SOBRE LA AUDITORÍA INFORMÁTICA Y LOPD DESDE LA EXPERIENCIA PERSONAL Y PROFESIONAL

UNIVERSIDAD CARLOS III DE MADRID
ESCUELA POLITECNICA SUPERIOR

Ingeniería Técnica en Informática de Gestión

Autor: Germán Ramírez Rodríguez
Tutor: Prof. Miguel A. Ramos
2009

A mis padres, todo un
ejemplo de sacrificio, en especial a
mi padre por recordarme cada mañana
antes de ir a uno de sus dos trabajos
diarios que “aprovechase el tiempo”.
A Ana, por siempre estar a mi lado, para
lo bueno y lo malo siempre te he tenido ahí para
apoyarme o para no confiarme mostrándome
los detalles que no todos ven.
Finalmente, a mis hermanos, que aunque
no fueron nunca el mejor apoyo, si lo
intentaron, y si que fueron un ejemplo
de cómo hacer las cosas.

Índice

1. Introducción

Durante tres años he trabajado mediante becas como “técnico de sistemas” en varias empresas e instituciones, y en ese tiempo he podido comprobar de primera mano como todas las empresas poseen métodos para controlar tanto la seguridad, como la eficiencia y efectividad de sus sistemas de información; y como en todas ellas esos procedimientos son falseados, esquivados, poco utilizados e incluso olvidados por su poco uso.

Como becario en todas ellas fui instruido en como realizar dichos procesos de seguimiento y control desde el primer día, y en todos ellos más tarde, también fui instruido de cómo debía falsearlos, saltármelos o no aplicarlos en determinadas ocasiones.

Es la realidad que yo he podido observar en mis experiencias laborables, no estoy hablando de un grupo de trabajo que se niega a realizar unos procedimientos agarrándose en el “siempre hemos trabajado así”, sino que además de esto el no conceder importancia por parte de los gestores a la documentación y forma de controlar sus proyectos, lleva a la pérdida continua de tiempo inútilmente. Al igual que un programador cuando sube a un repositorio una nueva versión pone un comentario a su nuevo archivo indicando sus nuevas “utilidades” y fecha de actualización, el no hacer algo tan sencillo como esto lleva a que un compañero elimine una versión mejorada con una propia inutilizando la labor del primero, esto que parece hoy en día increíble por los programas de ayuda que utilizamos en los repositorios, no es tan extraño cuando no se presta atención a como actualizamos la información, combinado además con la tendencia a utilizar “trucos” para agilizar los procesos.

En este proyecto parto de la base de que no estoy inventando nada nuevo, solo haciendo hincapié en la situación actual de las empresas que conozco directa o indirectamente sin incidir en su tamaño o experiencia como organización. Muchas empresas de seguridad se fundamentan en que no hay nada seguro al 100% pero que si no prestamos atención a ello ni siquiera damos “sensación de seguridad” a los futuros clientes o posibles atacantes del género que sean, es decir, ya no partimos de la base de que siempre existen agujeros si no de que una empresa puede aparentar ser más o menos sensible al ataque por parte de gente malintencionada en base a la imagen que da al exterior por lo que será más o menos propensa a ataques por ello, ahí es donde yo quiero reflejar en mi trabajo que muchas empresas hoy en día, partieron de unas buenas bases e ideas de cara a la organización segura y controlada de sus sistemas de información y acabaron derivando en “agilizar el proceso” lo cual influye negativamente en la seguridad y rendimiento de la empresa e incluso vulnerándose derechos sobre la protección de datos sin intención de ello, todo ello se incrementa en el tiempo hasta la llegada de una auditoría o la intrusión de una persona ajena a la empresa que produce daños en ésta.

El libro que tiene en sus manos muestra las bases de la auditoría informática, haciendo una importante referencia a la ley de protección de datos vigente en el territorio español, partiremos desde su concepto, sus productos, sus tipos, sus aplicaciones e incluso llegaremos a ver como abordarla, como sé que todo esto es poco para un comité de dirección incluyo las bases de la protección de datos en España a día de hoy, y la demostración a un nivel muy básico de un programa que puede ayudar a la implantación de las medidas aconsejadas por una auditoría, todo siempre con fines constructivos para la mejora de procesos desde el rendimiento hasta la imagen final de cara al cliente.

Cabe destacar que en la realización del libro he partido del REAL DECRETO 1720/2007 del 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la ley Orgánica 15/1999, del 13 de septiembre, de protección de datos de carácter personal, es importante destacar que el RD desarrolló esta ley con una nueva manera de tomar en cuenta el tratamiento de los ficheros en los que se almacenan datos y las normas sobre cómo tratarlos según su importancia.

Veamos un pequeño resumen de cada uno de los temas tratados en el libro:

1- ¿Qué es la auditoría informática?
Definición del amplio concepto de la auditoría informática, objetivos, aplicaciones en las empresas actuales, posibilidades de desarrollo.

2- Ámbitos de aplicación de la auditoría informática
Analizaremos los diferentes ámbitos de aplicación de la auditoría informática desde la **seguridad** (operativa de las aplicaciones de la empresa, de funciones de respaldo, frente a posibles sabotajes, personal informático disponible, etc), pasando por la **confidencialidad y seguridad de la información** (soportes, y acceso a estos)**,** lo cual además afectará a la **gestión de la calidad de la empresa** y finalizando con aspectos **jurídicos y económicos.**

3- Tipos de Auditoría Informática
Veremos una selección de los tipos de auditorías informáticas más destacables entre las que se suelen enfocar cualquier auditoría en base a unos objetivos que se desean mejorar en la empresa o institución.

4- Principales pruebas y herramientas de la auditoría informática.

El auditor dispone de una serie de pruebas y herramientas basadas en su experiencia propia, dichas pruebas podrían resumirse en "**Pruebas clásicas**" (revisión de aplicaciones en base a datos de prueba), "**Pruebas sustantivas**" verifican la exactitud, integridad y validez de la información y finalmente "**Pruebas de cumplimiento**" las cuales determinan si un sistema de control interno funciona adecuadamente (según la documentación, según declaran los auditados, según las políticas y procedimientos de la organización (normativa interna, códigos tipo, etc.), según los estándares externos o incluso según las certificaciones obtenidas en el pasado), es decir, lo que se quiera contratar para comprobar si se cumple.

5- Ventajas y Desventajas de la auditoría informática

Una auditoría nos proporciona una información que debemos poner en manos de las personas adecuadas, la idea es utilizar la información obtenida para mejorar y para ello analizamos las siguientes preguntas:

¿Qué se hace? <-> ¿Qué se debería hacer?

Lo que existe <-> Lo que debería existir

6- Resultados y Productos de una auditoría informática interna

Se analizan 2 principales aspectos de las auditorías informáticas internas, por un lado los objetivos pretendidos por la empresa (evaluación y mantenimiento de la calidad, custodia de activos o fiabilidad de los datos, control del cumplimiento de las certificaciones de la empresa, etc..) y por otro se hace un gran hincapié al reglamento vigente sobre las medidas de seguridad de los ficheros automatizados con datos personales que deben ajustarse a la LOPD.

i. R.D. 994/1999(RDLOPD 1720/2007 – Título VIII actualmente): Medidas de seguridad en el tratamiento de datos de carácter personal. Dispongo una trascripción del reglamento, dicha información es la que aparece en este apartado.

ii. Modelo Conceptual de la exposición final: Defino de una manera breve un ejemplo de informe interno de auditoría informática.

iii. Metodología CRMR

He creído interesante incluir esta metodología ya que define una manera de realizar una revisión de una manera simple y eficaz, no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones rápidas a problemas concretos y notorios:

1. Sistemática para la evaluación y cálculo del ciclo de seguridad
2. Perfiles profesionales de auditores informáticos

7- Resultados y Productos de una auditoría informática externa

Analizo las bases de una auditoría informática externa o independiente como son que tiene por objeto averiguar lo razonable, íntegro y auténtico de los estados, expedientes y documentos así como toda aquella información producida por los sistemas de la organización.

Seguidamente vuelvo a hacer hincapié en la ley de protección de datos sobre todo en la parte de los “códigos tipo”, algo que me parece muy interesante de cara al exterior de una empresa ya que tiene una orientación más bien “comercial” o de “marketing”.

a. Legislación Vigente

Puntualizo haciendo referencia a la legislación vigente en referencia al tema de la protección de datos, ya que a continuación hablaré en más profundidad de los códigos tipo.

b. La autorregulación: los códigos tipo

Me gustaría destacar que los códigos tipo no dejan de ser algo “voluntario” pero que en el momento que son adoptados por una entidad deben de ser llevados estrictamente imponiéndose sanciones en caso de no ser respetados.

i. Los códigos tipo inscritos

Existen muchos códigos tipo en nuestro país cada uno enfocado a un área de mercado y es por ello que he considerado interesante incluir un gran número de ellos en este libro, para poder comparar similitudes y diferencias entre ambos. Más adelante defino el procedimiento para su creación, como deben tratarse los datos personales y una vez finalizado este tratamiento los pasos a seguir ya que el trabajo no se realiza una única vez en el tiempo, sino que debe mantenerse una "continuidad".

3. Pasos previos a la recogida de información
4. Durante el tratamiento de los datos
5. Una vez finalizado el tratamiento

8- ¿Por qué no se aplica una auditoría informática? (con ejemplos)

En este apartado defino una serie de ejemplos donde han de existir una serie de procedimientos para realizar las cosas bien, aunque la experiencia me ha demostrado que en algunas empresas no se mantiene en el tiempo esta atención, lo que conlleva el declive de la calidad de procedimientos, efectividad y seguridad de éstos.

9- Soluciones a como afrontar el resultado de una auditoría informática

Intento enfocar que el resultado de un informe de auditoría informática es una crítica constructiva de cualquier empresa, y debe por tanto ser tomado en cuenta como tal. Defino tres grandes áreas hacia las que enfocar una auditoría y propongo soluciones como las certificaciones para mejorar principalmente en la gestión de la calidad del Software.

a. Seguridad y Protección de la Información
b. Gestión de la calidad del Software
c. Política de seguridad

10- Definición de una aplicación que afronta este problema:

Propongo una aplicación desde mi punto de vista que ayude en la difícil tarea de mantener unos niveles de calidad del software y seguridad de la información con el paso del tiempo dentro de la empresa.

i. Objetivo del programa
ii. Ámbito de la aplicación
iii. ¿Por qué usarlo?
iv. Ideas y Ventajas.

11- Experiencias previas del alumno

Defino una serie de experiencias vividas en diferentes empresas y entidades donde compruebo que una vez se tuvo intención de hacer las cosas bien, pero el resultado actual es otro muy distinto.

12- ¿Es la solución una certificación?

Defino una serie de razones de porque una certificación puede cubrir ampliamente las necesidades descubiertas en algunas auditorías.

2. Objetivo

Gracias a la experiencia laboral adquirida mientras realiza mis estudios universitarios, y a los conocimientos adquiridos en la Universidad Carlos III de Madrid, he definido mi proyecto fin de carrera como una posible solución que de un toque de atención a los dirigentes de cualquier empresa o institución que posea un Sistema de Información para agilizar y mejorar el rendimiento de su actividad, haciéndoles revisar hasta qué punto se está realizando lo que ellos creen tener controlado desde el departamento de sistemas y/o sistema de documentación.

En la asignatura de Auditoría Informática aprendí que siempre todo sistema tiene algo que mejorar, es decir, por muy bien que se realicen las cosas, una auditoría reflejará debilidades y puntos fuertes de la empresa, lo que en resumidas cuentas se transformarán en datos que siempre podrán ser obtenidos mejores sobre todo teniendo en cuenta que estamos en un mundo cambiante donde las tecnologías de la información nunca paran de avanzar ofreciendo nuevas oportunidades para romper barreras de seguridad, o de mejorar la eficiencia de un Sistema de Información. Un sistema que un año es impenetrable y muestra unas trazas de rendimiento muy óptimas puede quedar completamente obsoleto reduciendo el rendimiento de éste con la instalación de una nueva versión de un software de bases de datos, o creando cientos de nuevas grietas de seguridad que antes no existían. Es por ello, que debe analizarse muy a fondo cada nuevo avance en el sistema, desde antes de su implantación, realizándose un seguimiento después para comprobar su rendimiento y seguridad actuales. Insisto en que mi idea no es nueva, pero el fijar desde la dirección de la empresa hasta los departamentos una manera de hacer las cosas y poder comprobar en cualquier momento que se está siguiendo es vital.

Mi objetivo no es una crítica destructiva hacia nada ni nadie, sino todo lo contrario, una crítica constructiva con la aportación de una posible solución apoyándome en mi propia experiencia. Las auditorías sacan a la luz cosas que los dirigentes de las empresas normalmente desconocen y que casi siempre dejan caer sobre el departamento de sistemas en mayor o menor medida, las auditorías internas son una solución pero al igual que otras soluciones, todo lo que supone perder un tiempo a los empleados de lo que es su trabajo directo resulta molesto, y acaba por dejarse a un lado (posponiéndose indefinidamente) o esquivarse de alguna manera (solo se auditan X proyectos por área de trabajo), fundamentarse en que el cliente no exige ese nivel de documentación no excusa al dirigente de un proyecto para no documentar su trabajo, es por ello que hay que saber buscar un equilibrio entre control y rendimiento, definir unos recursos adecuados y eficientes para tal fin que controlen los procesos de un proyecto y ayuden a las personas que trabajan en él a realizar sus trabajos de una manera más eficiente.

3. ¿Qué es la auditoría informática?

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar el fallo. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallos.

El concepto de auditoría es mucho más que esto. La palabra auditoría proviene del latín *auditorius*, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Por otra parte, el diccionario Español Sopena lo define como: Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.

De todo esto sacamos como deducción que la *auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallos en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.*

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o una multinacional privada. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y reducción de costes, pero todo ello en base a una serie de objetivos que priorizarán más unos aspectos frente a otros.

La Auditoría Informática de sistemas de información es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Al auditar principalmente se estudian los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos, además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, hasta los mecanismos de control, los cuales pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la auditoría Informática son:

- El control de la función informática
- El análisis de la eficiencia de los Sistemas Informáticos
- La verificación del cumplimiento de la Normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos
- Comprobar la seguridad de la Información.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Eficiencia
- Eficacia
- Rentabilidad
- Seguridad
- Aseguramiento de la calidad.

Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

- Gobierno corporativo
- Administración del Ciclo de vida de los sistemas
- Servicios de Entrega y Soporte
- Protección y Seguridad
- Planes de continuidad y Recuperación de desastres.

La necesidad de contar con pautas a seguir predefinidas y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, CMMI e ITIL. Todo ello generará a su vez la creación de certificaciones oficiales (ISO 20000, SCAMPI) que dan un sello de calidad a la empresa / institución que los posea ya que garantizan una manera de hacer las cosas organizada, correctamente gestionada y eficaz, además de mantenerse en el tiempo ya que dichas certificaciones deben ser renovadas con el paso de los años.

La auditoría informática es un concepto mucho más amplio que el de la auditoría de la seguridad informática, partiendo de marcos de referencia como COBIT e ITIL y añadiendo la parte de seguridad informática estaremos enfocando en gran medida el significado de la auditoría informática, control de rendimiento y procesos por un lado y la seguridad de la información por otro.

4. Ámbitos de aplicación de la auditoría informática.

La Auditoría del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

En un principio veremos todo lo relacionado con la *seguridad*, luego trataremos todo aquello relacionado con la *eficacia* y terminaremos con la *evaluación del sistema informático*.

Los aspectos relativos al control de la **Seguridad de la Información** tienen tres líneas básicas en la auditoría del sistema de información:

- Aspectos generales relativos a la **seguridad**. En este grupo de aspectos habría que considerar, entre otros: la seguridad operativa de los programas, seguridad en suministros y funciones auxiliares, seguridad contra radiaciones, atmósferas agresivas, agresiones y posibles sabotajes, seguridad física de las instalaciones, del personal informático, etc.

- Aspectos relativos a la **confidencialidad y seguridad de la información**. Estos aspectos se refieren no solo a la *protección* del material (los soportes de la información), sino también al *control de acceso* a la propia información (a toda o a parte de ella, con la posibilidad de introducir modificaciones en la misma distintas personas poseedoras de distintos roles). La información de la que se dispone debe ser íntegra, y un control de acceso a esa información nos garantiza un servicio de no repudio.

- Aspectos **jurídicos y económicos** relativos a la **seguridad** de la información. En este grupo de aspectos se trata de analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho a la intimidad y el derecho a la información, además de controlar los cada vez más frecuentes delitos informáticos que se cometen en las empresas. La propia dinámica de las tecnologías de la información y su cada vez más amplia aplicación en la empresa, ha propiciado la aparición de estos delitos informáticos. En general, estos delitos pueden integrarse en dos grandes grupos: delitos contra el sistema informático y delitos cometidos por medio del sistema informático. En el primer grupo se insertan figuras delictivas tipificadas en cualquier código penal, como hurto, robo, revelación de secretos, etc.., y otro conjunto de delitos que ya no es tan frecuente encontrar, al menos con carácter general, perfectamente tipificados, como el denominado hurto de tiempo, destrucción de bases de datos, delitos contra la propiedad (material, terminales, discos duros,...). En el conjunto de delitos informáticos cometido por medio de sistemas informáticos cabría señalar, manipulaciones fraudulentas de bases de datos, falsificaciones, estafas, etc.

De la misma manera, a través de la auditoría del sistema de información será necesario controlar el adecuado equilibrio entre riesgos y costes de seguridad, y la eficacia del propio sistema.

En cuanto a la **Eficacia** del Sistema, ésta vendrá determinada, básicamente, por la aportación a la empresa de una información válida, exacta, completa, actualizada y oportuna que ayude a la adopción de decisiones, todo ello medido en términos de calidad, plazo y coste. Sin el adecuado control, mediante la realización de auditorías al sistema de información, esos objetivos serían difíciles de conseguir, con la siguiente repercusión en una adecuada dirección y gestión en la empresa.

Uno de los aspectos más significativos de la Auditoría Informática se refiere a los datos relativos a la **Rentabilidad** del Sistema, homogeneizados en unidades económicas de cuenta.

La rentabilidad del sistema debe ser medida mediante el análisis de tres valores fundamentales: la evaluación de los costes actuales, la comparación de esos costes actuales con magnitudes representativas de la organización, y la comparación de los costes del sistema de información de la empresa con los de empresas similares, preferentemente del mismo sector de actividad.

5. Tipos de Auditoría informática

Dentro de la auditoría informática destacan los siguientes tipos (entre otros):

- **Auditoría de la gestión:** Referido a la contratación de bienes y servicios, documentación de los programas, etc.
- **Auditoría legal del Reglamento de Protección de Datos**: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- **Auditoría de los datos**: Clasificación de los datos, estudio de las aplicaciones y análisis de los flujogramas.
- **Auditoría de las bases de datos**: Controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de la seguridad**: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de la seguridad física**: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.
- **Auditoría de la seguridad lógica**: Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de las comunicaciones**. Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la seguridad en producción**: Frente a errores, accidentes y fraudes.

6. Principales pruebas y herramientas para efectuar una auditoría informática

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas clásicas**: Consiste en probar las aplicaciones / sistemas con datos de prueba, observando la entrada, la salida esperada, y la salida obtenida. Existen paquetes que permiten la realización de estas pruebas.
- **Pruebas sustantivas**: Aportan al auditor informático suficientes evidencias para que se pueda realizar un juicio imparcial. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información obtenida.
- **Pruebas de cumplimiento**: Determinan si un sistema de control interno funciona adecuadamente (según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización).

Las principales herramientas de las que dispone un auditor informático son:

- **Observación**
- **Realización de cuestionarios**
- **Entrevistas a auditados y no auditados**
- **Muestreo estadístico**
- **Flujogramas**
- **Listas de comprobación de realización de requisitos**
- **Mapas conceptuales**

7. Ventajas y Desventajas de la auditoría informática.

Me gustaría primeramente considerar las ventajas y desventajas de un software de auditoría informática:

Ventajas

- Económico (a la larga, inversión de futuro)
- Extensión de pruebas
- Utilización de procedimientos de auditorías anteriores
- Eficacia
- Realización de cambios a un mínimo coste
- Elaboración de informes

Desventajas

- Costo inicial alto
- El código embebido puede ser borrado o modificado
- No se verifican procesos particulares sino genéricos
- Limitada habilidad para determinar si la aplicación es propensa a error.
- Sólo se verifican aplicaciones que se están ejecutando.
- Las vulnerabilidades de este tipo de software pueden permitir ataques.

Resumiendo auditar es comparar:

¿Qué se hace? <-> ¿Qué se debería hacer?
Lo que existe <-> Lo que debería existir

Una auditoría nos proporciona una información que debemos poner en manos de las personas adecuadas, es decir, al igual que la auditoría nos informa de las cosas que se están realizando bien en una empresa, también nos informa de las que se están haciendo mal, debemos utilizar la información de una manera adecuada para nuestro beneficio. Todo esto nos lleva a pensar en el

código ético de los auditores; ISACA tiene en cuenta este importante rasgo del perfil del auditor y define algunas normas que deberían seguirse:

- Servir con diligencia, lealtad y honradez los intereses de los auditores, accionistas, clientes y público en general.
- Confidencialidad, objetividad e independencia.
- Estándares, procedimientos y controles.
- Estar al día en auditoría en informática.
- Procurar pruebas objetivas suficientes.
- Informar a los interesados.
- Fomentar la formación e información.
- Altos estándares de conducta (profesional y privada)

Al realizar una auditoría el objetivo y el ámbito deben estar claros, en cada caso se realizará una revisión de control interno, su cumplimiento, sus costes, la eficacia y eficiencia de la gestión, todo ello nos aportará datos para poder comparar unos procesos con otros, unos departamentos con otros, e incluso personas, tanto en el tiempo, como en base a unos objetivos definidos. Una auditoría sea interna u externa genera un informe con una serie de recomendaciones en base a unos objetivos, un ámbito y una profundidad definiendo:

- Planes y objetivos
- Una revisión de controles y planes de riesgo
- Un cumplimiento de procedimientos internos y en base a una normativa externa
- Una administración de la seguridad
- Un proceso en entorno seguro
- Un desarrollo en entorno seguro
- Una continuidad

Llegados a este punto es donde la empresa debe decidir como abordar las recomendaciones definidas por el auditor para el bienestar de su empresa.

8. Resultados y Productos de una auditoría informática interna.

Objetivos de la auditoría interna:

- Revisión y evaluación de controles contables, financieros y operativos
- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento
- Custodia y contabilización de activos
- Examen de la fiabilidad de los datos
- Divulgación de políticas y procedimientos establecidos sobre todo teniendo en cuenta los certificados obtenidos gracias a ellos.
- Información exacta a la gerencia

En el caso de auditorías internas debería de tenerse muy en cuenta el marco de la LOPD, ya que su no cumplimiento puede causar fuertes multas a la empresa, algo tan sencillo como tirar a la basura currículos vitae de aspirantes a una plaza después de cubrirla supone el incumplimiento de la LOPD y en caso de ser descubierto una fuerte multa para la empresa por no tener controlada la forma de tratamiento de esos datos, eso era un ejemplo de datos impresos que recoge recursos humanos en breve espacio de tiempo, ahora veamos un poco más a fondo a que se refiere la LOPD en el tratamiento de ficheros con datos de carácter personal:

R.D. 994/1999 (RLOPD 1720/2007 – Título VIII actualmente): Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal

Artículo 96. Auditoría.

> **1.** A partir del nivel medio, los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.
Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 110. Auditoría. (Dentro de la sección 2 Medidas de seguridad de nivel medio)

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Artículo 81. Aplicación de los niveles de seguridad.

- **1.** Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

- **2.** Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

    - a) Los relativos a la comisión de infracciones administrativas o penales.

    - b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

    - c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

    - d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

    - e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

    - f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

- **3.** Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

    - a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

    - b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

    - c) Aquéllos que contengan datos derivados de actos de violencia de género.

- **4.** A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

- **5.** En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

    - a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

    - b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

- **6.** También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

- **7.** Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

- **8.** A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

En el artículo 82 se nos habla del encargado del tratamiento de los datos y pienso que es importante describir quien y cual es su función:

Encargado del tratamiento.

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

En el CAPITULO III del RD 1720 se nos definen una serie de medidas de seguridad aplicables (a ficheros automatizados) según su importancia, citaremos algunas de ellas:

SECCIÓN 1.ª MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO

Artículo 89. Funciones y obligaciones del personal.

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. Registro de incidencias.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. Gestión de soportes y documentos.

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. Copias de respaldo y recuperación.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

SECCIÓN 2.ª MEDIDAS DE SEGURIDAD DE NIVEL MEDIO

Artículo 95. Responsable de seguridad.

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo.

Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. Auditoría.

1. A partir del nivel medio de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.

Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. Gestión de soportes y documentos.

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. Identificación y autenticación.

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. Control de acceso físico.

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. Registro de incidencias.

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

SECCIÓN 3.ª MEDIDAS DE SEGURIDAD DE NIVEL ALTO

Artículo 101. Gestión y distribución de soportes.

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. Copias de respaldo y recuperación.

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. Registro de accesos.

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. Telecomunicaciones.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Ahora veremos detenidamente en que consiste un informe final de una auditoría realizada a una empresa y que consideraciones debemos tomar al leerlo. Veamos primero su estructura y posteriormente el concepto de cada uno de sus datos.

El informe comienza con una definición de objetivos y alcance de la auditoría. Posteriormente se enumeran los temas objeto de la auditoría:

Para cada tema, se seguirá el siguiente orden a saber:

a) **Situación actual.** Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.

b) **Tendencias**. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.

c) **Puntos débiles y amenazas**.

d) **Recomendaciones** y **planes de acción**. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.

e) Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe solo incluirá hechos importantes.
- El Informe consolidará los hechos que se describen en el mismo sin adornos ni accesorios ya que eso tiende a desviar la atención de los lectores.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados.

La consolidación de los hechos cumplirán, al menos los siguientes criterios:

- El hecho debe poder ser sometido a cambios.
- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
- No deben existir alternativas viables que superen al cambio propuesto.
- La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.
- La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Proceso seguido al encontrar un hecho o debilidad:

1. Hecho encontrado.
    - Será relevante para el auditor y para el cliente.
    - Será concreto, y además convincente.
    - No existirán hechos repetidos, por tanto deben de tomarse todos en cuenta y no tomar como cubierto un hecho con la solución de otro.
2. Consecuencias del hecho
    - Las consecuencias estarán redactadas de modo que sean directamente deducibles del hecho.
3. Repercusión del hecho
    - Aparecerán las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.
4. Conclusión del hecho
    - En casos en que la exposición de hechos haya sido muy extensa o compleja, el auditor reflejará una conclusión que lo resuma.

5. Recomendación del auditor informático
    - Será de simple lectura, por lo que se entenderá por si sola sin necesidad de presentaciones.
    - Será suficientemente soportada en el propio texto.
    - Será concreta y exacta en el tiempo, con lo que podrá ser verificada su implementación.
    - La recomendación irá dirigida expresamente a la persona o personas que puedan implementarla.

Carta de introducción o presentación del informe final

La carta de introducción tiene especial importancia porque en ella se resume la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargó o contrató la auditoría.

Aunque existirán tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- Tendrá como máximo cuatro folios.
- Incluirá fecha, naturaleza, objetivos y alcance.
- Cuantificará la importancia de las áreas analizadas.
- Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- Presentará las debilidades en orden de importancia y gravedad.
- En la carta de Introducción no poseerá nunca recomendaciones.

Una buena manera de presentar este informe en base a unos datos es fundamentándonos en una metodología reconocida y experimentada, pero a la vez sencilla y eficaz como lo es la CRMR (Computer resource management review).

Definición de la metodología CRMR

CRMR o Evaluación de la gestión de recursos informáticos, en esta terminología se destaca la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio de la gestión (management).

Esta manera de realizar una revisión no tiene en sí misma el grado de profundidad de una auditoría informática global, pero proporciona soluciones rápidas a problemas concretos y notorios.

Supuestos de aplicación

En función de la definición dada, la metodología abreviada CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

El método CRMR puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor informático encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

Áreas de aplicación

Las áreas en que el método CRMR puede ser aplicado se corresponden con las sujetas a las condiciones de aplicación señaladas en el punto anterior:

- Gestión de Datos.
- Control de Operaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

Ciertamente, el CRMR no es adecuado para evaluar la procedencia de adquisición de nuevos equipos (Capacity Planning) o para revisar muy a fondo los caminos críticos o las holguras de un proyecto complejo.

Objetivos:

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un Centro de Proceso de Datos. Las Recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijar responsabilidades.
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad.
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

Alcance:

Se fijarán los límites que abarcará el CRMR, antes de comenzar el trabajo.

Se establecen tres clases:

1. Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.
2. Medio. En este caso, el CRMR ya establece conclusiones y recomendaciones, tal y como se hace en la auditoría informática ordinaria.
3. Amplio. El CRMR incluye Planes de Acción, aportando técnicas de implementación de las recomendaciones, a la par que desarrolla las conclusiones.

Información necesaria para la evaluación del CRMR:

Se determinan en este punto los requisitos necesarios para que esta simbiosis de auditoría y consultoría pueda llevarse a cabo con éxito.

1. El trabajo de campo del CRMR ha de realizarse completamente integrado en la estructura del Centro de Proceso de Datos del cliente, y con los recursos de éste.
2. Se deberá cumplir un detallado programa de trabajo por tareas.
3. El auditor-consultor recabará determinada información necesaria del cliente.

Se tratan a continuación los tres requisitos expuestos:

1. Integración del auditor en el Centro de Procesos de Datos a revisar

   No debe olvidarse que se están evaluando actividades desde el punto de vista gerencial. El contacto permanente del auditor con el trabajo ordinario del Centro de Proceso de Datos permite a aquél determinar el tipo de esquema organizativo que se sigue.

2. Programa de trabajo clasificado por tareas

Todo trabajo habrá de ser descompuesto en tareas. Cada una de ellas se someterá a la siguiente sistemática:

- Identificación de la tarea.
- Descripción de la tarea.
- Descripción de la función de dirección cuando la tarea se realiza incorrectamente.
- Descripción de ventajas, sugerencias y beneficios que puede originar un cambio o modificación de tarea
- Test para la evaluación de la práctica directiva en relación con la tarea.
- Posibilidades de agrupación de tareas.
- Ajustes en función de las peculiaridades de un departamento concreto.
- Registro de resultados, conclusiones y Recomendaciones.

3. Información necesaria para la realización del CRMR

El cliente es el que facilita la información que el auditor contrastará con su trabajo de campo.

Se muestra a continuación una Checklist o lista de comprobaciones completa de los datos necesarios para confeccionar el CRMR:

- Datos de mantenimiento preventivo de Hardware.
- Informes de anomalías de los Sistemas.
- Procedimientos estándar de actualización.
- Procedimientos de emergencia.
- Monitorización de los Sistemas.
- Informes del rendimiento de los Sistemas.
- Mantenimiento de las Librerías de Programas.
- Gestión de Espacio en disco.
- Documentación de entrega de Aplicaciones a Explotación.
- Documentación de alta de cadenas en Explotación.

- Utilización de CPU, canales y discos.
- Datos de paginación de los Sistemas.
- Volumen total y libre de almacenamiento.
- Ocupación media de disco.
- Manuales de Procedimientos de Explotación.

Esta información cubre ampliamente el espectro del CRMR y permite ejercer el seguimiento de las recomendaciones realizadas.

Caso Práctico de una Auditoría de Seguridad Informática <<Ciclo de Seguridad>>

A continuación, un caso de auditoría de área general para proporcionar una visión más desarrollada y amplia de la función auditora.

Es una auditoría de Seguridad Informática que tiene como misión revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más importantes de aquél.

Ciclo de Seguridad

El objetivo de esta auditoría de seguridad es revisar la situación y las cuotas de eficiencia de la misma en los órganos más importantes de la estructura informática.

Para ello, se fijan los supuestos de partida:

El área auditada es la seguridad. El área a auditar se divide en: Segmentos.

Los segmentos se dividen en: Secciones.

Las secciones se dividen en: Subsecciones.

De este modo la auditoría se realizará en tres niveles.

Los segmentos a auditar, son:

- Segmento 1: Seguridad de cumplimiento de normas y estándares.
- Segmento 2: Seguridad de Sistema Operativo.
- Segmento 3: Seguridad de Software.
- Segmento 4: Seguridad de Comunicaciones.
- Segmento 5: Seguridad de Base de Datos.
- Segmento 6: Seguridad de Proceso.
- Segmento 7: Seguridad de Aplicaciones.
- Segmento 8: Seguridad Física.

Se darán los resultados globales de todos los segmentos y se realizará un tratamiento exhaustivo del Segmento 8, a nivel de sección y subsección.

Conceptualmente la auditoría informática en general y la de seguridad en particular, ha de desarrollarse en seis fases bien diferenciadas:

Fase 0. Causas de la realización del ciclo de seguridad.

Fase 1. Estrategia y logística del ciclo de seguridad.

Fase 2. Ponderación de sectores del ciclo de seguridad.

Fase 3. Operativa del ciclo de seguridad.

Fase 4. Cálculos y resultados del ciclo de seguridad.

Fase 5. Confección del informe del ciclo de seguridad.

A su vez, las actividades auditoras se realizan en el orden siguiente:

1. Comienzo del proyecto de Auditoría Informática.
2. Asignación del equipo auditor.
3. Asignación del equipo interlocutor del cliente.

4. Cumplimentación de formularios globales y parciales por parte del cliente.
5. Asignación de pesos técnicos por parte del equipo auditor.
6. Asignación de pesos políticos por parte del cliente.
7. Asignación de pesos finales a segmentos y secciones.
8. Preparación y confirmación de entrevistas.
9. Entrevistas, confrontaciones y análisis y repaso de documentación.
10. Cálculo y ponderación de subsecciones, secciones y segmentos.
11. Identificación de áreas mejorables.
12. Elección de las áreas de actuación prioritaria.
13. Preparación de recomendaciones y borrador de informe
14. Discusión de borrador con cliente.
15. Entrega del informe.

Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma.

El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad. Puede haber muchas causas: Reglas internas del cliente, incrementos no previstos de costes, obligaciones legales, situación de ineficiencia global notoria, etc.

De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

Estrategia y logística del ciclo de Seguridad

Constituye la FASE 1 del ciclo de seguridad y se desarrolla en las actividades 1, 2 y 3:

FASE 1. *Estrategia y logística del ciclo de seguridad*

1. Designación del equipo auditor.
2. Asignación de interlocutores, validadores y decisores del cliente.
3. El cliente debe rellenar un cuestionario inicial, para la realización del estudio inicial.

Con las razones por las cuales va a ser realizada la auditoría (Fase 0), el equipo auditor diseña el proyecto de Ciclo de Seguridad en base a una estrategia definida en función del volumen y complejidad del trabajo a realizar, que constituye la Fase 1 del punto anterior.

Para desarrollar la estrategia, el equipo auditor necesita recursos materiales y humanos. La adecuación de éstos se realiza mediante un desarrollo logístico, en el que los mismos deben ser determinados con exactitud. La cantidad, calidad, coordinación y distribución de los mencionados recursos, determina a su vez la eficiencia y la economía del Proyecto.

Los planes del equipo auditor se desarrollan de la siguiente manera:

1. Eligiendo el responsable de la auditoría su propio equipo de trabajo. Este ha de ser heterogéneo en cuanto a especialidad, pero compacto.
2. Recabando de la empresa auditada los nombres de las personas de la misma que han de relacionarse con los auditores, para las peticiones de información, coordinación de entrevistas, etc.
3. Mediante un **estudio inicial**, del cual forma parte el análisis de un formulario exhaustivo, también inicial, que los auditores entregan al cliente para su cumplimentación.

