CAPÍTULO 3

METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORÍA INFORMÁTICA

José María González Zubieta

3.1. INTRODUCCIÓN A LAS METODOLOGÍAS

Según el *Diccionario de la Lengua de la Real Academia Española,* MÉTODO es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra METODOLOGÍA como "conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal". 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, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, y cómo 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".

Asimismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales, desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo heterogéneos.

La proliferación de metodologías en el mundo de la auditoría y el control informáticos se pueden observar en los primeros años de la década de los ochenta, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos). Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de metodologías constituye una practica habitual. Una de ellas es la seguridad de los sistemas de información.

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada está más lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

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

Si definimos la "SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN" como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las 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 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 poder identificar así sus puntos débiles y 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 contramedida nace de la composición de varios factores expresados en el "gráfico valor" de la figura 3.1.

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

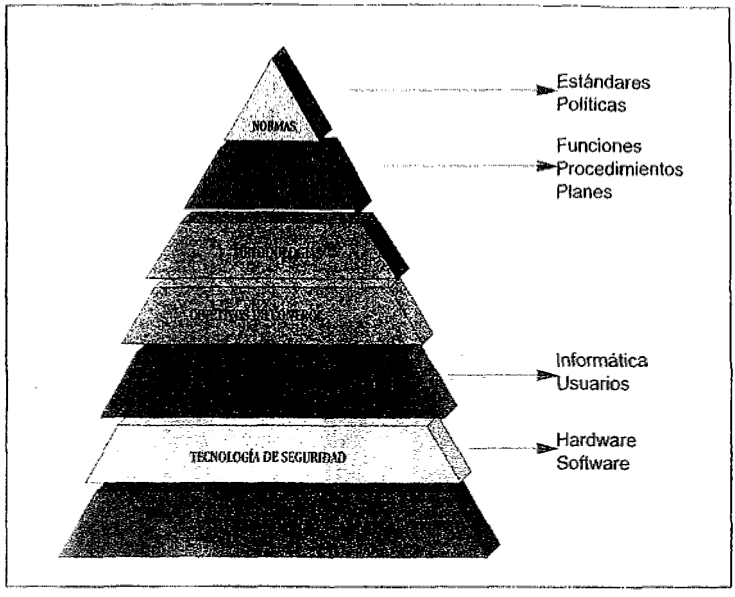

Figura 3.1. Factores que componen una contramedida

- **LA NORMATIVA** debe definir de forma clara y precisa todo lo que debe existir y ser cumplido, 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 sea el único control de un riesgo, pero no es frecuente.

- **LA ORGANIZACIÓN** la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Éste 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, ya que son estas las que realizan los procedimientos y desarrollan los Planes (Plan de Seguridad, Plan de contingencias, auditorías, etc.).

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

- **LOS OBJETIVOS DE CONTROL** son los objetivos a cumplir en el control de 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** son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos 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 **TECNOLOGÍA DE SEGURIDAD** están todos los elementos, ya sean **hardware** o **software,** que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifradores, autentificadores, equipos "tolerantes 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, así como la calidad de cada uno 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 productos que lleven a un sistema de información y sus centros de proceso de una situación inicial determinada (y a mejorar) a una situación mejorada.

En la figura 3.2 se expone la tendencia actual en la organización de la seguridad de sistemas en la empresa. Por una parte un comité que estaría formado por 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 día a día. La función de auditoría 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, con 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.

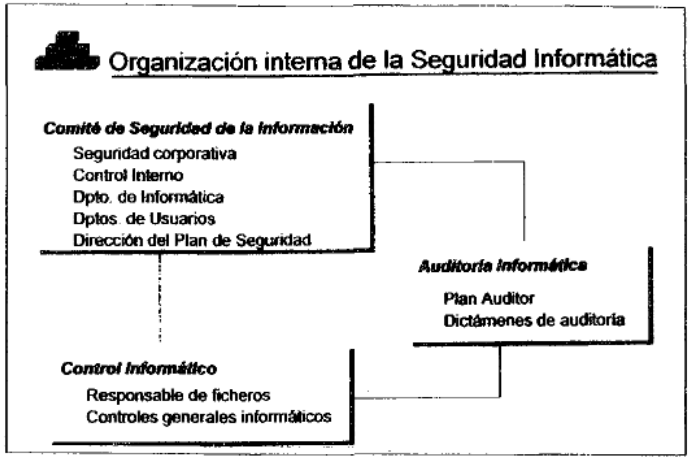

Figura 3.2. Organización interna de la seguridad informática

Queda, pues, por 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.

3.2. METODOLOGÍAS DE EVALUACIÓN DE SISTEMAS

3.2.1. Conceptos fundamentales

En el mundo de la seguridad de sistemas se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría 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 auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras 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(s) 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. Ejemplos: falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de soportes 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 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 difíciles de predecir. Ejemplo: por varias causas se rompen las dos entradas de agua, inundan las líneas telefónicas (pues existe un poro en el cable), hay un cortocircuito y se quema el transformador de la central local. En estos casos la probabilidad resultante es muy difícil de calcular.

Las metodologías de análisis de riesgos se utilizan desde los años setenta, en la industria del seguro basándose en grandes volúmenes de datos estadísticos agrupados en tablas actuarias. Se emplearon en la informática en los ochenta, 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, el hecho de 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).
- TRANSFERIRLOS (por ejemplo: uso de un centro de cálculo contratado).
- REDUCIRLOS (por ejemplo: sistema de detección y extinción de incendios).
- ASUMIRLOS. Que es lo que se hace si no se controla el riesgo en absoluto.

Para los tres primeros, se actúa si se establecen controles o contramedidas. 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.

3.2.2. Tipos de metodologías

Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informáticos, se pueden agrupar en dos grandes familias. Éstas 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, para seleccionar en base a la experiencia acumulada.

3.2.2.1. 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 que se debe 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 a elegir el método entre varias contramedidas podríamos aceptarlo.

Hay varios coeficientes que conviene definir:

- A.L.E. *(Annualized Loss Expentacy):* multiplicar la pérdida máxima posible de cada bien/recurso por la amenaza con probabilidad más alta.
- Reducción del A.L.E. *(Annualized Loss Expectancy):* Es el cociente entre el *coste anualizado* de la instalación y el mantenimiento de la medida contra el valor total del bien/recurso que se está protegiendo, en tanto por ciento.
- Retorno de la inversión (R.O.I.): A.L.E. original menos A.L.E. 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.

Por tanto, vemos con claridad dos grandes inconvenientes que presentan estas metodologías: por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otra 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.

3.2.2.2. Metodologías cualitativas/subjetivas

Basadas en métodos estadísticos y lógica borrosa (humana, no matemática, *fuzzy logic*). Precisan de la *involucración* de un profesional experimentado. Pero requieren menos recursos humanos/tiempo que las metodologías cuantitativas.

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

	Cuantitativa	Cualitativa / Subjetiva
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 depende de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodologías estándares. Difíciles de mantener o modificar Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Puede 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 3.3. Comparación entre metodologías cuantitativas y cualitativas

3.2.3. Metodologías más comunes

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

3.2.3.1. Metodologías de 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, de las que existen gran cantidad de ambas clases y sólo citaremos algunas de ellas.

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

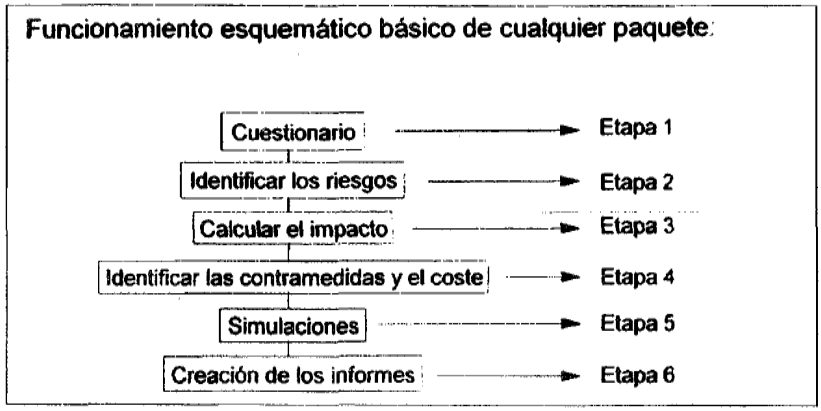

Figura 3.4. Esquema básico de una metodología de análisis de riesgos

En base a unos cuestionarios se identifican vulnerabilidades y riesgos y 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 distintas 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 un gran componente subjetivo.
- Y además se diferencian en el propio sistema de simulación.

