPD no significa que sea el único. Si existe una relación jurídica, negocial, laboral o contractual que implique la necesidad del tratamiento de datos personales para llevarla a término, e] tratamiento de los datos necesarios (y sólo de ellos) para el cumplimiento de la misma también sería legítimo. No obstante, si quisiéramos tratar dichos datos con otra finalidad no compatible con la inicial —por ejemplo, cederlos o comunicarlos a un tercero para que lleve a cabo operaciones de marketing con los mismos- sí que necesitaríamos e] consentimiento previo del interesado, ya que esta nueva finalidad no puede considerarse cubierta por la relación contractual, negocia', laboral e jurídica de que se trate.

Tampoco es necesario el consentimiento del interesado cuando los datos se recojan por parte de las Administraciones Públicas para el ejercicio de sus funciones propias en el ámbito de su competencia, lo que significa que, en general, en el terreno de la Administración Electrónica o e-Administración, siempre y cuando sólo se recojan aquellos datos necesarios para la relación administrativa de que se trate o para la prestación de un servicio público, las AA.PP, tampoco requerirían el contar con el consentimiento del afectado para el tratamiento de sus datos a través de Internet, De todas formas, esto tampoco significa que las Administraciones Publicas puedan tratar los datos personales para cualquier finalidad sin el consentimiento de los ciudadanos. Habrá ocasiones en las que la prestación de un determinado servicio tendrá carácter voluntario —por ejemplo, la remisión de un recordatorio de cita desde un hospital o centro de salud a un teléfono móvil mediante un mensaje MS- y el ciudadano decidirá libremente si consiente el tratamiento de sus datos personales con dicha finalidad.

Finalmente, el otro gran elemento legitimador de los tratamientos que un responsable puede llevar a cabo es que el mismo esté amparado en lo que dispongan las leyes. Aunque, en general, este mecanismo afecta en mayor medida a las AA.PP., ello no significa que las empresas privadas no deban realizar determinados tratamientos de datos personales porque así lo establecen las leyes. Pensemos, por ejemplo, en la obligación de comunicar a las autoridades tributarias las percepciones de los trabajadores de una empresa así como las retenciones practicadas o la comunicación a la Seguridad Social de los datos que la misma requiere. En todos estos casos, el tratamiento y la comunicación de datos personales vendría obligado por la ley y el consentimiento del afectado no jugaría ningún papel.

También existen otras posibilidades de legitimación previstas en la ley aunque tienen, en general, un impacto y una aplicación menor salvo en sectores muy específicos. Se trata de la existencia de un interés vital por parte del afectado, lo que permitiría el tratar sus datos sanitarios en los términos previsto en el apartado dedicado al tratamiento de datos especialmente protegidos (artículo 7 de la LOPD) y la posibilidad de procesar sin el consentimiento del interesado aquellos datos que figuren en fuentes accesibles al público, posibilidad que afecta, fundamentalmente, a aquellas compañías dedicadas a actividades de marketing y prospección comercial y a las que obtienen información sobre

solvencia patrimonial de los boletines oficiales. No obstante, en este último caso, el hecho de que no sea necesario el consentimiento de los interesados para el tratamiento de sus datos no exime a los responsables de dichos tratamientos de cumplir el resto de preceptos de la ley y, en particular, los relativos a calidad de datos e información al interesado, por lo que deberán establecerse los procedimientos oportunos para garantizar que se cumple con dichas previsiones legales.

Por lo tanto, antes de poner en marcha cualquier nuevo proyecto que implique el tratamiento de datos personales se deberá revisar si se cuenta con una habilitación legal clara para proceder a dicho tratamiento y, en caso de que la misma no existiera o hubiera dudas respecto de su aplicabilidad, se debería buscar una solución que, normalmente, pasaría por la solicitud del consentimiento a los interesados cuyos datos fueran a tratarse.

En este punto hay que tener en cuenta que la ley española sólo exige el consentimiento expreso cuando se trata de procesar datos especialmente protegidos o sensibles (ideología, religión, creencias, salud, origen racial o vida sexual) y considera válido el consentimiento tácito para el resto de datos personales. Ello quiere decir que se puede notificar a los interesados que sus datos van a ser tratados o cedidos a un tercero para una determinada finalidad Ki no se oponen u dicho tratamiento en un plazo razonable. En este sentido el nuevo Proyecto de Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece toda una serie de criterios y garantías para que la obtención de este consentimiento tácito se pueda considerar válida que, independientemente de que el Proyecto de Reglamento se apruebe definitivamente o no, deben de estudiarse e implantarse ya que constituyen el criterio de la Agencia Española de Protección de Datos para considerar válida esta forma de obtención del consentimiento.

En líneas generales, se podrá solicitar el consentimiento del interesado dirigiéndose al mismo e informándole en los términos previstos en los artículos 5 de la LOPD, concediéndole un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. En todo caso, será necesario que e] responsable del tratamiento tenga constancia de que la comunicación ha sido recibida por el destinatario de la misma ya que, en caso contrario, no podrá proceder al tratamiento de los datos referidos a ese interesado. Además, deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos, lo que en el entorno de Internet, no supone ninguna complicación.

En relación con un tratamiento de datos muy habitual en Internet, la suscripción y envío de boletines de noticias, habrá que garantizar el consentimiento del interesado y asegurarse de que pueden dar efectivamente de baja su suscripción en cualquier momento, lo que implica informarles de esta posibilidad en cada envio del boletín.

impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público,

exclusivamente, el censo promocional, los repertorios telefónicos en los términos provistos por su normativa específica y las listas do personas pertenecientes e grupos de profesionales, que contengan únicamente los datos de nombre, titulo, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

En todo caso, hay que tener en cuenta que cuando se trata de datos especialmente protegidos o sensibles, el nivel de protección que la ley les otorga es mas elevado y cuando los mismos se traten en base al consentimiento éste no podrá ser tácito sino que deberá ser expreso y afirmativo.

De cualquier manera, para evitar posible problemas en el futuro, ya sea por denuncias o por inspecciones de la autoridad de protección de datos competente, es necesario conservar prueba de la prestación del consentimiento por parte del interesado para poder demostrar en todo momento que los datos se han tratado legítimamente.

11.2.4 Información al interesado

Otro aspecto esencial y en el que las autoridades de protección de datos ponen un énfasis muy especial es la información al interesado respecto de los tratamientos que se van a llevar a cabo con sus datos personales. En este sentido, en el artículo 5 de la LOPD se establece que "'Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información_ b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. e) De Declarar la identidad y las direcciones postal y electrónica del responsable del tratamiento.

Indicar claramente para las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad .y dirección del responsable del tratamiento o. en su caso, de su representante". (...)*2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. (...) cuando los datos procedan de fuentes accesibles al público* y *se destinen a la actividad de publicidad o prospección comercial, (...) en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".*

Por lo tanto, el deber de suministrar información a las personas cuyos datos se recogen a través de Internet se describe claramente y de forma detallada en la normativa de protección de datos y las autoridades de control revisan con especial cuidado la información que se suministra a los interesados pues ella es la base para considerar válido o no el consentimiento que haya podido dar el titular de los datos y los usos posteriores de la información.