   Según los planes marcados, el equipo auditor, cumplidos los requisitos 1, 2 y 3, estará en disposición de comenzar la "tarea de campo", la operativa auditora del Ciclo de Seguridad.

Ponderación de los Sectores Auditados

Este constituye la Fase 2 del Proyecto y engloba las siguientes actividades:

FASE 2. *Ponderación de sectores del ciclo de seguridad.*

4. Asignación de pesos técnicos. Se entienden por tales las ponderaciones que el equipo auditor hace de los segmentos y secciones, en función de su importancia.
5. Asignación de pesos políticos. Son las mismas ponderaciones anteriores, pero evaluadas por el cliente.
6. Asignación de pesos finales a los Segmentos y Secciones. El peso final es el promedio del peso técnico y del peso político. La Subsecciones se calculan pero no se ponderan.

Se pondera la importancia relativa de la seguridad en los diversos sectores de la organización informática auditada.

Las asignaciones de pesos a Secciones y Segmentos del área de seguridad que se audita, se realizan del siguiente modo:

Pesos técnicos

Son los coeficientes que el equipo auditor asigna a los Segmentos y a las Secciones.

Pesos políticos

Son los coeficientes o pesos que el cliente concede a cada Segmento y a cada Sección del Ciclo de Seguridad.

Ciclo de Seguridad. Suma Pesos Segmentos = 100 **(con independencia del número de segmentos consideradas)**			
Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg1. Normas y Estándares	12	8	10
Seg2. Sistema Operativo	10	10	10
Seg3. Software Básico	10	14	12
Seg4. Comunicaciones	12	12	12
Seg5. Bases de Datos	12	12	12
Seg6. Procesos	16	12	14
Seg7. Aplicaciones	16	16	16
Seg8. Seguridad Física	12	16	14
TOTAL	**100**	**100**	**100**

Pesos finales

Son el promedio de los pesos anteriores.

El total de los pesos de los 8 segmentos es 100. Este total de 100 puntos es el que se ha asignado a la totalidad del área de Seguridad, como podría haberse elegido otro cualquiera. El total de puntos se mantiene cualquiera que hubiera sido el número de segmentos. Si hubieran existido cinco segmentos, en lugar de 8, la suma de los cinco habría de seguir siendo de 100 puntos.

Suma Peso Secciones = 20 (con independencia del número de Secciones consideradas)			
Secciones	**Pesos Técnicos**	**Pesos Políticos**	**Pesos Finales**
Secc1. Seg. Física de Datos	6	6	6
Secc2. Control de Accesos	5	3	4
Secc3. Equipos	6	4	5
Secc4. Documentos	2	4	3
Secc5. Suministros	1	3	2
TOTAL	20	20	20

Puede observarse la diferente apreciación de pesos por parte del cliente y del equipo auditor. Mientras éstos estiman que las Normas y Estándares y los Procesos son muy importantes, el cliente no los considera tanto, a la vez que prima, tal vez excesivamente, el Software Básico.

Del mismo modo, se concede a todos los segmentos el mismo valor total que se desee, por ejemplo 20, con absoluta independencia del número de Secciones que tenga cada Segmento. En este caso, se han definido y pesado cinco Secciones del Segmento de Seguridad Física. Cabe aclarar, solo se desarrolló un solo Segmento a modo de ejemplo.

Operativa del ciclo de Seguridad

Una vez asignados los pesos finales a todos los Segmentos y Secciones, se comienza la Fase 3, que implica las siguientes actividades:

FASE 3. *Operativa del ciclo de seguridad*

7. Preparación y confirmación de entrevistas.
8. Entrevistas, pruebas, análisis de la información, cruzamiento y repaso de la misma.

Las entrevistas deben realizarse con exactitud. El responsable del equipo auditor designará a un encargado, dependiendo del área de la entrevista. Este, por supuesto, deberá conocer a fondo la misma.

La realización de entrevistas adecuadas constituye uno de los factores fundamentales del éxito de la auditoría. La adecuación comienza con la completa cooperación del entrevistado. Si ésta no se produce, el responsable lo hará saber al cliente.

Deben realizarse varias entrevistas del mismo tema, al menos a dos o tres niveles jerárquicos distintos. El mismo auditor puede, y en ocasiones es conveniente, entrevistar a la misma persona sobre distintos temas. Las entrevistas deben realizarse de acuerdo con el plan establecido, aunque se pueden llegar a agregar algunas adicionales y sin planificación.

La entrevista concreta suele abarcar Subsecciones de una misma Sección tal vez una sección completa. Comenzada la entrevista, el auditor o auditores formularán preguntas al/los entrevistado/s. Debe identificarse quien ha dicho qué, si son más de una las personas entrevistadas.

Las listas de comprobación o “Checklist’s” son útiles y en muchos casos imprescindibles. Terminadas las entrevistas, el auditor califica las respuestas del auditado (no debe estar presente) y procede a la valoración de la información correspondiente.

Simultáneamente a las entrevistas, el equipo auditor realiza pruebas planeadas y pruebas sorpresa para verificar y cruzar los datos solicitados y facilitados por el cliente. Estas pruebas se realizan ejecutando trabajos propios o repitiendo los de aquél, que indefectiblemente deberán ser similares si se han reproducido las condiciones de carga de los Sistemas auditados. Si las pruebas realizadas por el equipo auditor no fueran consistentes con la información facilitada por el auditado, se deberá recabar nueva información y reverificar los resultados de las pruebas auditoras.

La evaluación de las listas de comprobación o Checklists, las pruebas realizadas, la información facilitada por el cliente y el análisis de todos los datos disponibles, configuran todos los elementos necesarios para calcular y establecer los resultados de la auditoría, que se materializarán en el informe final.

A continuación, un ejemplo de auditoría de la Sección de Control de Accesos del Segmento de Seguridad Física:

Vamos a dividir a la Sección de Control de Accesos en cuatro Subsecciones:

1. Autorizaciones
2. Controles Automáticos
3. Vigilancia
4. Registros

En las siguientes listas de comprobación o Checklists, las respuestas se calificarán de 1 a 5, siendo 1 la peor valoración y 5 la máxima puntuación.

Control de Accesos: **Autorizaciones**		
Preguntas	Respuestas	Puntos
¿Existe un único responsable de implementar la política de autorizaciones de entrada en el Centro de Cálculo?	Si, el Jefe de Explotación, pero el Director puede acceder a la Sala con acompañantes sin previo aviso.	4
¿Existe alguna autorización permanente de estancia de personal ajeno a la empresa?	Una sola. El técnico permanente de la firma suministradora.	5
¿Quiénes saben cuales son las personas autorizadas?	El personal de vigilancia y el Jefe de Explotación.	5
Además de la tarjeta magnética de identificación, ¿hay que pasar otra especial?	No, solamente la primera.	4
¿Se pregunta a las visitas si piensan visitar el Centro de Cálculo?	No, vale la primera autorización.	3
¿Se proveen las visitas al Centro de Cálculo con 24 horas al menos?	No, basta que vayan acompañados por el Jefe de Explotación o Director	3
TOTAL AUTORIZACIONES		**24/30** **80%**

Control de Accesos: **Controles Automáticos**		
Preguntas	Respuestas	Puntos
¿Cree Ud. que los Controles Automáticos son adecuados?	Si, aunque ha de reconocerse que a pie puede llegarse por la noche hasta el edificio principal.	3
¿Quedan registradas todas las entradas y salidas del Centro de Cálculo?	No, solamente las del personal ajeno a Operación.	3
Al final de cada turno, ¿Se controla el número de entradas y salidas del personal de Operación?	Sí, y los vigilantes los reverifican.	5
¿Puede salirse del Centro de Cálculo sin tarjeta magnética?	Si, porque existe otra puerta de emergencia que puede abrirse desde adentro	3
TOTAL CONTROLES AUTOMATICOS		**14/20** **70%**

Control de Accesos: **Vigilancia**		
Preguntas	Respuestas	Puntos
¿Hay vigilantes las 24 horas?	Sí.	5
¿Existen circuitos cerrados de TV exteriores?	Sí.	5
Identificadas las visitas, ¿Se les acompaña hasta la persona que desean ver?	No.	2
¿Conocen los vigilantes los terminales que deben quedar encendidos por la noche?	No, sería muy complicado.	2
TOTAL VIGILANCIA		**14/20** **70%**

Control de Accesos: **Registros**		
Preguntas	Respuestas	Puntos
¿Existe una política adecuada de registros?	No, reconocemos que casi nunca, pero hasta ahora no ha habido necesidad.	1
¿Se ha registrado alguna vez a una persona?	Nunca.	1
¿Se abren todos los paquetes dirigidos a personas concretas y no a Informática?	Casi nunca.	1
¿Hay un cuarto para abrir los paquetes?	Si, pero no se usa siempre.	3
TOTAL REGISTROS		**6/20** **30%**

Cálculos y Resultados del Ciclo de Seguridad

FASE 4. *Cálculos y resultados del ciclo de seguridad*

1. Cálculo y ponderación de Secciones y Segmentos. Las Subsecciones no se ponderan, solo se calculan.
2. Identificación de materias mejorables.
3. Priorización de mejoras.

En el punto anterior se han realizado las entrevistas y se han puntuado las respuestas de toda la auditoría de Seguridad.

El trabajo de levantamiento de información está concluido y contrastado con las pruebas. A partir de ese momento, el equipo auditor tiene en su poder todos los datos necesarios para elaborar el informe final. Solo faltaría calcular el porcentaje de importancia de cada área; éste se obtiene calculando el sumatorio de las respuestas obtenidas, recordando que deben afectarse a sus pesos correspondientes.

Una vez realizado los cálculos, se ordenarán y clasificarán los resultados obtenidos por materias mejorables, estableciendo prioridades de actuación para lograrlas.

Cálculo del ejemplo de las Subsecciones de la Sección de Control de Accesos:

Autorizaciones 80%

Controles Automáticos 70%

Vigilancia 70%

Registros 30%

Promedio de Control de Accesos 62,5%

Cabe recordar, que dentro del Segmento de Seguridad Física, la Sección de Control de Accesos tiene un peso final de 4.

Prosiguiendo con el ejemplo, se procedió a la evaluación de las otras cuatro Secciones, obteniéndose los siguientes resultados:

Ciclo de Seguridad: **Segmento 8, Seguridad Física.**		
Secciones	Peso	Puntos
Sección 1. Datos	6	57,5%
Sección 2. Control de Accesos	4	62,5%
Sección 3. Equipos (Centro de Cálculo)	5	70%
Sección 4. Documentos	3	52,5%
Sección 5. Suministros	2	47,2%

Conocidos los promedios y los pesos de las cinco Secciones, se procede a calcular y ponderar el Segmento 8 de Seguridad Física:

Seg. 8 = PromedioSección1 * peso + PromedioSecc2 * peso + PromSecc3 * peso + PromSecc4 * peso + PromSecc5 * peso / (peso1 + peso2 + peso3 + peso4 + peso5)

Ó

Seg. 8 = (57,5 * 6) + (62,5 * 4) + (70 * 5) + (52,5 * 3) + (47,2 * 2) / 20

Seg. 8 = 59,85%

A continuación, la evaluación final de los demás Segmentos del ciclo de Seguridad:

Ciclo de Seguridad. Evaluación y pesos de Segmentos		
Segmentos	Pesos	Evaluación
Seg1. Normas y Estándares	10	61%
Seg2. Sistema Operativo	10	90%
Seg3. Software Básico	12	72%
Seg4. Comunicaciones	12	55%
Seg5. Bases de Datos	12	77,5%
Seg6. Procesos	14	51,2%
Seg7. Aplicaciones	16	50,5%
Seg8. Seguridad Física	14	59,8%
Promedio Total Área de Seguridad	**100**	**63,3%**

Sistemática seguida para el cálculo y evaluación del Ciclo de Seguridad:

a. Valoración de las respuestas a las preguntas específicas realizadas en las entrevistas y a los cuestionarios formulados por escrito.
b. Cálculo matemático de todas las subsecciones de cada sección, como media aritmética (promedio final) de las preguntas específicas. Recuérdese que las subsecciones no se ponderan.
c. Cálculo matemático de la Sección, como media aritmética (promedio final) de sus Subsecciones. La Sección calculada tiene su peso correspondiente.
d. Cálculo matemático del Segmento. Cada una de las Secciones que lo componen se afecta por su peso correspondiente. El resultado es el valor del Segmento, el cual, a su vez, tiene asignado su peso.
e. Cálculo matemático de la auditoría. Se multiplica cada valor de los Segmentos por sus pesos correspondientes, la suma total obtenida se divide por el valor fijo asignado a priori a la suma de los pesos de los segmentos.

Confección del Informe del Ciclo de Seguridad

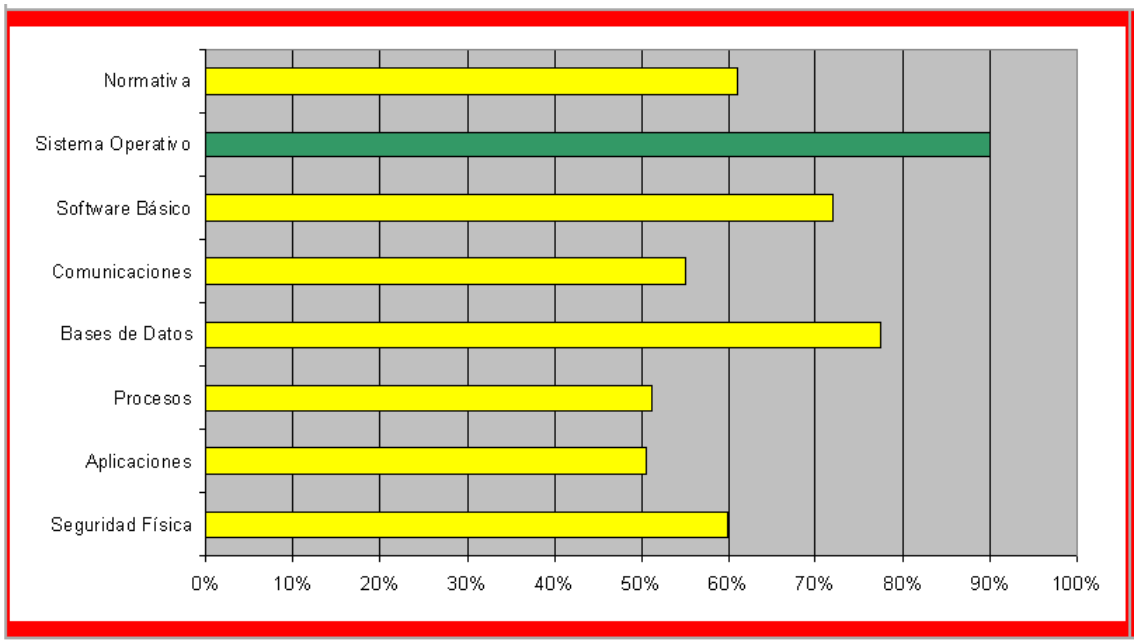
FASE 5. *Confección del informe del ciclo de seguridad*

1. Preparación de borrador de informe y Recomendaciones.
2. Discusión del borrador con el cliente.
3. Entrega del Informe y Carta de Introducción.

Ha de resaltarse la importancia de la discusión de los borradores parciales con el cliente. La referencia al cliente debe entenderse como a los responsables directos de los segmentos. Es de destacar que si hubiese acuerdo, es posible que el auditado redacte un contrainforme del punto cuestionado. Esta acta se incorporará al Informe Final.

Las Recomendaciones del Informe son de tres tipos:

1. Recomendaciones correspondientes a la zona roja. Serán muy detalladas e irán en primer lugar, con la máxima prioridad. La redacción de las recomendaciones se hará de modo que sea simple verificar el cumplimiento de la misma por parte del cliente.
2. Recomendaciones correspondientes a la zona amarilla. Son las que deben observarse a medio plazo, e igualmente irán priorizadas.
3. Recomendaciones correspondientes a la zona verde. Suelen referirse a medidas de mantenimiento. Pueden ser omitidas. Puede detallarse alguna de este tipo cuando una acción sencilla y económica pueda originar beneficios importantes.



Perfiles Profesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en explotación y en desarrollo de proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas telemáticos.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática y con experiencia en la Gestión de costes.

9. Resultados y Productos de una auditoría informática externa.

Una Auditoría Externa examina y evalúa los sistemas de información de una organización y emite una opinión independiente sobre los mismos, pero las empresas generalmente requieren de la evaluación de su Sistema de Información de forma independiente para otorgarle validez ante los usuarios del producto (clientes), es decir, disponer de un departamento de calidad que realice auditorías internas nos proporciona unas bases, nos hace mantenernos alerta para mantener el nivel de eficiencia, calidad y exigencia a la propia empresa, pero de cara al exterior disponer de una certificación, o una auditoría externa positiva es mejor valorado.

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

La Auditoría Externa o Independiente tiene por objeto averiguar lo razonable, íntegro y auténtico de los estados, expedientes y documentos así como toda aquella información producida por los sistemas de la organización.

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

Finalmente el resultado nos otorgará los siguientes productos:

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio
- Control de las actividades de investigación y desarrollo
- Sugerencias de elaboración de **códigos tipos**

Según la LOPD *"establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo".*

Se establece, además, la posibilidad de que contengan o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación, de manera que, en el supuesto de que tales reglas no se incorporen directamente a **códigos tipo**, las instrucciones u órdenes que los establezcan deberán atenerse a los principios en ellos previstos.

El objetivo de los **códigos tipo** es adecuar lo establecido en la normativa vigente en este ámbito a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos. A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto la LOPD y el RLOPD.

Su implementación y la adscripción a los mismos por parte de los profesionales son voluntarias. A pesar de constituir un instrumento de gran ayuda para cumplir la normativa vigente en materia de protección de datos, no son normas jurídicas vinculantes.

Por su parte, el RLOPD nos recuerda este carácter de códigos deontológicos* o de buena práctica profesional y que, únicamente, serán vinculantes para quienes se adhieran a los mismos.

Debemos detenernos en este punto aclarando que los responsables de ficheros no están obligados a participar en la elaboración de este tipo de códigos y, una vez elaborados e inscritos, están, del mismo modo, facultados para elegir libremente sobre su adhesión o suscripción, además de no implicar dicha adhesión el cumplimiento de la LOPD y su normativa de desarrollo.

No obstante, si un responsable se adhiere a un código tipo concreto, a partir de ese momento, queda obligado al cumplimiento de las disposiciones incluidas en el mismo y su incumplimiento podría ser sancionado por la entidad creada a estos efectos. Consecuencia de ello, el responsable suscriptor o adherido estará sometido a un control periódico por parte del citado órgano, que deberá verificar que cada una de las obligaciones aceptadas voluntariamente continúan siendo objeto de cumplimiento, resultando frecuente la creación de comités de control orientados a velar por el buen funcionamiento y aplicabilidad del código tipo.

El RLOPD no introduce ninguna novedad en este sentido, reconociendo igualmente la posibilidad de creación de códigos tipo por iniciativa de empresas, grupos de entidades pertenecientes a un mismo sector y Administraciones públicas y corporaciones de derecho público.

* El **código deontológico** es un documento que recoge un conjunto más o menos amplio de criterios, normas y valores que formulan y asumen quienes llevan a cabo una actividad profesional. Los códigos deontológicos se ocupan de los aspectos más sustanciales y fundamentales del ejercicio de la profesión que regulan. Estos códigos cada vez son más frecuentes en otras muchas actividades. Sin embargo, no siempre se cumplen, y aunque sí se respeten, quedan notables lagunas en cuanto a quién está encargado de hacerlos cumplir, así como las sanciones para quienes los vulneren.

A. Legislación Vigente

1.1. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Es la Ley vigente en la actualidad y que adapta la legislación española a la Directiva europea. Su ámbito de aplicación comprende **todos los ficheros que contengan datos de carácter personal**, con independencia de que se trate de ficheros automatizados o en formato papel. Incluye como otras novedades principales la definición del Encargado del Tratamiento, la regulación de los tratamientos de datos y las relaciones entre Responsable del Fichero y Encargado del Tratamiento, la definición de fuentes accesibles al público, el censo promocional e incorpora el nuevo derecho de oposición.

1.2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (RLOPD)

El RLOPD (que entró en vigor el día 19 de abril de 2008) desarrolla la LOPD y consolida la doctrina reguladora establecida por la AEPD en sus instrucciones y expedientes sancionadores, así como la interpretación que de la LOPD han efectuado los Tribunales a través de la jurisprudencia.

El RLOPD incrementa la protección ofrecida a los datos de carácter personal, pero, por otra parte, establece ciertas especialidades para facilitar la implantación de medidas de seguridad, que inciden sobre todo en el ámbito de las PYMES. Este nuevo Reglamento, que sustituye al RMS 994/1999(RLOPD TITULO VIII 1720/2007 actualmente), establece, entre otras cosas, las medidas de seguridad para los ficheros no automatizados, regula las relaciones entre el Responsable del Fichero y el Encargado del Tratamiento (permitiendo además la subcontratación), introduce novedades importantes con respecto a los ficheros sobre solvencia patrimonial y crédito y respecto al ejercicio de derechos, así como otras novedades que se desarrollan en detalle en este libro más adelante.

Las infracciones, sanciones o cuantía de las multas no se han modificado, pero sí se ha introducido, con respecto a las actuaciones previas al Procedimiento Sancionador de la AEPD, un límite temporal de doce meses a contar desde la fecha de la denuncia.

El vencimiento del plazo sin que se haya dictado y notificado el acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

2.1. Plazos de adaptación

La Disposición transitoria segunda del RLOPD recoge los plazos de implantación de las medidas de seguridad con arreglo a las siguientes reglas:

2.1.1. Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del RLOPD (19 abril 2008):

a) Se permite el plazo de un año desde su entrada en vigor (19 de abril de 2009, por lo que deberían ya estar implantadas) para la implantación de medidas de seguridad de nivel medio, exigibles a los siguientes ficheros:

- Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.
- Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

b) Una vez finalizado el plazo de un año (19 de abril de 2009) deberán haberse implantado las medidas de seguridad de nivel medio a aquéllos ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En el plazo de dieciocho meses (19 de octubre de 2009) las de nivel alto exigibles a los ficheros que contengan datos derivados de actos de violencia de género.

d) En los demás supuestos, cuando el RLOPD exija la implantación de una medida adicional no prevista en el RMS. Dicha medida deberá implantarse en el plazo de un año (19 de abril de 2009).

2.1.2. Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del RLOPD:

a) Las medidas de seguridad de nivel básico deberán estar implantadas desde el plazo de un año desde su entrada en vigor (19 de abril de 2009).

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor (19 de octubre de 2009).

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor (19 de abril de 2010).

2.2.1.3. Respecto de los ficheros creados con posterioridad a la fecha de entrada en vigor del RLOPD:

Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del RLOPD deberán tener implantadas, desde el momento de su creación, **la totalidad de las medidas de seguridad** reguladas en el mismo.

B. La autorregulación: Los códigos tipo

La aplicación de las obligaciones impuestas por la normativa vigente en materia de protección de datos de carácter personal no es algo sencillo. Las empresas, independientemente de la actividad que desarrollan, y, dentro de éstas, tanto los responsables de los ficheros que contienen datos personales como sus usuarios, se enfrentan, continuamente, a realidades complejas e importantes problemas a la hora de aplicar dicha normativa, suponiendo un gran esfuerzo hallar soluciones prácticas que permitan el desarrollo eficaz de su actividad.

La *autorregulación* es una vía que puede resultar de gran ayuda para los responsables de los ficheros o tratamientos de datos de carácter personal inmersos en este confuso panorama, tratando de adaptar la aplicación de la normativa de protección de datos a las peculiaridades propias de cada sector de actividad a través de los denominados códigos tipo. La elaboración de estos códigos, así como la adhesión a los mismos por parte de los responsables de tratamientos, debe ser cada día más frecuente en todos los sectores. Pese a ello, en la actualidad, existe un desconocimiento generalizado en relación con estos códigos y, más en concreto, su existencia, qué son realmente y su naturaleza.

Con carácter genérico y, en una primera aproximación, podríamos definir los códigos tipo como conjunto de normas de buena conducta, adoptados por entidades, generalmente pertenecientes al mismo sector, como modelos a seguir para el desarrollo de sus actividades profesionales; asimilables a los códigos deontológicos o de buena práctica profesional. Éstos constituyen una forma de complementar la regulación o, en algunos casos, suplir las lagunas o carencias de aquella, estableciendo, normalmente, medidas que no sólo respetan las previsiones legales sino que suponen garantías adicionales, reforzando el espíritu y finalidad de la Ley.

Las actividades objeto de regulación por los códigos pueden ser de muy diversa naturaleza, dado que el fin perseguido en su elaboración se centra en predefinir pautas o estándares de actuación generales a tener en cuenta por los sujetos pertenecientes a un determinado sector.

Al margen de los códigos tipo reguladores de otras materias concretas, se analizarán en este caso, aquellos que pretenden regular de forma unitaria, los tratamientos de datos de carácter personal realizados por personas físicas o jurídicas englobadas en el mismo sector de actividad.

En este ámbito, la Directiva 95/46/CE, utilizando la denominación de códigos de conducta, establece la posibilidad de adoptar este tipo de códigos, requiriendo a la Comisión Europea y a los Estados miembros para fomentar su desarrollo:

"los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presenta Directiva".

El Grupo de Trabajo Sobre la Protección de las Personas Físicas, en un Documento de Trabajo adoptado el 14 de enero de 1998[†], estableció una definición para este tipo de códigos, denominándolos, en ese caso, códigos de autorregulación y expresándose en los siguientes términos:

"cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión".

[†] Documento de Trabajo: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos en un país tercero ?, http:// europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1998/wp7_es.pdf.

La LOPD, que contempla también la posibilidad de elaborar códigos tipo cuyo ámbito de aplicación se circunscriba a una sola empresa, se refiere a los códigos tipo en su artículo 32, indicando que son aquellos en los que se *"establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo".*

Establece, además, la posibilidad de que contengan o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación, de manera que, en el supuesto de que tales reglas no se incorporen directamente a los códigos, las instrucciones u órdenes que los establezcan deberán atenerse a los principios en ellos previstos.

Analizaremos a continuación el objeto, la naturaleza, los sujetos habilitados para la adopción, el procedimiento de elaboración, el contenido, las ventajas, las garantías de cumplimiento, las obligaciones posteriores a su publicación, las ventajas que puede conllevar su adopción, así como los códigos que, a día de hoy, se encuentran registrados en el RGPD.

1. Objeto de los códigos tipo

Los códigos tipo en materia de protección de datos de carácter personal tienen por objeto adecuar lo establecido en la normativa vigente en este ámbito a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto la LOPD y el RLOPD.

2. Naturaleza de los códigos tipo

En relación con esta cuestión, la propia LOPD establece, únicamente, la posibilidad de formular códigos tipo y reconoce el carácter de códigos deontológicos o de buena práctica profesional de los mismos. Con base en ello, ya podíamos afirmar que su implementación y la adscripción a los mismos por parte de los profesionales son voluntarias. A pesar de constituir un instrumento de gran ayuda para cumplir la normativa vigente en materia de protección de datos, no son normas jurídicas vinculantes.

Por su parte, el RLOPD nos recuerda este carácter de códigos deontológicos o de buena práctica profesional y que, únicamente, serán vinculantes para quienes se adhieran a los mismos.

Debemos detenernos en este punto aclarando que los responsables de ficheros **no están obligados** a participar en la elaboración de este tipo de códigos y, una vez elaborados e inscritos, están, del mismo modo, facultados para **elegir libremente** sobre su adhesión o suscripción, además de no implicar dicha adhesión el cumplimiento de la LOPD y su normativa de desarrollo.

No obstante, si un responsable se adhiere a un código tipo concreto, a partir de ese momento, **queda obligado** al cumplimiento de las disposiciones incluidas en el mismo y su incumplimiento podría ser sancionado por la entidad creada a estos efectos. Consecuencia de ello, el responsable suscriptor o adherido estará sometido a un control periódico por parte del citado órgano, que deberá verificar que cada una de las obligaciones aceptadas voluntariamente continúan siendo objeto de cumplimiento, resultando frecuente la creación de comités de control orientados a velar por el buen funcionamiento y aplicabilidad del código tipo.

3. Sujetos habilitados para la adopción de códigos tipo

La Directiva 95/46/CE, además de autorizar a las asociaciones de profesionales, deja abierta la posibilidad a cualquier organización representante de otras categorías de responsables de tratamientos y, en transposición de ésta, el legislador español ha conferido dicha posibilidad a todos los responsables de tratamientos, ya sean de titularidad pública o privada, así como a las organizaciones en las que se agrupen, siempre que lo efectúen mediante acuerdos sectoriales, convenios administrativos o decisiones de empresas. Esto ha supuesto un cambio fundamental respecto de lo establecido en la LORTAD, dado que, si bien ésta no hacía alusión expresa a los sujetos habilitados para la adopción de códigos tipo, sí hacía referencia a los responsables de ficheros de titularidad privada, quedando excluidos, por tanto, todos los responsables de tratamientos de titularidad pública.

El RLOPD no introduce ninguna novedad en este sentido, reconociendo igualmente la posibilidad de creación de códigos tipo por iniciativa de empresas, grupos de entidades pertenecientes a un mismo sector y Administraciones públicas y corporaciones de derecho público

4. Procedimiento para la elaboración de códigos tipo

La LOPD no contempla ningún procedimiento específico para la adopción de códigos tipo, existiendo por ello una laguna en este punto, posiblemente motivada por la propia naturaleza de estos códigos, cuya **implementación es totalmente voluntaria**, laguna que no ha sido cubierta por el RLOPD. Como consecuencia de ello, salvo los requisitos formales establecidos por la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (artículos 68 y 70) para la solicitud de inscripción de los códigos tipo, su procedimiento de elaboración se ajustará, en cada caso, a la voluntad de los sujetos intervinientes en el mismo.

No obstante, el artículo 32.3 de la LOPD establece una obligación que se debe cumplir tras su elaboración, expresándose en los siguientes términos: "ser depositados e inscritos en el RGPD y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas".

El Registro podrá denegar su inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, requiriendo, en este caso, el Director de la AEPD a los solicitantes a fin de que efectúen las correcciones oportunas.

El RLOPD ha desarrollado la obligación de depósito y publicidad de los códigos tipo, estableciendo que para que estos puedan considerarse como tales deberán depositarse e inscribirse en el RGPD o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al RGPD, así como la obligación de la AEPD de dar publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

5. Contenido de los códigos tipo

La LOPD no regula el contenido que tienen que tener estos códigos. Ante esta laguna la AEPD recogió en su página web los aspectos de fondo del contenido de estos códigos[‡]. Se relaciona a continuación el **contenido mínimo** que, a tenor de lo expresado por la AEPD, deberían recoger:

- **Introducción**. Se expresarán las razones que han conducido al desarrollo del código, enumerando los valores añadidos que aporta su cumplimiento, a través de una exposición de motivos.

[‡] Vid. AEPD, *Aspectos de fondo del contenido de un código tipo,* https://www.agpd.es/index.php?idSeccion=242.

- **Ámbito de aplicación**. El ámbito de aplicación responderá a la actividad de los responsables de ficheros que los suscriben, debiendo quedar perfectamente delimitado.

- **Principios específicos del sector que representa**. El código tipo deberá incluir la aplicación de principios específicos en el sector que mejoren las previsiones legales, acotando estos principios y desarrollando el procedimiento de aplicación de los principios generales de protección de datos al caso concreto del sector representado.

- **Definiciones específicas**. Deberá incluir las definiciones que amplíen conceptos de la Ley y, especialmente, definiciones de carácter técnico del sector involucrado.

- **Condiciones de organización y procedimientos**. Entre otros aspectos, deberá singularizar los datos personales a tratar, identificar los posibles destinatarios de cesiones o transferencias internacionales y las leyes o previsiones que las amparan en el sector, delimitar las fuentes de recogida de los datos, permitir el ejercicio de los derechos de acceso, rectificación, cancelación y oposición en condiciones más favorables, estableciendo para ello el procedimiento que corresponda, así como incluir modelos para el ejercicio de estos derechos y cláusulas informativas para su introducción en los cuestionarios de recogida de los datos. Además, podrá incluir un sello de garantía identificativo del código tipo, que hará referencia a la vinculación al mismo.

- **Medidas de seguridad**. Deberá indicar el nivel mínimo de medidas de seguridad que se van a aplicar y hacer una enumeración de las mismas, pudiendo establecer el compromiso de cumplimiento de un nivel de medidas de seguridad mas alto que el correspondiente a los ficheros objeto de tratamiento en el sector que elabora el código tipo.

- **Comunicaciones y transferencias internacionales de datos.** Deberá analizar las diferentes situaciones que se puedan dar en el sector y el ámbito legal en el que se producen.

- **Procedimiento de autorregulación y control.** En relación con éste, resulta destacable el deber de aclarar que supone una vía opcional y que siempre se podrá acudir a la AEPD para presentar una reclamación ante el incumplimiento de la LOPD.

- **Régimen sancionador.** Tendrá que establecer el régimen de sanciones por incumplimiento del código tipo.

- **Relación de adheridos.** Contendrá la relación de adheridos, así como el compromiso del titular del código de comunicar altas, bajas o modificaciones de asociados a la Agencia.

- **Marco normativo.** Deberá establecer el marco normativo general y el específico del sector, incluyendo todas las instrucciones y recomendaciones que sean aplicables al sector.

- **Conclusiones**. Deberá contener un resumen de ventajas y/o garantías que ofrece el código a los titulares de los datos, modelos para el ejercicio de los derechos y un resumen de obligaciones que deben cumplir los responsables de los ficheros.

El RLOPD ha cubierto la laguna de la LOPD, regulando el **contenido mínimo** que deben incluir los códigos tipo, tal y se detalla a continuación:

- La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.

- Las previsiones específicas para la aplicación de los principios de protección de datos.

- El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.

- El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

- La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.

- Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.

- Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo.

- Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

- Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

- Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

- Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Este contenido deberá estar redactado en términos claros y accesibles y con suficiente grado de precisión.

Al margen del contenido mínimo indicado, los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

La adopción de medidas de seguridad adicionales a las exigidas por la LOPD y el RLOPD.

- La identificación de las categorías de cesionarios o importadores de los datos.

- Las medidas concretas adoptadas en materia de protección de los menores de determinados colectivos de afectados.

- El establecimiento de un sello de calidad que identifique a los adheridos al código.

- Finalmente, en virtud de lo establecido en el artículo 76 del RLOPD, se deberá incorporar a los códigos tipo un anexo con la relación de adheridos, que tendrá que mantenerse actualizada y a disposición de la AEPD.

- En el plazo de un año desde la entrada en vigor del RLOPD deberán notificarse a la AEPD las modificaciones que resulten necesarias en los códigos tipo inscritos en el RGPD para adaptar su contenido a lo expuesto anteriormente.

6. Ventajas derivadas de la creación de códigos tipo

Uno de los aspectos que debe tener en cuenta todo responsable de ficheros son las ventajas de distinta índole que la adopción de este tipo de códigos puede conllevar, como garantía frente a los titulares de los datos de carácter personal y a la propia AEPD, así como, de forma interna, a la organización del responsable del tratamiento.

En primer lugar, para los titulares de datos personales -ya consten en los ficheros del responsable del tratamiento o se trate de sujetos que, potencialmente, pueden estar interesados en la actividad desarrollada por el mismo-, la adopción de estos códigos suponen unas obligaciones impuestas por la normativa un código tipo en materia de protección de datos podrá ser interpretada como reguladora de esta materia y el modo más adecuado de llevarlas a la práctica en su sector concreto, demostrando el respeto por el derecho de los particulares a preservar sus datos personales.