En el INFOSEC'92 proyecto S2014 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: ANALIZY, 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. Citaremos algunas a modo de ejemplo:

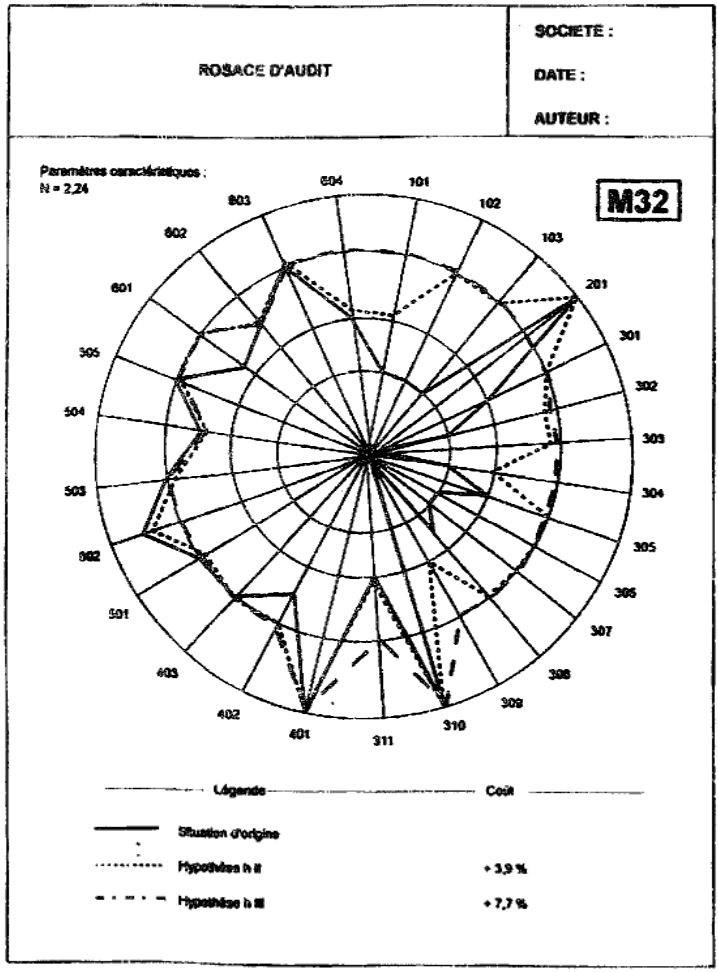

Figura 3.5. Diagrama de vulnerabilidad

CHAPITRE: Appréciation générale de la securité		Nº 1	Ponderation: 95		Page:
FACTEUR DE SECURITE: Organisation générale		Nº 01	Ponderation: 95		Page:
QUESTION	LIBELLE		NOTE	PONDE-RATION	RESPONSE PONDEREE
01	Existe-t-il un organigramme hiérachique de l'intreprise remis à jour périodiquement (au moins une fois par an)?			0,5	
02	Existe-t-il un organigramme fonctionnel de l'entreprise remis à jour périodiquement (au moins une fois par an)?			0,5	
03	Y e-t-il une réunion de Direction Générale de présentation de l'organigramme à laquelle participent tous les responsables de fonction?			0,5	
04	Existe-t-il une définition de fonction et partege des responsabilités pour chaque poste fiurant sur l'organigramme?			1	
05	La Direction Générale manifeste-t-elle son interét par des réunions specifiques de sécurité (hors CHSCT) au moins une fois par an?			1,5	
06	Existe-t-il un comité permanent chargé d'étudier tous les problèmes liés à la sécurité, composé de représentants de la D G , direction informatique et organisation, fonctions utilisateurs, audit interne, gstion de risques juridique et assurances, se réunissant au moins quatre fois par an?			3	
07	Le comple rendu de ces réunions est-il consigné dans un rapport précédemment cité?			1	
08	Y a-t-il un suivi et un contrôle des recommendations prescrites par le rapport précédemment cité?			1	
09	Y a-t-il eu une étude sur la vulnerabilité de l'entreprise face à différérents types de risques physiques ou non physiques (pas nécessairement informatiques) dans les trois derniéres annés (rapport écrit)?			3	
10	Cette étude a-t-elle entraine la mise en place d'un plan de sauvegarde de l'entreprise?			3	
11	Existe-t-il un responsable de la sécurité générale (bâtiments, environment, accés)?			2	
12	La sécurité informatique dispose-t-elle d'un poste spécifique sur l'organigramme avec un rattachement hiérchique élevé assorti d'une délinition de fonction précisant clairment les responsabilités et d'un bugget spécifique?			3,5	
13	Y a-t-il ou responsable "Assurances" dans l'entreprise?			0,5	
14	Le choix des garanties en melière informatique est-il le résultat d'une étude spécifique?			0,5	

Figura 3.6. Cuestionario para valorar la seguridad

MARION

Método documentado en dos libros de los cuales el más actual es *La Securité des reseaux-Methodes et Techniques* de J.M. Lamere y Leroux, J. Tourly. Tiene dos productos: MARION AP+, para sistemas individuales, y MARION RSX para sistemas distribuidos y conectividad.

Es un método cuantitativo y se basa en la encuesta anual de miembros del C.L.U.S.I.F. (base de incidentes francesa). No contempla probabilidades, sino esperanzas matemáticas que son aproximaciones numéricas (valores subjetivos).

La MARION AP+ utiliza cuestionarios y parámetros correlacionados enfocados a la representación gráfica de las distintas soluciones de contramedidas (figura 3.5), en cada uno de los factores (27 factores en seis categorías). Las categorías son: seguridad informática general, factores socioeconómicos, concienciación sobre la seguridad de software y materiales, seguridad en explotación y seguridad de desarrollo.

Secteur	Catégorie	
I	– Etablissements financiers.	2,20
	– Banques.	2,61
	– Assurances.	2,04
	– Agriculture.	1,24
	– Energie, extraction.	2,53
	– Métalurgie, sidérurgie.	2,00
	– Construction aéronautique, automobile, mécanique, électrique.	2,00
	– Electronique, optique, informatique.	2,35
II	– Verre, céramique.	1,82
	– Chimie, pharmacie.	2,28
	– Pétrole et dérivés.	2,61
	– Agro-alimentaire.	1,95
	– Textile, habillement	2,08
	– Indutries diverses.	2,28
	– Bâtiment, TP.	1,82
	– Transport.	1,78
	– Transmissions, télécommunications.	2,21
	– Distribution, commerce.	2,10
	– Hôtellerie.	2,41
	– Sociétés de services.	2,28
III	– Administration	2,14
	– Santé.	2,29
	– Enseignement.	1,35
	– Publicité, presse, éditions.	2,06
	– Divers.	1,63

DEFINICIÓN SECTORIAL I, II, III USADO.

Figura 3.7. Valores de ponderación para diferentes sectores

En la figura 3.6 se puede ver un cuestionario al que hay que responder sí con un 4, no con un cero, y 3 *no aplicable,* para luego aplicarles unos valores de ponderación según los sectores de la figura 3.7 de negocio de la empresa donde se esté pasando la metodología. El cuestionario de la figura 3.6 correspondería al factor 101.

El análisis de riesgos lo hace sobre diez áreas problemáticas con otros cuestionarios. Estas áreas son riesgos materiales, sabotajes físicos, averías, comunicaciones, errores de desarrollo, errores de explotación, fraude, robo de información, robo de software, problemas de personal. Sirve para evaluar el impacto (figura 3.8).

Groupe d'interview:	Fonction:	Auteur:
Participants:	Sous-Fontions:	Date:
Binôme d'interview:	Application:	

M11-U2

Type de Pertes / Type de Risques	Dommages matériels	Frais Suppl.	Pertes d'expl.	Pertes de biens	Pertes de fonds	Autres Pertes
1. Risques matériels						
2. Sabotage physique						
3. Pannes						
4. Erreurs (saisie, transmission)						
5. Erreurs (conception, realisation)						
6. Erreurs (exploitation)						
7. Fraude, détournement, sabotage inmatériel						
8. Détournement d'information						
9. Détournement de logiciel						
10. Problémes humains						

DEFINICIÓN CUALITATIVA DE PÉRDIDAS (MARIOM AP+)

Figura 3.8. Definición cualitativa de pérdidas

Las pérdidas posibles no deben sobrepasar nunca el valor del "RIESGO MÁXIMO ADMISIBLE", valor extraído de los valores dados por un estudio del Banco de Francia donde figuran 50 ratios para distintas áreas sectoriales ya mencionadas en la figura 3.7. El diagrama de la figura 3.5 se llama de radar, y la metodología MELISA usa uno similar. Esta metodología es de las más antiguas y difíciles de entender y manejar.