Hay que hacer un hincapié especia] en el hecho de que esta información sea clara,

comprensible y transparente, indicando de la forma más sencilla posible para qué se utilizarán los datos personales y si se van a comunicar o a ceder a terceros y, si es así, con qué propósito, ofreciendo siempre al interesado la posibilidad de oponerse o no dar su consentimiento a finalidades no conectadas con el propósito inicial de la recogida,

En el mundo *on-fine,* en el que se utilizan con frecuencia formularios electrónicos para la recogida de información, habrá también que tener en cuenta las disposiciones de la LOPD cuando se utilice este medio para recoger datos, debiendo constar la leyenda informativa en un lugar claramente visible y legible.

Por otra parte, si obtenemos datos personales —por ejemplo, números de teléfonos móviles o direcciones de correo electrónico- de fuentes accesible al público (teniendo en cuenta que sólo tienen dicho carácter las mencionadas en el artículo 3 de la LOPD y cuya definición se ha mencionado anteriormente en *este* trabajo) y los utilizamos para remitir comunicaciones comerciales o de marketing, deberemos hacer constar en cada una de las comunicaciones la fuente accesible al público de la que se tomaron los datos, la identidad del responsable del tratamiento y los derechos que asisten a los interesados.

Para resaltar la importancia de este apartado sobre la información a los afectados, baste señalar que el Grupo de Trabajo de Autoridades de Protección de Datos establecido en el artículo 29 de la Directiva de Protección de Datos (por lo que es conocido como Grupo de Trabajo del Articulo 29 o GT29) y que agrupa a todas las autoridades de protección de datos de los Estados miembros de la unión

Europea, ha dedicado varios documentos a este tema, entre los que merece la pena resaltar la Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea (WP 43, aprobada el 17 de mayo de 2001) y el Dictamen sobre una mayor armonización de las disposiciones relativas a la información (WP100, aprobado el 25 de noviembre de 2004[172].

En relación con el primero de ellos, quizás el de más interés para el tema que nos ocupa, las autoridades europeas de protección de datos dan una serie de pautas sobre cómo debería de abordarse la información a los interesados cuando se recogen sus datos a través de Internet,

En concreto, en relación con la información que se debe facilitar al interesado y el momento de hacerlo, el GT29 afirma que toda recogida de datos personales a través de una página web implica la necesidad de suministrar determinada información al interesado y señala que para cumplir dicha obligación es necesario:

- Declarar la identidad y las direcciones postal y electrónica del responsable del tratamiento.

- Indicar claramente para qué fines de tratamiento recoge los datos el responsable a través de un sitio web. Por ejemplo, si los datos personales se recogen tanto para firmar un contrato de cualquier

tipo (suscripción a Internet, pedido de un producto, etc.) corno para marketing directo, el responsable del tratamiento debe indicar claramente ambos fines.

- Especificar claramente si la información solicitada es obligatoria u opcional, teniendo muy en cuenta que la única información que puede ser obligatoria es aquella necesaria para prestar el servicio solicitado. La naturaleza obligatoria u opcional se puede indicar de diversas maneras (con un asterisco al lado de los campos obligatorios o añadiendo la palabra "opcional" junto a la información no obligatoria). Además, el que el interesado no facilite información opcional no debe llevar aparejado ningún perjuicio o utilizarse en su contra.
- Mencionar la existencia de los derechos de consentimiento u oposición, según el caso, respecto al tratamiento de datos personales, y de las condiciones para ejercer tales derechos así como los de acceso, rectificación y cancelación de datos.
- Informar sobre la persona o el servicio al que acudir para ejercer estos derechos y sobre la posibilidad de ejercerlos tanto en línea como en la dirección postal del responsable del tratamiento,
- Enumerar los destinatarios y cesionarios o las categorías de destinatarios y cesionarios para la información recopilada. Al recoger cualquier tipo de datos, los sitios web deberán indicar si los comunicarán o pondrán a disposición de terceros, en particular socios empresariales, filiales, etc., y por qué motivo, señalando si se trata de fines distintos de aquellos que motivan la recogida de datos o de marketing directo.

En el caso de que se pueda ejercer el derecho de oposición, los usuarios de Internet deberán tener la posibilidad real de oponerse a ello on-line marcando una casilla relativa a la comunicación de datos para fines distintos de la prestación del servicio solicitado, Puesto que el derecho de oposición se puede ejercer en cualquier momento, la posibilidad de ejercerlo en línea también debería indicarse en la información facilitada al interesado.

- Si se prevé que el responsable de los datos transfiera dichos datos a países no miembros de la Unión Europea, indicar si estos países ofrecen o no una adecuada protección de los interesados en cuanto al tratamiento de sus datos personales en el sentido que recoge el artículo 25 de la Directiva 9514 /CE y en el articulo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En este caso, se deberá facilitar información específica sobre la identidad y la dirección de los destinatarios (dirección postal o electrónica),
- Proporcionar el nombre y la dirección (postal y electrónica) del servicio o la persona responsable de responder a las preguntas relacionadas con la protección de los datos personales,
- Mencionar con claridad la existencia de procedimientos automáticos de recogida de datos, -como cookies o contenido activo- antes de usar dichos métodos173. Cuando se utilicen tales procedimientos, el

interesado deberá recibir la información que se ha venido indicando. Además, se le deberá informar del nombre de dominio del servidor que transmite los procedimientos automáticos de recogida, la finalidad de dichos procedimientos, su plazo de validez, si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio y la opción de que dispone todo usuario de Internet de oponerse a su uso, además de las consecuencias de desactivar dichos procedimientos.

- En caso de que otros responsables del tratamiento de los datos participen en la recogida de datos personales, el interesado deberá recibir información sobre la identidad de los responsables del tratamiento y la finalidad del tratamiento en relación con cada responsable.
- La información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio web, por ejemplo, cuando un sitio web conecta automáticamente al usuario a otro sitio para mostrarle publicidad en forma de pancarta publicitaria (banner.9, con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello. Por ejemplo, si el servidor de un responsable del tratamiento coloca una cookie, la información deberá facilitarse antes de que ésta se envíe al disco duro del usuario de Internet, además de la información habitualmente facilitada que se limita a dar el nombre del sitio transmisor y e] periodo de validez de la cookie.
- Destacar las -medidas de seguridad que garantizan la autenticidad del sitio, la integridad y la confidencialidad de la información transmitida a través de la red.
- La información se proporcionará en todos los idiomas utilizados en el sitio y, en particular, en los lugares donde vayan a recogerse datos personales.
- Los responsables del tratamiento deberán verificar la coherencia de la información proporcionada en los diversos documentos que comprometen al sitio (política de privacidad, formularios electrónicos, texto relativo a las condiciones generales de venta y otras comunicaciones comerciales).