En aras a la consecución de la confianza de los titulares de los datos, lo más frecuente es que la suscripción por parte de los responsables de tratamientos de datos de carácter personal a estos códigos traiga como consecuencia la posibilidad de utilizar un **sello de garantía** que los identificará como tales, con la finalidad de que produzca en los titulares de los datos el efecto anteriormente expuesto. En relación con la AEPD, dado que, como ya se ha reflejado anteriormente, los códigos tipo deben ser inscritos en el RGPD, previa revisión de su adecuación a las disposiciones legales y reglamentarias sobre la materia, si con posterioridad la Agencia considera que una actuación acorde con lo establecido en el código tipo suscrito es sancionable, el responsable podrá argumentar la doctrina de los actos propios, a fin de que dicha práctica no sea considerada como contraria a la Ley.

Del mismo modo, la adhesión a un código tipo tiene repercusiones internas para el propio responsable del tratamiento de datos, facilitándole información acerca de la manera de actuar en el proceso de tratamiento de los datos personales, especialmente, en relación con aquellos aspectos que generan a todos los profesionales una mayor inseguridad en sus actuaciones.

7. Garantías del cumplimiento de los códigos tipo

El RLOPD establece la obligación de incluir en los códigos tipo **procedimientos de supervisión independientes** para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio. Estos procedimientos deberán garantizar:

- La independencia e imparcialidad del órgano responsable de la supervisión.
- La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.
- El principio de contradicción.
- Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.
- La notificación al afectado de la decisión adoptada.

Del mismo modo, podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

8. Obligaciones posteriores a la inscripción del código tipo

Una vez publicado un código tipo, las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el mismo tendrán que cumplir las siguientes obligaciones establecidas en el RLOPD:

- Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior. Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

- Remitir a la AEPD una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

- Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al RGPD.

- Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

i. Códigos tipo inscritos

A día de hoy, únicamente se han inscrito doce códigos tipo, constando dos de ellos en el RGPD con anterioridad a la entrada en vigor de la LOPD y en su totalidad con carácter previo a la entrada en vigor del RLOPD. A continuación, analizaremos brevemente cada uno de ellos, centrándonos en su objeto y ámbito de aplicación, dado que es suficiente para conocer su espíritu y entrar en más detalles nos obligaría a extendernos demasiado. Para ello, se seguirá un orden cronológico por fecha de inscripción del más antiguo al más reciente.

Código Tipo de Telefónica de España, S.A.

Fecha Inscripción: 20/12/1994 (modificado en diciembre de 2003).

Siendo el primer código inscrito en el RGPD, concretó su objeto en establecer los principios a los que se sujeta la actuación de Telefónica de España en materia de protección de datos, regulando las condiciones organizativas y técnicas de los ficheros existentes en la actualidad o que puedan crearse en el futuro, así como las condiciones para la recogida y utilización de los datos, determinando el procedimiento a seguir en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por los afectados, así como los derechos específicos de los usuarios en el sector de las telecomunicaciones.

Este código resulta aplicable a los tratamientos de datos de carácter personal que se efectúen en España por Telefónica de España, sirviendo de punto de referencia para el resto de las empresas del Grupo, como parámetros deseables a los que se debe tender aun cuando no exista legislación de protección de datos en los países en los que estén establecidas.

Código Tipo de Asociación Multisectorial de la Información (ASEDIE).

Fecha de inscripción: 15/09/1999.

Constituye el objeto de este código establecer las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías para el ejercicio de los derechos de las personas, en su ámbito; resultando de aplicación a las relaciones que mantengan las empresas asociadas a la ASEDIE (Sector de Información Comercial) con las personas objeto de informes comerciales, con los usuarios de los mismos, así como a las relaciones que dichos asociados mantengan entre sí y con terceras personas, empresas, entidades u organismos relacionados de forma directa o indirecta con el ejercicio de la actividad de información comercial.

Del mismo modo, se aplica a los ficheros automatizados que contengan datos de carácter personal y de los que sean responsables las empresas asociadas a ASEDIE, cuya finalidad sea la prestación de servicios de información sobre la solvencia patrimonial y crédito.

Código Tipo de Fichero Histórico de Seguros del Automóvil (UNESPA).

Fecha de inscripción: 11/10/2000.

En relación con su objeto, este código se expresa en los términos que se recogen a continuación:

“El Fichero Histórico, cumple con la finalidad descrita en el artículo 24.3, párrafo segundo de la Ley 33/1995 en cuanto a fichero de colaboración estadístico actuarial para la tarificación y selección de riesgos, recogiendo información sobre los contratos de seguros del automóvil que el tomador ha suscrito en los últimos cinco años así como de los siniestros vinculados a dichos contratos.

Igualmente, el Fichero contribuirá a promover la transparencia en el mercado del seguro del automóvil y la aplicación equitativa y suficiente de las tarifas a los riesgos asegurados. Los asegurados tendrán un mayor acceso al conjunto de ofertas del sector y podrán buscar la que más se adecue a sus necesidades al permitírsele tener conocimiento de sus propios datos de siniestralidad, factor esencial para el cálculo de la prima del seguro. Por su parte las entidades aseguradoras tendrán una información exacta y precisa del riesgo que complementará la facilitada por el tomador en la solicitud de seguro, en su deber de declaración del riesgo.

Se entiende por siniestro el acaecimiento del hecho que, previsto en el contrato, es susceptible de dar lugar al pago de la indemnización por la entidad aseguradora con cargo a la póliza suscrita por el tomador." Su ámbito de aplicación se extiende al responsable del fichero, la empresa de servicios de tratamiento automatizado y todas las entidades aseguradoras autorizadas para operar en España en el ramo de responsabilidad civil de automóviles, sean o no asociadas a UNESPA, teniendo como único requisito imprescindible que estén inscritas en el Registro Especial de la Dirección General de Seguros.

Código Tipo de La Asociación Nacional de Fabricantes (ANF).

Fecha de inscripción: 21/12/2001.

El presente código arbitra un sistema, cuyo seguimiento asegura a los adheridos al mismo el pleno cumplimiento de sus obligaciones en materia de protección de datos de carácter personal. Podrán suscribir este código todas las empresas o profesionales adheridos a la ANF, resultando aplicable a los datos de carácter personal contenidos en ficheros sobre clientes.

Código Tipo de Agrupación Catalana de Establecimientos Sanitarios (ACES).

Fecha de inscripción: 28/12/2001.

La ACES es una asociación empresarial que tiene como finalidad el asesoramiento, defensa y representación de sus miembros, procurando en todo momento la optimización de métodos de trabajo y objetivos, en general, tendiendo fundamentalmente a la promoción de sus intereses sociales, laborales, profesionales y culturales.

Atendiendo a dicha finalidad se creó este código, cuyo ámbito de aplicación abarca tanto a sus socios de número -personas físicas o jurídicas que siendo de titularidad privada desarrollen su actividad principal dentro del sector sanitario como a los socios de honor -personas o entidades que presten o hayan prestado a la Agrupación o a la Sanidad ayudas o colaboraciones destacadas-, siempre previo acuerdo de la Asamblea General de ACES a propuesta de la Junta Directiva.

Código Tipo de Unió Catalana D'Hospitals (UNIÓ).

Fecha de inscripción: 12/07/2002 (modificado en julio de 2004).

La indiscutible y, legalmente reconocida, naturaleza sensible de los datos personales concernientes a la salud unida a la posibilidad de establecer códigos tipo, arrastraron a la UNIÓ a utilizar este instrumento con la finalidad de que los adheridos a este código preserven de cualquier violación la privacidad de las personas físicas y garanticen su autodeterminación informativa.

En relación con su ámbito subjetivo de aplicación, podemos afirmar que éste se extiende, no sólo a los asociados que manifiesten de forma expresa su adhesión al mismo, sino también a aquellas entidades no asociadas pero que, reuniendo las condiciones para poder serlo, con implantación territorial en cualquier territorio del estado, manifiesten su voluntad de adhesión al código de forma expresa.

Por su parte, el ámbito objetivo se centra en el tratamiento de datos de carácter personal contenidos en los ficheros de pacientes/historia clínica, sea cual sea su soporte y modalidad de tratamiento.

Código Tipo de Comercio Electrónico y Publicidad Interactiva (AUTOCONTROL-AECE-IAB SPAIN).Fecha Inscripción: 07/11/2002.

Nos encontramos ante un sector extremadamente dinámico y en permanente evolución, donde las posibilidades de obsolescencia normativa son mayores que en cualquier otro. Adaptarse a los cambios previendo soluciones a estos problemas de regulación es uno de los objetivos que inspiran el presente código, aplicable a la publicidad y al comercio electrónico realizado a través de medios electrónicos de comunicación a distancia, por personas físicas o jurídicas con establecimiento permanente en España o dirigidos de forma específica al mercado español.

Código Tipo de Odontólogos y Estomatólogos de España.
Fecha de inscripción: 12/07/2004.

Mediante la elaboración de este código el Ilustre Consejo de Colegios Oficiales de Odontólogos y Estomatólogos de España pretende ofrecer garantías para las personas cuyos datos de carácter personal se traten por los profesionales colegiados en los Colegios Oficiales de Odontólogos y Estomatólogos de España, fijando reglas específicas para el tratamiento de datos de carácter personal en el ámbito del ejercicio de esta profesión; todo ello, sin perjuicio de la aplicación de las obligaciones y deberes genéricos establecidos por las normas vigentes en materia de protección de datos de carácter personal aplicables a todas las personas, entidades o empresas titulares de ficheros que contengan datos personales.

Su ámbito de aplicación se extiende a todos los servicios profesionales prestados por odontólogos y estomatólogos colegiados en los Colegios Oficiales de Odontólogos y Estomatólogos españoles, que se adhieran al código, ya sean prestados en clínicas y/o consultorios dentales individuales o colectivos.

Código Tipo Universidad de Castilla-La Mancha.

Fecha de inscripción: 14/07/2004.

Esta institución académica, que ha mostrado siempre una especial sensibilidad por los temas relacionados con la seguridad informática y el respeto a todo lo relacionado con la protección de datos de carácter personal, ha sido la primera institución pública en implementar un código tipo en esta materia, con la pretensión de cumplir de la forma más sencilla y segura con la legislación, a través de un documento único que reúna todos los documentos esenciales, y servir de referente al resto de universidades españolas, contribuyendo, al mismo tiempo, al conocimiento de este derecho fundamental.

Se ha establecido como objeto de éste código garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar, resultando de aplicación a los datos de carácter personal que figuren en ficheros automatizados de la Universidad de Castilla-La Mancha y a toda modalidad de uso posterior de estos datos.

Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA).

Fecha de inscripción: 27/12/2004.

Este código ha establecido la siguiente distinción en relación con su objeto:

A. Respecto a los responsables de los ficheros: las condiciones de utilización y conservación de los datos de carácter personal, el régimen de cesión o comunicación, las directrices de la normativa interna de los asociados adheridos al código, la creación de un Comité de protección de datos en el seno de la ACRA y un régimen de infracciones y sanciones.

B. Respecto a los titulares de los datos de carácter personal: definir y delimitar los procedimientos para ejercer los derechos de los titulares de los datos de carácter personal en aras a obtener las mayores garantías de estos derechos, tanto en lo que se refiere a su difusión como a su ejercicio y la protección, en lo que concierne al tratamiento de los datos de carácter

personal, de las libertades públicas y los derechos fundamentales de los residentes en cualquiera de los centros o establecimientos asociados y adheridos al código, así como, su derecho al honor e intimidad personal y familiar.

En términos generales, es aplicable a los datos de carácter personal de los residentes registrados en soportes automatizados o no, que los hagan susceptibles de tratamiento, y a toda modalidad de uso posterior de los mismos, de los que sean responsables los asociados de ACRA que se adhieran al código tipo.

Código Tipo del Sector de la Intermediación Inmobiliaria. Asociación Empresarial de Gestión Inmobiliaria (AEGI).

Fecha de inscripción: 29/12/2004.

La AEGI, conocedora de la problemática que en cuanto al tratamiento de datos de carácter personal presenta el sector de la gestión inmobiliaria, consideró imprescindible el establecimiento de un marco que recoja un conjunto de normas de autorregulación que garantice que el sector cumple con las previsiones que la LOPD y sus reglamentos establecen, lo que debe traducirse en un beneficio de imagen y gestión hacia el cliente, estableciendo como ámbito de aplicación, en general, los tratamientos efectuados por las empresas adheridas para la prestación de sus servicios de gestión inmobiliaria y, en concreto, los siguientes tratamientos:

a) Tratamientos de datos destinados a captar clientes para compra, venta o alquiler de inmuebles (cliente potencial).

b) Tratamientos de datos involucrados directamente en operaciones de compraventa y/o alquiler de inmuebles o destinadas a la concreción futura de las mismas (fases previas o de reserva e intermediación concretada o no).

c) Tratamientos de datos relacionados en todo o en parte con la gestión inmobiliaria, como pudieran ser la gestión de la contratación de los suministros necesarios para la vivienda, de la financiación necesaria para la adquisición o arrendamiento de un inmueble (sea como mera intermediación o servicio propio), prestación de servicios de rehabilitación u obras en inmuebles.

d) aquellos derivados de operaciones de promoción o construcción inmobiliaria en la parte que concierne a las acciones destinadas a la venta o arrendamiento de las viviendas construidas.

e) cualesquiera comprendidos en el ámbito de la gestión inmobiliaria.

Código Tipo Veraz-Persus. Soluciones Veraz ASNEF-EQUIFAX, S. L.

Fecha de inscripción: 19/12/2006.

El objeto de este código tipo es establecer las condiciones de organización y régimen de funcionamiento del fichero Veraz-Persus, con el objeto de ofrecer a los beneficiarios unas garantías más amplias que las contenidas en la normativa dictada en materia de protección de datos de carácter personal.

El fichero Veraz-Persus, es un fichero de auto-inclusión en el que cualquier persona, por sí misma, o a través de su tutor legal, podrá solicitar su incorporación con el objeto de evitar el uso fraudulento de sus datos personales por terceros en perjuicio de su identidad, solvencia y patrimonio económico.

Después de este análisis de la figura de los códigos tipo en materia de protección de datos y, ya para finalizar, debemos insistir en que, si bien éstos no tienen carácter normativo, sino, como ya se ha indicado, de códigos deontológicos o de buena práctica profesional, constituyen un importante instrumento para facilitar el cumplimiento de la normativa de protección de datos de carácter personal, que como decíamos al comienzo, está resultando muy complejo y requiriendo un gran esfuerzo por parte de las entidades o personas físicas a las que les resulta de obligado cumplimiento la citada normativa.

9. Obligaciones básicas según la normativa

En este apartado haremos una exposición de las obligaciones principales que la normativa de protección de datos impone a los responsables de los ficheros de datos de carácter personal y demás personas que intervienen en algún momento en el tratamiento de los mismos.
Para ello, y con el objetivo de aportar una visión práctica en su desarrollo, hemos dividido el transcurso del tratamiento de los datos en tres momentos principales:

- con carácter previo a la recogida de los datos,
- durante el tratamiento de los datos y
- una vez finalizado el tratamiento.

De este modo, analizaremos cada una de las obligaciones, ubicándolas en el momento en el que deben ser tenidas en cuenta para una correcta aplicación de la normativa de protección de datos, ya que la propia LOPD establece en qué punto del tratamiento deben ser apreciadas unas y otras. Antes de la recogida de los datos seguiremos una serie de pasos

Pasos previos a la recogida de información

1º Creación y notificación de ficheros

¿Qué es un fichero de datos de carácter personal?

Debemos comenzar analizando qué es un fichero de datos de carácter personal y qué se entiende como tal a efectos de notificación.
La definición legal de fichero se encuentra recogida en el artículo 3.b) de la LOPD que se expresa en los siguientes términos:

"*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y*

acceso", definición que ha sido desarrollada por el RLOPD, en su artículo 5.1.k), quedando finalmente como:
"*todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*".

Nos encontramos ante una definición de carácter genérico y que puede resultar tan amplia que en la práctica no ha sido de gran ayuda, creando incluso confusión en numerosas ocasiones en las que, atendiendo a la misma, no queda claro si nos encontramos ante un fichero protegido por la normativa de protección de datos personales y que, por consiguiente, debe ser declarado ante la AEPD para su inscripción en el RGPD o, por el contrario, podríamos estar ante varios ficheros cuya declaración debe hacerse de forma independiente. Dentro de esta definición podemos englobar muchos términos utilizados habitualmente, tales como base de datos, aplicación, programa, tabla, fichero... *-en relación con el tratamiento informatizado-*, o cajonera, armario, archivo*... -si nos referimos a tratamientos no informatizados, sino manuales-.* Estos términos vienen a identificar los denominados **ficheros físicos**.

Frente a estos, existen los llamados **ficheros lógicos**, que podemos definir como ficheros o conjunto de ficheros físicos que contienen el mismo tipo de datos y son tratados para la misma finalidad.

La AEPD ha considerado que sólo los ficheros lógicos son objeto de declaración. Esto significa que, una vez identificados los ficheros físicos, el responsable de los mismos podrá agruparlos en ficheros lógicos atendiendo a los criterios indicados.

Así por ejemplo, en una empresa pueden existir diversos ficheros físicos con datos de clientes (datos bancarios, gestión de la relación comercial, marketing, gestión de impagados). Todos estos tienen datos de clientes y comparten la finalidad consistente en gestionar la relación con los mismos, de manera que se pueden agrupar en un único fichero lógico y declararse ante la AEPD, por ejemplo, bajo el nombre de clientes.

El concepto anteriormente indicado puede matizarse aún más teniendo en cuenta lo establecido en el artículo 2.c) de la Directiva 95/46/CE, dado que el mismo aclara la referencia a la forma de creación, almacenamiento, organización y acceso del fichero al indicar que el conjunto de datos tendrá esa consideración "ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

En cuanto al reparto geográfico, podemos afirmar que el concepto de fichero no va directamente vinculado a la exigencia de que el mismo se encuentre en una única ubicación. Es posible la existencia de ficheros distribuidos en lugares geográficos remotos entre sí, siempre y cuando la organización y sistematización de los datos responda a un conjunto organizado y uniformado de datos, sometido a algún tipo de gestión centralizada.

La AEPD se ha pronunciado en este sentido a través de un informe jurídico emitido en respuesta a una consulta planteada por una entidad que disponía de diversos centros, ubicados en distintos lugares y carentes de personalidad jurídica propia, disponiendo de información sometida a tratamiento similar repartida en ficheros idénticos y alojada en servidores diferentes, dada su ubicación en los distintos centros, pero administrados y gestionados de forma centralizada.

En relación con este tema, el RLOPD -artículo 56- viene a aclarar que:
"*la notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos*" y que "*cuando los datos de carácter personal objeto de tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados, o exista una copia en soporte no automatizado de un fichero automatizado, sólo será preciso una sola notificación, referida a dicho fichero*".

Lo primero que debemos pensar si deseamos crear un fichero que contenga datos personales, es que tenemos que enfrentarnos a un requisito, establecido en el artículo 25 de la LOPD, en virtud del cual es imprescindible que el fichero *"resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas*".

Si bien, del respeto de las garantías establecidas en la LOPD iremos hablando a lo largo de todo este apartado, debemos analizar antes de seguir adelante el significado de la expresión "[...] resulte necesario para el logro de la actividad u objeto legítimos [...]". Dicha "necesidad", con frecuencia viene establecida o se deriva del cumplimiento de la legislación aplicable a la actividad u objeto desarrollados por el responsable, tanto en términos generales como fruto de alguna norma sectorial. De ahí que algunos ficheros resultan imprescindibles para el desarrollo de cualquier actividad u objeto legitimo (ya sea empresarial, comercial, profesional...) y otros resultan específicos de cada sector. Incluso, al margen de los ficheros creados por imposición, cualquier persona, empresa o entidad, puede sentir la necesidad de crear ficheros con distintas finalidades, pero para su creación siempre ha de haber una justificación directamente vinculada a la actividad u objeto legítimos, sin existir limitación alguna en relación con el número de ficheros inscribibles.

En este orden de cosas, podemos poner como ejemplos más claros en los que se cumple este primer requisito para la creación de ficheros, aquellos en los que la necesidad de su creación es consecuencia directa del cumplimiento de una Norma que el titular debe aplicar para el desarrollo de su actividad u objeto legítimos, de lo que no cabe duda en ficheros como los que se describen a continuación:

A. Los ficheros tradicionalmente denominados personal, empleados, gestión laboral..., permiten llevar a cabo la gestión laboral de la actividad desarrollada por el responsable del fichero, así como un control detallado de las cuestiones relativas al personal laboral. En este sentido, la Ley 42/1997, de 14 de noviembre, Ordenadora de la Inspección de Trabajo y Seguridad Social, hace referencia a la conservación de información del personal

laboral por parte del empleador, al disponer en su artículo 11 que "*toda persona natural o jurídica estará obligada a proporcionar a la Inspección de Trabajo y Seguridad Social toda clase de datos, antecedentes o información con trascendencia en los cometidos inspectores, siempre que se deduzcan de sus relaciones económicas, profesionales, empresariales o financieras con terceros sujetos a la acción inspectora, cuando a ello sea requerida en forma*".

B. Otros de los ficheros más habitualmente declarados por los responsables son los denominados gestión fiscal y contable, gestión financiera, facturación... No cabe duda de la necesidad de estos ficheros para el logro de la actividad legítima de cualquier actividad económica. En este sentido, el artículo 142 de la Ley 58/2003, de 17 de diciembre, General Tributaria, que se expresa en los siguientes términos:

"*Las actuaciones inspectoras se realizarán mediante el examen de documentos, libros, contabilidad principal y auxiliar, ficheros, facturas, justificantes, correspondencia con trascendencia tributaria, bases de datos informatizadas, programas, registros y archivos informáticos relativos a actividades económicas, así como mediante la inspección de bienes, elementos, explotaciones y cualquier otro antecedente o información que debe de facilitarse a la Administración o que sea necesario para la exigencia de las obligaciones tributarias*", justifica la creación de dichos ficheros.

C. Poniendo como ejemplo el sector sanitario, en el que los derechos a la intimidad y a la protección de datos tienen una relevancia especial, cualquier centro sanitario, desde las clínicas en las que un único profesional desarrolla su actividad de forma autónoma hasta los grandes hospitales, tienen la obligación de disponer de un fichero con las historias clínicas de sus pacientes, cuya finalidad es la gestión de la prestación sanitaria prestada a los mismos. Fruto de la obligación de conservación de la documentación clínica, establecida en el artículo 17.1 de la Ley 41/2002, de 14 de noviembre, reguladora básica de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, se especifica que:

"*los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial*".

De lo anteriormente expuesto, podemos concluir que cualquiera de estos ficheros cumple con el requisito de ser necesario para el logro de la actividad u objeto legítimos de sus responsables. A pesar de que no siempre tiene que ser así, ni es la única justificación para que un fichero cumpla el requisito de ser necesario que venimos analizando, los más habituales surgen de la necesidad de cumplir con requisitos impuestos por diferentes legislaciones. No podemos olvidar que, fuera de estos supuestos, cualquier persona, empresa o entidad, puede necesitar crear ficheros con distintas finalidades, lo que no supondrá ningún problema siempre que exista una justificación directamente vinculada a su actividad u objeto legítimos.

10. Ficheros de titularidad privada

Los ficheros de titularidad privada son definidos en el artículo 5.1.l) del RLOPD como aquellos de los que son responsables las personas, empresas o entidades de derecho privado, independientemente de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, pero no se encuentran estrictamente vinculados al ejercicio de potestades de derecho público atribuida por su normativa específica.

Para la creación de estos ficheros hay que cumplir un procedimiento formal establecido en el artículo 27 de la LOPD, siguiendo los pasos que se describen a continuación:

A. **Notificación previa a la AEPD**, cumplimentando los modelos o formularios electrónicos aprobados al efecto por la AEPD en resolución de 12 de julio de 2006 y publicados en el Boletín Oficial del Estado de 31 de julio 2006, en los que se detallará necesariamente la identificación del responsable del fichero, el nombre del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y la procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la identificación del nivel de medidas de seguridad básico, medio o alto exigible y, en su caso la identificación del encargado de tratamiento donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos. Además, se declarará un domicilio a efectos de notificación. En función de lo establecido en el RLOPD, esta notificación podrá realizarse en diferentes soportes, tal y como se explica a continuación:

- En soporte electrónico -mediante comunicación electrónica o en soporte informático, utilizando el programa NOTA (Notificaciones Telemáticas a la Agencia) para la generación de notificaciones que la AEPD ha puesto a disposición de todos los ciudadanos.
- En soporte papel, utilizando igualmente los modelos aprobados por la AEPD.

Estos formularios se pueden obtener gratuitamente en la página web de la AEPD (www.agpd.es).

B. Si la notificación se ajusta a los requisitos exigibles, el Director de la AEPD, a propuesta del Registro General de Protección de Datos (en adelante, RGPD), acordará la inscripción del fichero asignándole el correspondiente código de inscripción. En caso contrario, dictará resolución denegando la inscripción, debidamente motivada y con indicación expresa de las causas que impiden la inscripción.
El art. 59.3 del RLOPD, introduce como novedad la posibilidad del Director de la AEPD de establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiere la notificación.

La notificación de la creación de ficheros de datos de carácter personal ante la AEPD es una obligación que corresponde al responsable de los mismos, de manera que cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el RGPD, la creación del correspondiente fichero.

Además, esta obligación no conlleva coste económico alguno.

Es importante destacar que la inscripción de los ficheros debe encontrarse actualizada en todo momento y es meramente declarativa, sin calificar que se estén cumpliendo las restantes obligaciones derivadas de la LOPD. Como consecuencia, que el RGPD acepte la inscripción de un fichero no conlleva, en ningún caso, un reconocimiento por parte de la AEPD de cumplimiento de ninguna otra obligación establecida en la normativa vigente en materia de protección de datos. Tal y como se expresa la propia AEPD en sus notificaciones:

"*La inscripción de un fichero en el Registro General de Protección de Datos, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en la Ley Orgánica 15/1999, sin que se esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones revistas en dicha Ley y demás disposiciones reglamentarias*."

No por ello, debemos restar importancia al cumplimiento de la obligación de *notificar los ficheros* ya que permite dar publicidad de su existencia, poniendo a disposición de todos los ciudadanos, los ficheros en los que podrían encontrarse sus datos personales, facilitándoles de este modo el conocimiento de lo siguiente:

-. La totalidad de ficheros en los que podrían encontrarse sus datos personales.

-. La identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la identificación del nivel de medidas de seguridad básico, medio o alto exigible y, en su caso, la identificación del encargado de tratamiento donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

-. Los responsables ante los que pueden ejercitar los derechos de acceso, rectificación, cancelación u oposición.

Pero las ventajas de la inscripción registral no alcanzan únicamente a los ciudadanos, sino que se extienden tanto a la AEPD como a los propios responsables de los ficheros.

En relación con la AEPD, podemos destacar que la inscripción de los ficheros le permite disponer de una relación actualizada de los ficheros inscritos, facilitándole:

- el cumplimiento de la obligación de velar por la publicidad de la existencia de los ficheros de datos con carácter personal[§],

[§] Artículo 37.1. j) LOPD.

- el conocimiento de todos los ficheros que deben cumplir con las obligaciones establecidas en la LOPD y su normativa de desarrollo,

- el ejercicio de las actividades que la normativa le encomienda como Autoridad de Control y

- el ejercicio del derecho de consulta de los ciudadanos.

Desde la perspectiva del responsable de los ficheros, podemos apreciar las siguientes ventajas respecto de la inscripción de ficheros en el RGPD:

  - Evitar la imposición de sanciones.
  - Mostrar el compromiso o la intención de cumplir con la normativa de protección de datos.
  - Facilitar a los titulares de los datos contenidos en sus ficheros el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Como resumen de lo expuesto hasta el momento, podemos hacernos eco de los principios que rigen la inscripción de ficheros, recogidos en la Memoria de la AEPD del año 2000:

- El responsable del fichero deberá efectuar una notificación de un tratamiento de un conjunto de tratamientos.

- La inscripción de un fichero de datos no prejuzga que se hayan cumplido el resto de las obligaciones derivadas de la Ley.

- La notificación de ficheros implica el compromiso por parte del responsable de que el tratamiento de datos personales declarados para su inscripción cumple con todas las exigencias legales.

- La notificación de los ficheros al Registro supone una obligación de los responsables del tratamiento, sin coste económico alguno para ellos, y facilita que las personas afectadas puedan conocer quiénes son los titulares de los ficheros ante los que deben ejercitar directamente los derechos de acceso, rectificación, cancelación y oposición.

- Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la AEPD.

- En la notificación deberán figurar necesariamente el responsable del fichero, la finalidad del mismo, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

- Deberá comunicarse a la APD cualquier cambio que se produzca con respecto a la declaración inicial y particularmente en la finalidad del fichero, en su responsable y en la dirección de su ubicación.

- El RGPD inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

- Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la AEPD hubiera resuelto sobre la misma, se entenderá inscrito el fichero a todos los efectos.

¿Deben inscribirse los ficheros temporales?

El RLOPD recoge la primera definición legal de ficheros temporales en su artículo 5.2.g). En virtud de esta se entienden como tales los "*ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento*". *Estos ficheros* ***no tienen que inscribirse****, pero sí tiene que estar inscrito el fichero de origen.* En este sentido se ha pronunciado la AEPD, facilitando además algunos ejemplos:

"Ej. si se crea un fichero temporal para organizar las vacaciones del personal a partir del fichero de recursos humanos, tendrá que estar inscrito el fichero de recursos humanos. Respecto del fichero de vacaciones tendrán que adoptarse las medidas de seguridad correspondientes. Un fichero creado para realizar tratamientos de datos periódicos, **SI** que tendrá que inscribirse.

Ej. Censo agrario, preinscripción anual en un polideportivo, ….".

1.1. Ficheros de titularidad pública

Los ficheros de titularidad pública son definidos en el artículo 5.1.m) del RLOPD como "los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público", como por ejemplo los colegios profesionales.

En relación con estos ficheros hay que tener en cuenta las disposiciones sectoriales establecidas por la LOPD. Con base en las mismas, podemos afirmar que la creación de los ficheros de las Administraciones Públicas sólo podrá hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o diario oficial correspondiente -artículo 22 LOPD-. Dicha disposición deberá indicar:

- La finalidad del fichero y los usos previstos para el mismo.
- Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
- El procedimiento de recogida de los datos de carácter personal.
- La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
- Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
- Los órganos de las Administraciones responsables del fichero.
- Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
- Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

El artículo 55 del RLOPD, establece un plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente, para que todo fichero de datos de titularidad pública sea notificado a la AEPD para su inscripción en el RGPD.

Cuando la actividad relacionada con la finalidad del fichero no pueda ser considerada como “pública” en sentido estricto, este se considerará privado, como por ejemplo el fichero de formación de un colegio profesional, cuya finalidad es dar formación a los colegiados o terceras personas.

1.2. La calidad de los datos

El principio de calidad de los datos, establecido en el artículo 4 de la LOPD, regirá el tratamiento de los datos de carácter personal en todas sus fases, desde el momento previo a la recogida de los mismos hasta que se cesa en su tratamiento.

Con carácter previo a la recogida de los datos el responsable del fichero o tratamiento debe tener en cuenta que, únicamente, podrá recogerlos para su tratamiento, así como someterlos al mismo, cuando sean adecuados,

pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas de su obtención, estando prohibida su recogida por medios fraudulentos, desleales o ilícitos.

El artículo 8 del RLOPD desarrolla los principios relativos a la calidad de los datos. En concreto, en relación con el momento previo al tratamiento de los datos podemos destacar los principios de lealtad y licitud y finalidad. En relación con estos, no añade nada a lo ya dispuesto en la LOPD, recordando la prohibición de recoger datos por medios fraudulentos, desleales o ilícitos, así como la única circunstancia que legitima su recogida, es decir, el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

1.3. La información al interesado

El artículo 5 de la LOPD establece uno de los principios fundamentales que, junto al consentimiento, regirá el tratamiento de los datos de carácter personal:

"Derecho de información en la recogida de datos".

El derecho establecido en este principio a favor de los titulares de los datos se convierte en una obligación para los responsables de los ficheros, en virtud de la cual tiene que informar al interesado, con carácter previo a la recogida de sus datos de carácter personal sobre algunos aspectos relacionados con el tratamiento de los datos, de manera que el interesado pueda tener la suficiente información como para consentir el tratamiento de forma consciente y libre. El legislador ha considerado, con buen criterio, que para ello es necesario conocer:

- La existencia de un fichero o tratamiento de datos de carácter personal.
- La finalidad de la recogida de los datos.
- Los destinatarios de la información.
- El carácter obligatorio o facultativo de la respuesta a las preguntas planteadas a los titulares de los datos.

- Las consecuencias de la obtención de los datos o la negativa a suministrarlos.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Debemos plantearnos que no siempre los datos son recabados del propio titular o interesado, de manera que analizaremos a continuación las vías más habituales a través de las cuales se obtienen datos personales para insertarlos en un fichero:

Del propio interesado

Cuando los datos son recabados de sus titulares, habrá que facilitar directamente a los mismos la información detallada anteriormente.

De terceros

Cuando los datos hayan sido facilitados por persona distinta al titular de los mismos, el responsable del fichero dispone de un plazo de tres meses desde el momento del registro de los datos para facilitarle la información que le permita consentir el tratamiento de sus datos de forma libre y consciente. Como consecuencia, tendrá que informarle del contenido del tratamiento, la procedencia de los datos, la existencia de un fichero o tratamiento, la finalidad para la que se han recabado los datos, los destinatarios de la información, la posibilidad de ejercitar los derechos de acceso, rectificación y oposición, así como de la identidad y dirección del responsable del tratamiento o su representante. La propia LOPD estable excepciones a esta obligación, afirmando que no será de aplicación cuando:

A. El interesado ya hubiera sido informado con anterioridad.

B. Una Ley lo prevea **expresamente**. Es preciso aclarar esta excepción, ya que, en ocasiones nos encontramos con previsiones normativas que no tienen rango de Ley en las que se prevé el tratamiento o cesión de datos de carácter personal o preceptos legales en los que la excepción del deber de informar no es fruto de la interpretación literal del artículo, ya que no se recoge expresamente. Para la correcta aplicación de esta excepción han de darse dos requisitos: que la norma en la que se prevé el tratamiento o la cesión de datos tenga rango de Ley y, además, que dicho tratamiento o cesión haya sido recogido por el legislador de forma expresa. Así se desprende de un Informe emitido por la AEPD en el año 20048, en el que concluye que la excepción del artículo 5.5 a la que venimos haciendo referencia será aplicable a supuestos "*en que el tratamiento o cesión de los datos de carácter personal aparece recogido expresamente en una norma con rango de Ley, pero no a aquellos supuestos en que la Ley "autorice" o "habilite" la cesión de datos, pero no la recoja de modo expreso y taxativo en su articulado, sin perjuicio de que en dichos supuestos la cesión se encontrará amparada por lo dispuestos en los artículos 6.2 u 11.2 de la Ley Orgánica 15/1999*" [**].