RISCKPAC

Todas las metodologías que se desarrollan en la actualidad están pensadas para su aplicación en herramientas. La primera de esta familia la desarrolló PROFILE ANALYSIS CORPORATION, y la primera instalación en cliente data de 1984. Según DATAPRO es el software más vendido.

Su enfoque es metodología cualitativa/subjetiva. Sus resultados son exportables a procesadores de texto, bases de datos, hoja electrónica o sistemas gráficos. Está estructurada en los tres niveles Entorno/Procesador/Aplicaciones con 26 categorías de riesgo en cada nivel. Tiene un "¿qué pasa si...?" con un nivel de riesgo de evaluación subjetiva del 1 al 5 y ofrece una lista de contramedidas o recomendaciones básicas para ayuda al informe final o plan de acciones.

CRAMM

Se desarrolló entre 1985 y 1987 por BIS y CCTA (CENTRAL COMPUTER & TELECOMUNICATION AGENCY RISK ANALISIS & MANAGEMENT METHOD, Inglaterra). Implantado en más de 750 organizaciones en Europa, sobre todo de la administración pública. Es una metodología cualitativa y pennite hacer análisis "¿Qué pasa si...?".

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" (figura 3.10) 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, y capacidad de aprendizaje al poseer una base de conocimiento o registro de incidentes que van variando las esperanzas matemáticas de partida y adaptándose a los entornos de trabajo.

En las figuras 3.9 y 3.10 se expone la metodología de análisis de riesgos PRIMA.

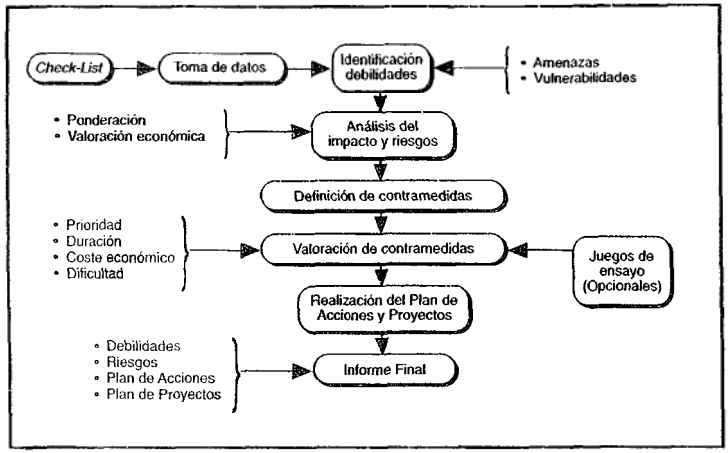

Figura 3.9. Fases de la metodología PRIMA

Con la misma filosofía abierta existen del mismo autor, en la actualidad, las siguientes metodologías:

- Análisis de riesgos.
- Plan de contingencias informática y de recuperación del negocio.
- Plan de restauración interno informático.
- Clasificación de la información.
- Definición y desarrollo de procedimientos de control informáticos.
- Plan de cifrado.
- Auditoría informática.
- Definición y desarrollo de control de acceso lógico. Entornos distribuidos y single *sig-on.*

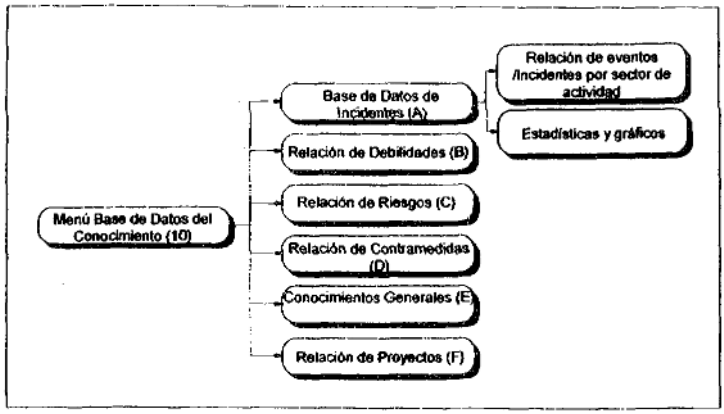

Figura 3.10. Lista de ayuda de la metodología PRIMA

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

También se manejan a veces los conceptos de plan de contingencias informática 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 informativo como un departamento más. Frecuentemente se realiza el informático.

DEFINICIÓN. 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 lo que da lugar a las metodologías. Esto es, 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, 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 I. ANÁLISIS Y DISEÑO. Se estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el coste/beneficio de las mismas. Ésta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión de que no es viable o es muy costoso su seguimiento. En la forma de desarrollar esta fase, se diferencian las dos familias metodológicas. Éstas son las de "RISK ANALISIS" y las de "BUSINESS IMPACT".

Las de Risk Analisis se basan en el estudio de los posibles riesgos desde el punto de vista de probabilidad de que los mismos sucedan. Aunque los registros de incidentes, al igual que ocurría 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 de Bussines Impact, se basan en el estudio del impacto (pérdida económica o de imagen) que ocasiona la falta 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 de esta fase en las metodologías de Risk Analisis 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 las estrategias de respaldo.

Las tareas para las de Business Impact 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 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. Éstas 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 Frame* o tiempo que la empresa puede asumir con paralización de la actividad operativo 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 normalidad, dado que pasar de la situación normal a la *alternativa* debe concluirse con la reconstrucción de la situación inicial antes de la contingencia, y esto es lo que no todas las metodologías incluyen.

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

Asimismo 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 para

desarrollar más tarde la herramienta que se necesite. El esquema de una herramienta debe tener al menos los siguientes puntos:

- base de datos relacionar
- módulo de entrada de datos
- módulo de consultas
- proceso de textos
- generador de informes
- ayudas *on-line*
- hoja de cálculo
- gestor de proyectos
- generador de gráficos

Existen en el mercado productos que cubren estas metodologías, en menor cantidad que los de análisis de riesgos y enfocados sobre todo a análisis de riesgos con datos de poca significación científica. Hoy en día la mayoría de los equipos profesionales desarrollan su software al comienzo de los trabajos tras definir la metodología.

Es importante para terminar este punto decir que una práctica habitual es realizar la fase I y contratar un servicio de *back-up* sin desarrollar las fases II y III. Esto no sólo constituye un error conceptual, sino que en realidad sólo se tiene un estudio y un contrato de servicios pero no un PLAN DE CONTINGENCIAS.

3.3. LAS METODOLOGÍAS DE AUDITORÍA INFORMÁTICA

Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorías de CONTROLES GENERALES como producto estándar de la auditores profesionales, que son una homologación de las mismas a nivel internacional, y las METODOLOGÍAS de los auditores internos.

El objetivo de las auditorías de controles generales es "dar una opinión sobre la fiabilidad de los datos del computador para la auditoría financiera". El resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestionarios estándares que dan como resultado informes muy generalistas.

Tienen apartados para definir "pruebas" y anotar sus resultados. Ésta es una característica clara de la diferencia con las metodologías de evaluación de la consultaría como las de análisis de riesgos *que no tienen estos apartados,* aunque también tratan de identificar vulnerabilidades o falta de controles. Esto es, la realización de pruebas es consustancial a la auditoría, dado que tanto el trabajo de consultaría como el análisis de riesgos espera siempre la colaboración del analizado, y

por el contrario la auditoría debe demostrar con pruebas todas sus afirmaciones, y por ello siempre debe contener el apartado de las pruebas. Llegando al extremo de que hay auditorías que se basan sólo en pruebas como la "auditoría de integridad".

Estas metodologías están muy desprestigiadas, pero no porque sean malas en sí 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 estas metodologías usa 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 que le permita empezar su trabajo rápidamente. Esto es una utopía. El auditor informático necesita 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 ésta 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 se trata de 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 3.7 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. Asimismo lo 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. Asimismo, 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. Éstos, aunque deben planificar

sus tiempos, en principio no deben constituir nunca su factor principal, dado que su función es la de vigilancia, y ésta se cumple si el auditado se siente vigilado.