11.2.5 Calidad de los datos

El principio de calidad de datos engloba varios apartados dentro del mismo (limitación de la finalidad, proporcionalidad, actualización y limitación de la conservación) y se podría enunciar, siguiendo a la LOE), de la siguiente forma: "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas pura las que se hayan obtenido **(Principio de Proporcionalidad) (...)** reo Mirón usarse para finalidades incompatibles con aquellas para las que los dalos hubieran sido recogidos **(Principio de Finalidad) („)** serán exactos y puestos al dio de forma que respondan con veracidad a la situación actual del afectado („) si resultaran ser inexactos, en todo o en parte, o incompletos, serán

cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados **(Principio de Actualización) (...)** serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados (Principio de Limitación del **Tiempo** de Conservación) ''

Además, también se establece la obligatoriedad de almacenar los datos personales de tal forma que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición y se prohíbe explícitamente la recogida de los mismos por medios fraudulentos, desleales o ilícitos, lo que incluye, por ejemplo, la obtención **de** datos del ordenador **del usuario** a través de *cookies, sypware o* contenido activo sin cumplir con los requisitos de información y legitimación que se han comentado en epígrafes anteriores.

El primer aspecto que debemos tener en cuenta es, pues, la necesidad de los datos que solicitamos a los afectados y aplicar una política de minimización de datos, consistente en solicitar y tratar la menor cantidad posible éstos y, siempre que sea posible, no utilizar ningún dato personal y permitir la utilización anónima de los servicios. Por ejemplo, si se trata de un sitio web dedicado a la venta de bienes o servicios, no *es* necesario identificar ni recoger ningún dato del usuario **hasta que éste** decide hacer una compra, momento en el que, nominalmente y salvo que se utilicen mecanismos de pago muy especializados que no son los habituales en transacciones a través de Internet, será necesario obtener ciertos datos para poder facturar el bien o servicio prestado o, incluso, para la entrega física del producto adquirido.

Igualmente, será necesario establecer procedimientos de actualización de la información para que ésta responda en todo momento a la situación real del afectado y refleje correctamente el estado de *sus* transacciones o requerimientos de servicio. En muchos casos, parte de la información almacenada podrá ser gestionada directamente por el usuario, ya que si se permite entregar la información para la solicitud del servicio o la adquisición del producto a través de Internet también es razonable que, tras utilizar mecanismos adecuados de identificación y autenticación, éste pueda gestionar sus datos —o, al menos, parte de ellos- por sí mismo.

Aquellos datos que respondan por ejemplo a pagos realizados, estado de los pedidos realizados o de los expedientes tramitados, en general y sin perjuicio del posible acceso en consulta a los mismos, deberán ser gestionados por el responsable **del tratamiento y, como se ha dicho, deberán habilitarse** los procedimientos de control necesarios para que la información esté siempre actualizada y responda con veracidad a la situación real de cada persona.

Igualmente, deberán de definirse los periodos durante los cuales deberá de conservarse la información de las personas, ya sea por necesidades derivadas de la relación existente entre el responsable del tratamiento y los afectados o por requerimientos legales que pudieran establecer periodos específicos de interesado deberá recibir la información que se ha venido indicando. Además, se le deberá informar del nombre de dominio del servidor que transmite los procedimientos automáticos de recogida, la finalidad de dichos procedimientos, su plazo de validez, si es necesaria o no la aceptación de dichos procedimientos para visitar el sitio y la opción de que dispone todo usuario de Internet de oponerse a su uso, además de las consecuencias de desactivar dichos procedimientos.

- En caso de que otros responsables del tratamiento de los datos participen cn la recogida de datos personales, el interesado deberá recibir información sobre la identidad de los responsables del tratamiento y la finalidad del tratamiento en relación con cada responsable.

- La información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio web. por ejemplo, cuando un sitio web conecta automáticamente al usuario a otro sitio para mostrarle publicidad en forma de pancarta publicitaria banners con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello. Por ejemplo, si el servidor de un responsable del tratamiento coloca una cookie, la información deberá facilitarse antes de que ésta se envié al disco duro del usuario de Internet. además de la información habitualmente facilitada que se limita a dar el nombre del sitio transmisor y el periodo de validez de la cookie.

- Destacar las medidas de seguridad que garantizan la autenticidad del sitio, la integridad y la confidencialidad de la información transmitida a través de la red.

- La información se proporcionará en todos los idiomas utilizados en el sitio y, en particular, en los lugares donde vayan a recogerse datos personales.

- Los responsables del tratamiento deberán verificar la coherencia de la información proporcionada en los diversos documentos que comprometen al sitio (política de privacidad. formularios electrónicos, texto relativo a las condiciones generales de venta y otras comunicaciones comerciales).

Respecto a cómo debe facilitarse la información, el GT29 considera que hay una información mínima que debe mostrarse directamente en la pantalla para garantizar el tratamiento leal de los datos:

- la identidad del responsable del tratamiento,
- la finalidad.
- el *carácter* obligatorio o no de la información solicitada.
- los destinatarios o las categorías de destinatarios de los datos recogidos.
- la existencia de los derechos de acceso y rectificación.
- la existencia del derecho de oposición a que los datos se comuniquen a terceros para fines distintos de la prestación del servicio solicitado y la manera de ejercerlo (por ejemplo, mediante una casilla que el usuario pueda marcar),
- la información que se deberá proporcionar al utilizar procedimientos automáticos de recogida,
- el nivel de seguridad durante todas las fases del tratamiento incluida la transmisión a través de redes.

En el caso de los métodos automáticos de recogida de datos esta información podría facilitarse mediante la técnica de una ventana emergente (popup window), sin olvidar que la legislación española establece que cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un

procedimiento sencillo y gratuito. Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente *necesario. para la prestación de un servicio de la sociedad* ***de la*** *información expresamente solicitado por el destinatario "".*

Igualmente, el GT29 considera que en la página de inicio del sitio y en todos los lugares donde se recojan datos personales en línea deberá poderse acceder directamente a información completa sobre la protección de datos personales -el documento que se conoce habitualmente como "Politica de Privacidad"- y que incluirá la forma de ejercer el derecho de acceso. El titulo del encabezado que deba seleccionarse con el ratón deberá estar resaltado, ser explícito y especifico, de manera que transmita al usuario de Internet una idea clara del contenido que se le va a mostrar (Protección de Datos Personales o Politica de Privacidad son dos posibles ejemplos).

Como conclusión, también hay que señalar que desde un punto de vista práctico, habrá que poner los medios necesarios para poder demostrar que se ha suministrado la información que la ley establece a todas aquellas personas cuyos datas son recogidos a través *de* Internet, de tal manera que cl procedimiento sea claro, transparente y auditable por parte de la autoridad de protección de datos competente.

11.2.5 Calidad de los datos

El principio de calidad de datos engloba varios apanados dentro del mismo (limitación de la **finalidad,** proporcionalidad, actualización y limitación de la conservación) y se podría enunciar, siguiendo a la 1.0PD. de la siguiente forma: *-Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados. pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legitimas para las que se hayan obtenido* **(Principio de Proporcionalidad) (...)** *no podrán usarse para finalidades incompatibles con aquellas para /*as *que los datos hubieran sido recogidos* **(Principio de Finalidad) (...)** *serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado (...) si resultaran ser inexactos. en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados* **(Principio de Actualización) (...)** *serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados* **(Principio de Limitación del Tiempo de Conservación)-.**

Además, también se establece **la obligatoriedad de** almacenar los datos personales de tal forma que permitan el ejercicio de los derechos de acceso. rectificación, cancelación y oposición y se prohíbe explícitamente la recogida de los mismos por medios fraudulentos, desleales o ilícitos, lo que incluye, por ejemplo, la obtención de datas del ordenador del usuario a través de *cookies, sypware* o contenido activo sin cumplir con los requisitos de información y legitimación que se han comentado en epígrafes anteriores.