C. El tratamiento tenga fines **históricos, estadísticos o científicos**.

D. La información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la AEPD o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Esta excepción sólo será posible a través de un acto administrativo de la AEPD en que se decida acerca de la procedencia o improcedencia de la excepción alegada en cada caso concreto. Dicho acto implicará la tramitación del

**
En el mismo sentido se pronunció la AEPD en una resolución de 8 de octubre de 2004: "*El artículo 5.5. también exceptúa de la obligación de informar cuando expresamente una Ley lo Prevea. De la interpretación literal del artículo resultaría que la obligación de informar debe estar expresamente exceptuada en una Ley para que se cumplan las condiciones previstas en este supuesto. Sin embargo la Directiva 95/46/CE, que ha sido transpuesta por la Ley 15/1999, en su artículo 11.2 especifica que no existe el deber de informar en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente previstos por ley, por lo que ha de interpretarse este supuesto de exclusión en los términos previstos en la Directiva, quedando excluida la obligación de informar cuando la cesión esté expresamente prevista en una Ley*".

correspondiente procedimiento administrativo, iniciado en todo caso por la propia solicitud del interesado.[††]

De fuentes de acceso público

Quizás convenga empezar preguntándose qué son fuentes de acceso público. Estas se encuentran definidas en el artículo 3.j) de la LOPD como aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Son, exclusivamente:

- El censo promocional.
- Las guías de teléfonos.
- Las listas de colegios profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo.

  El RLOPD, en su artículo 7 determina el alcance de las siguientes expresiones:

  - *Dirección profesional*: podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica.

  - *Datos de pertenencia al grupo:* considera como tales los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
- Los diarios y boletines oficiales.
- Los medios de comunicación social.

[††] Vid. AEPD, Informe Jurídico2002-0000 Procedimiento para la exención del deber de informar, https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/deber_informacion/common/pdfs/2002-0000_Procedimiento-para-la-exenci-oo-n-del-deber-de-informar.pdf

Se han planteado muchas dudas sobre si Internet es una fuente de acceso público. Con base en la definición, únicamente, podríamos considerarlo como tal si se encontrara incluido dentro de los medios de comunicación, pero a día de hoy los únicos medios de comunicación legalmente reconocidos son la prensa, la radio y la televisión. Como consecuencia de ello, podemos afirmar que **Internet**, como tal, **no es una fuente de acceso público**.

No obstante, a través de Internet podemos acceder a fuentes de acceso público. Por ejemplo, la lista de los profesionales pertenecientes a un colegio profesional no dejará de ser fuente de acceso público si accedemos a los datos a través de la página web del mismo. La AEPD ha confirmado esta interpretación, afirmando que "*Internet no es, a los efectos de protección de datos un "medio de comunicación social", sino un "canal de comunicación", por lo que no es fuente accesible al público"*.[‡‡]

Cuando los datos recabados en un fichero proceden de estas fuentes, el responsable tiene que informar al interesado de la procedencia de sus datos, la identidad y dirección del responsable del fichero o tratamiento y de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición. Información que acompañará cada comunicación que el responsable le realice.

En relación con el censo promocional o las listas de personas pertenecientes a grupos de profesionales, establece la LOPD (artículo 28) la limitación de incluir en dichas fuentes los datos estrictamente necesarios para cumplir la finalidad a que se destina cada listado, de manera que la inclusión de datos adicionales por las entidades responsables del mantenimiento de las mismas requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

Además, la LOPD establece los siguientes derechos a favor de los interesados:

- Respecto de los datos que consten en el censo promocional, a exigir gratuitamente la exclusión de la totalidad de los mismos por las entidades encargadas de su mantenimiento.

[‡‡] Vid. AEPD, I Sesión Anual Abierta de la AEPD "El nuevo reglamento de desarrollo de la ley orgánica de protección de datos: problemática, interpretación y aplicación", Madrid, 22 de abril de 2008, https:// www.agpd.es/portalweb/jornadas/1_sesion_abierta/common/faqs_bloque_1.pdf.

- En relación con los listados de los colegios profesionales, a que la entidad responsable de su mantenimiento indique gratuitamente que sus datos personales no podrán ser utilizados para fines de publicidad o prospección comercial.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique y, en el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, en el plazo de un año, contado desde el momento de su obtención.

Una vez tratada la información que debemos facilitar al titular de los datos en los supuestos más habituales de recogida de los mismos, podemos avanzar un poco más profundizando de forma muy somera pero clarificadora los extremos que, por resultar menos precisos o haber sido expresados de una forma muy genérica por el legislador, pueden dar lugar a dudas o interpretaciones erróneas.

En principio, parece que no tiene porqué generar problema alguno informar acerca de la identidad y dirección del responsable del tratamiento o su representante, la existencia de un fichero o tratamiento de datos de carácter personal, el carácter obligatorio o facultativo de la respuesta a las preguntas planteadas por el titular de los datos, las consecuencias de la obtención de los datos o la negativa a suministrarlos o la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación u oposición.

Por el contrario, consideramos oportuno desarrollar las siguientes expresiones en aras a aportar una mayor claridad en relación con la intención del legislador.

La finalidad de la recogida de los datos

Cuando el responsable de un fichero recaba datos para una finalidad específica, seguramente no le plantee ningún problema informar sobre la misma. No obstante, en la vida comercial, empresarial o profesional, no son pocos los casos en los que resulta muy importante para el responsable del fichero el uso de los datos para finalidades que exceden de una finalidad específica y fácil de definir. Desde que se ha establecido la relación inicial con el titular de los datos, lo más habitual y con tendencia ascendente, es que el responsable del fichero desee utilizar los datos con finalidades diferentes a la inicial. Entre las más comunes se encuentran la fidelización de clientes -basada en acciones como el envío de felicitaciones en fechas tan señaladas como Navidad, Año Nuevo o cumpleaños-, ofrecer otros productos o servicios que puedan resultar de interés -a través de campañas comerciales-, valorar la calidad de los productos o servicios prestados -utilizando encuestas de calidad o satisfacción-, enviar revistas informativas destinadas a lectores con un perfil predeterminado y hacer estudios de mercado de los gustos de los clientes.

Para el uso de los datos facilitados inicialmente con todas estas finalidades, lo que permitiría al responsable del fichero sacar un mayor aprovechamiento del mismo, traducido normalmente en un mayor beneficio económico, resulta imprescindible haber informado correctamente. Es a la hora de informar del uso de los datos para todas estas finalidades cuando el responsable del fichero puede encontrarse con problemas, principalmente, que el interesado se niegue a facilitar sus datos.

La experiencia nos ha aportado soluciones prácticas para solventar este problema, basadas en la redacción de cláusulas que, sin saltar las fronteras de lo legítimo, nos permiten ampliar y generalizar la finalidad para la que se recaban los datos.

Los destinatarios de la información

A medida que evoluciona la industria, el comercio e, incluso, la prestación de servicios por los profesionales, se extiende la colaboración con diversas personas, empresas o entidades en el desarrollo de un objeto social o actividad

legítima, fruto de la necesidad de recurrir a personas o empresas especializadas para cubrir carencias propias o abordar proyectos de mayor envergadura a la que una sola compañía puede hacer frente. En numerosas ocasiones, estas colaboraciones llevan implícita la necesidad de facilitar datos de carácter personal que constan en un fichero propio.

Si la LOPD no obligara a informar previamente al titular de los datos de los destinatarios de los mismos, correríamos el grave riesgo de que esto se convirtiera en una cadena de cesiones desconocidas para el afectado, rompiéndose de este modo su posibilidad de decisión acerca del tratamiento de sus datos personales, quebrando el derecho a la protección de los mismos. El ejemplo más claro en el que se producen constantemente este tipo de cesiones es entre las empresas pertenecientes a un mismo grupo.

No obstante, tal y como ha ocurrido con la finalidad de la recogida de los datos, en la práctica se han desarrollado soluciones que permiten que no resulte necesario dar una información detallada de cada destinatario de los datos que puede llegar a intervenir en el tratamiento de los mismos -nombre o razón social-, resultando suficiente informar acerca de la categoría de los destinatarios de la información y la finalidad de las cesiones.

Esta posibilidad se ha visto reforzado por el RLOPD, en el que el legislador ha manifestado de forma expresa que:

"*Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo*". [§§]

Forma que se debe adoptar para facilitar la información y acreditación del cumplimiento del deber de informar

§§ Artículo 12.2 RLOPD

La LOPD no impone a los responsables de ficheros o tratamientos forma alguna para facilitar al titular de los datos la información necesaria para el tratamiento de los mismos.

Lo más habitual y sencillo, a priori, es utilizar el mismo medio que se utiliza para la recogida de los datos también para facilitar la información. Si nos trasladamos a la práctica podemos afirmar que los sistemas de recogida de datos utilizados más frecuentemente son:

- **Oralmente.** En principio, teniendo en cuenta que la LOPD no impone a los responsables de ficheros o tratamientos forma alguna para informar al titular de los datos, sería suficiente con prestarlo de forma oral. Una alternativa es la colocación de carteles informativos en un lugar visible para las personas que facilitan los datos.
- **A través de formularios.** El artículo 5.2 de la LOPD establece expresamente que cuando se usen formularios o impresos para la recogida, figurará en los mismos la información necesaria, en forma claramente legible.
- **Contratos.** Si el titular de los datos firma un contrato se debe incluir en el mismo la información relativa al tratamiento de sus datos.
- **Telefónicamente**. Podría proporcionarse la información por el mismo medio, pero otra alternativa es enviar una comunicación posterior, aprovechando por ejemplo la entrega del producto adquirido por teléfono.

En la práctica, se venía recomendando adoptar siempre medios que permitan disponer de una prueba del cumplimiento de dicha obligación con fundamento en un Informe jurídico de la AEPD[***].

[***] Vid. AEPD, Informe Jurídico 0111/2005 *Prueba en relación con el cumplimiento del deber de información*, https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/deber_informacion/index-ides-idphp.php.

De este modo, a efectos de la Ley, será necesario que el responsable del tratamiento acredite la realización del envío, lo que sería posible tanto en el caso de que el envío se realice por el propio consultante como en caso de que el mismo se encomiende a una tercera empresa, que se certifique de algún modo la efectiva realización de los envíos, y exista un principio de prueba de que el envío efectivamente realizado ha llegado a su destino, lo que podría conseguirse, por ejemplo, mediante el acceso a las listas de devoluciones del servicio de correos.

El RLOPD -artículo 18- ha regulado de forma novedosa la acreditación del deber de informar, estableciendo el deber de utilizar un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado. Asimismo, el responsable deberá conservar el soporte en el que conste el cumplimiento del deber de informar, pudiendo utilizar medios informáticos o telemáticos para el almacenamiento de los soportes. Añade el legislador que, “en particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales”.

La información dirigida a los menores de edad

Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquellos.

Supuestos especiales

El artículo 19 del RLOPD ha introducido como novedad lo siguiente:

"*En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre".*

Consecuencia de ello, podemos afirmar que en los supuestos indicados en el precepto trascrito, habrá que **informar al titular** de los datos de los nuevos destinatarios de la información, adquiriendo también especial importancia la información relativa a la finalidad, dado que en principio, el tratamiento debe limitarse a la finalidad para la que se consintió inicialmente y ésta sólo podrá ampliarse en el caso de que se facilite la información acerca de nuevas finalidades y el afectado consienta el tratamiento de sus datos para las mismas.

1.4. El consentimiento del interesado

El principio del consentimiento del interesado, establecido en el artículo 6 de la LOPD, constituye una de las obligaciones principales en materia de protección de datos. Como norma general, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. Antes de seguir adelante, resulta conveniente detenerse en la definición de consentimiento del interesado, recogida en el artículo 3.K) de la LOPD: *"toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"* y analizar el significado de libre, inequívoco, específico en informado. Para ello, nada mejor que recurrir a la interpretación de la AEPD, expresada en un Informe jurídico emitido en el año 2000.

- **Libre**. Supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil.

- **Específico**. Referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.

- **Inequívoco**. Implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

- **Informado**. Requiere que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce. Precisamente por ello, el artículo 5.1 de la LOPD impone el deber de informar a los interesados de una serie de extremos que en el mismo se contienen. De este modo, el consentimiento se encuentra íntimamente relacionado con la información para la recogida de los datos, ya que para que se cumplan los requisitos del mismo el responsable del fichero o tratamiento debe informar previa y correctamente al titular de los datos de la existencia del fichero o tratamiento y de las finalidades para las que se destinarán los datos. Como consecuencia de ello, la solicitud de consentimiento debe referirse a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para la que se recaban los datos y las restantes condiciones que concurran en el tratamiento o serie de tratamientos. Así lo ha recogido el RLOPD en su artículo 12.1.

No obstante, la propia LOPD establece excepciones a la obligación de obtener el consentimiento para el tratamiento de los datos de carácter personal, en concreto:

A. Que la Ley disponga otra cosa.

B. Que los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.

C. Que los datos se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

D. Que el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado, cuando dicho tratamiento resulte necesario para la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

E. Que los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

En estos casos, en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y, siempre que una Ley no disponga lo contrario, la LOPD concede al mismo la posibilidad de oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.

Revocación del consentimiento

El derecho del titular de los datos a **revocar el consentimiento** prestado para el tratamiento de sus datos ha sido reconocido por el legislador en la LOPD, a través de los artículos 6.3, en el que se recoge expresamente este derecho[†††] y 16.1, en el que se establece la obligación para el responsable del tratamiento de hacer efectivo el derecho del titular de los datos a que sean cancelados, lo

[†††] Art. 6.3 de la LOPD: *"El consentimiento a que se refiere el artículo podrá ser revocado cuando exista* ***causa justificada*** *para ello y no se le atribuyan efectos retroactivos"*

que conlleva la imposibilidad para el responsable de continuar en el tratamiento consentido anteriormente.

Asimismo, en el artículo 11.4 se reconoce expresamente el derecho del titular de los datos a **revocar el consentimiento** prestado para la cesión de los mismos[‡‡‡].

El RLOPD -artículo 17- ha desarrollado la revocación del consentimiento en relación con la forma de llevarlo a cabo, estableciendo la posibilidad de realizarlo a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En concreto, reconoce como medios adecuados un envío franqueado al responsable del tratamiento o, incluso, la llamada a un número de teléfono gratuito o a los servicios de atención al público establecidos por el mismo.

Por el contrario, no se considerarán conformes a lo dispuesto en la LOPD, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

Las consecuencias que implica la revocación del consentimiento para el responsable del tratamiento se detallan a continuación:

- Cesar en el tratamiento de los datos del interesado en un plazo máximo de diez días a contar desde la fecha de la recepción de la revocación.
- Si el interesado hubiera solicitado la confirmación del cese en el tratamiento de sus datos, deberá responder expresamente a la solicitud.
- Si los datos hubieran sido cedidos previamente, deberá comunicar la revocación del consentimiento a los cesionarios, en el plazo indicado en el punto anterior, para que éstos cesen en el tratamiento de los datos en caso de que aún lo mantuvieran.

‡‡‡ Art. 11.4 de la LOPD: *"El consentimiento para la comunicación de los datos de carácter personal tiene también un **carácter revocable**".*

Forma de prestar el consentimiento

Teniendo en cuenta que la LOPD establece la necesidad de manifestar el consentimiento de forma expresa y por escrito, únicamente, para el tratamiento de algunos tipos de datos, podemos afirmar que, como norma general, admite el consentimiento tácito. Dentro del consentimiento inequívoco que exige para el tratamiento de los datos de carácter personal, distingue tres categorías de consentimiento en función de los datos objeto de tratamiento:

- **Tácito**. Suficiente para el tratamiento de todos los datos, salvo los especialmente protegidos -ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual-. En este sentido se ha pronunciado la AEPD en un informe jurídico reciente[§§§] afirmando que:

"El consentimiento, salvo cuando el tratamiento se refiera a los datos especialmente protegidos, regulados por el artículo 7 de la Ley Orgánica, podrá obtenerse de forma expresa o tácita, es decir, tanto como consecuencia de una afirmación específica del afectado en ese sentido, como mediante la falta de una manifestación contraria al tratamiento, para la que se hayan concedido mecanismos de fácil adopción por el afectado y un tiempo prudencial para dar la mencionada respuesta negativa".

- **Expreso**. En función de lo establecido en el artículo 7.2 de la LOPD, los datos de carácter personal que revelan la ideología, afiliación sindical, religión y creencias del afectado sólo podrán ser tratados con su consentimiento expreso y por escrito, salvo en los casos de ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros.

[§§§] Vid. AEPD, Informe Jurídico 93/2008 *Formas de obtener el consentimiento mediante web: Consentimientos tácitos*, https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/consentimiento/index-ides-idphp.php.

- **Expreso y por escrito**. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente. Así se desprende del artículo 7.2 de la LOPD.

Teniendo en cuenta que corresponde al responsable del tratamiento la prueba de la existencia del consentimiento del titular de los datos para su tratamiento, por cualquier medio de prueba admisible en derecho, a pesar de no resultar necesario, lo más recomendable es disponer del consentimiento expreso y por escrito.

El responsable del tratamiento podrá solicitar el consentimiento del interesado para el tratamiento de sus datos de carácter personal a través del procedimiento establecido en el artículo 14 del RLOPD, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos, en virtud del cual, una vez que el responsable ha informado al afectado, deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. En concreto, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

Finalmente, el RLOPD establece que cuando se solicite el consentimiento del interesado a través de este procedimiento, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar desde la fecha de la anterior solicitud.

Consentimiento para el tratamiento de los datos de menores de edad

Una novedad importante del RLOPD es la regulación del consentimiento para el tratamiento de los datos de menores de edad -ya que nada se regula al respecto en la LOPD-, estableciendo la edad de catorce años para poder consentir en el tratamiento de los datos de carácter personal, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

No obstante, se establece una limitación para el responsable del fichero o tratamiento en relación con los datos que se pueden obtener del menor, ya que en ningún caso podrán recabarse a través de este datos que permitan obtener información sobre los demás miembros del grupo familiar o las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. Únicamente podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización de los mismos para el tratamiento de los datos.

Finalmente, se impone al responsable del fichero o tratamiento la obligación de articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. En algunos supuestos, como el de obtención de los datos a través de una página web, parece difícil articular un sistema que permita al responsable disponer de esta garantía. Para este caso concreto la AEPD ha propuesto y admitido como válida la opción de poner una casilla en la que se deba indicar la edad en la que resulte imposible introducir una fecha más antigua a dieciocho años desde la fecha[****].

[****] Vid. AEPD, I Sesión Anual Abierta de la AEPD "El nuevo reglamento de desarrollo de la ley orgánica de protección de datos: problemática, interpretación y aplicación", Madrid, 22 de abril de 2008, https:// www.agpd.es/portalweb/jornadas/1_sesion_abierta/index-ides-idphp.php.

2. Durante el tratamiento de los datos

2.1. La calidad de los datos

De nuevo está presente el principio de calidad de los datos que, si bien no se puede olvidar en ninguna de las fases en las que hemos dividido el tratamiento de los mismos, adquiere especial relevancia en este momento.

En virtud de lo establecido en el artículo 4 de la LOPD, los datos personales:

A) No pueden usarse para finalidades incompatibles con aquellas para las que se han recogido
B) Tienen que ser exactos y puestos al día, de forma que respondan con veracidad a la situación actual de su titular y
C) Tienen que ser almacenados de forma que permitan el ejercicio del derecho de acceso.

El uso de los datos en relación con la finalidad para la que se obtuvieron. En virtud de lo establecido en el artículo 4 de la LOPD, los datos de carácter personal objeto de tratamiento no pueden usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos y no se considerarán como tales el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Después de esta afirmación, parece casi inevitable detenerse a analizar la expresión “finalidades incompatibles”, utilizada por primera vez en la LOPD, suponiendo un cambio de redacción respecto del artículo 4 de la LORTAD, en el que se establecía que los datos no podrían usarse para “finalidades distintas” a aquellas para las que hubieran sido recogidos. La utilización del término incompatibles puede suponer un peligro para el respeto al derecho a la protección de datos por parte de los responsables de los ficheros y tratamientos, ya que interpretando el término incompatible en su sentido estricto, pocas finalidades resultarían incompatibles con aquella para la que se obtuvieron los datos.

Debemos seguir interpretando este principio como la imposibilidad de uso de datos para finalidades distintas, tal y como se recogía en la LORTAD, ya que así lo ha interpretado el Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, que viene a identificar el citado término con "fines distintos".

Así, dispone la citada sentencia en su Fundamento Jurídico 5 que "La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático («habeas data») y comprende, entre otros aspectos, la posición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, F. 5, 94/1998, F. 4)".

Asimismo, la sentencia vuelve a interpretar este precepto cuando indica que "la cesión de los mismos (datos) a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos (art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado"[††††].

La AEPD reproduce esta interpretación en su informe jurídico 0078/2005: "Tratamiento de datos para fines incompatibles"[‡‡‡‡].

[††††] Este argumento es reiterado en el posterior Fundamento Jurídico 14.

[‡‡‡‡] Vid. AEPD, Informe Jurídico 0078/2005 *Tratamiento de datos para fines incompatibles*, https:// www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/consentimiento/index-ides-idphp.php.

La propia LOPD afirma que no se considerará incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos y el artículo 9 RLOPD desarrolla el tratamiento de los datos con estos fines, estableciendo que para la determinación de los mismos se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

Exactitud de los datos

Los datos de carácter personal objeto de tratamiento tienen que ser exactos y puestos al día de forma que respondan con veracidad a la situación actual de su titular, de manera que si los datos registrados resultan inexactos, en todo o en parte, o incompletos, el responsable del fichero o tratamiento se verá obligado a cancelarlos y sustituirlos de oficio por los correspondientes datos rectificados o completados.[§§§§]

Ejercicio del derecho de acceso

Los datos de carácter personal tienen que ser almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados. Este derecho será desarrollado en el apartado 5.4.1.

[§§§§] La Jurisprudencia ha tenido ocasión de analizar el alcance de este principio en las siguientes sentencias: Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 6 de julio de 2001; Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 5 de noviembre de 1998; Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 18 de octubre de 2000; Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 26 de mayo de 1999; Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 19 de enero de 2001; Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 9 de febrero de 2000; Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 9 de marzo de 2001.

2.2. El deber de secreto

El deber de secreto es uno de los principios básicos en materia de protección de datos de carácter personal, establecido en el artículo 10 de la LOPD.

Al margen del deber de secreto profesional establecido en relación con algunas profesiones, tales como la abogacía o la medicina, la LOPD establece una obligación de guardar secreto que afecta, no sólo al responsable del fichero, sino a todas las personas que intervienen en cualquier fase del tratamiento de los datos de carácter personal, con independencia de la actividad profesional de cada una de ellas. En concreto, establece el sometimiento al secreto profesional respecto de los datos de carácter personal y al deber de guardarlos.

Al margen de las sanciones en materia de protección de datos en las que pudiera derivar la vulneración de este principio, es importante tener en cuenta que la revelación de secretos se encuentra tipificada como delito en el Código Penal -artículos 197 a 200-, castigando el apoderamiento, utilización o modificación de datos de carácter personal o familiar de un tercero que se encuentren registrados en ficheros o soporte informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo o registro público o privado, sin autorización y en perjuicio de tercero.
Del mismo modo, se castiga a los que accedan a los mismos por cualquier medio, sin autorización, así como a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Para evitar sanciones de la AEPD como consecuencia de la vulneración de este principio por parte de los usuarios de los datos, se recomienda al responsable del fichero o tratamiento establecer por escrito una política de información y formación con el objetivo de ponerles en conocimiento de sus funciones y obligaciones en materia de protección de datos personales.

2.3. La seguridad de los datos

Este principio, establecido en el artículo 9 de la LOPD, impone al responsable del fichero, todos los posibles encargados del tratamiento y todas las personas que intervienen en el mismo, la obligación de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. De este modo, no se podrán registrar datos de carácter personal en ficheros que no reúnan las condiciones determinadas por el RLOPD con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

El RLOPD dedica todo su Título VIII al desarrollo de las medidas de seguridad en el tratamiento de datos de carácter personal, estableciendo unas disposiciones generales -relativas a todos los ficheros o tratamientos de datos de carácter personal, independientemente del soporte en el que se encuentren- y las medidas de seguridad aplicables con carácter específico a los ficheros y tratamientos automatizados y manuales, respectivamente.

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles (básico, medio y alto), definidos en función del tipo de datos contenidos en dichos ficheros o sometidos a tratamiento.

Las medidas incluidas en cada uno de estos niveles tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

A. Nivel básico.

Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

Las medidas de seguridad aplicables para los ficheros y tratamiento de datos de nivel básico son las que se detallan a continuación:

1. Para todos los ficheros (automatizados o no).

1.a. Personal.

- Definir las funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios.
- Definir las funciones de control y las autorizaciones delegadas por el responsable.
- Difundir entre el personal, de las normas que les afecten y las consecuencias por su incumplimiento.

1.b. Incidencias.

- Llevar un registro de incidencias en el que se detalle: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras.
- Elaborar un procedimiento de notificación y gestión de las incidencias.

1.c. Control de acceso.

- Disponer de una relación actualizada de usuarios y accesos autorizados.
- Controlar los accesos permitidos a cada usuario según las funciones asignadas.
- Implantar mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- Conceder permisos de acceso sólo el personal autorizado.

- Adoptar las mismas medidas para personal ajeno con acceso a los recursos de datos.

1.d. Gestión de soportes.

- Crear un inventario de soportes.
- Identificar el tipo de información que contienen los soportes.
- Restringir el acceso al lugar de almacenamiento de los soportes.
- Autorizar las salidas de soportes (incluidas a través de e-mail).
- Implantar medidas para el transporte y el desecho de soportes.

2. Solo para ficheros automatizados.

2.a. Identificación y autenticación.

- Implantar mecanismos de identificación y autenticación personalizada de los usuarios.
- Crear un procedimiento de asignación y distribución de contraseñas.
- Almacenar las contraseñas de forma ininteligible.
- Cambiar las contraseñas con una periodicidad mínima de 1 año.

2.b. Copias de respaldo.

- Hacer una copia de respaldo semanal.
- Establecer procedimientos de generación de copias de respaldo y recuperación de datos.
- Verificar semestralmente los procedimientos.
- Reconstruir los datos a partir de la última copia o grabarlos manualmente en su caso, si existe documentación que lo permita.
- Realizar copia de seguridad y aplicar el nivel de seguridad correspondiente, si se realizan pruebas con datos reales.

3. Solo para ficheros no automatizados.

3.a. Criterios de archivo.

- El archivado de documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3.b. Almacenamiento.

- Dotar a los dispositivos de almacenamiento de mecanismos que obstaculicen su apertura.

3.c. Custodia de soportes.

- Establecer criterios de diligente y custodia de la documentación por parte de la persona a cargo de la misma, durante su revisión tramitación, para evitar accesos no autorizados.

B. Nivel medio.

Además de las medidas de seguridad de nivel básico, deberán implantarse las de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Los relacionados con la prestación de servicios de información sobre solvencia patrimonial y crédito.
- Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

- Aquellos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad del comportamiento de los mismos.

Las medidas de seguridad aplicables para los ficheros y tratamiento de datos de nivel medio son las que se detallan a continuación:

1. Para todos los ficheros (automatizados o no).

1.a. Personal.

- Definir las funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios.
- Definir de las funciones de control y las autorizaciones delegadas por el responsable
- Difundir entre el personal, de las normas que les afecten y las consecuencias por su incumplimiento.

1.b. Incidencias.

- Llevar un registro de incidencias en el que se detalle: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras
- Elaborar un procedimiento de notificación y gestión de las incidencias.

1.c. Control de acceso.

- Disponer de una relación actualizada de usuarios y accesos autorizados.
- Controlar los accesos permitidos a cada usuario según las funciones asignadas.

- Implantar mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- Conceder permisos de acceso sólo el personal autorizado.
- Adoptar las mismas medidas para personal ajeno con acceso a los recursos de datos.

1.d. Gestión de soportes.

- Crear un inventario de soportes.
- Identificar el tipo de información que contienen los soportes.
- Restringir el acceso al lugar de almacenamiento de los soportes.
- Autorizar las salidas de soportes (incluidas a través de e-mail).
- Implantar medidas para el transporte y el desecho de soportes.

1.e. Auditoría.

- Realizar una auditoría, interna o externa, al menos cada dos años.
- Realizar una auditoría ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad, pese a no haber transcurrido el plazo indicado en el punto anterior.
- Verificar y controlar la adecuación de las medidas de seguridad implantadas.
- Emitir un informe de las detecciones de deficiencias y propuestas correctoras.
- Analizar el informe del responsable de seguridad y remitir las conclusiones al responsable del fichero.

2. Sólo para ficheros automatizados.

2.a. Gestión de soportes.

- Registrar la entrada y salida de soportes en el que se detalle: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega.

2.b. Identificación y autenticación.

- Implantar mecanismos de identificación y autenticación personalizada de los usuarios.
- Crear un procedimiento de asignación y distribución de contraseñas.
- Almacenar las contraseñas de forma ininteligible.
- Cambiar las contraseñas con una periodicidad mínima de 1 año.

2.c. Copias de respaldo.

- Hacer una copia de respaldo semanal.
- Establecer procedimientos de generación de copias de respaldo y recuperación de datos.
- Verificar semestralmente los procedimientos.
- Reconstruir los datos a partir de la última copia o grabarlos manualmente en su caso, si existe documentación que lo permita.
- Realizar copia de seguridad y aplicar el nivel de seguridad correspondiente, si se realizan pruebas con datos reales.

3. Solo para ficheros no automatizados.

3.a. Criterios de archivo.

- El archivado de documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3.b. Almacenamiento.

- Dotar a los dispositivos de almacenamiento de mecanismos que obstaculicen su apertura.

3.c. Custodia de soportes.

- Establecer criterios de diligente y custodia de la documentación por parte de la persona a cargo de la misma, durante su revisión tramitación, para evitar accesos no autorizados.

C. Nivel alto.

En los siguientes ficheros o tratamientos de datos de carácter personal, además de las medidas de nivel básico y medio, se aplicarán las medidas de nivel alto:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquéllos que contengan datos derivados de actos de violencia de género.

Las medidas de seguridad aplicables para los ficheros y tratamiento de datos de nivel básico son las que se detallan a continuación:

1.- Para todos los ficheros (automatizados o no).

1.a. Personal.

- Definir las funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios.
- Definir de las funciones de control y las autorizaciones delegadas por el responsable
- Difundir entre el personal, de las normas que les afecten y las consecuencias por su incumplimiento.

1.b. Incidencias.

- Llevar un registro de incidencias en el que se detalle: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras
- Elaborar un procedimiento de notificación y gestión de las incidencias.

1.c. Control de acceso.

- Disponer de una relación actualizada de usuarios y accesos autorizados.
- Controlar los accesos permitidos a cada usuario según las funciones asignadas.
- Implantar mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados.
- Conceder permisos de acceso sólo el personal autorizado.
- Adoptar las mismas medidas para personal ajeno con acceso a los recursos de datos.

1.d. Gestión de soportes.

- Crear un inventario de soportes.
- Identificar el tipo de información que contienen los soportes, utilizando un sistema de etiquetado que dificulte la identificación para las personas diferentes de los usuarios.
- Restringir el acceso al lugar de almacenamiento de los soportes.
- Autorizar las salidas de soportes (incluidas a través de e-mail).
- Implantar medidas para el transporte y el desecho de soportes.
- Cifrar los datos en la distribución de soportes.
- Cifrar la información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).

1.e. Auditoría.

- Realizar una auditoría, interna o externa, al menos cada dos años.
- Realizar una auditoría ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad, pese a no haber transcurrido el plazo indicado en el punto anterior.
- Verificar y controlar la adecuación de las medidas de seguridad implantadas.
- Emitir un informe de las detecciones de deficiencias y propuestas correctoras.

- Analizar el informe del responsable de seguridad y remitir las conclusiones al responsable del fichero.

2.- Sólo para ficheros automatizados.

2.a. Registro de accesos. (No resulta de aplicación si el responsable del fichero es una persona física y es el único usuario.)

- Llevar un registro de accesos en el que se haga constar: usuario, hora, fichero, tipo de acceso, autorizado o denegado.
- Revisar el responsable de seguridad el registro de accesos mensualmente y elaborar un informe con toda la información.
- Conservar la información del registro de accesos al menos 2 años.

2.b. Gestión de soportes.

- Registrar la entrada y salida de soportes en el que se detalle: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega.

2.c. Identificación y autenticación.

- Implantar mecanismos de identificación y autenticación personalizada de los usuarios.
- Crear un procedimiento de asignación y distribución de contraseñas.
- Almacenar las contraseñas de forma ininteligible.
- Cambiar las contraseñas con una periodicidad mínima de 1 año.

2.d. Copias de respaldo.

- Hacer una copia de respaldo semanal.
- Establecer procedimientos de generación de copias de respaldo y recuperación de datos
- Verificar semestralmente los procedimientos.
- Reconstruir los datos a partir de la última copia o grabarlos manualmente en su caso, si existe documentación que lo permita.

- Realizar copia de seguridad y aplicar el nivel de seguridad correspondiente, si se realizan pruebas con datos reales.
- Conservar una copia de respaldo en lugar diferente del que se encuentren los equipos informáticos que los tratan.

3. Solo para ficheros no automatizados.

3.a. Control de acceso.

- Limitar el acceso al personal autorizado.
- Establecer mecanismos que permitan identificar los accesos a documentos accesibles por múltiples usuarios.

3.b. Criterios de archivo.

- El archivado de documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3.c. Almacenamiento.

- Dotar a los dispositivos de almacenamiento de mecanismos que obstaculicen su apertura.
- Localizar los armarios, archivadores u otros elementos donde se almacenen los ficheros en áreas con acceso protegido con puertas con llave u otro dispositivo equivalente.

3.d. Custodia de soportes.

- Establecer criterios de diligente y custodia de la documentación por parte de la persona a cargo de la misma, durante su revisión o tramitación, para evitar accesos no autorizados.

3.e. Copia o reproducción.

- Limitar la posibilidad de realización a los usuarios autorizados.
- Destruir las copias desechadas.

Como resumen de las medidas de seguridad aplicables a los ficheros o tratamientos de datos de carácter personal, haremos uso de un cuadro extraído de la Guía de Seguridad creada por la AEPD en abril de 2008*****

	Nivel Básico	Nivel Medio	Nivel Alto
Responsable de seguridad		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
Personal	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
Incidencias	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	**SOLO FICHEROS AUTOMATIZADOS** Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	

*****
Vid. AEPD *Guía de Seguridad*, https://www.agpd.es/portalweb/canalresponsable/guia_documento/common/pdfs/guia_seguridad.pdf.

	Nivel Básico	Nivel Medio	Nivel Alto
Control de acceso	▯Relación actualizada de usuarios y accesos autorizados. ▯Control de accesos permitidos a cada usuario según las funciones asignadas. ▯Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. ▯Concesión de permisos de acceso sólo por personal autorizado. ▯Mismas condiciones para personal ajeno con acceso a los recursos de datos.	**SOLO FICHEROS AUTOMATIZADOS** ▯Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	**SOLO FICHEROS AUTOMATIZADOS** ▯Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. ▯Revisión mensual del registro por el responsable de seguridad. ▯Conservación 2 años. ▯No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. **SOLO FICHEROS NO AUTOMATIZADOS** ▯Control de accesos autorizados. ▯Identificación accesos para documentos accesibles por múltiples usuarios.
Identificación de usuarios	**SOLO FICHEROS AUTOMATIZADOS** ▯Identificación y autenticación personalizada. ▯Procedimiento asignación y distribución de contraseñas. ▯Almacenamiento ininteligible de contraseñas. ▯Periodicidad del cambio de contraseñas (>1 año).	**SOLO FICHEROS AUTOMATIZADOS** ▯Límite de intentos reiterados de acceso no autorizado.	
Gestión de soportes	▯Inventario de soportes. ▯Identificación del tipo de información que contienen, o sistema de etiquetado. ▯Acceso restringido al lugar de almacenamiento. ▯Autorización de las salidas de soportes (incluidas a través de e-mail). ▯Medidas para el transporte y el desecho de soportes.	**SOLO FICHEROS AUTOMATIZADOS** ▯Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizada para recepción/entrega.	**SOLO FICHEROS AUTOMATIZADOS** ▯Sistema de etiquetado confidencial. ▯Cifrado de datos en la distribución de soportes. ▯Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado).