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

También es interesante aclarar que hay herramientas software de ayuda a la auditoría de cuentas que aunque se les llame herramientas de auditoría, sólo lo son para los auditores de cuentas, y esto no es auditoría informática sino ayuda a la auditoría de cuentas.

Es decir, que no es lo mismo ser una informática de los auditores que ser auditor informático. La auditoría financiera es *un dictamen sobre los estados de cuentas.* Y la auditoría informática es una auditoría en sí misma, y si el auditor informático no certifica la integridad de los datos informáticos que usan los auditores financieros, éstos no deben usar los sistemas de información para sus dictámenes. Tal es la importancia de la existencia de los auditores informáticos, que son los garantes de la veracidad de los informes de los auditores financieros que trabajan con los datos de los sistemas de información.

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

3.4. 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 las siguientes:

- **Funciones.** Ubicación de la figura en el organigrama de la empresa. Debe existir una clara segregación de funciones con la Informática y de control interno informático, y éste debe ser auditado también. Deben describirse las funciones de forma precisa, y la organización interna del departamento, con todos sus recursos.

- **Procedimientos** para las distintas tareas de las auditorías. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

- **Tipos de auditorías** que realiza. Metodologías y cuestionarios de las mismas. Ejemplo: revisión de la aplicación de facturación, revisión de la LOPD, revisión de seguridad física, revisión de control interno, etc. Existen tres tipos de auditorías según su alcance: la Full o completa de una área (por ejemplo: control interno, informática, limitada a un aspecto; por ejemplo: una aplicación, la seguridad lógica, el software de base, etc.), la Corrective Action Review (CAR) que es la comprobación de acciones correctivas de auditorías 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., así como realizar una evaluación global de resumen para toda la auditoría. En nuestro país esta evaluación 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 auditoría en cuestión.

CICLO DE AUDITORÍAS

Nivel Exposición	Evaluación	Frecuencia Visitas
10 - 9	"B"	18 meses
	"R"	9 meses
	"M"	6 meses
8 - 7	"B"	18 meses
	"R"	12 meses
	"M"	9 meses
6 - 5	"B"	24 meses
	"R"	18 meses
	"M"	12 meses
4 - 1	"B"	36 meses
	"R"	24 meses
	"M"	18 meses

Figura 3.11. Nivel de exposición para definir la frecuencia de la auditoría

- **Nivel de exposición.** Como ejemplo podemos ver la figura 3.11. 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 la última auditoría realizada sobre ese tema definir la fecha de la repetición de la misma auditoría. 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 repartiese en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas, deberá 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 nos dé un resultado de horas de trabajo previstas y, por tanto, de 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 cubrir fácilmente 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 de las que existen en la actualidad.

Las metodologías de auditoría 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 así esta función se consolidará en las entidades, esto es, por el "respeto profesional" a los que ejercen la función.

3.5. CONTROL INTERNO INFORMÁTICO. SUS MÉTODOS Y PROCEDIMIENTOS. LAS HERRAMIENTAS DE CONTROL

3.5.1 La función de control

Hoy en día la tendencia generalizada es contemplar, al lado de la figura del auditor informático, la de control interno informático. Tal es el caso de la organización internacional I.S.A.C.A. (Information Systems Audit and Control Association) que con anterioridad se llamó The EDP Auditors Association Inc.

Aunque hay una cierta polémica profesional con esta función y no existe una aceptación tan clara como la función de auditoría informática, parece razonable y sin intención de crear doctrina definirla como existe en general en muchas multinacionales.

La función de Control Informático Independiente debería ser en primer lugar independiente del departamento controlado. Ya que "por segregación de funciones la informática no debería controlarse a sí misma". Partiendo de la base de un concepto en el que la seguridad de sistemas abarca un campo mucho mayor de lo que es la seguridad lógica, podríamos decir que:

- El área informática monta los procesos informáticos seguros.
- El Control interno monta los controles.
- La Auditoría Informática evalúa el grado de control.

Por tanto, podríamos decir que existen claras diferencias entre las funciones de control informático y las de auditoría informática.

La Auditoría Informática

- Tiene la función de vigilancia y evaluación mediante dictámenes, y todas sus metodologías van encaminadas a esta función.
- Tiene sus propios objetivos distintos a los auditores de cuentas, aunque necesarios para que éstos puedan utilizar la información de sus sistemas para sus evaluaciones financieras y operativas. Evalúan eficiencia, costo y seguridad en su más amplia visión, esto es todos los riesgos informativos, ya sean los clásicos (confidencialidad, integridad y disponibilidad), o los costos y los jurídicos, dado que ya no hay una clara separación en la mayoría de los casos.
- Operan según el plan auditor.
- Utilizan metodologías de evaluación del tipo cualitativo con la característica de las pruebas de auditoría.
- Establecen planes quinquenales como ciclos completos.
- Sistemas de evaluación de repetición de la auditoría por nivel de exposición del área auditada y el resultado de la última auditoría de esta área.
- La función de soporte informático de todos los auditores (opcionalmente), aunque dejando claro que no se debe pensar con esto que la auditoría informática consiste en esto solamente.

Control Interno Informático

- Tiene funciones propias (administración de la seguridad lógica, etc.).
- Funciones de control dual con otros departamentos.
- Función normativa y del cumplimiento del marco jurídico.

- Operan según procedimientos de control en los que se ven involucrados y que luego se desarrollarán.
- Al igual que en la auditoría y de forma opcional pueden ser el soporte informático de control interno no informático.

Podemos pasar ya a proponer las funciones de control interno más comunes:

- Definición de propietarios y perfiles según "Clasificación de la Información" (utilizando metodología).
- Administración delegada en Control Dual (dos personas intervienen en una acción como medida de control) de la seguridad lógica.
- Responsable del desarrollo y actualización del Plan de Contingencias, Manuales de procedimientos y Plan de Seguridad.
- Promover el Plan de Seguridad Informática al Comité de Seguridad.
- Dictar Normas de Seguridad Informática.
- Definir los Procedimientos de Control.
- Control del Entorno de Desarrollo.
- Control de Soportes Magnéticos según la Clasificación de la Información. Control de Soportes Físicos (listados, etc.).
- Control de Información Comprometida o Sensible.
- Control de Microinformática y Usuarios.
- Control de Calidad de Software.
- Control de Calidad del Servicio Informático.
- Control de Costes.
- Responsable del Departamento (gestión de recursos humanos y técnicos). Control de Licencias y Relaciones Contractuales con terceros.
- Control y Manejo de Claves de cifrado.
- Relaciones externas con entidades relacionadas con la Seguridad de la Información.
- Definición de Requerimientos de Seguridad en Proyectos Nuevos.
- Vigilancia del Cumplimiento de las Normas y Controles.
- Control de Cambios y Versiones.
- Control de Paso de Aplicaciones a Explotación.
- Control de Medidas de Seguridad Física o corporativa en la Informática.
- Responsable de Datos Personales (LOPD y Código Penal).
- Otros controles que se le designen.
- Otras funciones que se le designen.

Todas estas funciones son un poco ambiciosas para desarrollarlas desde el instante inicial de la implantación de esta figura, pero no debemos perder el objetivo de que el control informático es el componente de la "actuación segura" entre los usuarios, la informática y control interno, todos ellos auditados por auditoría informática.

Para obtener el entramado de contramedidas o controles compuesto por los factores que veíamos en la figura 3.1, deberemos ir abordando proyectos usando distintas metodologías, tal como se observa en la figura 3.12, que irán conformando y mejorando el número de controles.

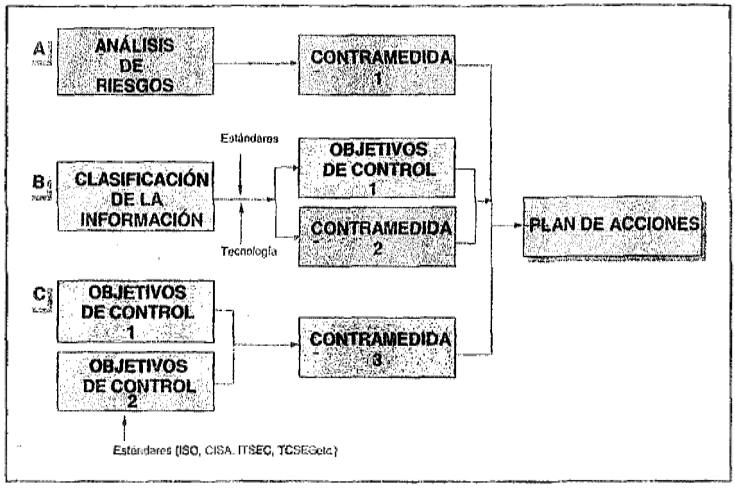

Figura 3.12. Obtención de los controles

Este plan de proyectos lo llamaremos "Plan de Seguridad Informática". Dos de estos proyectos de vital importancia son la "Clasificación de la Información" y los "Procedimientos de Control". El punto B) de la figura corresponde al primero y el C) al segundo, y sus metodologías se ven a continuación.