El primer aspecto que debemos tener en cuenta es, pues, la necesidad de los datos que solicitamos a los afectados y aplicar una política de minimización de datos, consistente en solicitar y tratar la menor cantidad posible éstos y, siempre que sea posible, no utilizar ningún dato personal y permitir la utilización anónima de las servicios. **Por**

ejemplo, si se trata de un sitio web dedicado a la venta de bienes o servicios, no es necesario identificar ni recoger ningún dato del usuario hasta que éste decide hacer una compra, momento en el que, normalmente y salvo que se utilicen mecanismos de pago muy especializados que no son los habituales en transacciones a través de Internet, será necesario obtener cienos datos para poder facturar el bien o servicio prestado o, incluso, para la entrega física del producto adquirido.

Igualmente, será necesario establecer procedimientos de actualización de la información para que ésta responda en todo momento a la situación real del afectado y refleje correctamente el estado de sus transacciones o requerimientos de servicio. **En** muchos casos. pene de la información almacenada podrá se gestionada directamente por el usuario, ya que si se permite entregar la información para la solicitud del servicio o la adquisición del producto a través de Internet también es razonable que, tras utilizar mecanismos adecuados de identificación y autenticación, éste pueda gestionar sus datos o al menos, parte de ellos- por sí mismo.

Aquellos datos que respondan por ejemplo a pagos realizados, estado de los pedidos realizados o de los expedientes tramitad" en general y sin perjuicio del posible acceso en consulta a los mismos, deberán ser gestionados por el responsable del tratamiento y, como se ha dicho, deberán habilitarse los procedimientos de control necesarios para que la información esté siempre actualizada y responda con veracidad a la situación real de cada persona.

Igualmente, deberán de definirse los periodos durante los cuales deberá de conservarse la información de las personas, ya sea por necesidades derivadas de la relación existente entre el responsable del tratamiento y los afectados o por requerimientos legales que pudieran establecer periodos específicos de conservación de la información (por ejemplo. en relación con historias clínicas o datos tributarios).

Una vez definidos estos periodos de mantenimiento de la información, se deberán implantar los procedimientos y controles necesarios para proceder a la cancelación y borrado de dichos datos una vez que los mismos se han cumplido *y.* por ello, la información ya no resulta necesaria ni se debe seguir manteniendo.

Finalmente, hay que tratar el complejo asunto de las finalidades compatibles. Como regla general y dada la estricta interpretación dada por el Tribunal Constitucional del significado de la palabra "compatible" (cf. STC 2922000), sería aconsejable no utilizar los datos personales para finalidades sobre las cuales no se haya informado previamente al afectado y, en caso de ser necesario, se le haya solicitado su consentimiento ya sea expreso o tácito según el tipo de datos de que se trate.

11.2.6 Confidencialidad de la información

En términos de protección de datos, este principio se conoce como "Deber de Secreto" y se refiere a la obligación del responsable del tratamiento y de cualquier otra persona que participe en el mismo, ya sea como empleado del responsable, corno encargado del tratamiento o en cualquier otro papel, de no revelar a nadie los datos personales que conozcan en el ejercicio de su actividad, incluso después de haber cesado en la misma o de haber finalizado su relación con el responsable del tratamiento.

Esta obligación de secreto depende, pues, en última instancia, de la voluntad de las personas aunque ello no exime al responsable de tomar todas las medidas a su alcance para limitar los riesgos de fugas de información ilícitas.

En primer lugar, se deben definir clara y cuidadosamente las necesidades de información de cada persona en relación con la actividad que realiza. Para ello, se puede utilizar como gula el conocido criterio "*need to know*" o, lo que es lo mismo, cada persona sólo debería poder acceder a aquella información que le resulta estrictamente necesaria para el desarrollo de sus funciones.

Una vez definidas estas necesidades de información, se deberían implantar las herramientas técnicas necesarias de identificación, autenticación y control de accesos para que cada persona accediera únicamente a la información que necesita para su trabajo.

Esta definición y concreción de accesos no siempre resulta una tarea fácil por diversos motivos. El primero de los mismos es la reticencia de cienos empleados a que se les limiten sus capacidades de acceso a la información ya que esta medida se puede considerar como una falta de confianza e, incluso, como una pérdida de status dentro de la organización.

Además, también ha de señalarse que no siempre es sencillo delimitar claramente si una persona nunca debe de tener acceso a cientos tipos de información. Por ello, es conveniente ejercitar tanto la delimitación rigurosa como la necesaria flexibilidad para permitir un correcto funcionamiento de las organizaciones públicas y privadas. Finalmente, será la gerencia de la organización la que decida *en* aquellos casos limite o fronterizos *en* los cuales no existe una solución clara y evidente.

No obstante, aparte de la necesaria implantación de las medidas técnicas de control de accesos, no hay que olvidar que las mismas no garantizan, ni mucho menos, la confidencialidad de la información ya que. en último extremo y aunque hubiera medidas de seguridad física tan drásticas que hicieran prácticamente imposible la salida de ningún soporte de datos de la organización, siempre cambiaría la posibilidad de que una persona guardara en su memoria determinada información y que la divulgara con posterioridad.

E**n** este sentido, hay tres herramientas indispensables que ayudan a minimizar los riesgos de fugas de información: formación, control y establecimiento de responsabilidades.

La educación y formación de los trabajadores es indispensable. Hay que desarrollar una importante labor de concienciación respecto de la confidencialidad de la información que manejan para que esta conciencia forme parte de la cultura de la entidad y. además de la planificación de cursos y otras actividades formativas. es una buena idea entregar personalmente a cada trabajador un pequeño dossier con sus obligaciones respecto a la confidencialidad de la información y las responsabilidades en que puede incurrir si viola dicha confidencialidad. Para reforzar su compromiso, también ayuda que tras conocer cabalmente sus obligaciones, firme (física o electrónicamente) un documento en el que reconoce que ha sido informado de sus obligaciones y responsabilidades así como de las consecuencias de su incumplimiento.

Las herramientas de control dependerán en buena medida del tipo de organización de que se trate pero, en todo caso, siempre es una buena idea establecer mecanismos de registro de los accesos a la información de cada usuario de los sistemas de información (si se trata de *acceder* a datos especialmente protegidos este registro de los accesos es obligatorio en España) *y* limitar las posibilidades de salida de soportes de información fuera de las dependencias de la organización o de transmisión de la mismas a través de Internet, por ejemplo. limitando el tamaño de los ficheros adjuntos a un correo electrónico o evitando que cienos tipos de datos puedan ser adjuntados a dichos mensajes. En este caso, hay que valorar los beneficios que se obtienen en cuanto a control de la información frente a las incomodidades o falta de eficiencia que pudieran suponer estas limitaciones.