	Nivel Básico	Nivel Medio	Nivel Alto
Copias de respaldo	**SOLO FICHEROS AUTOMATIZADOS** Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		**SOLO FICHEROS AUTOMATIZADOS** Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
Criterios de archivo	**SOLO FICHEROS NO AUTOMATIZADOS** El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos ARCO.		
Almacenamiento	**SOLO FICHEROS NO AUTOMATIZADOS** Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		**SOLO FICHEROS NO AUTOMATIZADOS** Armarios, archivadores,… de documentos en áreas con acceso protegido con puertas con llave.
Custodia soportes	**SOLO FICHEROS NO AUTOMATIZADOS** Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
Copia o reproducción			**SOLO FICHEROS NO AUTOMATIZADOS** Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.

	Nivel Básico	Nivel Medio	Nivel Alto
Auditoría		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones al responsable del fichero.	
Telecomunicaciones			**SOLO FICHEROS AUTOMATIZADOS** Transmisión de datos a través de redes electrónicas cifrada.
Traslado de documentación			**SOLO FICHEROS NO AUTOMATIZADOS** Medidas que impidan el acceso o manipulación.

El RLOPD establece, además, algunos supuestos especiales en relación con las medidas de seguridad aplicables a los ficheros o tratamientos, en concreto, relativas a los siguientes:

A. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento"[†††††].

[†††††] Artículo 103 del RLOPD: "*Registro de accesos.*
1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

B. Ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. En relación con estos, será suficiente la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. Por ejemplo, la detracción de la cuota sindical de la nómina a petición del empleado.
- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

AEPD ha emitido un Informe Jurídico, relativo a las medidas de seguridad en los ficheros de nóminas y demás especialidades, en respuesta a la consulta planteada por un responsable de ficheros[‡‡‡‡‡].

C. Ficheros o tratamientos que contengan datos relativos a la salud referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado. Del mismo modo que en el caso anterior, resultará suficiente la implantación de las medidas de seguridad de nivel básico, en los ficheros o tratamientos que contengan este tipo de datos, únicamente, con motivo del cumplimiento de deberes públicos (desarrollado en el apartado 3.2). Con el fin de facilitar la implantación de las medidas de seguridad, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto o de la naturaleza de los datos que contengan, requieran la aplicación

---

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

‡‡‡‡‡ Vid. AEPD, Informe Jurídico 0156/2008 *Medidas de seguridad en los ficheros de nóminas y demás especialidades*, https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/common/pdfs/2008-0156_Medidas-de-seguridad-en-los-ficheros-de-n-oo-minas-y-dem-aa-s-especialidades.pdf.

de un nivel de medidas de seguridad diferente al del sistema principal, el propio RLOPD otorga al responsable del fichero la posibilidad de segregar este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos.

Productos de software.

En relación con las medidas de seguridad aplicables a los ficheros de datos de carácter personal, la disposición adicional única del RLOPD introduce una novedad, imponiendo una obligación a las empresa que desarrollan productos de software destinados al tratamiento automatizado de datos personales, que deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar dichos productos.

Por ello, todas las aplicaciones de software que utilicemos en nuestras organizaciones para el tratamiento de ficheros de datos de carácter personal deberán acreditar el nivel de seguridad que permiten alcanzar y deberemos evaluar si el mismo es suficiente de acuerdo con el nivel de seguridad que requiera cada fichero.

Si no es así, deberemos sustituir la aplicación por otra que sí nos permita implementar las medidas de seguridad adecuadas. Asimismo, esta materia deberá ser incluida en la Auditoría bienal de aquellas organizaciones que posean ficheros de nivel medio o alto.

2.4. La cesión de los datos

Como punto de partida, debemos saber que la LOPD -artículo 3.i)- define la cesión o comunicación de datos como “toda revelación de datos realizada a una persona distinta del interesado”, regulándola en su artículo 11. Como principio rector, los datos de carácter personal sólo podrán cederse si se cumplen dos requisitos:

- Que se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
- Consentimiento previo del interesado.

No obstante, existen algunos supuestos en los que no se exige el segundo requisito: consentimiento del interesado. El apartado segundo del citado precepto los recoge expresamente:

- Cuando la cesión está autorizada en una Ley.

  Tradicionalmente, se ha discutido mucho sobre la posibilidad de interpretar esta excepción en sentido amplio, considerando que la cesión de datos puede encontrarse amparada por una norma con rango inferior al de Ley, pero la AEPD ha sentado a través de numerosos informes y resoluciones el criterio de que la interpretación de la misma ha de hacerse en sentido estricto y, únicamente, admite la aplicación de esta excepción cuando la cesión se encuentra recogida en una norma con rango de Ley o superior.

  El RLOPD -artículo 10.2.a)- ha desarrollado esta excepción añadiendo la posibilidad de que se encuentra autorizada en una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

  "El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.
  El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas."

- Cuando se trate de datos recogidos de fuentes accesibles al público.

En virtud de lo establecido en el artículo 10.2.b) del RLOPD podrá realizarse una cesión amparada en esta excepción cuando el tercero a quien se comuniquen los datos tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

No obstante, las Administraciones públicas sólo podrán comunicar al amparo de la misma los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.

- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

- Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. En relación con esta excepción, el RLOPD -artículo 10.4- ha recogido dos nuevos supuestos:

    - Que los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.
    - Que la comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Añade el artículo 10.5 del RLOPD que*: "En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud."*

Es importante indicar que el destinatario o cesionario, definido en el propio RLOPD como la persona física o jurídica, pública o privada, órgano administrativo o ente sin personalidad jurídica que actúa en el tráfico como sujeto diferenciado al que se revelen los datos, se obliga, por el solo hecho de la comunicación, al cumplimiento de la LOPD y su normativa de desarrollo.

Cesión o comunicación de datos entre empresas del mismo grupo.

Respecto de los grupos de empresas, es importante aclarar que la AEPD considera que las comunicaciones de datos realizadas entre las empresas integrantes de un mismo grupo se consideran cesiones a terceros, sometidas a los requisitos descritos. Como consecuencia, no se considera válido el consentimiento obtenido mediante cláusulas genéricas que se limiten a recoger el consentimiento para la cesión de datos a empresas del grupo.

La AEPD emitió en el año 2004 un informe jurídico[§§§§§], como respuesta a una consulta en la que se planteaba si resultaba conforme a derecho el tratamiento y comunicación de datos entre las empresas de un mismo grupo con fines de publicidad y promoción, en el que tras analizar la cláusula utilizada para la obtención del consentimiento, concluye considerar la cesión como ajustada a derecho porque dicha cláusula incluía todos los requisitos exigidos en el artículo 5.1 de la LOPD, lo que implica que el consentimiento ha sido otorgado válidamente.

2.5. El acceso a datos por cuenta de terceros

La LOPD define al encargado de tratamiento en el artículo 3.g) como:

"La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" y el artículo 5.1.i) del RLOPD se expresa en los siguientes términos: "La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".

La AEPD reproduce la doctrina de la Audiencia Nacional sobre el alcance de este concepto en su Informe jurídico 0309/2008[******], clarificando el significado de encargado de tratamiento y su alcance. Así, la Sentencia de 28 de septiembre de 2005 recuerda que:

§§§§§ Vid. AEPD, Informe Jurídico 325/2004 *Comunicación de datos entre empresas de un mismo grupo*, https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2004-0325_Comunicaci-oo-n-de-datos-entre-empresas-de-un-mismo-grupo.pdf.

****** Vid. AEPD, Informe Jurídico 0309/2008 *Los ensobrados y recepción de direcciones de personas físicas para efectuar envíos configura a la empresa como encargado de tratamiento*, https://212.170.242.196/portalweb/canaldocumentacion/informes_juridicos/conceptos/common/pdfs/2008-0309_Los-ensobrados-yrecepci-oo-n-de-direcciones-de-personas-f-ii-sicas-para-efectuar-env-ii-os-configura-a-la-empresa-comoencargado-del-tratamiento.pdf.

"La diferencia entre encargado del tratamiento y cesión en algunos casos reviste cierta complejidad, pero como ha señalado esta Sección en la reciente sentencia de 12 de abril de 2005 (recurso 258/2003) lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquél con objeto de prestarle un servicio en un ámbito concreto..... Siendo esencial para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargado. En suma, existe encargo de tratamiento cuando la transmisión o cesión de datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado".

En consecuencia, para determinar si nos encontramos en presencia de un encargado del tratamiento deberá analizarse si su actividad se encuentra limitada a la mera prestación de un servicio al responsable, sin generarse ningún vínculo entre el afectado y el supuesto encargado. Además, será preciso que corresponda al responsable el poder de decisión sobre la finalidad que justifica el tratamiento, de manera que si el tratamiento procede de la voluntad del encargado, este tendrá en todo caso la condición de responsable.

Se entenderá que una empresa es encargada del tratamiento cuando no puede decidir sobre el contenido, finalidad y uso del tratamiento y siempre que su actividad no le reporte otro beneficio que el derivado de la prestación de servicios propiamente dicha, sin utilizar los ficheros generados en modo alguno en su provecho, puesto que en ese caso pasaría a ser responsable del fichero.

El artículo 12 de la LOPD regula el acceso a datos por cuenta de terceros. En cumplimiento de lo establecido en el mismo, las prestaciones de servicios al responsable de los ficheros que impliquen un acceso a datos de carácter personal contenidos en los mismos, deben regularse a través de un contrato escrito en el que se establezcan los términos en los que se producirá el citado acceso o tratamiento de datos personales.

El servicio prestado podrá tener o no carácter remunerado y ser temporal o indefinido. El contrato deberá recoger, como mínimo, el siguiente contenido:

- Obligación del encargado del tratamiento de tratar los datos conforme a las instrucciones del responsable del fichero o tratamiento.
- Prohibición de utilizar los datos con fin distinto al que figura en el contrato.
- Prohibición de comunicar los datos a terceras personas, ni siquiera para su conservación.
- Medidas de seguridad que, en virtud del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en adelante, RLOPD), el encargado del tratamiento está obligado a cumplir en el tratamiento de los datos personales.
- Obligación de devolver los datos al responsable del fichero o destruirlos una vez concluida la prestación contractual.
- Responsabilidades del encargado del tratamiento por incumplimiento de las anteriores obligaciones, en cuyo caso será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

El RLOPD recoge que se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado, así como la obligación del responsable del tratamiento de velar por que el encargado del mismo reúna las garantías para el cumplimiento de lo dispuesto en dicho cuerpo normativo. Esto se traducirá en la práctica en la necesidad de que el responsable del fichero articule algún sistema que le permita llevar un control de la actividad desarrollada por su prestador de servicios.

Por ejemplo, establecer en el contrato de acceso y tratamiento de datos la posibilidad del responsable del fichero de solicitar el informe de las auditorías realizadas.

En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato en el que se ha regulado el acceso a datos, se considerará responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente. No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio.

Posibilidad de subcontratación de los servicios.

La LOPD no establece nada en relación con la posibilidad de subcontratación de los servicios por parte del encargado de tratamiento.

En su Memoria del año 2000, la AEPD realizaba la interpretación que se recoge a continuación, al analizar la figura del encargado de tratamiento:
"En lo referente a la cesión de los datos, de lo establecido en la el artículo 12.2 se desprende que no se producirá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. Ello implica, a nuestro juicio, la posibilidad de proceder a una subcontratación de este tipo de servicios por parte del encargado del tratamiento, debiendo siembre el responsable ser parte de la relación jurídica, ya que cualquier transmisión de los datos a un tercero que no corresponda al responsable del fichero habrá de ser considerada cesión"

No obstante, la AEPD consciente de que la subcontratación de servicios es una realidad y que prohibirla originaría muchos problemas en la práctica, establece en la citada Memoria fórmulas a través de las cuales se podría realizar y, además, la Memoria de 2001 admitió la subcontratación cuando se cumplieran determinados requisitos.

El Artículo 21 del RLOPD regula por primera vez la posibilidad de subcontratar servicios por parte del encargado de servicios, sentando como regla general la prohibición del encargado del tratamiento de subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del mismo, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

No obstante, admite la posibilidad de subcontratar sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

- Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.
- Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.
- En este caso, el subcontratista será considerado encargado del tratamiento y, como tal tendrá que cumplir las obligaciones que la normativa le impone.

Si durante la prestación del servicio resulta necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados.

Conservación de los datos por el encargado del tratamiento.

Si bien el artículo 22 del RLOPD regula la conservación de los datos por el encargado de tratamiento, establece unas obligaciones que resultan sumamente confusas.

En su primer apartado establece que, una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento y a continuación que no procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación. También establece la obligación para el encargado de tratamiento de conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento. Pensemos que aquí es donde se puede crear la confusión, dado que si se cumple esta obligación, el encargado de tratamiento no podrá destruir o devolver los datos, cumpliendo la obligación impuesta en el primer apartado.

Las medidas de seguridad en relación con el encargado del tratamiento.

El artículo 82 del RLOPD establece algunas obligaciones en relación con este tema, en concreto:

- Cuando un encargado de tratamiento preste sus servicios en los locales del responsable, esto deberá constar en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el mismo.
- Cuando el acceso sea remoto, habiéndose prohibido al encargado incorporar los datos objeto de tratamiento a sistemas o soportes distintos de los del responsable, este deberá dejar constancia de ello en su documento de seguridad, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
- Cuando un encargado de tratamiento preste los servicios contratados en sus propios locales, deberá elaborar un documento de seguridad o completar el que ya tuviera, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

- En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en el RLOPD.

2.6. Prestaciones de servicios sin acceso a datos personales

El RLOPD regula una figura novedosa en materia de protección de datos: las prestaciones de servicios sin acceso a datos personales, estableciendo la obligación para el responsable del fichero o tratamiento de adoptar las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Dispone, además, que cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio, no resultando necesario firmar un contrato de acceso y tratamiento de datos, en los términos establecidos en el artículo 12 de la LOPD.

¿En las prestaciones sin acceso a datos existen obligaciones de seguridad?

La respuesta de la AEPD a esta pregunta se encuentra al alcance de todos los ciudadanos a través de su página web[††††††]:

"Cualquier actividad que suponga un contacto directo o indirecto con el sistema de información y/o su entorno físico o lógico puede ser susceptible de poner en riesgo la seguridad de los datos:

[††††††] Vid. AEPD, I Sesión Anual Abierta de la AEPD "El nuevo reglamento de desarrollo de la ley orgánica de protección de datos: problemática, interpretación y aplicación", Madrid, 22 de abril de 2008, https:// www.agpd.es/portalweb/jornadas/1_sesion_abierta/common/faqs_bloque_1.pdf.

- *Limpieza.*
- *Seguridad.*
- *Mantenimiento o reparación de instalaciones (que no se refiera al propio sistema de información).*

Incluye servicios de destrucción o almacenamiento de soportes cuando el prestador desconozca el criterio de archivo o no pueda recuperar dato alguno."

2.7. La modificación de ficheros

Siguiendo lo dispuesto en el artículo 58 del RLOPD y, dado que la inscripción de un fichero de datos de carácter personal que obra en el RGPD debe encontrarse actualizada en todo momento, cualquier modificación que afecte al contenido de la misma deberá ser previamente notificada a la AEPD o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el RGPD. Cuando se trate de un fichero de titularidad pública debe adoptarse, con carácter previo a la notificación, la correspondiente norma o acuerdo en los términos previstos al tratarla creación de ficheros.

2.8. Las transferencias internacionales de datos

La norma general no permite al responsable de los ficheros realizar transferencias internacionales de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta LOPD, salvo que cumplan los siguientes requisitos:

- Se haya observado lo dispuesto en la LOPD.
- Se obtenga autorización previa del Director de la AEPD.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la AEPD atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos.

En la actualidad se consideran países con nivel de protección adecuado al que presta la LOPD los Estados Miembros de la Unión Europea, Islandia, Liechtenstein, Noruega y los Estados que la Comisión Europea ha declarado que garantizan un nivel de protección adecuado: Suiza, Argentina, Guernsey, Isla de Man, las entidades estadounidenses adheridas a los principios de Puerto Seguro, Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos de América.

La propia LOPD reconoce algunas excepciones a la norma general, de manera que no será necesaria la autorización previa del Director de la AEPD en los siguientes supuestos:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos la gestión de servicios sanitarios.
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

- Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquélla sea acorde con la finalidad del mismo.
- Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

El RLOPD introduce una novedad al definir la transferencia internacional de datos como el *"Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español."*

Esto supone un cambio ya que, si bien realizando una interpretación literal de la LOPD un movimiento de datos a países de la Unión Europea supone una transferencia internacional de datos para la que no se necesita autorización previa del Director de la AEPD, de la definición aportada por el RLOPD se desprende que dicho movimiento de datos no se considera transferencia internacional.

3. Una vez finalizado el tratamiento

3.1. La cancelación y el bloqueo de los datos

En función de lo establecido en el artículo 4.5 de la LOPD, el responsable de ficheros se verá obligado a cancelar los datos de carácter personal cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados, de manera que no podrá conservarlos en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales los hubiera recabado o registrado.

El RLOPD recuerda la obligación de cancelar los datos cuando dejan de ser necesarios o pertinentes para la finalidad para la cual han registrados o recabados, añadiendo que, no obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la LOPD y el RLOPD. En este sentido, debemos saber que un procedimiento de disociación es todo tratamiento de datos personales que permita la obtención de datos disociados.

3.2. La supresión de ficheros

Cuando el responsable de un fichero decida su supresión, deberá notificarla a AEPD o a las autoridades de control autonómicas competentes, a fin de proceder a la supresión del mismo en el RGPD.

Cuando se trate de un fichero de titularidad pública debe adoptarse con carácter previo a la notificación la correspondiente norma o acuerdo en los mismos términos que en los casos de creación y modificación de ficheros, ya tratados anteriormente. Una vez tramitado el procedimiento establecido, el Director de la AEPD dictará resolución acordando la cancelación de la inscripción del fichero.

Hasta ahora hemos hablado de la supresión de ficheros a instancia de parte, pero el artículo 61 del RLOPD establece la posibilidad de que sea el propio Director de la AEPD quien, en ejercicio de sus competencias, acuerde de oficio la cancelación de la inscripción de un fichero. Para ello, han de concurrir circunstancias que acrediten la imposibilidad de que exista y ha de seguirse el mismo procedimiento que en los casos de supresión a instancia del responsable del fichero.

3.2.1. El deber de secreto

El deber de secreto, es una obligación que subsistirá en relación con los usuarios de los datos, aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

RLOPD frente a la LOPD legalmente hablando

El Ordenamiento Jurídico español se fundamenta en una estricta jerarquía normativa creada al amparo de la Constitución de 1978. Esto implica que las normas de rango inferior deben desarrollar las disposiciones de rango superior sin entrar en conflicto. Sin embargo, un legislador puede llegar a elaborar una norma que contradiga a otra de rango superior y que esta sea aprobada, pero vulneraría este principio constitucional.

El reglamento de desarrollo de la LOPD ha tardado ocho años en ver la luz y ahora resulta que algunos de sus artículos podrían correr el riesgo de ser declarados inconstitucionales por contradecir una Ley Orgánica.

La **LOPD** definió un ámbito de aplicación objetivo extensible a todas las **personas físicas**, siempre que no fuesen materias clasificadas, datos de terrorismo o ficheros personales mantenidos por particulares. Sin embargo, el **RLOPD** establece nuevas excepciones del ámbito de aplicación. ¿Se puede estar dentro del ámbito de aplicación de la LOPD y fuera del RLOPD? Parece que esto les ocurrirá a los datos *profesionales o corporativos* de personas físicas que presten sus servicios en personas jurídicas y de los empresarios individuales cuando sean tratados como tal (¿y qué ocurre con las personas físicas que trabajen para empresarios individuales?)

Rizando el rizo, las listas de los colegios profesionales se consideran *fuentes accesibles al público* en ambas normas. Sin embargo, como acabamos de ver, los datos contenidos en ellas están fuera del ámbito de aplicación del RLOPD. Teniendo esto en cuenta, una nueva lectura del Reglamento nos revela que se prevé el ejercicio del **derecho de oposición** por parte de los titulares de los datos disponibles en estas fuentes accesibles al público.

Supongamos pues, que un abogado tiene un despacho en su domicilio y ejerce el derecho de oposición en las listas de su colegio, porque no desea recibir publicidad. Sin embargo, una empresa de marketing podría no tener por qué respetar esta oposición si quisiera mandarle, por ejemplo, un fax a las 3 de la madrugada ofreciendo muebles de oficina.

Otra *divertida* paradoja del RLOPD es la figura del **Responsable del Tratamiento** como sujeto diferenciado del **Responsable del Fichero** y del **Encargado de Tratamiento**. El Reglamento ha querido dotar de autonomía a esta figura sin llegar a definirla concretamente (art. 46.2 RLOPD). Esta ambigüedad termina careciendo de sentido cuando acudimos a la LOPD y comprobamos que las figuras sujetas al régimen sancionador son exclusivamente el Responsable del Fichero y el Encargado de Tratamiento (art. 43.1 LOPD).

Aceptando este tratamiento diferenciado, podríamos concluir que el irresponsable del Tratamiento es la única figura que no tiene responsabilidad, lo que resulta especialmente *jocoso* ya que es la figura de mayor responsabilidad.

10. ¿Por qué no se aplica una auditoría informática? (con ejemplos)

Hasta ahora todo lo escrito no dejan de ser argumentos a como se hace una auditoría, ventajas e inconvenientes de ésta, los productos obtenidos, pero una vez analizado todo lo anterior llegamos al momento de "tomar medidas" es decir, si algo se ésta haciendo mal, debería de empezar a hacerse bien porque sabemos que puede mejorarse. Pero realizar cambios en una empresa para adaptarse a un nuevo modelo o para mejorar el rendimiento de una instalación no es todo lo sencillo que la dirección de la empresa piensa. Veamos algunos ejemplos:

- **Migración de bases de datos**. No voy a entrar en marcas pero todo el que ha trabajado en proyectos de larga duración o de mantenimiento ha visto llegar el momento en que la base de datos llevaba demasiado tiempo obsoleta, y el problema del tiempo de acceso a ésta ya no era el único problema, sino que empezábamos a hablar de incompatibilidad con nuevos módulos instalados. En este momento la política de "mientras funcione, vamos bien" se encuentra completamente sitiada y se ve obligada a ceder, momento en el cual, se debería preparar todo un proyecto para llevar a buen término la migración, servidores nuevos con imágenes de la base de datos actualizada, turnos nocturnos para hacer el cambio y afectar lo menos posible al funcionamiento de la aplicación, varias pruebas en servidores de prueba, pero en el momento de cambiarlo todo siempre hay problemas, y es el momento en que hay que tomar decisiones rápidas, se prueban varias configuraciones con el mismo resultado, y después de horas de trabajo y en función a la preparación de las personas designadas para el cambio, se optará por vías intermedias que permitan el funcionamiento de la aplicación con el resultado de haber mejorado en parte el rendimiento de la aplicación con la nueva versión instalada, pero con montones de fallos de seguridad debido a los problemas de la instalación. Esta instalación produce dos consecuencias directas en la dirección para futuras instalaciones: "Esperar a una nueva versión de la aplicación para la nueva instalación de bases de datos" o "asignar un mayor presupuesto en tiempo y dinero para la próxima migración". Es decir si la auditoría te advertía de los problemas de una base de datos esos problemas se pueden haber sustituido por otros, y desde la

dirección no quieren desperdiciar el dinero de la empresa, por lo que en la próxima auditoría se tomarán de otra los problemas de bases de datos.

- El centro de proceso de datos (CPD) posee una seguridad relativa ya que pese a que se debe tener una llave para acceder a él, la puerta permanece abierta la mayor parte del tiempo y con la llave puesta. Este caso se ve mucho en empresas no muy grandes donde el CPD no deja de ser "el cuartito donde suelen estar los de sistemas cuando no están en su mesa". Desde la dirección de la empresa pueden considerar que este tema es muy importante y tienden a realizar un gasto en seguridad del tipo "tarjetas magnéticas" que no siempre es la mejor solución, es decir, el CPD requiere de refrigeración, por ello siempre suele tener aire acondicionado propio, pero cuando tiene que realizar cambios la persona de sistemas tiende a dejar la puerta abierta para poder salir cargando cosas o simplemente para no enfriarse demasiado dentro de la habitación, estas habitaciones deberían de ser amplios espacios donde circule el aire sin problemas, pero normalmente son cuartos donde los servidores se apilan unos encima de otros y donde poder dar 3 pasos en línea recta se convierte en complicado, con todo esto lo que quiero decir, es que la seguridad es muy relativa, ya que si no se entiende el problema desde su base no se pueden tomar las medidas adecuadas, es por ello que deben hablar todos los elementos implicados en cada cambio para hacer las cosas en la dirección adecuada. De poco sirve usar tarjetas magnéticas en vez de llaves para abrir puertas si las puertas permanecen abiertas, de poco sirve ampliar el cuarto del CPD con 2 armarios contiguos a este, si la alimentación de ese nuevo espacio queda fuera de él pudiendo cualquier persona desenchufar un servidor para "cargar su móvil", son casos típicos que he vivido, y por desgracia son mas frecuentes de lo que parecen, aunque la dirección entiende de este asunto que el problema no es la coordinación sino el "hacer caso a la auditoría".

- La seguridad respecto a visitas tiene fisuras de seguridad. Es decir, llega una persona nueva a la empresa, se toman datos de esa persona, pero luego solo se le indica donde debe ir sin acompañarle. En una empresa grande suele darse mucho este caso, y el problema está en que en esa distancia la persona puede optar por ir en otra dirección en base a sus intenciones, si alguien ajeno a la empresa atraviesa la puerta, debería ser acompañado hasta su destino por la persona que va a ver, o por alguien de seguridad. La dirección entiende normalmente que este peso debe caer sobre los empleados de la empresa en general y sobre los agentes de seguridad en particular, el resultado final suele ser que los agentes hacen este trabajo o directamente se mantiene la política de indicar a la persona hacia donde debe dirigirse. Nuevamente la culpa se le hecha a que la auditoría no fijaba correctamente como hacer las cosas y por tanto es mejor no darle tanta importancia.

- Para finalizar hablaré un poco del uso de metodologías que en muchas auditorías se recomienda para mejorar la calidad y rendimiento de los proyectos de la empresa. No estoy hablando de obtener una certificación, sino de seguir una metodología, es decir, algo tan sencillo como fijar hacer unas cosas en unos tiempos y en base a un esquema, generando la documentación necesaria en cada momento. En resumen, estructurar y hacer el proyecto en base a esa estructura puede ser algo muy útil o una verdadera perdida de tiempo debido a la poca implicación por parte de los empleados. El equipo debe estar realmente implicado en seguir la metodología, en caso contrario, el proyecto fracasará o sufrirá un retraso muy importante incluyendo el sobreesfuerzo del equipo. La dirección suele intentar implantar esta recomendación en diferentes proyectos y al ver como se tuercen estos proyectos opta por continuar como habían realizado hasta ahora, ya que la idea de “siempre lo hemos hecho así” saben que da resultados óptimos, y finalmente las metodologías terminan por ser abandonadas por orden directa de la dirección con el objeto de no perder más dinero con ello.

11. Soluciones para afrontar el resultado de una auditoría informática.

Una auditoría informática por norma siempre saca a la luz las debilidades de la empresa siendo entonces los dirigentes de la empresa los que deben valorar las prioridades para hacerse cargo de cubrir esas debilidades.

Primeramente debemos “enfocar” la auditoría informática que vamos a realizar, es decir, no podemos decir a una empresa, “auditarnos” al contrario, debemos mentalizarnos de qué parte es la que queremos valorar principalmente en la empresa, si queremos publicitarnos demostrando que seguimos unos códigos tipo muy exigentes de acuerdo a la LOPD debemos solicitar que se nos audite orientados en ese camino, si en realidad queremos analizar las brechas de seguridad, deberíamos enfocar la auditoría a este campo, incluso si lo que queremos es analizar una gestión adecuada del desarrollo software, es decir, generar un conjunto de directrices que consten de una serie de módulos que expliquen en detalle cómo la entidad puede sacar mayor provecho de sus recursos informáticos, ese debemos indicar que es el cometido de la auditoría. Estas disciplinas informáticas están entrelazadas y son mutuamente dependientes, por lo cual deben plantearse de forma aislada pero sin olvidar la influencia que cada una ejerce sobre las otras.

Una aplicación de principios informáticos le permite ofrecer operaciones de Gestión de Servicios Informáticos completamente integrados a sus clientes tanto internos como externos.

Veamos ahora los distintos aspectos a tratar después de una auditoría informática.

A. Seguridad y Protección de la Información

ITIL representa mucho más que una serie de libros útiles sobre Gestión de Servicios TI. Un marco de mejores prácticas en la Gestión de Servicios TI representa un conjunto completo de organizaciones, herramientas, servicios de educación y consultoría, marcos de trabajo relacionados, y publicaciones. Las disciplinas de Gestión de Servicios que se encuentran en el corazón de ITIL encajan en dos grupos diferenciados:

Soporte de Servicio

Este grupo se centra en la actividad y el apoyo cotidianos de los servicios informáticos.

Centro de Atención al Usuario

La función del Centro de Atención al Usuario (CAU) es la cara de la informática ante sus usuarios, por lo que es de vital importancia en toda entidad. El personal del Centro de Atención al Usuario registra, resuelve o eleva y cierra todos los incidentes. Asimismo brinda asistencia técnica de primera instancia en un nivel superior, y propone iniciativas de mejora de servicio y reducción de costes. Es esencial para el buen desarrollo del negocio que los clientes y usuarios perciban que están recibiendo una atención personalizada y ágil que les ayude a:

- Resolver rápidamente las interrupciones del servicio.
- Emitir peticiones de servicio.
- Informarse sobre el cumplimiento de los **SLAs**.
- Recibir información comercial en primera instancia.

Gestión de Incidentes

Gestión de Incidentes registra, clasifica, supervisa y cierra todos los incidentes de forma controlada y homogénea. Esto permite restaurar los niveles de servicio con la mayor rapidez posible y ayuda a reducir el número de incidentes nuevas. Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el **SLA** correspondiente.

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el Centro de Servicios (Service Desk) debe jugar un papel esencial en el mismo.

Gestión de Problemas

La identificación, investigación y clasificación de problemas es una función fundamental en el ámbito de Gestión de Servicios Informáticos. Reduce de forma proactiva los volúmenes de incidentes y mejora continuamente la infraestructura informática subyacente.

Las funciones principales de la **Gestión de Problemas** son:

- Investigar las causas subyacentes a toda alteración, real o potencial, del servicio TI.
- Determinar posibles soluciones a las mismas.
- Proponer las peticiones de cambio necesarias para restablecer la calidad del servicio.
- Realizar Revisiones Post Implementación para asegurar que los cambios han surtido los efectos buscados sin crear problemas de carácter secundario.

Gestión de Activos y Configuraciones

Esto proporciona los cimientos vitales que son necesarios para la Gestión de Incidentes, Problemas y Cambios. Registra, y se encarga de la auditoría y la seguridad de todos los elementos de configuración que se encuentren en la infraestructura informática, así como sus relaciones desde su adquisición hasta su obsolescencia. Llevar el control de todos los elementos de configuración de la infraestructura TI con el adecuado nivel de detalle y gestionar dicha información a través de la Base de Datos de Configuración (**CMDB**).

Proporcionar información precisa sobre la configuración TI a todos los diferentes procesos de gestión.

Interactuar con las Gestiones de Incidentes, Problemas , Cambios y Versiones de manera que estas puedan resolver más eficientemente las incidencias, encontrar rápidamente la causa de los problemas, realizar los cambios necesarios para su resolución y mantener actualizada en todo momento la **CMDB**.

Monitorizar periódicamente la configuración de los sistemas en el entorno de producción y contrastarla con la almacenada en la **CMDB** para subsanar discrepancias.

Gestión de Cambios

La función de Gestión de Cambios es asegurar que se emplee un enfoque homogéneo para la evaluación e implantación de todo cambio a la infraestructura informática de la manera más eficiente, siguiendo los procedimientos establecidos y asegurando la calidad y continuidad del servicio. Permite evaluar el riesgo y el impacto, así como los requisitos en lo que se refiere a recursos asociados con los cambios propuestos. Todo esto supone las siguientes ventajas:

- Reducción a medio/largo plazo de los costes asociados.
- Mejora y consistencia de los servicios prestados.
- Simplificación de todos los procesos asociados al soporte al servicio: Incidencias, Problemas, Cambios, Versiones, etc.

Gestión de Versiones

La Gestión de Versiones es la encargada de diseñar, poner a prueba e instalar en el entorno de producción los cambios establecidos, todo ello debe realizarse proporcionando un marco sistemático para implantaciones de hardware de envergadura o críticas, implantaciones de software de envergadura o conjuntos de cambios empaquetados. Tiene en cuenta todos los aspectos técnicos y no técnicos de una edición, desde la política y planificación de edición iniciales hasta el desarrollo, pruebas e implantación controlados. Todo ello nos lleva a:

- Establecer una política de implementación de nuevas versiones de hardware y software.
- Implementar las nuevas versiones de software y hardware en el entorno de producción tras su verificación en un entorno realista de pruebas.
- Garantizar que el proceso de cambio cumpla las especificaciones de la **RFC** correspondiente.

Asegurar, en colaboración con la **Gestión de Cambios y Configuraciones**, que todos los cambios se ven correctamente reflejados en la **CMDB**.

Provisión de Servicio

Estos procesos tienen en cuenta la planificación a largo plazo y mejoras en la prestación de servicios informáticos

Gestión de Niveles de Servicio

Pretende garantizar una calidad satisfactoria de prestación de servicios informáticos mediante la fijación de objetivos realistas y acordados entre el proveedor y el cliente. Mediante un proceso de monitorización, emisión de informes y revisión de los niveles de servicio reales se destacan las áreas problemáticas y se facilita una mejora continua en el servicio.

Los principales beneficios de una correcta Gestión de Niveles de Servicio son:

- Los servicios TI son diseñados para cumplir sus auténticos objetivos: cubrir las necesidades del cliente.
- Se facilita la comunicación con los clientes impidiendo los malentendidos sobre las características y calidad de los servicios ofrecidos.
- Se establecen objetivos claros y medibles.
- Se establecen claramente las responsabilidades respectivas de los clientes y proveedores del servicio.
- Los clientes conocen y asumen los niveles de calidad ofrecidos y se establecen claros protocolos de actuación en caso de deterioro del servicio.
- La constante monitorización del servicio permite detectar los "eslabones más débiles de la cadena" para su mejora.
- La gestión TI conoce y comprende los servicios ofrecidos lo que facilita los acuerdos con proveedores y subcontratistas.
- El personal del Service Desk dispone de la documentación necesaria (**SLAs**, **OLAs**,etc.) para llevar una relación fluida con clientes y proveedores.
- Los **SLAs** ayudan a la Gestión TI tanto a calcular los cálculos de costes como a justificar su precio ante los clientes.