3.5.2. Metodologías de clasificación de la información y de obtención de los procedimientos de control

Clasificación de la información

No es frecuente encontrar metodologías de este tipo, pero la metodología PRIMA tiene dos módulos que desarrollan estos dos aspectos y que vemos a continuación.

Contemplando la figura 3.12 podríamos preguntarnos si es suficiente con un análisis de riesgos para obtener un plan de contramedidas que nos llevará a una situación de control como se desea. La respuesta es no, dado que todas las entidades de información a proteger no tienen el mismo grado de importancia, y el análisis de riesgos metodológicamente no permite aplicar una diferenciación de contramedidas según el activo o recurso que protege, sino por la probabilidad del riesgo analizado.

Tiene que ser otro concepto, como el que se baraja en la clasificación de la información. Esto es "SI IDENTIFICAMOS DISTINTOS NIVELES DE CONTRAMEDIDAS PARA DISTINTAS ENTIDADES DE INFORMACIÓN CON DISTINTO NIVEL DE CRITICIDAD, ESTAREMOS OPTIMIZANDO LA EFICIENCIA DE LAS CONTRAMEDIDAS Y REDUCIENDO LOS COSTOS DE LAS MISMAS".

Por ejemplo, si en vez de cifrar la red de comunicaciones por igual somos capaces de diferenciar por qué líneas va la información que clasificamos como Restringida a los propietarios de la misma, podremos cifrar solamente estas líneas para protegerla sin necesidad de hacerlo para todas, y de esa manera disminuiremos el costo de la contramedida "cifrado".

Tradicionalmente el concepto de información clasificada se aplicó a los documentos de papel, aunque los criterios y jerarquías nunca han sido más de dos (secreto y no). Con la tecnología de la información, el concepto ha cambiado, e incluso se ha perdido el control en entornos sensibles. Nace pues el concepto de ENTIDAD DE INFORMACIÓN como el objetivo a proteger en el entorno informático, y que la clasificación de la información nos ayudará a proteger especializando las contramedidas según el nivel de confidencialidad o importancia que tengan.

Esta metodología es del tipo cualitativo/subjetivo, y como el resto de la metodología PRIMA tiene listas de ayuda con el concepto abierto, esto es, que el profesional puede añadir en la herramienta niveles o jerarquías, estándares y objetivos a cumplir por nivel, y ayudas de contramedidas.

Ejemplos de Entidades de Información son: una pantalla, un listado, un archivo de datos, un archivo en un "streamer", una microficha de saldos, los sueldos de los directivos, los datos de tipo "salud" en un archivo de personal, una transación, un JCL, un editor, etc.

O sea los factores a considerar son los requerimientos legislativos, la sensibilidad a la divulgación (confidencialidad), a la modificación (integridad), y a la destrucción.

Las jerarquías suelen ser cuatro, y según se trate de óptica de preservación o de protección, los cuatro grupos serían: Vital-Crítica-Valuada-No sensible o bien Altamente confidencial-Confidencial-Restringida-No sensible.

PRIMA, aunque permite definirla a voluntad, básicamente define:

- Estratégica (información muy restringida, muy confidencial, vital para la subsistencia de la empresa).

- Restringida (a los propietarios de la información).

- De uso interno (a todos los empleados).
- De uso general (sin restricción).

Los pasos de la metodología son los siguientes:

1. IDENTIFICACIÓN DE LA INFORMACIÓN.

2. INVENTARIO DE ENTIDADES DE INFORMACIÓN RESIDENTES Y OPERATIVAS. Inventario de programas, archivos de datos, estructuras de datos, soportes de información, etc.

3. IDENTIFICACIÓN DE PROPIETARIOS. Son los que necesitan para su trabajo, usan o custodian la información.

4. DEFINICIÓN DE JERARQUÍAS DE INFORMACIÓN. Suelen ser cuatro, porque es difícil distinguir entre más niveles.

5. DEFINICIÓN DE LA MATRIZ DE CLASIFICACIÓN. Esto consiste en definir las políticas, estándares objetivos de control y contramedidas por tipos y jerarquías de información.

6. CONFECCIÓN DE LA MATRIZ DE CLASIFICACIÓN. En la figura 3.13 se observa un ejemplo de matriz de clasificación en la que se relaciona cada entidad de información con los elementos que se correlacionan, como son transacción, archivos, soportes, propietarios, y jerarquía. En esta fase se cumplimenta toda la matriz, asignándole a cada entidad un nivel de jerarquía, lo que la asocia a una serie de hitos a cumplir según el punto anterior, para cuyo cumplimiento deberemos desarrollar acciones concretas en el punto siguiente.

7. REALIZACIÓN DEL PLAN DE ACCIONES. Se confecciona el plan detallado de acciones. Por ejemplo, se reforma una aplicación de nóminas para que un empleado utilice el programa de subidas de salario y su supervisor lo apruebe.

8. IMPLANTACIÓN Y MANTENIMIENTO. Se implanta el plan de acciones y se mantiene actualizado.

Y así se completa esta metodología.

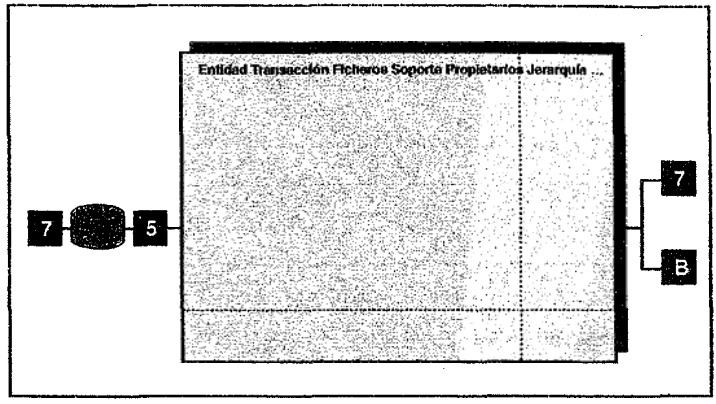

Figura 3.13. Ejemplo de matriz de clasificación

Obtención de los procedimientos de control

Otra metodología necesaria para la obtención de los controles expresados en la figura 3.1, es "la Obtención de los Procedimientos de Control". Es frecuente encontrar manuales de procedimientos en todas las áreas de la empresa que explican las funciones y cómo se realizan las distintas tareas diariamente, siendo éstos necesarios para que los auditores realicen sus revisiones operativas, evaluando si los procedimientos son correctos y están aprobados y sobre todo si se cumplen.

Pero podríamos preguntarnos si desde el punto de vista de control informático es suficiente y cómo se podrían mejorar.

La respuesta nos la da la metodología que se expone a continuación, que nos dará otro plan de acciones que tal como trata de expresar la figura 3.12, contribuirá sumándose a los distintos proyectos de un plan de seguridad para mejorar el entramado de contramedidas.

Metodología

Fase I. Definición de Objetivos de Control.

Se compone de tres tareas.

Tarea 1. Análisis de la empresa. Se estudian los procesos, organigramas y funciones.

Tarea 2. Recopilación de estándares. Se estudian todas las fuentes de información necesarias para conseguir definir en la siguiente fase los objetivos de control a cumplir (por ejemplo, ISO, ITSEC, CISA, etc.).

Tarea.3. Definición de los Objetivos de Control.

Fase II. Definición de los Controles.

Tarea 1. Definición de los Controles. Con los objetivos de control definidos, analizamos los procesos y vamos definiendo los distintos controles que se necesiten.

Tarea 2. Definición de Necesidades Tecnológicas (hardware y herramientas de control).

Tarea 3. Definición de los Procedimientos de Control. Se desarrollan los distintos procedimientos que se generan en las áreas usuarias, informática, control informático y control no informático.

Tarea 4. Definición de las necesidades de recursos humanos.

Fase III. Implantación de los controles.