Finalmente, hay que establecer y explicar claramente a los empleados las responsabilidades en que pueden incurrir por la divulgación ilícita de datas personales, tanto internamente dentro de la organización, con las medidas disciplinarias que la violación de las reglas de confidencialidad pudieran llevar consigo, hasta las posibles responsabilidades civiles por daños causados e. incluso. en determinados casos, las implicaciones penales de ciertas actuaciones.

11.2.7 Derechos de acceso, rectificación, cancelación y oposición

Un elemento esencial del régimen de protección de datos es la posibilidad de que los interesados puedan ejercer su derecho a conocer la información que sobre ellos poseen los responsables que tratan sus datos, a modificarla o cancelarla cuando sea incompleta o inexacta o su tratamiento no se ajuste a lo establecido por la ley y a oponerse -en determinadas circunstancias y para determinadas finalidades- al tratamiento de sus datos personales. Aunque la Directiva de Protección de Datos permitiría cobrar una tasa que cubriera el coste efectivo de proporcionar, modificar o cancelar la información, la ley española consagra la gratuidad del ejercicio de estos derechos ante responsables establecidos en España.

Cuando una persona ejerce estos derechos ante un responsable de tratamiento, independientemente de que éste decida acceder o no a la petición. siempre debe responder al afectado, bien concediéndole el derecho solicitado o denegándoselo, en cuyo caso deberá motivar la denegación y notificarle que puede recurrir su decisión ante la autoridad de protección de datos competente.

Dentro del ámbito de Internet, hay dos aspectos interesantes que resaltar respecto del ejercicio de estos derechos. En primer lugar hay que considerar la necesidad de asegurarse de la identidad del afectado cuando este ejerce sus derechos *on-line y,* a continuación, la consideración de permitir el ejercicio de las derechos *ondina* cuando los servicios también se prestan de este modo.

En efecto, en el entorno tradicional de gestión en papel, se solicita para probar la identidad que se incluya una fotocopia del Documento Nacional de Identidad así como una solicitud firmada pidiendo el ejercicio del derecho.

En Internet, estas garantías sc cumplirían sin ningún tipo de problemas si se utilizaran firmas *y* certificados digitales reconocidos en los términos establecidos en la Ley 59/2003. de 19 de diciembre. de firma electrónica y su

legislación de desarrollo. No obstante, conviene realizar algunas matizaciones que quizás podrían avalar el ejercicio de estos derechos *on-line* en otras condiciones.

Por ejemplo, operaciones tan importantes como las ligadas a la banca electrónica se llevan a cabo, en la mayor parte de los casos, sin que se exija la utilización de certificados digitales sino que se utilizan mecanismos de autenticación definidos por las propias entidades bancarias sin unas garantías tan estrictas. En otro tipo de servicios, es muy frecuente que para acceder a los mismos sea suficiente con identificarse mediante un código de usuario y una contraseña.

Por ello, parece razonable que los mismos criterios que sirven para identificar a un usuario para acceder al servicio debieran ser suficientes para autenticarle cuando quiera acceder o modificar sus datos personales y. de hecho, en muchos sitios web se sigue esta política.

No obstante, es de esperar que con la introducción del Documento Nacional de Identidad electrónico (e-DNI) y la posibilidad de utilizar los certificados electrónicos que contiene, cada vez sea mayor el número de responsables que decida utilizar estos nuevos servicios para identificar y autenticar a las personas que ejercen sus derechos *on-line.*

De nuevo, un aspecto importante en relación con el ejercicio de los derechas es la prueba de que las mismos se han satisfecho por parte del responsable. Cuando no hay un acceso o modificación directa de los datos por parte del propio usuario, es posible que también se pueda solicitar el ejercicio de los mismos a través de Internet, bien mediante la cumplimentación de un formulario o la remisión de un correo electrónico. En este punto, hay que retomar de nuevo el problema de la prueba de la identidad ya que si en el primero de los casos, es posible solicitar una identificación y autenticación previa a la presentación del formulario, ello no es posible si se utiliza un correo electrónico ordinario. No obstante, siempre es posible adjuntar una imagen digital del Documento Nacional de Identidad a la petición del ejercicio del derecho y, en su caso, incluir una firma digitalizada en cl mismo correo electrónico a través del que se realiza la petición.

Otro aspecto que se ha de tener en cuenta y que es muy específico de la legislación española es que la cancelación de los datos no lleva aparejada la supresión risita de la información en una primera instancia, sino que los mismos quedan "bloqueados" y a disposición de las AA.PP., Jueces y Tribunales para la atención de posibles responsabilidades derivadas del tratamiento durante el plazo de prescripción de las mismas. Durante el tiempo que los datos permanecen bloqueados, únicamente podrán ser tratados para la atención de dichas responsabilidades y a solicitud de las autoridades administrativas y judiciales, lo que deberá ser tenido en cuenta para evitar el uso de estos datos para otras finalidades ya no permitidas: los procedimientos y sistemas de bloqueo deben estar perfectamente configurados pan evitar posibles mores que podrían conducir a una denuncia ante la autoridad de protección de datos competente y, en su caso, a la declaración de una infracción.

Finalmente, también hay que considerar los plazos para hacer efectivos los derechos: el de acceso hay que contestarlo en el plazo máximo de un mes y el resto en un plazo de diez días.

11.2.8 Transferencias internacionales de datos personales

Una transferencia internacional de datos es el envió de datos personales desde un país del Espacio Económico Europeo (Unión Europea más Noruega. Islandia y Liechtenstein) a otro país n, cualquiera que sea la finalidad e incluyendo la transmisión para la prestación de un servicio por parte de un encargado de tratamiento.

La Sentencia Lindqvist del Tribunal de Justicia de las Comunidades Europeas"' ha venido a clarificar un aspecto importantísimo a este respecto: la mera publicación de datos personales en una página web no puede considerarse una transferencia internacional de datos, por lo que en este ámbito no regirán las normas que regulan éstas, lo que no quiere decir que no deban de cumplirse el resto de preceptos de la ley en relación con, por ejemplo, la legitimación de los tratamientos y las cesiones de datos, el derecho de información o la calidad de datos.

En el caso de que se vaya a realizar la transferencia a un tercer país. habrá que saber primero si se considera un destino adecuado de protección de datos", en cuyo caso no es necesario adoptar ninguna otra medida. Si el país de destino no figura entre aquéllos que gozan de un nivel adecuado de protección, se deberá estudiar si se puede llevar a cabo la transferencia en base a alguna de las excepciones del artículo 34 de la LOPD: por aplicación de tratados o convenios en los que sea parte España: para prestar o solicitar auxilio judicial internacional; si es necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios; cuando se refiera a transferencias dinerarias conforme a su legislación específica; si el afectado ha dado su consentimiento inequívoco; cuando sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado; si resulta necesaria para la celebración o ejecución de un contrato celebrado o por celebrar. en interés del afectado, por el responsable del fichero y un tercero; si es necesaria o legalmente exigida para la salvaguarda de un interés público; cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial o cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.

Si no podemos aplicar ninguna de esta excepciones, deberemos solicitar a la AEPD una autorización para la transferencia aduciendo las garantías adecuadas que, generalmente, se plasmarán en un contrato entre el exportador y el importador en un país tercero. Existen tres Decisiones de la Comisión Europea que establecen un conjunto de cláusulas tipo estándares que pueden utilizarse para la realización de estos contratos y que aportan las garantías adecuadas para dichas transferencias.