Gestión Financiera de los Servicios IT

También denominado gestión de costes, este proceso brinda información de gestión esencial sobre los costes de activos y servicios informáticos. Mediante un proceso que entraña presupuestar y contabilizar, se desvelan los costes reales y así puede demostrarse el valor que supone la informática para el negocio, a mayor calidad de los servicios mayor es su coste, por lo que es necesario evaluar cuidadosamente las necesidades del cliente para que el balance entre ambos sea óptimo. Todo ello nos conlleva a:

Los principales beneficios de una correcta Gestión Financiera de los Servicios Informáticos se resumen en:

- Se reducen los costes y aumenta la rentabilidad del servicio.
- Se ajustan, controlan, adecuan y justifican (si es de aplicación) los precios del servicio aumentando la satisfacción del cliente.
- Los clientes contratan servicios que le ofrecen una buena relación coste/rentabilidad.
- La organización TI puede planificar mejor sus inversiones al conocer los costes reales de los servicios TI.
- Los servicios TI son usados más eficazmente.
- La organización TI funciona como una unidad de negocio y es posible evaluar claramente su rendimiento global.

Gestión de Capacidad

El objetivo primordial de la Gestión de la Capacidad es poner a disposición de clientes, usuarios y el propio departamento TI los recursos informáticos necesarios para desempeñar de una manera eficiente sus tareas y todo ello sin incurrir en costes desproporcionados. Con este proceso se pretende alinear los niveles de servicios informáticos con las necesidades actuales y futuras del negocio. Tiene que ver con el aprovechamiento de los recursos informáticos existentes así como con procurar que los recursos nuevos estén disponibles de forma oportuna y eficiente.

Los principales beneficios derivados de una correcta **Gestión de la Capacidad** son:

- Se optimizan el rendimiento de los recursos informáticos.
- Se dispone de la capacidad necesaria en el momento oportuno, evitando así que se pueda resentir la calidad del servicio.
- Se evitan gastos innecesarios producidos por compras de "última hora".
- Se planifica el crecimiento de la infraestructura adecuándolo a las necesidades reales de negocio.
- Se reducen de los gastos de mantenimiento y administración asociados a equipos y aplicaciones obsoletos o innecesarios.
- Se reducen posibles incompatibilidades y fallos en la infraestructura informática.

Gestión de Demanda

La Gestión de Disponibilidad procura optimizar y racionalizar el uso de los recursos TI, es decir, que todos los sistemas y servicios funcionen según se requiera y que se mantenga la disponibilidad de forma fiable y rentable. Con el suministro y la provisión de información, las empresas también deben considerar la gestión de seguridad para impedir el uso no autorizado de la información.

Gestión de Continuidad/Disponibilidad de los Servicios IT

Este proceso asegura que los grandes fallos producidos en equipos o instalaciones técnicos asociados con la prestación de Servicios IT se gestionen de forma eficiente y que los niveles de servicios se restauren a un nivel aceptable en los plazos acordados. La estrategia de la Gestión de la Continuidad del Servicio debe combinar equilibradamente procedimientos:

- **Proactivos**: que buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos**: cuyo propósito es reanudar el servicio tan pronto como sea posible (y recomendable) tras el desastre.

Gestión de la seguridad

La Gestión de la Seguridad de la Información se remonta al albor de los tiempos. La criptología o la ciencia de la confidencialidad de la información se realiza desde el inicio de nuestra civilización y ha ocupado algunas de las mentes matemáticas más brillantes de la historia, especialmente (y desafortunadamente) en tiempos de guerra.

Sin embargo, desde el advenimiento de las distintas redes de comunicación y en especial Internet los problemas asociados a la seguridad de la información se han agravado considerablemente y nos afectan prácticamente a todos. Que levante la mano el que no haya sido victima de algún virus informático en su ordenador, del spam (ya sea por correo electrónico o teléfono) por una deficiente protección de sus datos personales o, aún peor, del robo del número de su tarjeta de crédito.

La información es consustancial al negocio y su correcta gestión debe apoyarse en tres pilares fundamentales:

Confidencialidad: la información debe ser sólo accesible a sus destinatarios predeterminados.

Integridad: la información debe ser correcta y completa.

Disponibilidad: debemos de tener acceso a la información cuando la necesitamos.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

¿Por qué no cualquiera?

En el entorno de negocios de hoy día, las entidades tanto privadas como públicas no pueden sobrevivir sin servicios informáticos fiables. Proporcionar y mejorar continuamente estos servicios es el desafío diario al que se enfrentan los profesionales informáticos que pretenden mantenerse al corriente con las necesidades cambiantes de sus clientes y usuarios, así como anticiparse a ellas. Los servicios ligados a la informática se han convertido en una función estratégica en la estructura empresarial de cada entidad. A medida que se asoman de las sombras donde meramente desempeñan la función de apoyo, cada vez más son los protagonistas en calidad de función que añade valor que impulsa el negocio hacia el futuro.

Una herramienta – todas las respuestas

Gestión de Servicios Informáticos, ITIL brinda un conjunto homogéneo de la "Mejor Práctica de Gestión de Servicios Informáticos" aplicables a todas las entidades, con independencia de su tamaño, y se apoya en una estructura sistemática de homologaciones, acreditaciones, organismos de formación, herramientas y consultoras.

Las ventajas principales que brinda la aplicación de los principios de ITIL son:
Infraestructura informática optimizada para cubrir las necesidades de negocios existentes y previstas Coste total de propiedad (TCO por sus siglas en inglés) permanentemente reducido, incluyendo el coste de servicio.
Mayor calidad de Servicio Informático para aumentar la confianza en los sistemas informáticos y la prestación de servicios.

Preparar una lista de comprobaciones para revisar regularmente ayudará a tener claro en todo momento los objetivos de adaptarse a una certificación:

LISTA DE COMPROBACIÓN PARA LA REVISIÓN DE REQUISITOS

CRITERIO	Tipo	Anotaciones	SI/NO/NA
CLARIDAD E IDONEIDAD			
1. ¿Se han separado los requisitos funcionales o de capacidad de los que no lo son? ¿Se ha identificado el tipo de los requisitos no funcionales?			
2. ¿Es la terminología consistente con la terminología del usuario?	SIS		
3. ¿Son los términos o conceptos que se utilizan claros y consistentes? ¿Están las siglas documentadas?			
4. ¿El requisito es claro y sin ambigüedades? ¿se entiende? ¿demasiado críptico o demasiado descriptivo?			
5. ¿Es preciso el requisito? ¿es demasiado preciso?			
6. ¿Sobra el requisito? ¿es demasiado general? ¿aporta algo?			
7. ¿Hay múltiples requisitos en uno? ¿Está el requisito demasiado “troceado”?			
COMPLETITUD			
8. ¿Proporciona el cliente la información suficiente para especificar lo que quiere?. Si no es así, ¿están identificadas las medidas que se van a tomar?	CLI		
9. ¿Es el conjunto de requisitos suficiente para especificar el Sistema/SW/HW requerido?	SIS SW HW		
10. ¿Se ha realizado y documentado un análisis de viabilidad? ¿son razonables los requisitos? ¿son técnicamente posibles? ¿son económicamente viables?			
11. ¿Se analizado el impacto si no se cumplen los requisitos?			
12. ¿Se han considerado los temas de seguridad (*security, safety*) del sistema?			
13. ¿Se ha evaluado el impacto del proyecto en los usuarios y en otros sistemas?			

CRITERIO	Tipo	Anotaciones	SI/NO/NA
14. ¿Están priorizados los requisitos? ¿es necesario?			
15. ¿Están los requisitos correctamente priorizados?			
16. ¿Se han definido criterios para asignar niveles de prioridad a los requisitos?			
17. ¿Hay requisitos que se contradicen total o parcialmente? ¿existe el riesgo de que ello ocurra (repetición, múltiples referencias)?			
18. ¿Se han definido completamente los atributos de todos los requisitos?			
19. ¿Se han definido los supuestos y las restricciones del Sistema/SW/HW?	SIS SW HW		
ESTÁNDARES			
20. ¿Sigue la documentación de requisitos los estándares establecidos para el proyecto y la organización?			
21. ¿Se han recogido los requisitos utilizando las herramientas y metodologías establecidas para el proyecto y la organización?			
INTERFACES			
22. ¿Se han definido claramente todas las interfaces externas y sus requisitos?			
23. ¿Se han definido claramente todas las interfaces internas y sus requisitos?	SIS SW HW		
24. ¿Es un requisito de interfaz o un requisito funcional?			
25. ¿Están suficientemente especificadas las operaciones de usuario?			
26. ¿Hay información sobre las forma de introducir datos/órdenes y presentar mensajes?			
27. La interfaz de usuario, ¿está recogida por los requisitos? ¿es demasiado explícita o demasiado genérica?			

CRITERIO	Tipo	Anotaciones	SI/NO/NA
MANTENIMIENTO			
28. ¿Se han definido los requisitos para el mantenimiento del Sistema?	SIS CLI		
RENDIMIENTO			
29. Se han identificado los requisitos de rendimiento del sistema?			
FIABILIDAD			
30. ¿Existen requisitos de fiabilidad?			
31. ¿Se han definido requisitos de detección, reporte y recuperación de errores?			
32. ¿Se han considerado eventos no deseados y especificadas las respuestas requeridas?			
PRUEBAS			
33. ¿Es posible definir una prueba para el requisito? ¿es medible?			
34. ¿Faltan requisitos que faciliten la verificabilidad del sistema?			
35. ¿Se han establecido criterios de validación para todos los requisitos? ¿son idóneos?.			
TRAZABILIDAD			
36. ¿Todos los requisitos del nivel superior se trazan a requisitos de este nivel? ¿Existen requisitos no trazados al nivel superior? ¿Por qué?	SIS SW HW		

SIS -> Sistemas
SW -> Software
HW -> Hardware
CLI -> Cliente

El área de Calidad del Software permite a los proyectos medir la calidad de los sistemas que se construyen y compararla con la calidad media de la empresa. A partir de los datos obtenidos desde las herramientas utilizadas en el área, se obtienen dos informes: uno ejecutivo, cuya audiencia es el equipo de gestión de la operación, y uno detallado, destinado al equipo de desarrolladores.

Los resultados recopilados tanto en el informe ejecutivo como en el detallado son obtenidos mediante herramientas que comprueban la conformidad del código fuente respecto a una adaptación de la norma de calidad ISO-9126.

En colaboración con los proyectos, que poseen el conocimiento funcional de los sistemas, se elaboran recomendaciones a medida que dirigen las líneas a seguir para trabajar los aspectos más susceptibles de mejora.

Se proporcionan guías de buenas prácticas (reglas de codificación y métricas) para que tanto los líderes de los proyectos como los desarrolladores conozcan y entiendan qué no hay que hacer y por qué.

B. Gestión de la calidad del Software

La función principal del área es velar porque el código que se desarrolla tenga una calidad mínima en función de una serie de reglas y buenas prácticas que **deben** cumplirse. Esta comprobación se realiza a través de unas auditorías que conocemos con el nombre de **QA-SW internos.** Estas auditorías posibilitan:

- Uniformización del concepto de calidad de código en la empresa.
- Garantía de calidad en desarrollos realizados internamente y hacia el cliente final.
- Identificación de problemas relacionados con el código desarrollado en las operaciones.

Otra función es la aplicación del proceso de auditoría a código que no ha sido desarrollado y que conocemos como **QA-SW a código realizado por terceros**. Estas auditorías permiten:

- Comparar la calidad del código desarrollado internamente frente al código desarrollado por otros proveedores.
- Identificación de oportunidades en clientes.
- Identificación de áreas de mejora en código que hemos heredado, facilitando su evolución y mantenimiento.

Tanto para los QA-SW internos, como los QA-SW a código desarrollado por terceros se realizan las siguientes actividades:

- Identificación con periodicidad mensual de las operaciones objetivo de la auditoría de métricas interna.
- Ejecución de la auditoría, elaboración y divulgación de los resultados a los responsables de calidad, riesgo y de la operación y a los directores del Mercado en el que se desarrolla la operación.
- Por el momento se analizan operaciones basadas en tecnología Java. En un futuro se ampliará el abanico de tecnologías a desarrollos .NET.

- La comprobación de conformidad respecto a la norma ISO-9126 permite detectar posibles problemas en función de una serie de características de calidad establecidas por la propia norma: mantenibilidad, eficiencia, usabilidad, testabilidad, reusabilidad y portabilidad.

Dentro del área se ofrecen los siguientes servicios:

- Realización de QA-SW internos o QA-SW a código realizado por terceros. Utilizando los criterios recomendados para un desarrollo se realizan con periodicidad mensual auditorías a operaciones elegidas o propuestas por los diferentes Mercados. Es un servicio que no conlleva coste alguno para la operación.
- Realización de QA-SW particularizados según el contexto establecido por el cliente. En este caso se debe realizar un esfuerzo para particularizar las herramientas en función de los requisitos del cliente (nomenclatura, buenas prácticas, etc.). Adicionalmente se realiza un análisis manual del código incidiendo en los aspectos desvelados por los resultados obtenidos mediante el uso de las herramientas de auditoría. En caso de ser necesario, se apoya a la operación en la presentación de los resultados al cliente final. Es un servicio que conlleva un coste debido al esfuerzo manual que requiere, tanto para la particularización de la herramienta, como para la realización del análisis manual.

C. Política de seguridad

La necesidad de definir una política de seguridad es algo absolutamente indiscutible. Las actuaciones voluntarias de un departamento de TI en materia de seguridad siempre estarán lejos de conseguir muchos de los objetivos que nos marcamos en esa visión multidimensional del problema. Ni la tecnología es el único problema, ni evidentemente es la única solución.

El cumplimiento de la LOPD representa un indiscutible impulsor del sector de la seguridad en España. Aprovechar la necesidad legal de su cumplimiento para extender el alcance de las iniciativas tomadas hacia una política de seguridad general mas allá del estricto dato personal, es una decisión tomada por numerosas empresas.

Resultará interesante hablar de qué pasos podemos dar para conseguir una política de seguridad correcta. Existen numerosos procedimientos que determinan la calidad de un sistema en este aspecto, BS, ISO, AENOR, etc., cuyos aspectos están fuera del alcance de este capítulo. Sin embargo, todos aquellos responsables de poner en marcha una política de seguridad saben de la dificultad innata a la tarea de ajustar una iniciativa como ésta a la idiosincrasia de la empresa. Desde el momento en el que una política de seguridad afecta a toda la compañía, a todos y cada uno de sus departamentos, ya sabemos que nos enfrentamos a una tarea compleja cuyo éxito depende en gran medida del **compromiso de los implicados** en su definición fundamentalmente, pero de toda la compañía en general.

Fases fundamentales

Sin pretender dar un recetario, exponemos unos puntos de reflexión extraídos de experiencias de profesionales de la seguridad, y que recogen algunas de las dificultades y métodos para la definición inicial de una política de seguridad y acercarnos a ese compromiso deseado de la compañía. Son puntos muy prácticos que arrojan algo de luz sobre los pasos previos necesarios a dar en su definición.

Establecemos cinco fases fundamentales con objetivos muy definidos, aunque sólo comentaremos las tres primeras por ser las más orientadas a dar esos primeros pasos organizativos:

- Fase 1. Organización y análisis.
- Fase 2. Desarrollo de un estudio sobre las necesidades de privacidad.
- Fase 3. Evaluación de las necesidades tecnológicas para la protección de la privacidad.
- Fase 4. Desarrollo de la política y planes.
- Fase 5. Implementación del plan.

Fase 1. Organización y análisis

Esta fase supone la puesta en marcha de la iniciativa y requiere una toma de datos básica, así como estructurar un grupo de trabajo capaz de ponerla en marcha.

Podemos definir ocho puntos a tener en cuenta en esta fase:

- **Desarrollo de una filosofía general de privacidad**. Es decir, establecer un equilibrio de consenso entre las perspectivas de bajo y alto riesgo. Una perspectiva de bajo riesgo es aquella en la que una política de seguridad está en marcha, la diseminación de información está fuertemente controlada, las políticas se establecen por tipo de dato, todas las salidas de información fuera de la empresa necesitan ser previamente aprobadas, etc. Por el contrario, una perspectiva de alto riesgo es aquella en la que políticas no severas están en marcha, la información se controla débilmente, existen políticas globales poco específicas y se permite a las unidades de negocio y departamentos el tomar sus propias decisiones sobre el uso de la información. Ambos extremos delimitan una filosofía de privacidad llena de grises. Definir a priori la filosofía más cercana a nuestras necesidades es muy conveniente y complicado pues, dentro de la misma compañía, existirán departamentos más decididos por una política de bajo riesgo, mientras otros abogarán por una de alto riesgo.

- **Responsable de privacidad**. Los más elevados niveles de la dirección deben apoyar los planes de privacidad ante toda la compañía. Es un indicador de la importancia que este asunto tiene para la compañía. Aunque el apoyo es fundamental, no es lo más recomendable que este nivel esté involucrado en el día a día del desarrollo del plan de seguridad. Simplemente por no ser lo más efectivo. Un director de nivel medio es más adecuado para coordinar la tarea. La persona encargada deberá dedicar gran parte de su tiempo a esta tarea que, en ocasiones, requerirá una dedicación total. Debe mantener una *buena relación con todos los departamentos* de la empresa y con los recursos externos.

- **Creación del Grupo de trabajo de privacidad (Privacity Task Force).** Es necesario crear un grupo de trabajo interdepartamental liderado por el responsable de privacidad y con representación de todos los departamentos de la compañía (dos por departamento, uno principal y otro suplente). El mejor rol posible del CEO sería asegurarse de que el grupo de trabajo de seguridad obtiene los recursos, la participación y la cooperación necesarios para este desempeño. La función del CEO en este sentido es la de dejar constancia de la importancia del grupo en todos sus reportes directos, así como dar el apoyo necesario para situar la importancia de la tarea asignada al grupo creado.

- **Organización a nivel departamental** .Cada departamento deberá tener su propio equipo de privacidad que desarrolle los trabajos de investigación, evaluación o implementación, liderados por su representante en el Grupo de trabajo. Debería constituirse con niveles de supervisión y técnicos.

- **Evaluación de la capacidad del Grupo de trabajo.** Es necesario evaluar las capacidades y conocimientos del grupo de trabajo, formación, experiencia en asuntos relacionados con la privacidad, etc. Igualmente, es una tarea a desarrollar por cada miembro del grupo de trabajo en su grupo departamental. Identificar correctamente esto permitirá identificar necesidades de formación y/o contratación de ayuda externa (legal, consultoría, etc.). El objetivo es cubrir las carencias detectadas en el apartado anterior.

- **Establecer el calendario de trabajo**. Será imprescindible desarrollar una agenda de reuniones periódicas desde el primer momento, con objetivos concretos. Una reunión de frecuencia fija será necesaria, además de las que el proceder vaya marcando. Serán necesarias para formar subcomités, identificar responsabilidades, asignar tareas entre departamentos, etc. Los grupos departamentales deberán reunirse con la frecuencia necesaria para respetar las agendas y compromisos del Grupo de trabajo global.

- **Campaña de concienciación**. La iniciativa necesita ser apoyada y conocida por toda la compañía. Los distintos grupos de trabajo tendrán escaso éxito sin el apoyo y conocimiento de todos los empleados. Se deben utilizar todos los medios de comunicación interna: newsletters, intranets, reuniones, marketing interno, etc.; así como plantear planes de formación al respecto para las nuevas incorporaciones y para los empleados.

- **Establecer el escenario para el inicio del estudio de necesidades de privacidad**. Notificar a los empleados el tipo de información que será necesaria recoger en el inicio del estudio (a acometer en la siguiente fase).

Fase 2. Desarrollo de un estudio sobre las necesidades de privacidad

La compañía debe comenzar a conocer los diferentes tipos de datos e información que almacena y utiliza. Esta fase ayuda a la compañía a identificar esos datos, determinar su origen, establecer cómo deben ser utilizados, identificar de qué forma y cómo se diseminan. Además, este proceso ha de identificar aquellas leyes y regulaciones gubernamentales y requerimientos internos que pueden gobernar la forma en la que se recogen y difunden esos datos.

Establecer un sistema de inventario de datos

Apoyarse en una base de datos es una herramienta útil para almacenar la información recogida. Probablemente, los campos indicados constituyan una buena base de partida para la construcción de dicha base. El inventario ha de ser lo más profundo posible. Ninguna compañía debería tener una falsa percepción de seguridad como fruto de un inventario de datos incompleto. Es muy común leer en el periódico un caso concreto sobre problemas de privacidad de un determinado tipo de datos y prematuramente concluir con que no somos vulnerables. Los campos de esta base de datos bien podrían ser: descripción del dato, departamento responsable, fuente, sistema donde reside, dónde residen copias en papel, cómo y dónde se utilizan internamente, cómo y dónde se distribuyen, política existente sobre el uso de datos, leyes al respecto del uso de esos datos, incidentes previos respecto a su uso, notas del grupo de seguridad sobre esos datos, etc.

Puesta en marcha del proceso de inventario

Son muchas las fuentes de datos que hay que considerar. Cada departamento debe determinar qué tipo de datos recoge, crea o utiliza. El grupo departamental debe proporcionar esta información al grupo de seguridad. Las compañías no deben presuponer que el departamento de TI conoce todos los datos utilizados por los demás departamentos o unidades de negocio.
Los almacenes de datos surgen “como setas” en las compañías. Por ejemplo, ficheros de los usuarios, ficheros de los proveedores, del canal de partners, registros desde el web site, registros de empleados, ficheros de I+D, ficheros de suscripción para newsletters corporativas, etc. En cualquier caso, las compañías deben ser muy realistas en este aspecto, ya que todos los departamentos y unidades de negocio se sienten como propietarios absolutos de esos datos. Hay una barrera cultural al cambio. Existe una tendencia observada en el tiempo a no cooperar totalmente con las iniciativas de ámbito global. La mejor herramienta para conseguir esa profundidad en el análisis de los datos puede que no sea enviar un formulario enorme a cada supervisor para que sea completado, sino una aproximación más de concienciación en la que tanto supervisores clave como expertos técnicos son encuestados sobre cómo son manejados los datos.

Tres puntos de la estrategia global puesta en marcha pueden ayudar a vencer resistencias:

1. Campaña de información interna sobre la importancia de la privacidad, realizada en la fase anterior, proporcionando al empleado una forma de proporcionar feedback sobre vulnerabilidades potenciales de la privacidad.

2. Comenzar el proceso formal de inventario de datos.

3. Crear y distribuir una encuesta a los empleados clave para recoger sus entradas sobre la vulneración de la privacidad.

La compañía puede triangular estas tres fuentes de información y obtener valiosa información mientras construye el inventario de datos.

Existencia de políticas previas

¿Existe ya alguna política previa asociada a determinado tipo de dato? ¿Incluso cuando no se haya identificado como política? Si existe, es el momento de recogerla, ya esté escrita o no, para su posterior análisis por el grupo de seguridad. Este proceso debe examinar si las políticas existentes no contradicen las nuevas. No se deben cambiar las existentes si se adaptan bien a las nuevas.

Leyes actuales. LOPD

¿Existe una normativa especial que gobierne el manejo de los datos que manipulamos? La asesoría legal es un aspecto muy importante para evitar posibles malas interpretaciones o acciones incorrectas en lo que respecta a la normativa existente.

Asesoría y cobertura de seguros

Se deben estudiar las ofertas de compañías de seguros en materia de coberturas por interrupción de actividad y/o violación de privacidad. Las grandes compañías suelen tener un departamento de análisis de riesgos, bajo cuyo paraguas caería la responsabilidad de evaluar los riesgos y las coberturas de los seguros asociados.

Identificar problemas de privacidad pasados y presentes

Desafortunadamente, muchas compañías no comienzan a tomarse en serio la seguridad hasta que existe algún incidente. El grupo de trabajo debe ser informado sobre cómo se actuó en este sentido. El mayor obstáculo se presenta cuando se recurre a la "memoria institucional" y vemos que los implicados en el problema ya no están en la compañía o que la memoria tiende a ser muy selectiva.

Revisar políticas de seguridad y problemas de los partners de negocio

¿Podríamos ser vulnerables por las prácticas de nuestros proveedores, canal, etc.? Estos partners de negocio deben ser informados de la puesta en marcha del plan. El mayor obstáculo es conseguir su cooperación, la que dependerá en gran medida del número de partners y la capacidad de influencia en sus procesos.

Chequear la reputación entre organismos jurídicos especializados

Las compañías deberían contactar directamente con organizaciones jurídicas o no jurídicas, pero con algún interés existente en indagar en la privacidad con la que tratamos nuestros datos, y chequear si han encontrado algún problema. De paso, aprovechar para informar sobre el desarrollo de un nuevo plan de privacidad.

Consolidación de resultados y clasificación de datos

Una vez recogida toda la información, es la hora de consolidar en informes todo lo correspondiente a esta fase, con especial atención a la clasificación de los datos recogidos en base a criterios de sensibilidad e importancia de su privacidad. A partir de esto, puede comenzarse a adelantar un borrador sobre la política de seguridad y procedimiento en el manejo de ese tipo de datos.

Como resultado de esta fase, deberíamos tener muy claro el inventariado de datos y su clasificación según su sensibilidad e importancia, así como toda la normativa legal que les afecta.

En este apartado, un subcomité del grupo de seguridad debería iniciar la siguiente fase, en estrecha colaboración con el departamento de TI o un consultor externo de tecnologías de la información, para llevar a cabo una evaluación de la tecnología que puede ayudar a mantener el nivel de privacidad deseado.

Fase 3. Evaluación de las necesidades tecnológicas para la protección de la privacidad

Es necesario evaluar las capacidades existentes en la empresa para operar e implantar la tecnología necesaria para asegurar la privacidad de la información corporativa. Esta evaluación requiere un detenido análisis de tecnologías, personal de seguridad, fondos para seguridad y planes de seguridad. Este estudio debería ser llevado a cabo por un subcomité de la Task Force, en trabajo conjunto con el departamento IT y, si fuera necesario, contar con una consultoría externa.

Las funciones de este subcomité irían orientadas a:

- Asesorar al Grupo de trabajo sobre aspectos tecnológicos.
- Preparar reuniones sobre problemas tecnológicos específicos.
- Educar al Grupo de trabajo sobre el potencial y limitaciones de la tecnología.
- Examinar las capacidades en materia de seguridad en las tecnologías de la información.
- Revisar problemas tecnológicos derivados de las necesidades de privacidad detectadas en la fase anterior.
- Revisar los procedimientos y planes de seguridad de la información existentes.
- Testear la seguridad de la tecnología de la información.
- Ayudar en las pruebas sobre las debilidades existentes en los procedimientos en torno a la privacidad.

Las tecnologías sobre las que tenemos que reflexionar en cada uno de los aspectos necesarios se pueden clasificar perfectamente en:

1. Tecnologías para la protección de la información almacenada en sistemas.
2. Tecnología para la protección de los datos en tránsito.
3. Tecnología para la protección de las comunicaciones de voz.
4. Tecnologías para la protección física de las copias de información.
5. Tecnología para el cumplimiento de las especificaciones de “Puerto Seguro” (Safe Harbor).

En este punto resulta fundamental conocer lo que la tecnología nos ofrece y seleccionar los elementos que nos permitan afrontar cada uno de estos aspectos.

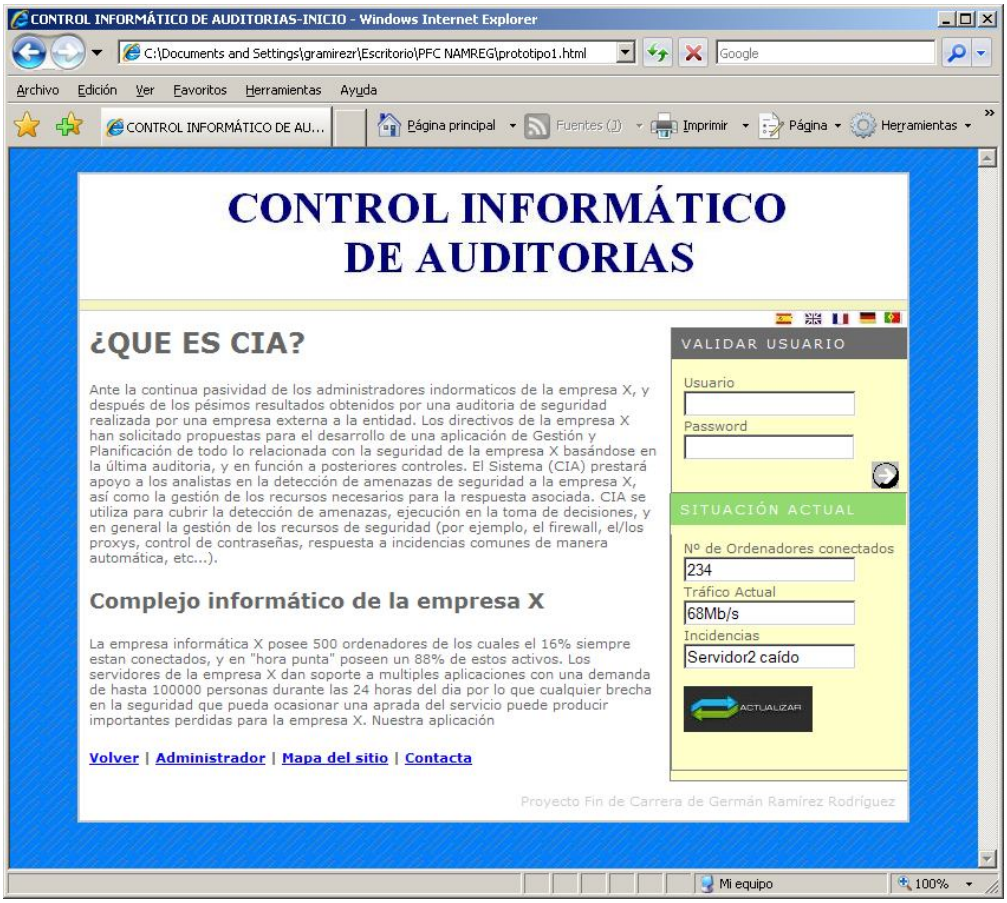
En cualquier caso, es **IMPRESCINDIBLE** que el subcomité tecnológico del Grupo de trabajo revise las capacidades, conocimientos y certificaciones de todo el staff responsable de la gestión de la red y control de los productos de software, y recomendar formación adicional si fuera necesario. En términos tecnológicos, los sistemas se constituyen tan seguros como los conocimientos de las personas que los operan. No caigamos en el repetido error de dar la operación de determinados sistemas a personas inexpertas o sin la debida formación. Todos los sistemas requieren ser operados por personal cualificado y certificado. No descuidemos este aspecto que la experiencia nos enseña, ya que puede ser fuente de posteriores problemas o vulnerabilidades en la integridad del sistema.

12. Definición de una aplicación que afronta este problema:

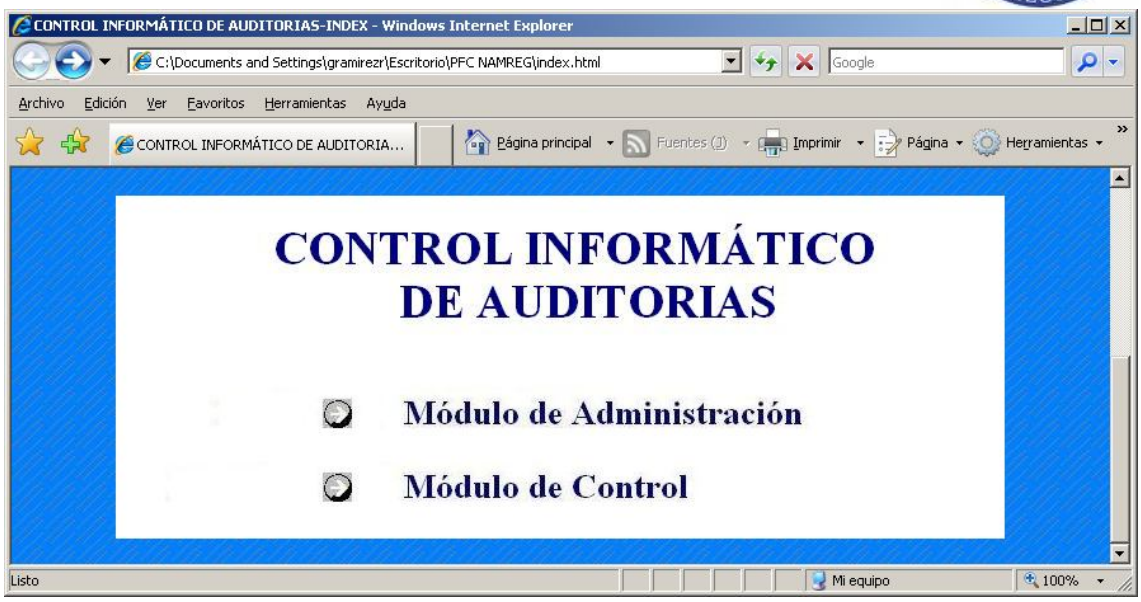
Todo lo expresado hasta el momento en esta publicación puede parecer mas o menos interesante, pero una solución al problema que estoy dejando entrever es la creación de una aplicación que sea capaz de controlar que en una empresa se están siguiendo una serie de rutinas recomendadas bien por una auditoría, bien por ser procedimientos definidos en base a la experiencia de los departamentos de la empresa; muchas veces la dirección de las empresas entregan el control de esta tarea al departamento de sistemas y en caso de empresas de mayor volumen al departamento de calidad.

Mi propuesta consiste en una combinación de auditoría informática, del modelo COBIT y la estandarización de procesos como en las certificaciones del tipo CMMI, todo ello acompañado de la experiencia del departamento de sistemas que instale esta aplicación en su empresa y que podrá aportarle el software o datos que considere necesario. La idea es crear una aplicación que sea capaz de testear a una empresa desde su red hasta el control de procesos en base a su metodología software detectando que tareas no se están realizando, localizando los fallos de seguridad existentes, aportando nuevas ideas para generar una mayor seguridad y eficiencia en la empresa, así como localizando en que puntos un proyecto no esta siguiendo las pautas correctas que pueden llevar a un fracaso de este tanto en tiempo como en costos. Todo ello combinado con el constante control de que todo siga realizándose tal y como se ha definido por los responsables de área, e informando de su incumplimiento a los responsables definidos previamente.

La aplicación “Control Informático de Auditorías” (CIA de ahora en adelante) responde a todas estas necesidades de una manera centralizada e indexada, es decir, combina el funcionamiento de varios programas software registrando y testeando sus resultados para informar en caso de anomalías, también gestiona la documentación de cualquier proyecto informando de si se esta siguiendo los procedimientos de la manera adecuada y con los datos adecuados. CIA permite el acceso a toda la información en cualquier momento siempre y cuando se disponga de los permisos adecuados.



Disponer de un módulo de control multipuesto proporcionará un apoyo fundamental para los departamentos de calidad, de sistemas o los jefes de proyecto, puesto que permite canalizar buena parte de los procesos y controles diarios, además de una mejora significativa para los usuarios de los recursos de la empresa, ya que se sientan las bases para poder obtener la obtención de certificaciones en base a la realización de procedimientos en los proyectos, y controla los niveles de seguridad y eficiencia de la red de la empresa con atención especializada desde la propia empresa.



Este módulo de control multipuesto gestionará las agendas de los usuarios poniendo especial atención a incluir en ellas "citas" para (recordar) la realización de procesos como son: Realizar Back-ups, mantener actualizado la documentación de los proyectos, control de los hitos de cada proyecto, control de licencias y equipos, el módulo será la puerta de entrada a partir de la cuál los usuarios podrán acceder a estos servicios, ofreciendo la lista de incidencias dirías, de tareas a realizar por el usuario, y todo lo relativo a los equipos y profesionales que dependen de ellos.

La inclusión de todas las agendas en el módulo, permitirá que desde cualquier punto se pueda obtener un informe del estado actual de la empresa, o de cada uno de los eslabones que la componen pudiendo realizarse una nueva consulta o prueba diagnóstica en cualquier momento.