Una vez definidos los controles, las herramientas de control y los recursos humanos necesarios, no resta más que implantarlos en forma de acciones específicas.

Terminado el proceso de implantación de acciones habrá que documentar los procedimientos nuevos y revisar los afectados de cambio. Los procedimientos resultantes serán:

- Procedimientos propios de control de la actividad informática (control interno informático).
- Procedimientos de distintas áreas usuarias de la informática, mejorados.
- Procedimientos de áreas informáticas, mejorados.
- Procedimientos de control dual entre control interno informática y el área informática, los usuarios informáticos, y el área de control no informático.

3.5.3. Las herramientas de control

Ya hemos hablado de todas las capas de la figura 3.1, excepto del último substrato de la pirámide, esto es, las herramientas de control. En la tecnología de la seguridad informática que se ve envuelta en los controles, existe tecnología hardware (como los cifradores) y software. Las herramientas de control son elementos software que por sus características funcionales permiten vertebrar un control de una manera más actual y más automatizada. Pero no olvidemos que la herramienta en sí misma no es nada. Ya hemos visto en el punto anterior que el control se define en todo un proceso metodológico, y en un punto del mismo se analiza si existe una herramienta que automatice o mejore el control para más tarde definir todo el control con la herramienta incluida, y al final documentar los procedimientos de las distintas áreas involucradas para que éstas; los cumplan y sean auditados. O sea, comprar una herramienta sin más y ver qué podemos hacer con ella es, un error profesional grave, que no conduce a nada, comparable a trabajar sin método e improvisando en cualquier disciplina informática.

Las herramientas de control (software) más comunes son:

- Seguridad lógica del sistema.
- Seguridad lógica complementaria al sistema (desarrollado a medida).
- Seguridad lógica para entornos distribuidos.
- Control de acceso físico. Control de presencia.
- Control de copias.
- Gestión de soportes magnéticos.
- Gestión y control de impresión y envío de listados por red.
- Control de proyectos.
- Control de versiones.
- Control y gestión de incidencias.
- Control de cambios.
- Etc.

Todas estas herramientas están inmersas en controles nacidos de unos objetivos de control y que regularán la actuación de las distintas áreas involucradas. Por ejemplo, si el objetivo de control es "separación de entornos entre desarrollo y producción", habrá un procedimiento en desarrollo de "paso de aplicaciones a explotación" y otro en explotación de "paso a explotación de aplicaciones de desarrollo". Soportado todo por una herramienta de control de acceso lógico que en un proceso de clasificación ha definido distintos perfiles en desarrollo y explotación, y tras implantarlo en la herramienta, impide acceder a uno y a otros al entorno que no es el suyo. Por tanto, para pasar una aplicación de uno a otro cuando está terminada, se necesita un procedimiento en el que intervengan las dos áreas y un control informático que actúa de llave. Esto que parece dificultoso, no lo es en la práctica.

Sólo a modo de ejemplo pongamos los objetivos de control en el acceso lógico al igual que deberíamos ir haciendo en cada una de las herramientas de control antes enumeradas.

Objetivos de control de acceso lógico

- Segregación de funciones entre los usuarios del sistema: productores de software, jefes de proyecto (si existe un proceso metodológico así), técnicos de sistemas, operadores de explotación, operadores de telecomunicaciones, grupos de usuarios de aplicaciones (con perfiles definidos por la Clasificación de la información), administrador de la seguridad lógica (en control dual al ser de alto riesgo), auditoría, y tantos como se designen.

- Integridad de los "log" e imposibilidad de desactivarlos por ningún perfil para poder revisarlos. Fácilmente legibles e interpretables por control informático.

- Gestión centralizada de la seguridad o al menos única (por control informático).

- Contraseña única (a ser posible) para los distintos Sistemas de la red. Y la autentificación de entrada una sola vez. Y una vez dentro, controlar los derechos de uso.

- La contraseña y archivos con perfiles y derechos inaccesibles a todos, incluso a los administradores de seguridad.

- El sistema debe rechazar a los usuarios que no usan la clave o los derechos de uso correctamente, inhabilitando y avisando a control, que tomara las medidas oportunas.

- Separación de entornos. Significa que los distintos usuarios pueden hacer solamente lo qué y cómo se ha autorizado que hagan para su función. Habrá tantos entornos como se precisen y el control tendrá que estar en situación normal como en emergencia y no entorpecer la operatoria.

- El log, o los log's, de actividad no podrán desactivarse a voluntad, y si se duda de su integridad o carencia, resolver con un terminal externo controlado.

- El sistema debe obligar al usuario a cambiar la contraseña, de forma que sólo la conozca él, que es la única garantía de autenticidad de sus actos.

- Es frecuente encontrar mecanismos de *auto-logout,* que expulsan del sistema a la terminal que permanece inactiva más de un tiempo determinado, que son ayudas adicionales a la seguridad.

Muchos de estos objetivos se pueden sacar de los propios estándares (ISO, Libro Naranja, ITSEC, etc.).

Este ejemplo nos puede servir para introducir otra metodología del compendio PRIMA, utilizada para la implantación del control sobre los "Entornos distribuidos", verdadero reto de nuestros días.

Todo estaba controlado en los grandes sistemas en su nivel C2/E2 (no es mucho, pero suficiente para el nivel comercial, según los fabricantes). Y llega la proliferación de los entornos distribuidos... "el caos". ¿Está controlada la seguridad lógica en la actualidad? ¡Cada responsable de seguridad debe planteárselo! ¿Se cumple el marco jurídico sin seguridad lógica?

Se podría implantar el control de acceso lógico, sistema a sistema con los propios software de seguridad de cada uno de ellos, con un enorme esfuerzo de recursos humanos y complicada operativo. Podemos resolver mejor el problema adquiriendo e instalando un software de control de entornos distribuidos. ¿Pero qué hacer... cómo abordar el problema? ¿Ver muchos productos y escoger uno? ¿Será lo mejor para el futuro? ¿Cómo lo están haciendo los demás?

La forma más apropiada de resolver este problema, hasta donde se pueda, es utilizar un método práctico que paso a desarrollar.

ANÁLISIS DE PLATAFORMAS. Se trata de inventariar las múltiples plataformas actuales y futuras (MVS, UNIX, AIX3.2.5., TANDEN GUARDIAN D30, etc. que más tarde nos servirán para saber qué productos del mercado nos pueden ser válidos, tanto los productos actuales como los futuros planes que tengan los fabricantes.

CATÁLOGO DE REQUERIMIENTOS PREVIOS DE IMPLANTACIÓN. Desde el primer momento nace esta herramienta (control del proyecto), que inventaría lo que no se va a conseguir (limitaciones), así como lo necesario para la implantación, inventariado como acciones y proyectos, calendarizados, y su duración para su seguimiento y desarrollo.

ANÁLISIS DE APLICACIONES. Se trata de inventariar las necesidades de desarrollar INTERFACES con los distintos software de seguridad de las aplicaciones y bases de datos. Estos desarrollos deberían entrar en el catálogo de R.P.I. como proyectos a desarrollar. Por ejemplo: DB2, Oracle 7.1.6. SAP R/3.2.2, Checkpoint

Firewall-1, OFFICE 2.6, o la propia de Recursos Humanos, etc. Es importante la conexión a Recursos Humanos para que se detecten automáticamente las alteraciones en los empleados (altas, bajas, cambios). También en este punto conviene ver si el producto/interfaces soporta el tiempo real, o el proceso batch, o sus posibilidades de registros de actividad.

INVENTARIO DE FUNCIONALIDADES Y PROPIETARIOS. En este punto trataremos todo el esquema de funcionalidades de la seguridad lógica actual. Es el momento de crear unas jerarquías de estándares a cumplir (clasificación de la información) y tratar de definir en ese momento los controles que se deberían tener, ya sea de usuarios de las aplicaciones como de los usuarios de los sistemas y el uso de las herramientas.

Este punto es importante para ver si con el nuevo esquema de control al que vamos perdemos objetivos de control o nos salen acciones nuevas para el catálogo de R.P.I.'S.

Es importante inventariar también en este punto la situación de la administración de la seguridad lógica en los distintos entornos y las características de las contraseñas, así como la operativa tanto de los usuarios de los distintos sistemas como de las distintas administraciones de seguridad y el control de *log o reporting*.

Todo este inventario nos servirá para hacer un análisis de mejoras y pérdidas o limitaciones en los nuevos escenarios con los software de control de los entornos distribuidos, según convenga para elegir el mejor en costo/beneficio.