Por lo tanto, si vamos a realizar transferencias internacionales a terceros países, deberemos ajustar nuestros procedimientos e introducir los mecanismos de control adecuados para asegurar que sc ha cumplido con todos los trámites legales y con todas las exigencias que marca la ley a este respecto.

11.2.9 Medidas de seguridad

Aun siendo este un aspecto crucial en la correcta protección de los datos de carácter

personal en Internet, este artículo no se detendrá mucho en él. ya que existe otro capítulo de este libro que trata en profundidad estos aspectos.

No obstante, hay que señalar que en lo que respecta a los datos de carácter personal, en España existe una regulación de obligado cumplimiento aplicable también a todos aquellos datos personales que se tratan a través de Internet. Se trata del Real Decreto 994/1999. de 1 1 de junio. por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personan".

En ella se establecen tres niveles de seguridad (básico, medio y alto) en función de los tipos de datos y tratamientos que se realizan sobre ellos y establece la obligatoriedad de confeccionar y mantener actualizado un documento de seguridad en el que se detallen las medidas que se han adoptado pan cumplir con lo previsto en el Reglamento. No obstante, en el apanado cn el que se aborden las listas de controles se incluirán algunos relativos al cumplimiento de estas medidas de seguridad.

11.2.10 Comunicaciones comerciales no solicitadas *(spam)*

La remisión de comunicaciones comerciales no solicitadas -hecho conocido como *sponr*- a través de Internet, fundamentalmente mediante el uso de los servicios de correo electrónico, es uno de los aspectos más detestado por los usuarios de Internet y que más puede deteriorar la imagen de una organización si no se hace conforme a los requisitos legales, además del riesgo que supone el poder ser sancionados por la autoridad de control.

La Directiva 58/2002/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) contiene las previsiones básicas a las que debe someterse el envío de estas comunicaciones. En nuestro derecho interno, la norma que rige estas no solicitadas se encuentra en los artículos 20 a 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (I.SSI) en la redacción dada a los mismos por la Disposición Adicional Primera de la Ley 32/2003 General de Telecomunicaciones.

En relación con la información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos, las realizadas por vía electrónica deberán ser claramente identificables como tales e indicar a la persona física o jurídica en nombre de la cual se llevan a cabo. Si se realizan por correo electrónico, deberán incluir al comienzo del mensaje la palabra "Publicidad".

Seguidamente, se establece la prohibición de enviar comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

No obstante, la norma dispone un régimen más flexible en aquellos casos en los que exista una relación contractual previa, siempre que el remitente de la comunicación hubiera obtenido de forma licita los datos de contacto del destinatario y los emplee para el envió de comunicaciones comerciales referentes a productos o servicios de su propia empresa que

sean similares a los que inicialmente fueron objeto de contratación con el cliente.

Pero aun en este casa el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Igualmente, se establecen una serie de derechos de las personas que reciban estas comunicaciones, como el de revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente mediante un procedimiento sencillo y gratuito, facilitándoles información accesible por medios electrónicos sobre dichos procedimientos.

Además, el GT29 ha adoptado el 27 de febrero de 2004 el Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/51KE (WP90)In en cl que hacen una serie de reflexiones de gran interés para aquellas organizaciones que desean utilizar los medios de comunicación electrónicos para la remisión de publicidad y ofertas promocionales de una manera respetuosa con los derechos de las personas y. en este punto, hay que mencionar explícitamente que según la legislación española, las reglas relativas a las comunicaciones comerciales no solicitadas son de aplicación tanto a las personas físicas como jurídicas.

11.3 CONTROLES

Finalmente, y a modo de un complemento práctico a lo dicho hasta ahora, se propone una lista de controles. que en ningún caso debe entenderse como exhaustiva, que deberían establecerse en las organizaciones para ayudar a la efectiva implantación de una política correcta en materia de protección de datos, especialmente en relación con los tratamientos llevados a cabo a través de Internet. Dichos controles se agruparán en función de los epígrafes contemplados en el apanado segundo de este trabajo.

- Establecer procedimientos de gestión de la notificación de tratamientos de datos personales.
- Revisar todos las sistemas de información que operan a través de Internet para comprobar si todos ellos han sido notificados a la autoridad de protección de datos competente.
- Incluir dentro de los procesos de diseño y desarrollo de nuevos sistemas o de modificación de los existentes la verificación de si es necesario actualizar la notificación a la autoridad de protección de datos para incluir el sistema nuevo o modificado.

11.3.1 Notificación de los tratamientos

- Establecer procedimientos de gestión de la notificación de tratamientos de datos personales.
- Revisar todos las sistemas de información que operan a través de Internet para comprobar si todos ellos han sido notificados a la autoridad de protección de datos competente.

- Incluir dentro de los procesos de diseño y desarrollo de nuevos sistemas o de modificación de los existentes la verificación de si es necesario actualizar la notificación a la autoridad de protección de datos para incluir el sistema nuevo o modificado.

- Revisar periódicamente los tratamientos notificados para comprobar si todavía se ajustan a la realidad cambiante de una organización y. caso de no ser así, lanzar el procedimiento de modificación de la notificación.

- Tener en cuenta que las direcciones IP y las de correo electrónico se pueden considerar como datos de carácter personal y, por ello, los logs que las recogen serán tratamientos de datos personales.

- Recordar que los datos sobre personas recogidos en bloggs. chats y otras herramientas interactivas también han de ser tenidos en cuenta en la declaración de ficheros.

11.3.2 Encargo de tratamientos

- Establecer cláusulas modelo que puedan incluirse en los contratos generales. con las adaptaciones que resulten necesarias en cada caso.

- Establecer procedimientos para incluir las cláusulas que recojan las obligaciones establecidas en la normativa de protección de datos en cualquier contrato que se firme con un tercero al que se le encarguen operaciones que lleven aparejado el tratamiento de datos personales.

- Asegurarse que con cualquier proveedor de servicios de tratamiento de datos personales se firma un contrato que los regule.

- Prestar atención al hecho de que determinados encargos —como quizás las mediciones de audiencia en las que se recogen datos de otras organizaciones- pueden no constituir un acceso por terceros a nuestra información, sino una auténtica cesión de datos a otro responsable, cuyas reglas son completamente distintas.

11.3.3 Legitimación de los tratamientos

- Verificar siempre la habilitación que existe para tratar datos personales.

- Si es necesario contar con el consentimiento, establecer procedimientos de solicitud del mismo que cumplan los requisitos legales sobre información.

- En los procedimientos de gestión del consentimiento, contemplar siempre la conservación de la prueba de que cl consentimiento se ha prestado.

- En el caso de que se pueda utilizar el consentimiento tácito, establecer mecanismos de comprobación de que los interesados han recibido realmente la comunicación y. cuando ello no se pueda comprobar. diseñar los mecanismos necesarios para que no sc traten sus datos personales con la finalidad solicitada.