El usuario puede solicitar un informe del estado actual de la red para una hora determinada, y la aplicación realizará los procesos pertinentes para la obtención de ese informe de manera automática, además, al integrarse con el servidor de correo, permite al usuario concretar con más personas la realización del informe para organizar una reunión e incluso que estas personas puedan solicitar nuevos diagnósticos actualizados para la reunión.

La integración de las agendas para facilitar el acceso a las mismas no es obstáculo para que su gestión continúe descentralizada y bajo la responsabilidad de las unidades que hasta ahora han estado realizando esta tarea.

Con el fin de garantizar el éxito de la aplicación, no basta con tener la tecnología más puntera, sino que hay que tener en cuenta otro tipo de factores tales como son el modelo organizativo, el modelo metodológico, la adecuada gestión del cambio, el compromiso firme de todos los departamentos involucrados en el proyecto, etc., siempre asegurando la máxima motivación de los distintos colectivos que utilizarán el sistema.

Podemos invertir mucho dinero en tecnología y sin embargo no estar mejorando nuestra situación actual, debemos adaptarnos a los requerimientos del entorno

El proyecto deberá contar con el liderazgo de representantes al más alto nivel de la organización, así como disponer de un equipo de trabajo interno, capaz de desarrollar un criterio propio y de proponer decisiones en base a las recomendaciones u opciones presentadas por el equipo de proyecto.

Para que sea eficaz, el proceso participativo deberá estar guiado, de modo que se identifiquen claramente los pasos a seguir y la función de cada uno de los intervinientes. Aquí la labor del departamento de sistemas y de los jefes de equipo de todos los proyectos es más que importante ya que su experiencia fijará el ritmo de la implantación y la dirección a seguir en cada momento.

En este sentido, entendemos que el papel de este grupo en el proyecto debe caracterizarse por:

- Aportar soluciones y modelos estándar de mercado que sirvan de punto de partida a los procesos de especificación de requisitos y toma de decisiones. En general no se trata de inventar nuevas soluciones tecnológicas, sino de encontrar la mejor combinación de elementos que cubra las necesidades de la empresa.

- Proporcionar el equipo de trabajo con los niveles de especialización técnico y funcionales necesarios para elaborar, a partir de los requisitos y necesidades detectadas, los trabajos de detalle que conduzcan a la implementación final del sistema.

- Aportar un punto de vista práctico. Las soluciones propuestas deben ser realistas y orientadas a su posterior implantación, teniendo siempre presente no sólo la bondad de dichas soluciones desde el punto de vista técnico, sino también su adecuación a las características particulares de la empresa, así como la viabilidad de su implementación en la herramienta software seleccionada SAP y su mantenimiento posterior.

Objetivo del programa

- Localizar vulnerabilidades del sistema de información.
- Control de número de licencias en uso y necesarias de la empresa.
- Control de la actividad de los servidores de la empresa.
- Control y gestión de recursos empleados en cada proyecto.
- Control del flujo de datos en la red de la empresa.
- Control de la generación de documentación de cada proyecto.
- Seguimiento del cumplimiento de hitos de los diferentes proyectos.
- Gestión documental referente a cualquier proyecto de manera que pueda reutilizarse en el futuro como experiencia.
- Garantizar que una empresa mantiene su nivel de calidad mas haya de posibles certificaciones obtenidas en el pasado.

Ámbito de la aplicación

- Jefes de proyecto.
- Área de gerencia de la empresa.
- Departamento de calidad de la propia empresa.
- Departamento de sistemas de la propia empresa.
- Departamento de seguridad de la empresa.
- Dirección técnica de la empresa.
- Área de gobierno de la empresa.

¿Por qué usarlo?

Podría nombrar varias razones para argumentar que un proyecto de este calibre es **necesario** para cualquier empresa que quiera mantener el control sobre todo lo relativo a los proyectos y seguridad de su empresa, pero prefiero centrarme en que seamos conscientes del valor que tiene esta aplicación de cara a futuros clientes, es decir, al igual que el disponer de una auditoría posibilita o certificación a una empresa para poder afrontar proyectos de una mayor envergadura, responde a la necesidad y/o requerimientos de clientes que desean saber que disponen de un modelo contrastado con el que se obtienen resultados en los plazos indicados, la aplicación CIA garantiza mantener el control sobre todos los proyectos de acuerdo al nivel de calidad exigido por el cliente o por la propia empresa.

Un enfoque metodológico es la base de un buen funcionamiento siempre que este flexibilizado con la ayuda de los responsables de departamento adaptándose a cada momento y evolucionando con el tiempo para poder ser integrado en la aplicación, por ejemplo, un proyecto de 1 año podrá soportar más carga de trabajo en sus inicios por disponer de sus recursos al 100% pero en periodos vacacionales no se podrá disponer de ellos en un 100% y habrá que distribuir el trabajo de una manera coherente.

La metodología exige un conjunto de mecanismos orientados a asegurar el cumplimiento de las características enumeradas. Estos mecanismos son los siguientes, y que se definen al inicio del proyecto:

- Definición de las herramientas de trabajo y acuerdo sobre su forma de uso.
- Definición de estándares de documentación y comunicación interna del proyecto, previo acuerdo de los miembros del Comité de Seguimiento y Dirección Operativa.

- Seguir un método para el Desarrollo de Proyectos como por ejemplo Métrica V3, cuya misión principal es proporcionar a la compañía y a los jefes de proyectos un instrumento eficaz para desarrollar los diferentes tipos de proyectos que se realizan en ella, culminándolos repetitivamente con éxito.
- El Método es aplicable a los proyectos tanto internos como para clientes externos y facilita la gestión multiproyecto en la compañía.
- El Método para la Gestión de Proyectos lo componen:
    - Un manual corporativo, que presenta y explica las etapas, fases, procesos y pasos recomendados para la aplicación del Método, al tiempo que proporciona listas de comprobación para cada una de las fases del ciclo de vida del proyecto y formatos estándar para la documentación y transmisión de los datos clave del proyecto.
    - Una carpeta de guías, técnicas, herramientas y normas aplicables, aplicables a la gestión de proyectos corporativas, del área y unidad de negocio.
- El Método para la Gestión de Proyectos Métrica V3 es consistente con los estándares marcados por el Project Management Institute (PMI) en el Project Management Body Of Knowledge (PMBOK), que actúa “de facto” como norma internacional para la gestión de proyectos.
- PMI es la organización internacional de referencia para quienes se dedican profesionalmente a la gestión de proyectos. Cuenta con más de 200.000 miembros en 150 países.
- PMI establece estándares para la gestión de proyectos, organiza seminarios, desarrolla programas formativos y edita publicaciones especializadas dirigidas a aquellos profesionales interesados en la calidad y buenas prácticas en el ámbito de la gestión de proyectos. Asimismo otorga certificaciones PMP (Project Management Proffesional) a aquellos profesionales que acrediten la adecuada formación y/o experiencia y superen un riguroso examen, entre otros requisitos.
- Las características más destacadas del Método Métrica V3 para la Gestión de Proyectos son las siguientes:

  - Está basado en el ciclo de vida del proyecto y dispone de listas de comprobación al final de cada fase del mismo.
  - Promueve la aplicación a lo largo del ciclo de vida del proyecto de los factores de gestión contrastados por la experiencia y la investigación como críticos para el éxito del mismo, tales como la definición de la misión del proyecto, la planificación, las tareas técnicas o la resolución de problemas.
  - Comprende los procesos clave de gestión de proyectos en un procedimiento integrado (Gestión de clientes, Gestión conjunta de actividades, calendario y costes, Aseguramiento de calidad, Gestión de configuración y Gestión de riesgos) y facilita la aplicación de otros procesos complementarios o de mejora de la gestión como Ingeniería Concurrente o Calidad Total.
  - Proporciona guías y herramientas para facilitar su aplicación.
  - Es un instrumento eficaz en el ámbito de la gestión de proyectos para reforzar la integración de las diferentes áreas y personas que intervienen en la ejecución de un proyecto.
- Mejora de los contenidos de cada Biblioteca, incluyendo ejemplos de buenas prácticas identificados por el uso de los proyectos.
- Creación de nuevas bibliotecas de buenas prácticas demandadas por Unidades de Gestión y áreas.
- Inclusión de herramientas útiles para los responsables de proyecto a la hora de diseñar la estructura metodológica de su operación.

Debemos hacer especial hincapié en que toda la formación que se desarrolle sea por la necesidad directa identificada en las operaciones, para dar soluciones concretas a necesidades productivas concretas, en el soporte y ayuda a operaciones concretas (a la hora de poner en marcha la metodología), y en la accesibilidad internacional mejorada mediante el soporte multi-idioma

Ideas y Ventajas.

La idea principal consiste en sacar el máximo rendimiento de la experiencia acumulada por los diferentes departamentos de la empresa, sus conocimientos pueden ser utilizados en la aplicación controlando los factores que ellos consideran más importantes para la empresa. Todo este trabajo aplicado es accesible tanto por los propios responsables de los diferentes departamentos como por los dirigentes de la empresa gracias a la universalidad de la aplicación, la cual permite tanto modificar los procesos y aplicaciones que realiza de manera automática como los resultados y partes estadísticos que puede generar en cualquier momento.

Su universalidad se basa en la capacidad de adaptación a los diferentes programas del mercado, tanto para su ejecución y obtención de resultados. Todo ello combinado con la seguridad ofrecida por el certificado digital, lo cual autentica al usuario unívocamente ofreciendo los servicios de integrabilidad, autenticidad, gestión de la información de cada usuario así como el no repudio de las acciones de cada usuario.

Me gustaría hacer referencia a un artículo escrito por D. José de Jesús Angel Angel sobre "*Como comprar un software de seguridad informática*" donde se resalta una y otra vez que lo que buscamos debe adaptarse a lo que conocemos y necesitamos, para ello debemos buscar al personal adecuado para asesorarnos y ser conscientes de los servicios que deseamos cubrir, todo ello subrayando que no una mayor inversión económica nos proporcionará un producto que funcione mejor:

"Muchas veces cuando se quiere proveer de "seguridad" a un sistema de información, una de las decisiones mas difíciles es decidir que tipo de software tenemos que adquirir y que método me permite hacerlo, sin duda, la decisión definitiva depende de un estudio detallado y largo, según sea el tamaño de la corporación a la cual queremos proveer de seguridad. Sin embargo en muchas ocasiones tanto se carece de los recursos como del personal adecuado para poder realizar dicho estudio, en muchos casos se justifica un gasto que permita realizar satisfactoriamente todo el proceso, pero en otros muchos casos no es posible hacer ese gasto, pero entonces, cómo proveer de seguridad a nuestra información sin caer presa de los vendedores, en muchos casos muy lejanos de la verdadera solución.

Existe una forma no simple pero si esquemática de cómo hacer tal elección, el detalle consiste en por ejemplo haciendo la similitud a una "enfermedad", si alguien tiene una molestia y quiere resolver ese problema además de quedar inmune a esa y otras "enfermedades", entonces lo que hace es acudir a un médico, pero quedan dos opciones mas, una mejor y otra no buen vista, la primera consiste en acudir a un especialista que supondríamos resolverá nuestro problema de manera mas contundente, por otro lado existe solo acudir a una farmacia y pedir alguna "medicina", el primer método es frecuentemente mas costoso, el segundo es muy riesgoso y en muchos casos contraproducente.

[…]Después de todo esto el médico en base a su experiencia y preparación emite un diagnóstico del posible mal y dictamina que medicamentos debemos de ingerir, y de que forma debe de ser administrado.

Pues bien, en el caso de la seguridad de la información es algo parecido a este proceso, el comprar un "producto" que "cure" nuestros problemas de seguridad es similar a comprar los "medicamentos" que debemos de ingerir para curar alguna eventual "enfermedad" y/o prevenirla. Entonces

el problema es contratar a un "doctor" que nos proporcione un diagnóstico y a partir de ahí nos recomiende que tipo de solución necesitamos, es claro, que quizá en muchos casos no es rentable realizar esto, por lo tanto por mientras no podamos conseguir a un profesional de la seguridad de la información, tan fácil como un médico, quizá baste que el encargado actual de nuestro sistema haga ese trabajo. Entonces, que método tenemos que seguir para poder comprar la solución adecuada a nuestro problema, pues bien al igual que en el caso médico primero debemos identificar que "enfermedad" tenemos o cuales son nuestras debilidades para así fortalecerlo. Como en el caso de la salud de un humano hay veces que es muy difícil saber que enfermedad se tiene e incluso si es una enfermedad totalmente desconocida o nueva, así mismo en el caso de la seguridad de la información existen "enfermedades" que aun no se conocen o que son muy complicadas. Sin embargo hay otras que están muy bien identificadas y pueden ser curadas satisfactoriamente, este tipo de "enfermedades" de la seguridad de la información tienen ya una "medicina" conocida y efectiva. Entonces el principio para poder tener seguridad en la información, lo básico es saber si tenemos esas "enfermedades" ya conocidas y entonces podremos administrar con seguridad la "medicina" que es efectiva ya en ese caso.

Pues bien es un grave error sin saber que tipo de problema tenemos decidamos comprar una "medicina", es decir, un producto que se nos ofrece por alguna otra razón.

Así también es un error muy frecuente que quienes venden algún producto desconocer por completo para que sirven realmente y en muchas ocasiones superestimar o equivocar lo que realmente hacen los productos.

Bien, entonces el método que se sugiere es reconocer que "enfermedades" tiene nuestro sistema y así poder adquirir el producto que sea efectivo para tal caso. Algunas de las similitudes a "enfermedades" conocidas de la información son; no tener confidencialidad, no tener integridad de datos, no autenticar al usuario, el no poder rechazar la autoría de un mensaje, el controlar el acceso, la confirmación de una acción, etc. Además de saber que "mal" tenemos que "curar" también tenemos que saber donde esta localizado y que tan grave pueda ser, quizá no sea necesario ni una "curita", de forma similar, a que como todos sabemos siempre en nuestro cuerpo existen bacterias malignas que sin embargo si la población no es considerable, entonces no representan problema alguno

Lo anterior representa el lenguaje actual de la seguridad de la información, así pues ***dado algún sistema de información nuestro primer paso es identificar que tipo de problema de seguridad podemos tener y así comprar el producto exactamente necesario y/o realizarlo uno mismo.***

Veamos un ejemplo:

Este ejemplo se refiere a un sistema que todo mundo conoce, así poder identificar más fácilmente que tipo de problemas de seguridad tenemos. Entonces veamos el escenario de un cajero automático (ATM), en este caso dividamos el sistema en tres partes, la parte del cliente, es decir donde físicamente tenemos al cajero automático, la parte de la transmisión de la información, y la parte del banco, que es donde se procesa la información que se envía desde el cajero.

En el caso del cajero tenemos los problemas o las eventuales "enfermedades" de, ***control de acceso*** *(permitir con seguridad que un usuario entre con seguridad al sistema del cajero), el problema de* ***autenticación*** *(como poder estar seguro de que el poseedor de la tarjeta es el dueño), el problema de el* ***no repudio*** *(como estar seguro de que un cliente no pueda negar que efectúo una operación, por ejemplo que retiro efectivo), etc.*

Ahora en el caso de la transmisión de la información, ésta en general se lleva acabo por medio de micro-ondas y se trasmite de una antena del cajero a otra antena en el banco. En este caso los problemas existentes son primero la ***confidencialidad****, es decir como estar seguro que la información enviada viajara sin ser vista por personas no autorizadas, también tenemos el problema de la* ***integridad****, es decir que nos garantiza que la información no vaya ha ser cambiada, modificada o borrada, etc.*

Para la tercera parte, los problemas son primero el verificar la autenticidad del origen de la información, es decir como saber si realmente la información que llega es de un cajero real, además si la transacción solicitada sea realmente la que se solicita. Otro problema mas es la autorización del banco, así como que el banco no pueda rechazar la operación que autorizo, etc.

Los problemas anteriores o "enfermedades" que pudiera tener nuestro sistema tienen solución, es decir hay "tratamiento" para ello, y entonces poder adquirir un producto o una marca de "medicamento" que cure estas "enfermedades".

Existen dos problemas entonces como saber que tipo de "enfermedades" eventuales puedo tener, y que producto "medicina" hay para poder curarlo.

Por ejemplo:

1) *El problema ("la enfermedad") de la confidencialidad en la transmisión de la información por un canal inseguro, se puede resolver si existe en ambos lados de la comunicación un algoritmo simétrico que cifre la información antes de salir del origen y que la descifre en el momento en que llegue a su destino. Los algoritmos usados en este caso pueden estar en software o en hardware, y son variados los productos que lo tienen integrado, los algoritmos más recomendados actualmente son TDES, RC4-128, AES. El problema de la confidencialidad también puede darse por ejemplo en una base de datos permanente, donde se desea que esta información deba de ser vista solo por personas*

autorizadas, en este caso también puede cifrarse la información y ser descifrada solo cuando se quiera utilizar. Este problema lo podemos tener por ejemplo en: la transmisión de información por Internet, el envío de e-mails, llamadas telefónicas, transmisión de radio, transmisión de televisión, secretos industriales, secretos de estado, etc.

2) *El problema de la Integridad, puede controlarse por medio de un esquema que usa una* ***función Hash*** *que determina si la información ha sido modificada o borrada, en este caso se toman las medidas que proceden en el caso necesario. Este tipo de esquemas también se pueden tener tanto en software como en hardware. En nuestro ejemplo la integridad se debe de tener ya que si un usuario realiza un retiro de 300 dólares, esta orden no debe de ser alterada para el buen cumplimiento de la cuenta del cliente. Este problema por ejemplo, puede encontrarse también en voto electrónico, donde es prioritario no alterar los resultados, en los archivos de un abogado, donde es prioritario no alterar documentos que pueden ser evidencia para algún litigio, en la transmisión de alguna transacción bancaria alta, etc.*

3) *El problema de la autenticación, es uno de los más complicados de resolver, aun actualmente, el demostrar la identidad de una persona, es uno de los mas grandes problemas que existen, en la practica se ha resuelto de varias formas, cuando la comunicación es a larga distancia como Internet la firma digital ha llegado a ser la mejor forma de poder autenticar tanto a una persona como a una entidad, aunque existen limitaciones y algunos problemas de adaptación. Actualmente el algoritmo de firma digital más usado se llama RSA. El algoritmo de firma digital esta contenida en un elemento que se llama certificado digital. El problema de la autenticación se presenta en una variedad muy grande de aplicaciones, por ejemplo al cambiar un cheque, al viajar por avión, al hacer algún tramite, al firmar un contrato, o simplemente al identificarse con una autoridad, etc. En nuestro ejemplo el problema de la autenticación lo tenemos al demostrar que el portador de una tarjeta es el verdadero dueño, en este caso se usa un esquema de identificación vía un NIP, es decir si el poseedor de la tarjeta conocer el NIP que corresponde a la tarjeta, entonces el dueño es quien teclea el NIP correcto. Otro problema de autenticación lo tenemos en saber de donde*

provienen los mensajes, a este tipo de autenticación se le conoce como autenticación del origen de los mensajes, y se resuelve con un algoritmo MAC, por ejemplo lo tenemos en nuestro ejemplo al mostrar que los mensajes provienen precisamente del cajero que dice ser.

4) *Desde el punto de vista legal un problema muy importante es el no-repudio, que el resolverlo representa una manera probatoria de que alguien no niegue ser autor de ciertos actos. El no-repudio se resuelve con la firma digital, conjuntamente con un esquema de time-stamping. Por lo general estos servicios se contratan de forma independiente ya que tiene que haber un elemento legal extra que lo confirme. Estos servicios se contratan con un notario electrónico, conjuntamente con un certificado digital. En nuestro ejemplo este problema no es resuelto, es decir que no existen elementos probatorios legales para probar que un usuario realizo un retiro o no lo hizo, de forma similar, no existen elementos probatorios para que se le demuestre al banco que hizo o no hizo alguna emisión.*

5) *Entre otros problemas más están: el control de acceso, el anonimato, la revocación, la confirmación, la autorización, etc.*

Aunque pareciera un poco distante este vocabulario al vocabulario comercial ésta es la forma más seguras, de poder primero conocer que tipo de problema de seguridad de la información tenemos, y después de poder adquirir el producto o la solución exacta para poder reducir al mínimo el riesgo que pueda tener nuestra información.

Algo importante, es hacer notar que en muchas ocasiones es necesario ***hacer una solución a la medida del problema que tengamos por resolver,*** *sin embargo en varios casos podremos ya comprar algún dispositivo o software que este en el mercado.*

Claro esta que en la mayoría de los mercados es muy difícil que los productos tengan especificaciones tan técnicas, sin embargo el poder hacer una mejor elección del producto necesario parte de poder identificar con precisión que tipo de problema de seguridad tenemos que resolver, de la misma forma que poder encontrar a un vendedor que tenga los conocimientos adecuados para poder identificar bien la solución de nuestro problema concreto.

Vale comentar que quizá para una sola PC o un pequeño sistema si podamos evitar tal análisis, y quizá solo con un antivirus, un firewalls, la buena elección y administración de passwords y eventualmente con un certificado digital podamos contar con la seguridad óptima."

Finalmente me gustaría destacar la idea de que la aplicación pese a utilizar varios programas, los cuales generan sus propios informes, permite al usuario preparar una plantilla donde "meter" esos informes de un manera legible y comparativa, es decir, tanto si genera un pdf, como un texto plano como unas gráficas, la aplicación da la posibilidad al usuario de tratar los datos de la manera que considere mas interesante para él, de esta manera, la aplicación almacenará la información que resulte realmente útil para solución de futuros errores o generación de partes estadísticos de rendimiento.

13. Experiencias previas del alumno.

Durante 3 años he trabajado principalmente como becario de sistemas en varias empresas e instituciones y quisiera compartir algunas de las experiencias obtenidas de estos trabajos:

Trabajé durante 2 años en una importante institución académica como becario de redes y telefonía. En aquella institución se intentaba llevar un control con más o menos eficiencia de las incidencias informáticas producidas por los usuarios o el propio servicio de informática, la aplicación se encontraba en su segunda versión por lo que presentaba una serie de herramientas realmente útiles como puede ser el caso de no solo buscar incidencias únicamente por usuario si no también por despacho, o tipo de incidencia, o combinación de otros parámetros. Hasta aquí, es lo que esperamos de cualquier servicio de informática de cualquier empresa o institución de un tamaño medio-grande. Pero ahora definiré problemas detectados, como se dieron lugar a ellos y como se detectaron:

- Al comenzar mi trabajo se me informó de que existía una 2ª aplicación donde se actualizaban los datos de todos los edificios de aquella institución en lo referente a las rosetas de datos y teléfono. Además, coincidí durante un mes con un técnico que me informó de además una hoja de cálculo donde se recogían los datos de los 3 edificios de los que yo me hacía cargo con el único fin de que el resto de la gente perteneciente al CAU pudiera conocer si en caso de que un usuario les preguntase por la conexión de una roseta, ellos pudieran responder si tenía conexión y cual era la dirección IP que debían configurar para el ordenador. Cual sería mi sorpresa cuando después de realizar el proceso por duplicado durante 10 meses, cuando hablando con mí responsable de las comunicaciones de datos de toda la institución, me dijo que desconocía dicha hoja y que dejara de introducir datos en ella por temas de seguridad. Mi responsable no estaba informado de tal hoja, y de hecho quería que no existiera tal hoja, por lo que se comunicó con el jefe del servicio

de informática de mi área quien respondió que “siempre se había hecho así”. Al parecer con la construcción de los edificios se partió de este rudimentario método para llevar la información de las conexiones, pero ahora simplemente se mantenía por inercia y por parecer algo útil para la comunicación entre departamentos. La falta de coordinación entre responsables, así como la **no existencia** de un “manual de procedimientos” habían desembocado en esta situación que por supuesto traería más consecuencias.

- La empresa que nos suministraba el servicio de conexión y datos frecuentemente nos mandaba “avisos” de que algunas ip´s estaban descargando contenido con derechos de autor, por lo que solicitaban que se cortara la conexión y finalizara la descarga de esos contenidos. Hubo un caso frecuente basado siempre en una conexión que poseía la misma MAC desde diferentes puntos de acceso, es decir, que cada vez que acudíamos a esa roseta, no había nunca un ordenador enchufado a ella, y que nos sirvió para eliminar muchas conexiones que no tenían porque estar hechas, el final resultó ser que una persona de mantenimiento la cual había llamado algunas veces solicitando al CAU información sobre diferentes rosetas de diferentes despachos a donde tenía acceso en horas de trabajo, conectaba su portátil para descargar datos con derechos de autor, esta persona fue descubierta debido a que dejó en una ocasión su portátil conectado dentro de uno de los centros de datos donde él conectaba directamente su portátil al conmutador el cual por defecto le daba una dirección dinámica.

- Como norma se me explicó que al trasladar un ordenador de un sitio a otro, la conexión de la roseta debía quitarse para evitar que nadie se conectara allí, este procedimiento era bastante adecuado, pero en ocasiones se vaciaban despachos sin informarnos, y luego eran ocupados por otras personas quienes conectaban sus equipos en esas conexiones produciendo problemas como ip´s duplicadas, u ordenadores en la red sin antivirus y con software peligroso. En parte algunos de estos casos no se darían de no haber existido la hoja de cálculo con la cual se informaba de la configuración de esas rosetas.

- En general estos casos no eran comunes ya que existían técnicos en el servicio de informática que formaban a los becarios para que no dieran información de las rosetas a los usuarios inicialmente, pero me reitero en que el hecho de no existir un manual de procedimientos (que más tarde se realizó) daba lugar a este tipo de errores.

- Como norma, cuando se detectaba mucho tráfico en un ordenador, este era desconectado si no estaba en una lista de servidores “permitidos”, este era “limpiado” por el servicio de informática y finalmente vuelto a configurar en su red. Los ordenadores que más sufrían este tipo de cortes eran los utilizados en stands para dar información a alumnos, ya que eran objetivos fáciles para transformarlos en servidores p2p, al no tener las actualizaciones nunca al día. Más tarde se decidió crear una red controlada en cuanto a puertos abiertos se refiere para estos ordenadores, así como el envío de una “recomendación” trimestral a los dueños de estos ordenadores para que los actualizasen.

- Era curioso como se llevaba un control exhaustivo de las conexiones realizadas en cada centro de datos, pero como no se controlaba parte del material, es decir, de cara a conocer el patrimonio de una institución no se controlaban los teléfonos que se ponían, ni los que quedaban en almacén, sin embargo cuando existió un problema de actualización de teléfonos, la empresa que nos suministraba el servicio de voz ofreció cambiar los modelos antiguos por nuevos, pero al ir sustituyéndolos, no se disponía mas que de poco mas de la mitad de los que supuestamente se tenía, esto, en principio significaba que se habrían ido estropeando, y al no poder ser reparados y/o estar fuera del periodo de garantía eran deshechos, pero sin quedar constancia de ello, la empresa suministradora del servicio de voz fue la mayor beneficiada de esta falta de control.

- En vista de todo lo aprendido, y observado en este trabajo, como despedida y para mis futuros sucesores realicé un manual de procedimientos que para mi satisfacción se utilizó para instruir a mi sucesor. En él definía como se realizan las cosas y porque se hacen así, ya que en muchas ocasiones el realizar las cosas como siempre se han hecho daba lugar a la no necesidad de realizar estas acciones, bien por ser recurrentes, o por ser en perjuicio sin ser conscientes de ello. No tiene sentido realizar un procedimiento si, este a su vez depende de otro departamento, y este no es informado de ello. Solo el conocer porque se hacen las cosas, y para que influye directamente en que estas se realicen correctamente.

- En los servidores y centros de control, se intentaba colocar los cables adecuadamente para que no fuera una locura después localizar las conexiones, pero no servía de nada todo esto si las siguientes conexiones que se hacen no siguen este mismo control, es decir, hay que seguir un procedimiento y no hacer lo que venga mas cómodo en ese momento, porque si no, nos encontramos con realizar tareas de 2 minutos en 5-10min.

Mas tarde trabajé durante ocho meses como becario de sistemas en una consultora informática de la que más tarde sería trasladado a otro centro como técnico informático y trabajando para la filial de una empresa internacional. Durante esos ocho meses aprendí mucho más a fondo el funcionamiento de una empresa en cuanto a la gestión de datos se refiere, aprendí desde configurar ordenadores en base a un estándar de la empresa hasta como todos los días se realizaban copias de seguridad de cierta información, semanalmente de otra, y finalmente una mensual de mayor tamaño. Todo ello me llevó a "ver las 2 caras de la moneda", es decir, puede resultar muy útil hacer cambiar a los usuarios su contraseña cada 3 meses, pero si luego la ponían en un papel pegado al monitor, ¿de que servía? Era importante realizar las copias de seguridad, pero si no se comprobaban si los soportes seguían funcionando correctamente después de algunos años ¿para que las hacíamos? Intentaré resumir mis "experiencias" en los siguientes puntos:

- Como administradores de sistemas teníamos acceso a cualquier ordenador de la empresa, pero eso no debería de permitirnos ver la pantalla de los usuarios en cualquier momento. Es decir, mi responsable me explicó como usar un par de programas para utilizar remotamente ordenadores, este programa tenía la opción de pedir al usuario que estuviera delante de su ordenador la autorización, pero claro, esto es un procedimiento y no siempre dábamos a que apareciera el requerimiento de dicha autorización. ¿de que sirve decir que seguimos una normativa si luego lo hacemos "a veces"? Es como si poseemos la ISO por reciclar todos los materiales como corresponde, pero a la hora de verdad echamos el papel a la papelera porque "nos pilla mas a mano", y un envoltorio de un caramelo al papel de reciclaje porque "nos pilla de paso", incluso algo que no parece tan grave como no destruir los currículos de candidatos como exige la normativa porque "hoy no funcionaba la destructora". Son detalles, es verdad, pero si queremos que se nos certifique por hacer algo, debemos respetar ese "algo" siempre, es por ello que muchas certificaciones deben renovarse cada cierto tiempo demostrando

que siguen haciéndose las cosas como en el momento de certificarse.

- Como norma general a cualquier usuario nuevo se le daba como contraseña inicial “123456” y se le obligaba a cambiarla al iniciar por primera vez haciendo que esta estuviera caducada, pero todo esto valía de poco si el usuario volvía a poner de contraseña “123456” o tecleando su mismo nombre de usuario en la contraseña porque “así no se le olvidaba”.

- En mi anterior trabajo ya había sido consciente de lo que era tener un centro de control de datos demasiado confuso por no poner un poco de atención a ordenar todos los cables de las conexiones, y en esta ocasión era consciente de la locura existente, intenté organizarlo, pero se me pidió que no lo hiciera ya que mis cambios producían parones de trabajo, y en principio me pareció lógico, el problema vino el día que unos compañeros confundieron 2 rosetas y en vez de conectarse a donde debían, crearon un bucle inutilizando el 80% de la red de la oficina, ese día durante 4 horas revisé todos los servidores de la oficina sin saber porque había todo dejado de funcionar hasta que caí en la cuenta de que algunos usuarios se habían trasladado de sitio, con lo que habían modificado sus conexiones, al revisarlas una por una, localicé como una conexión independiente de ADSL, entraba a una salida de uno de los switch, como otro servidor que debía conectarse independientemente a la red local iba directo a otro servidor, finalmente encontré una tercera conexión que unía al primer y último switch que casualmente estaban conectados en cascada haciendo un bucle entre todos ellos. El haber tenido orden en los cables del centro de control, así como apuntada y controlada todas las conexiones de la oficina hubiera reducido notablemente estas 4 horas de búsqueda.

- Me parece interesante la idea de esta empresa de re-vender los equipos informáticos antiguos a los empleados a un coste muy básico para así poder deshacerse de ellos, e incluso sacarles algún "provecho" pero no entiendo como ordenadores que han sido servidores, o simplemente que han contenido software de la empresa son vendidos con un simple formateo, en principio estos ordenadores no van a causar "problemas" ya que los tienen actuales empleados de la empresa, pero hay muchas herramientas para sacar la información de los discos duros de una manera casi gratuita para poder ver desde el código de algún programa que haya estado en el ordenador, hasta las cuentas de correo con todo lo que esto representa en los ordenadores o el código completo de una aplicación desarrollada en el ordenador.

- Algo que marcó un antes y un después en la empresa, y en el control de equipos informáticos fueron 2 infecciones llegadas por el uso de "pen-drive" de manera sucesiva, supuestamente todos los equipos poseían un antivirus corporativo actualizado, pero algunas veces los usuarios cancelaban la actualización del antivirus para "no retrasarse" o lo desconectaban en algún momento para poder utilizar algún tipo de aplicación en ese momento. Los usuarios eran administradores de sus máquinas y por ello responsables de ellas, pero si los usuarios no ponían atención en estos detalles, y sin un software que comprobara las maquinas, estos ordenadores estaban a merced de casi cualquier troyano o virus. Y Así fue, un usuario trajo música en un "*pen-drive"* con un *troyano* y la infección no tardó en extenderse a la oficina, todos los ordenadores con antivirus desactualizados fueron infectados, a partir de ese momento se tomaron 2 nuevas normas en la empresa. Los usb eran inutilizados para conectar soportes de datos desde el departamento de sistemas, y semanalmente desde sistemas se dedicarían a comprobar que las maquinas de la oficina poseían antivirus actualizado mediante software. Hasta el momento solo se habían comprobado los antivirus y actualizaciones de los ordenadores de la empresa solo

si una persona del departamento de sistemas accedía al ordenador por algún problema.

- Sorprendente fue el día que recibimos un envío del servicio técnico que nos atendía por temas de garantía de los ordenadores de la empresa, y para acolchar la caja del lector de DVD del envío utilizaron papel “en tiras” de algunos documentos y facturas de ellos, de primeras la idea me pareció genial, por la manera de reutilizar papel y contaminar menos ya que el corcho utilizado en embalajes es altamente contaminante, pero también pienso que fue un error usar el papel obtenido de una destructora con las cuchillas en mal estado lo que provocaba que no todo estuviese cortado, además de usar como ” materia prima” correos de uno de los comerciales de su empresa, ya que perteneciendo a otra empresa pude leer, un pedido para un proyecto de otra empresa realizado al comercial del SAT, puede parecer poco importante, pero que yo tuviera acceso a esa información de esa manera tan indirecta no era algo que debiera producirse en condiciones normales.

- Un día la conexión a Internet de la empresa falló, el proveedor tenía problemas con uno de nuestros servidores que estaba recibiendo un ataque y decidió “cortar la conexión”. El jefe de sistemas habló reiteradas veces con el proveedor del servicio para re-establecer la conexión, conexión que se reestableció hasta que los técnicos del proveedor junto al jefe de sistemas localizaron un problema derivado de un puerto abierto en la conexión del servidor el cual permitía por una vulnerabilidad del sistema operativo administrar el equipo, siendo este servidor usado como servidor *p2p.* Quizás el control de actualizaciones de estos servidores de una manera regular y no esporádica hubiera evitado problemas como este.

Finalmente de la consultora informática pasé a trabajar como técnico informático en una filial conjunta con otra empresa internacional que se hacía cargo de un proyecto de bastante envergadura donde vi realmente la cantidad de cosas que se hacen mal en una gran empresa, cosas como que existan manuales de procedimientos pero que nadie los haya leído, cosas como que existan aplicaciones para controlar maquinas de la empresa, y nadie sabe como funcionan porque las hizo alguien que ya no estaba trabajando con ellos, pero que ahora mas o menos funcionan “re-iniciándolas” :

- Como técnico se me explicó desde el primer día como dar respuesta a las incidencias más comunes (70% de los casos), pero no fue hasta pasado mes y medio cuando descubrí debajo de una gran pila de papeles algunos manuales de procedimientos para responder a las incidencias, quizás leer estos manuales hubiera restado horas de explicaciones a mis compañeros.