ADMINISTRACIÓN DE LA SEGURIDAD. Se analizarán, de las distintas opciones del mercado, las características de cada producto.

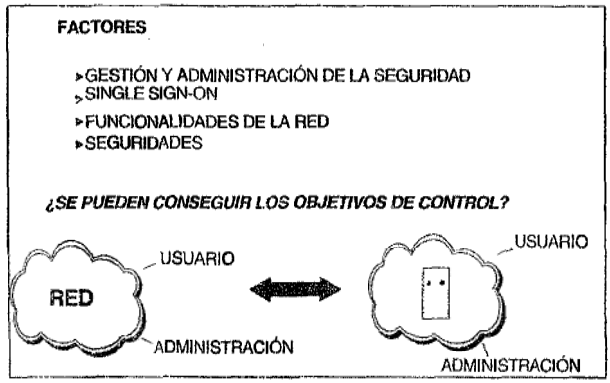

Figura 3.14. Herramientas de control de los entornos distribuidos

No olvidemos que se trata de conseguir que el escenario de los entornos distribuidos se pueda controlar como si de un computador con un solo control de acceso (véase la figura 3.14) se tratara. E incluso mejorando el nivel de control si se puede. Esto hará necesario un conjunto de software a instalar en cada plataforma, sumado a una serie de interfaces en las plataformas que lo necesiten y que a los efectos nos hará observar la seguridad lógica total como un todo.

En este punto nos interesa ver las siguientes funcionalidades u objetivos de control requeridos al nuevo sistema de control de acceso:

- ¿Permite el producto establecer un conjunto de reglas de control aplicables a todos los recursos del sistema?
- ¿Permite el producto al administrador de seguridad establecer un perfil de privilegios de acceso para un usuario o un grupo de usuarios?
- ¿Permite el producto al administrador de seguridad asignar diferentes administradores?
- ¿Permite el producto al administrador de seguridad asignar a estos administradores la posibilidad de gestionar privilegios de acceso para grupos y recursos definidos (por ejemplo, sistemas y aplicaciones)?
- ¿Permite a un administrador pedir acceso para el mismo, tanto como para cualquier usuario de su área de responsabilidad?
- ¿Impide el producto que un administrador se provea él mismo de sus propias peticiones?

Hay que recapitular todos los objetivos de control que se están demandando al conjunto de entornos, en lo referente a la administración de la seguridad, y saber con precisión cuál de las soluciones a analizar cumple mejor los requerimientos.

Es importante pensar en la conexión automática con la información del estado de los recursos humanos que componen el conjunto de usuarios para formatear incompatibilidades por segregación de funciones marcadas por la clasificación de la información y por tener actualizadas las bajas/altas y períodos de ausencia del parque de usuarios.

Son muchos otros los aspectos que deben exigirse, como son que se pueda soportar más de un perfil en un usuario, o que se puedan definir perfiles de todo un departamento o puesto de trabajo, asignaciones temporales de los *backup* de cada empleado para períodos de ausencia del titular, que el perfil de un ingeniero no pueda acceder a una aplicación crítica, que se sincronicen *password* en todos los entornos, etc. En resumen, tantos cuantos objetivos de control se le exijan.

SINGLE SIGN ON. Este concepto podemos definirlo como: "Que es necesario solamente un *password* y un *User ID,* para un usuario, para acceder y usar su

información y sus recursos, de todos los sistemas como si de un solo entorno se tratara". Evidentemente a este concepto habría que añadir todos los conceptos ya vistos en un control de acceso lógico *(time-out,* salvapantallas, log, etc.).

Además podríamos enumerar algunos de los requerimientos que se le piden a la plataforma dentro de este apartado:

- Sobre qué soporta el producto el single sig-on, ¿Windows 3.1, Windows NT, Windows 2000, Unix workstation, terminal 3270, un usuario remoto entrando a través de un servidor de acceso remoto?
- ¿El producto faculta al usuario de un recurso a acceder vía *single sig-on* mientras otros usuarios acceden al mismo recurso directamente?
- ¿El producto encripta las transacciones del *single sig-on* entre la *workstation y* el servidor de seguridad?

FACILIDAD DE USO Y REPORTING. En este punto se valora la "interfaz de usuario" y la calidad de la misma (si tiene interfaz gráfica, si tiene help menús, tanto para el usuario como para el administrador, si tiene mensajes de error, si enseña el perfil de un determinado usuario al administrador, mensajes en las modificaciones como *"are you sure?",* mensajes a través de las aplicaciones, etc.).

Asimismo se evalúa el nivel de *reporting* para los administradores y auditores. Así como:

- ¿El producto ofrece un report de todas las plataformas y aplicaciones a las que los usuarios tienen acceso, así como un report de todos los usuarios que tienen acceso a una plataforma o aplicación?
- ¿Un report de todas las demandas que un administrador ha hecho, o en una fecha dada, o durante un período de tiempo, o a un centro de costo, o de todas las inactividades, o de todos los usuarios activos y privilegios de acceso de un centro de costo, o de demandas pendientes en orden de antigüedad de la demanda, o un report de actividad, de las aplicaciones y sistemas (por ejemplo, el número de demandas aceptadas, pendientes y rechazadas por cada sistema)?
- ¿Un log de violaciones?

En cualquier caso todo registro debe tener garantizada su integridad incluso para los administradores, no pudiendo desactivarse a voluntad, dado que quien quiera hacer algo "no permitido", lo primero que hará es asegurarse de que no quede constancia del hecho.

SEGURIDADES. En este punto se trata de ver aspectos de seguridad clásicos del propio producto, como que el administrador no vea las *password* de los usuarios, una longitud de *password* mínima, que el producto requiera un ID y *password* de

longitud mínima para el acceso al propio producto, el administrador pueda paralizar a un usuario determinado, dual control en las funciones de riesgo (esto es, con un user ID es necesario una *first password* y una *second password* como acceso dual de dos administradores físicos), cifrado de *password,* privacidad en la propagación de *password* en todo momento, acceso a los auditores para poder ver la ID database, un registro de rechazos e intentos infructuosos, la posibilidad de *recovery y backup* (incremental) de todo el sistema de seguridad, la posibilidad del *mirroring* de la database de seguridad para los planes de contingencias de conmutación en tiempo cero al centro alternativo, etc.

También facilidades especiales tales como que se pueda restringir el acceso a un recurso local a un usuario.

Hemos de hacer notar que las limitaciones que vayamos encontrando para todos los productos, tendremos que resolverlas con exclusiones o procedimientos que constarán en el catálogo de R.P.I.'s, verdadero artífice de la metodología que nos obligará a resolver las acciones antes de implantar el producto, y que será un control del proyecto durante su desarrollo.

ADQUISICIÓN, INSTALACIÓN E IMPLANTACIÓN. FORMACIÓN. MANUALES DE PROCEDIMIENTOS DE CONTROL. Tras los pasos anteriores, no queda más que comprar el producto e instalarlo, así como implantar el nuevo esquema de seguridad lógica. Y tras esto, dar la formación apropiada a los implicados y desarrollar los procedimientos de control, que generarán procedimientos operativos para los usuarios de aplicaciones, los usuarios informativos, y los administradores de seguridad lógica.

Todo este complejo proceso es vital hacerlo de modo ordenado y usando un método que permita en todo momento saber qué se "quiere" y qué se "puede" conseguir con los productos existentes de control de entornos, tratando de suplir con procedimientos de control los huecos que no podamos cubrir con tecnología. Aun así, el reto que tenemos por delante es importante, porque las soluciones que ofrecen los fabricantes van muy detrás frente a la proliferación de entornos y aplicaciones nuevos, y sólo una actitud responsable de estandarización en sus soluciones propietarias de seguridad, hará que los fabricantes de soluciones para entornos distribuidos tengan productos de seguridad cada vez mejores, y que en vez de "adaptar el nivel de seguridad lógica a los productos, sean los productos los que resuelvan las situaciones nuevas de seguridad lógica".

3.6. CONCLUSIONES

Son muchas pues las metodologías que se pueden encontrar en el mundo de la auditoría informática y control interno. Muchas hemos visto en este capítulo. Pero como resumen se podría decir que la metodología es el fruto del nivel profesional de cada uno y de 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 auditoría y el control "LA ACTITUD y LA APTITUD", con una actitud vigilante y una formación continuada.