- Establecer procedimientos de gestión de las respuesta negativas a la solicitud de consentimiento tácito para asegurar que las mismas se tienen en cuenta y se excluyen del tratamiento los datos personales de quienes asi lo solicitan.

- Verificar que siempre que se desee utilizar los datos personales de los afectados para finalidades diferentes de aquellas que constituyen la relación negocial, administrativa. juridica o labor-al primaria, se ofrezcan en los instrumentos que la regulan (normalmente un contrato) la posibilidad de dar o no su consentimiento para esta nueva finalidad mediante, por ejemplo, la existencia de una casilla en la que se preste o no el consentimiento, casilla que, caso de no ser marcada, debería representar la negativa al tratamiento.

- Si se recogen datos especialmente protegidos, tener en cuenta que el consentimiento ha de ser expreso.

- Si se realizan suscripciones a boletines de información u otras publicaciones, asegurar de que en cada número se ofrece la posibilidad de darse de baja del servicio.

11.3.4 Información al interesado

- Redactar una cláusula informativa tipo con todos los elementos previstos cn la ley y consensuada por todos los departamentos que tratan datos personales y que se pueda adaptar a cada recogida concreta de datos. En la misma debería constar claramente el departamento o unidad encargada de atender el ejercicio de los derechos de acceso. rectificación, cancelación y oposición.

- Redactar una política de privacidad completa, clara y transparente.

- Incluir un enlace a la política de privacidad en la página de inicio de la web de la organización y en cualquier otro lugar en el que se recojan datos personales. El enlace debería de estar en un lugar bien visible y tener un título claro y descriptivo.

- En cada lugar donde se recojan datos personales, incluir en la misma pantalla la cláusula informativa correspondiente.

- Marcar claramente los campos que son de cumplimentación obligatoria cuando se utilicen formularios electrónicos. Expresar claramente las consecuencias. si las hubiere, de no rellenar los campos opcionales.

- En el caso de utilizar datos procedentes de fuentes accesibles al público. asegurarse de que en cada comunicación que se realice en base a los mismos se incluya información sobre el origen de los mismos, la identidad del responsable del tratamiento y los derechos que asisten a sus receptores.

- En el caso de utilización de cookies, contenido activo o conexiones ocultas a servidores de terceros, establecer procedimientos para que la información al interesado se produzca antes del almacenamiento o ejecución de los mismos.

- Prestar atención a que la información se muestre en todos los idiomas en los que se proporcionan servicios o información en el sitio web.

- Verificar periódicamente la actualización de la información sobre tratamiento de datos personales y la coherencia de la misma que se ofrece en los distintos lugares del sitio web.

- Asegurarse de que cl procedimiento de suministro de información es auditable y está establecido de tal forma que permita demostrar que todos las interesados han recibido la información que marca la ley.

11.3.5 Calidad de los datos

- Definir claramente qué datos de carácter personal se precisan y no solicitar más que los estrictamente necesarios (minimización de datos).

- Establecer procedimientos de definición y revisión periódica de las finalidades para las que se utilizan los datos personales y comprobar que coinciden con las que aparecen en la información suministrada a los usuarios. Caso de no ser así, contemplar las medidas necesarias para actualizar la información de forma coherente en todos los lugares donde aparezca y. en su caso, solicitar de nuevo el consentimiento de los interesados.

- Definir procedimientos de actualización de oficio de los datos personales en base a la información de que se disponga, actuando con la debida diligencia.

- Definir plazos de conservación de la información -incluida la que se mantiene en archivos históricos o bloqueados con carácter previo a su cancelación definitiva- y establecer los procedimientos, preferiblemente automáticos, de revisión y cancelación.

- No recoger datos personales a través de sistemas "invisibles" (cookies, soleare. contenido activo. hiperenlaces ocultos, etc.) salvo que sc informe puntualmente de ello al usuario con carácter previo a su utilización y se obtenga su consentimiento cuando sea necesario.

- Procurar, siempre que sea posible, la utilización anónima de los servicios ofertados a través de Internet.

11.3.6 Confidencialidad de la información

- Definir procedimientos de concienciación, formación e información a todos los empleados que acceden a datos de carácter personal para darles a conocer sus obligaciones y las responsabilidades en que pueden incurrir caso de no cumplirlas. El procedimiento debería incluir la firma de un compromiso de confidencialidad por parte de todos los trabajadores.

- Definir cuidadosamente las necesidades de información de cada persona y limitar las accesos a la misma en función de dichas necesidades.

- Instalar las herramientas tecnológicas necesarias para identificar, autenticar y controlar el acceso a los recursos.

- Controlar el tamaño y los tipos de ficheros adjuntos que se remiten a través de los mensajes de correo electrónico y otros sistemas de intercambio de ficheros para limitar los riesgos de difusión masiva de información no autorizada.

11.3.7 Derechos de acceso, rectificación, cancelación y oposición

- Asegurarse de que se identifica y autentica adecuadamente a las personas que ejercen sus derechos antes de entregarles cualquier información. En caso de dudas, requerir aclaraciones o elementos adicionales de identificación y autenticación.

- Establecer procedimientos (on-line en la medida de lo posible) de atención a las peticiones de ejercicio de los derechos por parte de los ciudadanos, cuidando de que las mismas scan revisadas por las personas adecuadas dentro de la organización.

- Vigilar que se cumplan los plazos establecidos y se conteste adecuadamente a los interesados. informándoles de la posibilidad de recurrir la decisión de la organización ante la autoridad de protección de datos competente si se le deniega el ejercicio del derecho.

- Guardar prueba de todo el proceso de atención de los derechos, incluyendo la recepción y la contestación al afectado.

- Implantar sistemas de formularios electrónicos para el ejercicio de los derechos, tras haber autenticado a la persona.

11.3.8 Transferencias internacionales de datos personales

- Verificar que las transferencias se realizan a un pais adecuado y. de no ser así, comprobar que se dispone de la autorización del Director de la Agencia Española de Protección de Datos para la misma o que se puede invocar alguna excepción a la regla de la adecuación.

- Definir procedimientos de notificación o autorización a la A EPD de las nuevas transferencias que se vayan a realizar. Establecer la debida conexión con los procedimientos de notificación antes señalados.

- Comprobar que se informa adecuadamente a los interesados cuando sus datos van a ser transferidas a un tercer país que carece de la protección adecuada.

11.3.9 Medidas de seguridad

- Catalogar todos los sistemas de información y aplicaciones que tratan datos personales para incluirlos en el documento de seguridad, definir el nivel de seguridad aplicable a cada uno y precisar las medidas de seguridad que se implantarán.

- Establecer los mecanismos y procedimientos de actualización del documento de seguridad si se producen cambios organizativas. tecnológicos o legales.

- Delimitar y difundir las obligaciones y responsabilidades del personal en materia de seguridad.

- Instaurar procedimientos seguros de asignación y distribución de códigos de usuario, contraseñas o certificados digitales e instalar las herramientas necesarias de identificación y autenticación de usuarios.

- Instalar y mantener actualizadas herramientas de control de acceso a las recursos.

- Definir procedimientos para la notificación y gestión de incidencias, incluyendo información sobre procesos de recuperación realizados y autorización escrita de los mismos cuando sea necesario.