- Existía una aplicación accesible desde el wifi de la entidad con la cual se controlaban todas las impresoras de la entidad (unas 200 en total) y nadie sabía exactamente como configurarla, pero funcionaba, un técnico que había trabajado allí la creó cuando se instalaron como complemento a la configuración de la red en su día para ahorrar problemas de desplazamiento con las impresoras, actualmente se utilizaba de manera diaria, pero esta aplicación a veces no funcionaba y se sabía que reiniciándola una o dos veces, volvía a funcionar y permitía controlar las impresoras, aunque el periodo de reinicio de la aplicación dejaba sin supervisión las impresoras durante unos 20 – 30 minutos. Pienso que formalizar esta aplicación de una manera más “corporativa” y estable sería lo correcto, además de que eliminar su acceso desde el wifi de un lugar de acceso público sería bastante mas seguro. No olvidemos que conocer el código de esa aplicación permitiría controlar posibles vulnerabilidades no tenidas en cuenta por su creador años atrás.

- Pasaron 2 meses hasta que me enteré también de manera fortuita de que existía una aplicación para guardar las incidencias que ocurrían diariamente, aplicación que usaban solo algunos técnicos sin tener muy claro su fin y no de manera regular. Solo uno de ellos la usaba con asiduidad puesto que la aplicación fue idea suya y la usaba como “base de conocimiento” para los casos que no recordaba como resolver o que simplemente nunca había visto pero algún compañero sí.

14. ¿Es la solución una certificación?

En otras palabras ¿seguir un modelo prefijado como lo son las certificaciones de calidad de desarrollo software solucionaría este tipo de problemas?

La respuesta no es ni un “sí” ni un “no” por la simple razón de que lo importante no es seguir un modelo prefijado, sino ubicar todos tus procesos en base a ese modelo descubriendo de esta manera si no estas realizando procesos vitales en tu organización, además de organizar de una manera coherente todo lo que realizabas antes por simple inercia. De esta manera estaremos cumpliendo con los objetivos básicos de una empresa de servicios: **Mantener satisfecho al cliente**, y **rentabilizar todo lo queque se hace.** “*Lo mejor es enemigo de lo bueno*” por ello debemos saber que es lo que necesitamos exactamente en cada momento.

Podemos partir de realizar un SCAMPI en nuestra empresa, lo cual identificará fortalezas y debilidades de los procesos, revelará riesgos de desarrollo/adquisición, y determinará niveles de capacidad y madurez. El SCAMPI se utiliza ya sea como parte de un proceso o programa de mejoramiento, o para la calificación de posibles proveedores. El método define el proceso de evaluación constando de preparación; las actividades sobre el terreno; observaciones preliminares, conclusiones y valoraciones; presentación de informes y actividades de seguimiento.

"*Debido a la necesidad de regularse la información que poseen las organizaciones era precisa la existencia de alguna normativa o estándar que englobase todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla, ante esta disyuntiva apareció el BS 7799, o estándar para la gestión de la seguridad de la información, un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización. Esta normativa británica acabó desembocando en la actual* ***ISO/IEC 17799:2000*** *– Code of practice information security management.* (aunque actualmente se sigue una versión de 2005)

En un principio se consideraba por parte de las empresas que tenían que protegerse de lo externo, de los peligros de Internet, pero con el paso del tiempo se están percatando de que no sólo existen este tipo de amenazas sino que también hay peligros dentro de la organización y todos éstos deberían ser contemplados a la hora de regularse. La aparición de esta normativa de carácter internacional ha supuesto una buena guía para las empresas que pretenden mantener de forma segura sus activos.

La ISO/IEC 17799:2000 o la rebautizada por ISO 27002:2005 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Esta norma se estructura en 10 dominios en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización:

- *Política de seguridad*
- *Aspectos organizativos para la seguridad*
- *Clasificación y control de activos*
- *Seguridad del personal*
- *Seguridad física y del entorno*
- *Gestión de comunicaciones y operaciones*
- *Control de accesos*
- *Desarrollo y mantenimiento de sistemas*
- *Gestión de continuidad del negocio*
- *Conformidad legal*

En resumen esta norma pretende aportar las bases para tener en consideración todos y cada uno de los aspectos que puede suponer un incidente en las actividades de negocio de la organización.

Esta norma es aplicable a cualquier empresa, ***sea cual sea el tamaño****, la* ***actividad de negocio*** *o el* ***volumen del mismo****, esto es lo que se denomina el principio de* ***proporcionalidad de la norma****, es decir que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización. De la misma forma, dos organizaciones que tengan actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos/informaciones. En pocas palabras, esta norma debe tenerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser implementados con los últimos avances, eso dependerá de la naturaleza de la propia organización.*

Como hemos comentado la ISO/IEC 17799:2000 es una guía de buenas prácticas, lo que quiere decir que no especifica como se deben proteger los aspectos que aparecen indicados en ella, ya que estas decisiones dependerán de las características de la organización. Es por ello que en la actualidad no es posible que las organizaciones se puedan certificar contra este estándar, ya que no posee las especificaciones para ello.

Por el contrario, la precursora de esta norma, el BS 7799 sí que posee estas dos partes, una primera que representa el código de buenas prácticas y una segunda que los las especificaciones para la gestión de la seguridad de los sistemas de información, y es contra esta segunda parte contra la que las organizaciones que lo deseen pueden certificarse. La ISO (Internacional Organization for Standardization) en la actualidad está trabajando para confeccionar esta segunda parte del ISO/IEC 17799 con el objetivo de que las organizaciones puedan certificarse contra esta norma de carácter internacional.

Así mismo esta normativa internacional ha servido a su vez como precursora para otras de carácter nacional y en el caso de España, en noviembre de 2002 ya surgió la normativa UNE-ISO/IEC 17799 Código de buenas prácticas para la Gestión de la Seguridad de la Información elaborada por AENOR y que a su vez está desarrollando la segunda parte de esta normativa para que las empresas de ámbito nacional puedan certificarse contra ella.

Como conclusiones se puede decir que la normativa ISO/IEC 17799:2000 debe ser utilizada como un índice de los puntos que pueden provocar algún tipo de incidente de seguridad en una organización para que éstas se puedan proteger de los mismos, sin olvidarse aquellos que puedan parecer más sencillos de controlar hasta llegar a los que pueden suponer un mayor dispendio de recursos a las organizaciones." (Artículo de Daniel Cruz en Julio 2003)

Una empresa que no sea desarrolladora de software siempre posee un equipo que se mueve con flexibilidad y rapidez para el mantenimiento de programas. Seguir un modelo certificado significa para cualquier empresa poder competir al nivel que desee, pero debe ser consciente de su compañía, es decir, ¿Qué se tiene?, ¿Qué se quiere mejorar? y ¿Qué se necesita realmente? En resumen conocer nuestro contexto. Además de que debemos saber priorizar en cada momento que necesitamos en ese momento, si nuestra empresa esta en un punto muy determinante de un proyecto, los recursos deben dedicarse a ese proyecto, y la certificación ya se tendrá en cuenta mas tarde, pero debemos saber que es lo mas importante de cada momento para saber que recursos asignar y durante

cuanto tiempo, porque también es importante los recursos que empleamos en esta tarea, si vamos a poner a dirigir los procesos de la empresa, esta persona tiene que ser alguien experimentada y con conocimiento, ya que debe poseer credibilidad para organizar la empresa.

Todo esto nos llevará a conocer de una manera organizada nuestro avance a través de hitos, de manera que podremos diagnosticar nuestra situación en cada momento. No se trata de hacer continuas auditorías sobre la empresa, sino de localizar que se tiene en ese momento y como esta avanzando, así como dar a conocer lo que es, para que es y como lo podemos mejorar.

Un modelo como el CMM establece un conjunto de prácticas o procesos clave agrupados en Áreas Clave de Proceso (KPA - Key Process Area). Para cada área de proceso define un conjunto de buenas prácticas que habrán de ser:

- Definidas en un procedimiento documentado
- Provistas (la organización) de los medios y formación necesarios
- Ejecutadas de un modo sistemático, universal y uniforme (institucionalizadas)
- Medidas
- Verificadas

Una certificación no significa que debamos invertir una ingente cantidad de dinero en ello, pero si significa que debamos de implicarnos en ello, instituciones como AETIC colaboran con empresas para fomentar la certificación, pero podemos empezar por modelos de standarización gratuitos como los existentes en www.INTECO.es que son un primer paso para empezar a hacer las cosas de una manera coordinada, organizada y coherente. Existe además un servicio de autodiagnóstico en base a un modelo CMMI, el cual, nos detecta debilidades y da recomendaciones, además de ofrecerte un seguimiento y comparativa entre nuestra empresa y el resto del mercado.

ITIL define un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de las TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

Dicha biblioteca tiene su origen en un conjunto de libros, cada uno de ellos dedicado a una práctica específica dentro de la gestión de las TI. Tras la publicación inicial de estos libros, su número creció rápidamente (dentro la versión 1) hasta unos 30 libros, seguidamente en su versión 2 se fueron agrupando en conjuntos lógicos destinados a tratar los procesos de administración que cada uno cubre. De esta forma, diversos aspectos de los sistemas de TIC, de las aplicaciones y del servicio se presentan en conjuntos temáticos. Actualmente existe la nueva versión ITIL v3.

Aunque el tema de Gestión de Servicios (Soporte al Servicio y Entrega de Servicios) es el más ampliamente difundido e implementado, el conjunto de mejores prácticas ITIL provee un **conjunto completo de prácticas** que abarca no sólo los procesos y requerimientos técnicos y operacionales, sino que se relaciona con la gestión estratégica, la gestión de operaciones y la gestión financiera de una organización moderna.

Los ocho libros de ITIL y sus temas son:

Gestión de Servicios de TI

1. *Prestación de Servicios*
2. *Soporte al Servicio*

Otras guías operativas

3. *Gestión de la infraestructura de TI*
4. *Gestión de la seguridad*
5. *Perspectiva de negocio*
6. *Gestión de aplicaciones*
7. *Gestión de activos de software*

Para asistir en la implementación de prácticas ITIL, se publicó un libro adicional con guías de implementación (principalmente de la Gestión de Servicios):

8. *Planeando implementar la Gestión de Servicios*

Adicional a los ocho libros originales, más recientemente se añadió una guía con recomendaciones para departamentos de TIC más pequeños:

9. *Implementación de ITIL a pequeña escala*

CMMI cubre desde la explotación (CMMI-ITIL) hasta el desarrollo (CMMI-DEV) cubriendo todo el ciclo de vida, es decir, es una guía para la mejora en base a un modelo de madurez, que combinado con el Benchmark nos indica que hacer pero no como hacerlo, no es una metodología ni una gestión de proyectos, pero si una combinaciones de ambos que nos imprime un marco sobre el que moverse.

Existen 6 niveles de madurez basándonos en CMMI:

0- INCOMPLETO: El proceso no se realiza, o no se consiguen sus objetivos.

1- EJECUTADO: Proceso impredecible, pero controlado. El proceso se ejecuta y logra su objetivo.

2- GESTIONADO: Además de ejecutarse, el proceso se planifica, se revisa y se evalúa para comprobar que cumple los requisitos. (similar a METRICA).

3- DEFINIDO: Estandarización de procesos adatados a la tipología de cada proyecto y siguiendo la política de procesos de la organización:

- Desarrollo de requisitos software
- Solución Técnica
- Verificación
- Validación

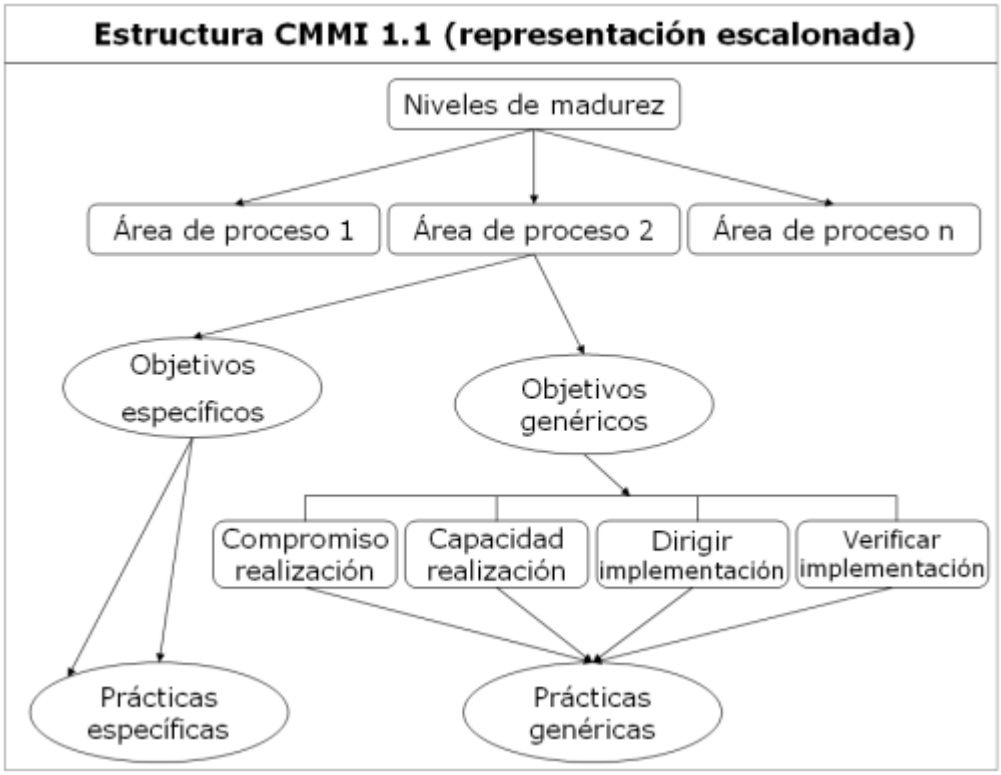
4- GESTIONADO CUANTITATIVAMENTE:

- Puesta en escena (Performance) de los procesos organizativos
- Gestión cuantitativa de proyectos

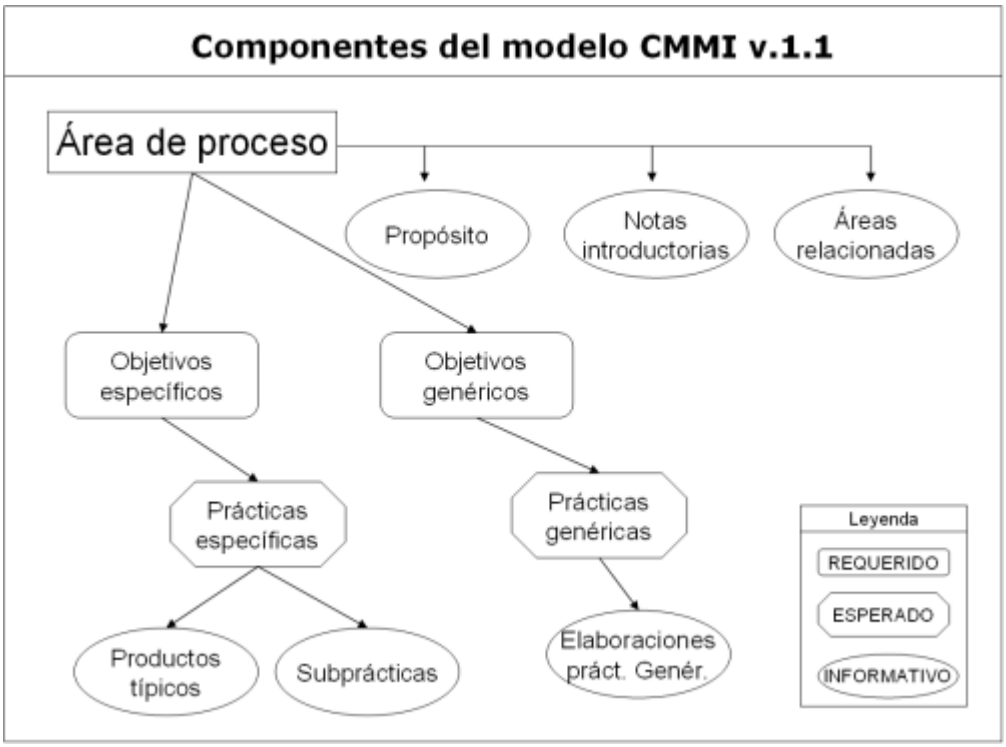
5- EN OPTIMIZACIÓN: Además de ser un proceso cuantitativamente gestionado, de forma sistemática se revisa y modifica o cambia para adaptarlo a los objetivos del negocio:

- Análisis causal
- Innovación y despliegue organizativo.
- Mejora continua.

Lo que queremos es hacer una gestión del conocimiento, es decir, que la empresa no represente una entrada y salida del producto, sino organizar unos procesos para cuando exista un problema en el producto final, poder localizar y arreglar/mejorar el producto desde el punto exacto en que sea hace mal. Seguir una estructura CMMI que dictamine como organizar los pasos a seguir es algo sobradamente útil y eficaz, pero son los jefes de proyecto los que deben decidir en cada situación que es lo que mejor se adapta a su proyecto. Por ejemplo, existe el modelo para software (CMM-SW) el cual establece 5 Niveles de Madurez para clasificar a las organizaciones, en función de qué áreas de procesos consiguen sus objetivos y se gestionan con principios de ingeniería. Es lo que se denomina un modelo escalonado, o centrado en la madurez de la organización. La selección de las Áreas de Proceso están prefijadas, habiendo 7 áreas de proceso para el nivel de madurez 2 (ML2), 11 para el ML3, 2 para el ML4 y 2 más para el ML5.



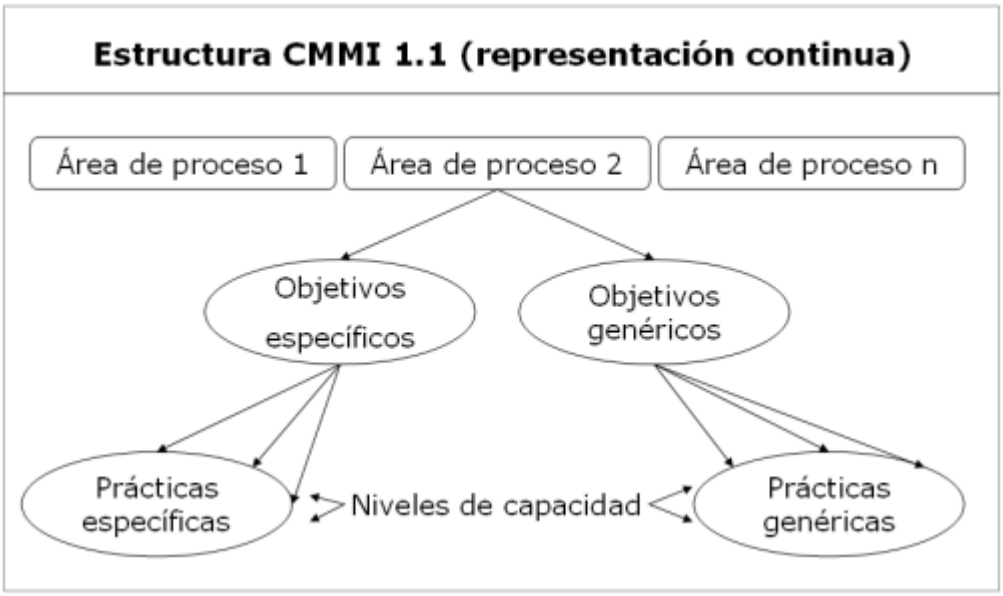
El modelo para ingeniería de sistemas (SE-CMM) establece 6 Niveles de Capacidad posibles para cada una de las 22 áreas de proceso implicadas en la ingeniería de sistemas. La organización puede decidir cuales son las Áreas de Proceso que quiere mejorar determinando así su perfil de capacidad.



En el equipo de desarrollo de CMMI había defensores de ambos tipos de representaciones. El resultado fue la publicación del modelo con dos representaciones: continua y escalonada.

No son equivalentes, y cada organización/proyecto puede optar por adoptar la que se adapte a sus características y prioridades de mejora. Pero con ello si existe un control de fases equivalente que nos indica que un Nivel de Madurez equivale a tener en un conjunto de áreas de proceso determinado un determinado Nivel de Capacidad.

La visión continua de una organización mostrará la representación de nivel de capacidad de cada una de las áreas de proceso del modelo.



La visión escalonada definirá a la organización dándole en su conjunto un nivel de madurez del 1 al 5.

En el ámbito de la gestión de seguridad informática los modelos del NIST (2003), el BS-7799 o ISO 17799 (Cano 2001) son referentes interesantes que no establecen “comos” operacionales sino que definen líneas generales de acción que deben ser afinadas y contextualizadas en la realidad de cada organización. Sin embargo en el modelo del NIST, detallado en el documento “Security Metrics Guide for Information Technology Systems”, se desarrolla el concepto de métrica de seguridad basado en la manera como se ejecutan y alcanzan objetivos y metas de seguridad informática, lo cual se materializa en los resultados deseados de la implementación de los programas de implementación requeridos para tal fin.

Esta dinámica sugerida por el modelo del NIST, esta soportada por un programa de métricas de cuatro componentes interdependientes:

- Soporte de la gerencia.
- Políticas y prácticas.
- Métricas cuantificables de ejecución y logro.
- Análisis de métricas.

Cada uno de ellos establece una serie de requisitos y procedimientos de análisis que para contar con un reporte de la gestión de la seguridad como insumo para la toma de decisiones sobre el tema, así como las responsabilidades de los niveles y cargos de las personas que intervienen.

El modelo es exigente (dado el alto grado de detalle, datos y operatividad que requiere para su aplicación) y con una alta dosis de cuestionarios requeridos para detallar cada una de las áreas de evaluación que son objeto de esta guía. Sería temerario pensar que la guía fuese la solución al complejo conjunto de relaciones que sugiere la gestión de seguridad, unida al detalle de la inversión, pero si sugiere un **camino formal para construir un puente entre la incertidumbre que propone la administración de la seguridad y el debido reporte y rendición de cuentas de los recursos** que se le entregan a la función de seguridad.

15. Glosario de Términos

Accesos Autorizados. Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
Ejemplo. El acceso que realiza la empresa de mantenimiento informático.

Afectado o interesado. Persona física titular de los datos que sean objeto del tratamiento.
Ejemplo. En esta definición entraríamos todos los individuos de los que se pueden obtener datos. Debemos tener claro, que el titular de los datos no es quien los posee en un fichero, sino el propio individuo al que corresponden esos datos.

Algoritmo MAC, (Message Authentication Code) función que devuelve un valor de longitud fija que es válida como identificador.

Autenticación. Servicio que permite poder estar seguro de que el usuario que accede al sistema es realmente ese usuario. Procedimiento de comprobación de la identidad de un usuario.
Ejemplo. Cualquier mecanismo o programa que permita identificar la contraseña de acceso, la huella dactilar, la firma electrónica, etc.

Cancelación. Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.
Ejemplo. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento. Los datos de carácter personal deberán

ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Cesión o Comunicación de Datos. Tratamiento de datos que supone su revelación a una persona distinta del interesado.
Ejemplo. Se considera cesión de datos la simple comunicación, visualización o consulta que un tercero realice, aunque sea a distancia y sin creación de un nuevo fichero o tratamiento nuevo.

Código deontológico. Es un documento que recoge un conjunto más o menos amplio de criterios, normas y valores que formulan y asumen quienes llevan a cabo una actividad profesional.

Confidencialidad, servicio que nos garantiza que la información enviada viajara sin ser vista por personas no autorizadas.

Consentimiento del Interesado. Toda manifestación de voluntad, libre, inequívoca, específica e informada, por la que el interesado consienta el tratamiento de datos personales que le conciernen.
Ejemplo. Supone que el titular autoriza el tratamiento de sus datos. Como regla general, no se podrán tratar datos de carácter personal sin el consentimiento de su titular. Además, en algunos casos concretos, la Ley exige una determinada forma de consentimiento; por ejemplo, por escrito.

Contraseña. Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.
Ejemplo. Se ha impuesto el anglicismo “password”, pero también se pueden considerar contraseñas grabaciones para reconocimiento de voz, etc.

Control de Acceso. Mecanismo que en función de la identificación ya autenticada permite acceder a ciertos datos y/o recursos.
Ejemplo. En los ficheros de nivel alto, este control de accesos debe generar un fichero lógico de control de accesos y de denegación de accesos.

Copia de Respaldo. Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
Ejemplo. Comúnmente llamada copia de seguridad.

Dato Disociado. Aquél que no permite la identificación de un afectado o interesado.
Ejemplo. Dato que no permite identificar a nadie. Por ejemplo, los datos estadísticos, que no permiten identificar a las personas.

Datos de Carácter Personal. Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
Ejemplo. Nombre, DNI, dirección, profesión, dirección de correo electrónico, datos bancarios y cualquier otro tipo de información que esté vinculada a una persona física. La Ley sólo protege a las personas físicas. Las personas jurídicas no están bajo su amparo.

Datos de Carácter Personal Relacionados con la Salud. Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.
Ejemplo. Los integrantes de la Historia Clínica, datos de minusvalía, prácticas sexuales, etc.

Derechos ARCO. Son los derechos de acceso, rectificación, cancelación y oposición.

Destinatario o Cesionario. La persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Ejemplo. La Agencia Tributaria es destinatario de los datos referentes a los salarios y retenciones efectuadas por una empresa a sus empleados.

Documento. Todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
Ejemplo. Historia clínica, una carta, una grabación de video vigilancia, etc.

Encargado del Tratamiento. La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Ejemplo. En ocasiones, la persona que efectúa el tratamiento de los datos no es el propio responsable del fichero, sino un tercero al que éste contrata para que realice una tarea en su nombre. Este tercero no decide sobre la finalidad, el objeto y el tratamiento de los datos, sino que recibe instrucciones del responsable del fichero para tratarlos. El ejemplo típico es la elaboración de las nóminas por una gestoría.

Exportador de Datos Personales. La persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.
Ejemplo. Las empresas que tienen una autorización para efectuar transferencia internacional de datos.

Fichero. Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Ejemplo. Un fichero es tanto el conjunto de fichas en papel de los pacientes que un dentista guarda por orden alfabético, como la más sofisticada base de datos de clientes de una multinacional en forma automatizada.

Ficheros de Titularidad Privada. Los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
Ejemplo. Todos los ficheros de empresas privadas o públicas, comunidades de vecinos, profesionales independientes, etc. También aquellos ficheros de entidades públicas cuya finalidad no sea estrictamente pública (por ejemplo, el fichero de Formación de un Colegio Profesional).

Ficheros de Titularidad Pública. Los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.
Ejemplo. Los ficheros de instituciones y organismos públicos, colegios profesionales, salvo que por su actividad sean considerados privados. Por ejemplo, el censo de habitantes de un municipio.

Firma digital, conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

Fuentes Accesibles al Público. Son aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.
Ejemplo. Exclusivamente son el censo promocional, las guías de servicios de comunicaciones electrónicas (guías de teléfonos), listas de colegios profesionales, diarios y boletines oficiales y los medios de comunicación social.

Función Hash, método para generar claves o llaves que representen de manera casi unívoca a un documento, registro, archivo, etc., resumir o identificar un dato a través de ella.

Integridad, servicio que garantiza que la información no vaya ha ser cambiada, modificada o borrada, etc.

No repudio, servicio que garantiza que un usuario efectúo una operación u acción dentro del sistema.

Persona Identificable. Toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.
Ejemplo. Aquella que puede ser identificada por los datos que poseemos en nuestros ficheros. Por ejemplo, número de historia clínica, fecha de nacimiento...

Proporcionalidad de la norma, todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en el tamaño de la organización a la hora de considerar la cantidad de activos a proteger.

Repositorio, almacén lógico utilizado para organizar cronológicamente los cambios de la documentación de un proyecto o de ficheros de programación de un grupo de trabajo.

Responsable del Fichero o del Tratamiento. Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Ejemplo. El responsable de los ficheros es la empresa. La palabra clave en esta definición es “decida”, que nos permitirá distinguirlo de la figura del

"encargado del tratamiento". Existen dos tipos de ficheros en función de su responsable: ficheros de titularidad pública (por ejemplo, el padrón municipal) y ficheros de titularidad privada (los mantenidos por cualquier empresa privada, por ejemplo, fichero de personal).

Responsable de Seguridad. La persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
Ejemplo. Es la persona interna de la compañía, designada por el responsable del fichero, encargada de controlar y coordinar las medidas de seguridad que se hayan implementado en la compañía. No tiene responsabilidad de cara al exterior.

Sistema de Información. Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
Ejemplo. Es el conjunto de recursos que una organización utiliza para el tratamiento de los ficheros de información.

Soporte. Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
Ejemplo. CD, DVD, Pen-Drive, disquetes, papel, etc.

Tercero. La persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del trata-miento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
Ejemplo. Cualquiera que sin autorización acceda a la información.

Transferencia Internacional de Datos. Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la

realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.
Ejemplo. El envío de un fichero de clientes de una organización a un país fuera del espacio económico europeo.

Tratamiento de Datos. Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
Ejemplo. Encontraría cabida aquí cualquier tipo de operación con datos personales: confección de nóminas, elaboración de listas de alumnos o asistentes a un congreso, envío de mailing, etc.

Usuario. Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.
Ejemplo. No confundir usuario con empleado. Usuario es cualquiera que esté autorizado al acceso a la información, aunque la vinculación con la organización no sea laboral.

16. Acrónimos

AEPD. Agencia Española de Protección de Datos: www.agpd.es.
AETIC. Asociación de empresas de electrónica, Tecnologías de Información y Telecomunicaciones de España.
ARCO. Son los derechos de acceso, rectificación, cancelación y oposición para el almacenamiento de información personal.
BENCHMARK. Técnica utilizada para medir el rendimiento de un sistema o componente de un sistema.
BS 7799, estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad.
CIA. Control Informático de Auditorías.
CMDB. Base de Datos de Configuración
CMM. Capability Maturity Model. Modelo de Capacidad y Madurez, es un modelo de evaluación de los procesos de una organización.
CMM-SW. Modelo para el Software. Se basa en la madurez de los procesos.
CMMI. Capability Maturity Model Integration. Modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software.
CMMI-DEV. CMMI para el Desarrollo. En él se tratan procesos de desarrollo de productos y servicios.
CPD. Centro de Proceso de Datos. Lugar donde normalmente se encuentran los servidores de la empresa.
CRMR. Computer resource management review. Traducido, evaluación de la gestión de recursos informáticos.
DNI. Documento Nacional de Identidad.
Firewalls. Programa que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve mas allá del firewall.
Insumo. Bien consumible utilizado en el proceso productivo de otro bien.
INTECO. Instituto Nacional de Tecnologías de la Comunicación.
ISO. Internacional Organization for Standardization. Organización internacional para la estandarización/normalización.

ITIL. Information Technology Infrastructure Library. Biblioteca de Infraestructura de Tecnologías de Información, el cual define un marco de trabajo de buenas prácticas aplicables en una empresa.

LOPD. Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

LORTAD. Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

MÉTRICA. Bases para la sistematización de las actividades que dan soporte al ciclo de vida del software.

NIST. "Security Metrics Guide for Information Technology Systems", modelo que desarrolla el concepto de métrica de seguridad basado en la manera como se ejecutan y alcanzan objetivos y metas de seguridad informática

NOTA. Programa de notificación de ficheros al RGPD: Notificaciones Telemáticas a la Agencia.

OSI. Oficina de seguridad del internauta

PMI. Project Management Institute

PMBOK. Project Management Body Of Knowledge, se utiliza como norma internacional para la gestión de proyectos.

RGPD. Registro General de Protección de Datos.

RDLOPD. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

RSA. Algoritmo de cifrado asimétrico basado en una clave pública con la que ciframos los mensajes, y una clave privada que solo conoce el propietario con la cual se descifran los mensajes.

SAT. Servicio de asistencia Técnica.

SCAMPI. Standard CMMI Appraisal Method for Process Improvement. Método oficial SEI para proveer puntos de referencia de sistemas de calificación en relación con los modelos CMMI.

SLA (Service Level Agreement). Acuerdo de Nivel de Servicio, es un documento habitualmente anexo al Contrato de Prestación de Servicios. En el SLA se estipulan las condiciones y parámetros que comprometen al prestador del servicio (habitualmente el proveedor) a cumplir con unos niveles de calidad de servicio frente al contratante de los mismos (habitualmente el cliente).

TI. Tecnologías de la información.

17. Bibliografía

Libros utilizados:

J.M. Alonso, J.L.García, Antonio Soto, David Suz, José Helguero, Mª Estrella Blanco, Miguel Vega y Héctor Sánchez. 2009.
La protección de datos personales. Soluciones en Entornos Microsoft. España. Microsoft Ibérica S.R.L.

Real Decreto:

REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (B O E núm. 17, de 19 de Enero de 2008)

Artículos:

ISO 17799: La Gestión de la seguridad. *Julio 2003 Daniel Cruz*.
http://www.virusprot.com/Art41.htm
Como comprar un software de Seguridad Informática. *Septiembre 2003*
José de Jesús Ángel Ángel http://www.virusprot.com/Art44.html
***Apuntes sobre la inversión y gestión de la gestión Informática*.** Junio 2004
Jeimy J. Cano **http://www.belt.es/expertos/experto.asp?id=2340**
La Auditoría informática dentro de las etapas de Análisis de Sistemas Administrativos. Noviembre 2000 *Eduardo Horacio Quinn*
http://www.monografias.com/trabajos5/audi/audi.shtml

Apuntes:

Miguel A. Ramos. Febrero 2008. **Apuntes de Auditoría Informática de la Universidad Carlos III de Madrid.**

Enlaces de Internet utilizados como referencias:

Fundamentos de la Gestión TI.

http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

¿Habla ITIL? http://www.axiossystems.com/es/downloads/itil.pdf

Auditoría Informática. Ingeniería del Software III. Gabriel Buades 2.002 http://dmi.uib.es/~bbuades/auditoría/index.htm

Definición de CMMI. 4 oct 2009 http://es.wikipedia.org/wiki/CMMI

Tercer congreso iberoamericano de seguridad informática. Sesión 12. Dra Sandra Cristina Riascos E. http://cibsi05.inf.utfsm.cl/presentaciones/sesion12/HERRAMIENTAS_UTILIZADAS_PARA_LA_AUDITORÍA.pdf

RDLOPD comparada a LOPD. 10 de Febrero de 2008. Audea Seguridad informática. http://www.abogados-lopd.es/noticias/rlopd-vs-lopd/

www.acens.com (algunas definiciones

Agradecimientos:

- **Miguel Angel Ramos**. Su dedicación y buen hacer me ha llevado a finalizar este libro como algo de lo que sentirme orgulloso. Gracias por contestar mis correos con tanta celeridad mostrándome los errores y el mejor camino a seguir en cada momento.

- **Antonio Folgueras.** Sus buenas maneras y su ímpetu por querer hacer las cosas lo mejor posible me han sido transmitidas desde el primer correo hasta la última palabra escrita en este documento. Gracias por ayudarme a organizar adecuadamente todo lo relacionado con COBIT para evitar que “me pusieran un ojo morado” en la presentación.

- **Profesorado Universidad Carlos III de Madrid**. En líneas generales me he sentido instruido por un gran nivel de calidad, si bien los primeros años es mas difícil encontrar buenos profesores, en los últimos me ha sido imposible no encontrarlos, tanto titulares como asociados garantizan una enseñanza ilusionante, en el tintero seguro que me dejaré alguno, pero quiero dar las gracias a: Julio Alba, Carlos Linares, Araceli Sanchís, Paloma Martinez, Fuensanta Medina, Juan Manuel Canelada, Benjamín Ramos, Pablo Martín, Raúl Pérez, Mayte Vicente, Soledad Escolar y Elisenda Molina.