3.7. EJEMPLO DE METODOLOGÍA DE AUDITORÍA DE UNA APLICACIÓN

Metodología de trabajo

Revisión de controles sobre aplicaciones

Objetivo

Determinar que los sistemas producen informaciones exactas y completas en el momento oportuno. Esta área es tal vez la más importante en el trabajo de auditorías informativas.

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 auditoría y para las pruebas.

3. Obtener informaciones generales sobre el sistema. En esta etapa, se definen los objetivos y el alcance de la auditoría, y se identifican los usuarios específicos que estarían afectados por la auditoría (plan de entrevistas).

4. Obtener un conocimiento detallado de la aplicación/sistema. Se pasan las entrevistas con los usuarios y el personal implicado en el sistema a revisar; se examina la documentación de usuarios, de desarrollo y de operación, y se identifican los aspectos más importantes del sistema (entrada, tratamiento, salida de datos, etc.), la periodicidad de procesos, los programas fuentes, características y estructuras de archivos de datos, así como pistas de auditoría.

5. Identificar los puntos de control críticos en el sistema. Utilizando organigramas de flujos de informaciones, identificar los puntos de control críticos en entrevistas con los usuarios 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 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 interfaz entre procedimientos manuales y automáticos.

6. Diseño y elaboración de los procedimientos de la auditoría.

7. Ejecución de pruebas en los puntos críticos de control. Se podría incluir la determinación de las necesidades de herramientas informativas de ayuda a la auditoría no informática. Se revisa el cumplimiento de los procedimientos para verificar el cumplimiento de los estándares y los procedimientos formales, así como los procesos descritos por los organigramas de flujos. Así se verifican los controles internos del cumplimiento de a) planes, políticas, procedimientos, estándares, b) del trabajo de la organización, c) requerimientos legales, d) principios generales de contabilidad y e) prácticas generales de informática.

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

Controles de preparación de datos

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.

Revisar que se dé la formación del "uso del terminal" 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, verificar 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 cumple las normas y requerimientos legales.

Revisar los procedimientos de corrección de errores.

Comprobar la existencia de períodos de retención para documentos fuente 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 límite, 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 log's de acceso por líneas 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, totales de batch, 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 en el 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 auditoría 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 en los 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, en el momento de la actualización de los archivos de transacción, referencia y maestros.

Identificación de transacciones por el uso de números de batch, 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 interfaz entre jobs o programas.

Comprobar que existen validaciones entre totales de control, manuales y automáticos, en puntos de la interfaz entre procesos manuales y automatizados.

Verificar que los log's de actividad de sistemas son revisados por los responsables, para investigar accesos y manipulaciones no autorizados.

Ver los controles sobre la entrada de datos.

Controles de salida de datos

Determinar si los usuarios comparan totales de control de los datos de entrada con totales de control de datos de salida.

Determinar si el 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, etc.

Comparar la lista de distribución de informes con los usuarios que los reciben en realidad. ¿Hay personas que reciben el informe y 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, así como 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 produce la documentación de sistemas, programas, operaciones y funciones, y procedimientos de usuario.

Existencia de una persona específica encargada de la documentación y que mantiene un archivo de documentos ya distribuidos y a quiénes.

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 acepten 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 rearranque documentados y comprobados para cada aplicación en uso actualmente. (No confundir con el plan de contingencias.)

Procedimientos escritos para la transferencia de materiales y documentos de *backup* entre el C.P.D. principal y el sitio de *backup* (centro alternativo). Mantenimiento de un inventario de estos materiales.

Existencia de un plan de contingencia.

Identificación de aplicaciones y archivos 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 críticas en el entorno de *backup,* con los materiales del plan de contingencia (soportes magnéticos, documentación, personal, etc.).

Determinación de qué se revisa, si cada aplicación de un sistema es crítica y si debería incluirse en el plan de contingencia.

Grabación de todas las transacciones ejecutadas por teleproceso, cada día; para facilitar la reconstrucción de archivos actualizados durante el día en caso del fallo del sistema.

Existencia de procesos manuales para sistemas críticos 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 responsables de áreas sobre la adquisición, desarrollo y uso de software de auditoría.

Uso de software de auditoría únicamente por personas autorizadas.

Participación del auditor en la adquisición, modificación/adaptación, instalación de paquetes de software de auditoría.

Participación del auditor en la planificación, diseño, desarrollo e implantación de software de auditoría desarrollado internamente.

Formación apropiada para los auditores que manejan software de auditoría.

Participación del auditor en todas las modificaciones y adaptaciones del software de auditoría, ya sea externo o de desarrollo propio. Actualización de la documentación de software.

Verificación de que los programas de utilidad se utilizan correctamente (cuando no se puede utilizar el software de auditoría).

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 diseño 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 particulares o reforzamientos de procesos manuales

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.

Preparación del informe. Recomendaciones.

Informe previo

Para mantener una relación buena con el área revisada, se emite un informe previo de los puntos principales de la revisión. Esto da a los responsables del área revisada la posibilidad de contribuir a la elaboración del informe final y permitirá una mejor aceptación por parte de ellos.

Informe final de la revisión

Se emite el informe final después de una reunión con los responsables del área implicados en la revisión. El contenido del informe debería describir los puntos de control interno de la manera siguiente:

- Opinión global (conclusión).
- Problema(s) específico(s).
- Explicación de la violación de los controles internos, planes organizacionales, estándares y normas.
- Descripción de los riesgos, exposición o pérdidas que resultarían de las violaciones.

Cuando sea posible, se identificará el impacto de cada problema en términos económicos. Se da una solución específica y práctica para cada debilidad. Se identificarán las personas que se responsabilizarán de cada aspecto de las soluciones. Las recomendaciones son razonables, verificables, interesantes económicamente y tienen en cuenta el tamaño de la organización.

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

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 auditada 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 las recomendaciones para asegurarse de que el trabajo de revisión produce resultados concretos.

3.8. LECTURAS RECOMENDADAS

James A. Schweitzer. *Managing Infortnation Security* (Administrative, Electronic, and Legal Measures to Project Business Information). Butterworths. ISBN 0-409-90195-4.

J. M. Lamete. *La Seguridad Informática* (Metodología). Ediciones Arcadia. ISBN 84-86299-13-6.

J. M. Lamere. *La securité des petits et moyens systèmes informatiques. Dunod* informatique. ISBN 2-04-018721-9.

J. M. Lamere, Y. Leroux, J. Orly. *La securité des reseaux* (Methodes et techniques). Dunod informatique. ISBN 2-04-018886-X.

3.9. CUESTIONES DE REPASO

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

2. ¿Cuáles son los componentes de una contramedida o control (pirámide de la seguridad)? ¿Qué papel desempeñan las herramientas de control? ¿Cuáles son las herramientas de control más 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 auditoría 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 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 el *Single Sign On?* ¿Por qué es necesario un software especial para el control de acceso en los entornos distribuidos?

CAPÍTULO 4

EL INFORME DE AUDITORÍA

José de la Peña Sánchez

4.1. INTRODUCCIÓN

El tema de este capítulo es el **Informe de Auditoría Informática,** que a su vez es el objetivo de la Auditoría Informática.

Para comprender ésta, en función del Informe que realiza un, digamos, experto o perito –al que llamaremos Auditor Informático–, conviene explicar someramente el contexto en el que se desenvuelve hoy su práctica.

La sociedad actual, está en fase tecnológica; apenas guarda recuerdo práctico de anteriores etapas evolutivas (la artesanal, por ejemplo); más aún, las va olvidando a creciente velocidad, generación tras generación.

El dominio de la tecnología como motor de cambio social acelerado y como catalizador de cambios tecnológicos que se superponen, se hace rabiosamente evidente en las llamadas Tecnologías de Información y Comunicaciones de uso en las organizaciones. (Tras el mainframe y los terminales tontos, surgieron los PC's y las redes, el EDI, los entornos distribuidos, las arquitecturas cliente/servidor, las redes TCP/IP –intranets, extranets, redes privadas virtuales...–, los accesos remotos y móviles mediante portátiles y teléfonos móviles, y, finalmente –por ahora–, se nos proponen terminales domésticos vinculados con el equipo de televisión y terminales cuasitontos de trabajo conectados a servidores dominantes descentralizados... Y todo en un período no superior a ¡treinta y cinco años!)

Está claro: las tecnologías de la información, al tiempo que dominan de modo imparable las relaciones humanas (personales, familiares, mercantiles, internacionales...), tienen un ciclo de vida cada vez más corto.