- Revisar las incidencias notificadas pan detectar posibles vulnerabilidades de los sistemas de información.

- Establecimiento de procedimientos de pruebas sin la utilización de datos reales. En el caso de que sea imprescindible utilizar datos reales. extender al entorno de pruebas las mismas medidas de seguridad que en el entorno de producción.

- Implantar procedimientos de identificación, almacenamiento, acceso y gestión de soportes de información, incluyendo la gestión y registro de entrada y salida de los mismos y medidas para su desecho cuando se trate de sistemas afectados por los niveles medio y alto.

- Diseñar procedimientos de salvaguardia y recuperación de la información.

- Para los sistemas de información de nivel alto, instalar herramientas de cifrado para la distribución de soportes y la transmisión de datos a través de redes de telecomunicaciones e implantar mecanismos de registro de los accesos a la información.

- Realizar una auditoría de revisión de los sistemas de seguridad al menos bienalmente.

- Nombrar un responsable de seguridad encargado de supervisar la implantación y funcionamiento de las medidas de seguridad y, en particular, revisar las notificaciones de incidencias, los registros de accesos y los informes de auditoría para que proponga las medidas correctoras que estime oportunas.

11.3.10 Comunicaciones comerciales no solicitadas (spam)

- Definir las medidas y los procedimientos adecuados para no remitir comunicaciones comerciales no solicitadas por correo electrónico u otro medios telemáticos a aquellas personas que no nos han otorgado su

consentimiento o, en el caso de mantener una relación contractual con la organización, se han opuesto a ello.

- Definir procedimientos de gestión y control del consentimiento y de la revocación del mismo.

- Establecer mecanismos para identificar claramente con la palabra "Publicidad" todas los mensajes comerciales o promocionales.

- Permitir, en la medida de lo posible. que tanto el consentimiento como la revocación del mismo puedan realizarse on-line, tras la conecta identificación de la persona y siempre de modo gratuito.

- En cada caso en el que los datos recogidos puedan ser utilizados para la remisión de mensajes comerciales no solicitados, procurar al usuario la posibilidad de aceptar su envio, siendo aconsejable que la opción por defecto sea la no remisión de los mismos.

11.4 CONCLUSIONES

La utilización de Internet por parte de las distintas organizaciones, públicas y privadas, crece cada dia. Este crecimiento se produce de forma tanto cuantitativa como cualitativa pero es este último aspecto. el ofrecimiento de servicios cada vez más sofisticados a través de la Red, lo que implica un mayor riesgo.

En efecto, hace tan sólo unos pocos años. Internet se utilizaba fundamentalmente para dar información estática que se actualizaba con cierta periodicidad. Hoy en dia hay muchas organizaciones que tiene el corazón de su negocio en los servicios que prestan a través de Internet y ello supone, en la mayor parte de los casos, la recogida y tratamiento de datos personales.

Este tratamiento de datos de carácter personal supone no sólo una gran oportunidad de negocio o la posibilidad de prestar cada vez mejores y más personalizados servicios a las ciudadanos por parte de las A A.PP. sino también un riesgo importante, tanto en términos de pérdida de imagen, credibilidad y confianza como. en el caso de empresas privadas, económico, ya que las sanciones previstas en la legislación de protección de datos española son elevadas.

Por todo ello, es necesario que las distintas organizaciones sean conscientes del marco legal en el que han de desenvolverse sus operaciones de tratamiento de datos personales y adoptar las medidas necesarias para adaptarse a él. En muchos casos, estas medidas entrañan más un rediseño de procesos y la adopción de una serie de medidas organizativas que imbuyan a la organización de una "cultura de protección de datos" en todos los ámbitos de la misma que grandes inversiones tecnológicas (aunque en algunos casos estas también pueden ser necesarias).

Este trabajo ha pretendido presentar los aspectos que cualquier organización debería de tener cn cuenta a la hora de abordar su presencia en Internet de una forma respetuosa con el derecho fundamental a la protección de datas de los ciudadanos desde una perspectiva eminentemente práctica• procurando poner de manifiesto los problemas que se presentan o las decisiones que hay que tomar en la

realidad, en el día a día de una compañía u organismo público, teniendo siempre en cuenta las orientaciones dadas por las autoridades de protección de data europeas que son el marco comúnmente aceptado a la hora de implantar políticas adecuadas y eficaces en esta materia.

11.5 LECTURAS RECOMENDADAS

Smith, Gordon E. *Network Auditing: A Control Assesment Approoch.* John Wiley & Sons, 1999.

Lam, Kevin; LeBlane, David y Smith, Ben. *Assessing Network Secttrin:* (Pro-One-Offs). Microsoft Press. 2004.

Musaj, Yusufali F. *Neroark consultants handbook: a compete resource for assessing. auditing. analy ring. and evaluating any nenvork environment.* John Wiley & Sons, 2002.

Guerrero Picó, María del Carmen. *El Impacto de Internet en el Derecho Fundamental ala Protección de Datos de carácter PersonaL* Civitas, 2007.

Corripio Ginkigado. Maria de los Reyes. *Regulación jurídico de los tratamientos de datos personales realizados por el sector privado en Internet.* Agencia de Protección de Datos. 2000.

Fernández Esteban, Maria Luisa. *Nuevas tecnologías. Internet y derechos fundamentales.* McGraw-Hill, 1998.

Aparicio Salom, Javier. Estudio *sobre la Ley Orgánica de Protección de Datos de Carácter Personal.* Aranzadi, 2000.

Vizcaíno Calderón. Miguel. *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal.* Civitas, 2001.

Del Peso Navarro. Emilio. *Ley de protección de datos. La nueva LORTAD.* Diaz de Santos S.A. 2000.

Estadella Yuste, Olga. La protección de la intimidad frente a la transmisión internacional de datos personales. Tatos. 1995.

11.6 CUESTIONES DE REPASO

1. ¿Cuáles son las normas esenciales en materia de protección de datos cn España y la Unión Europea?
2. Enumerar y definir los principios esenciales de la protección de datos personales.
3. ¿Qué aspectos se deberían tener en cuenta cuando se contrata a un encargado para la realización de tratamientos de datos personales de los que nuestra organización es responsable?
4. Enumerar las excepciones a la notificación de datos personales a la autoridad de control competente que establece la legislación española.
5. ¿Qué elementos introducirla en un procedimiento que regulara la obtención y gestión del consentimiento a través de Internet en su organización?

6. Establezca un plan de actuación para garantizar que en todos los lugares del sitio web de su organización en que sea necesario se da la información adecuada y coherente sobre cl tratamiento de datos personales. Confeccione con carácter previo una política de privacidad clara. transparente y completa.
7. ¿Cómo cumplida con el deber de información previo al almacenamiento de una cookie en el ordenador de un usuario que se conecta a su sitio web?
8. Establezca una política de conservación de datos aplicable a su organización.
9. Prepare un plan de formación y educación sobre sus responsabilidades en materia de protección de datos dirigidas a los técnicos de sistemas y bases de datos de su organización. Incluya un documento con el compromiso de confidencialidad que los mismos deberán firmar.
10. ¿En qué condiciones podría su organización enviar comunicaciones comerciales no solicitadas a sus clientes?