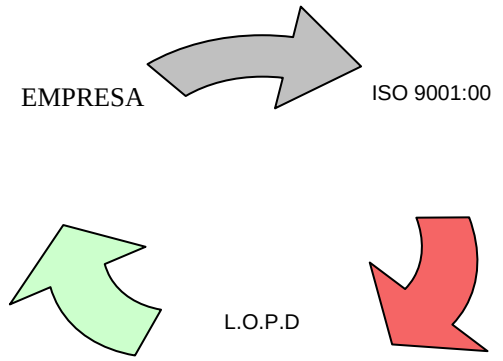
INTEGRACIÓN ISO*PD*



Guillermo Campamá
Director de
EuQuality Networks, S.L.

La integración de Sistemas es hoy, una realidad. Sistemas de Gestión de Calidad, Medio Ambiente y Prevención de Riesgos Laborales son los mayores exponentes y, sobre Gestión Integrada encuentran su lugar en nuestras relaciones de documentación externa aplicable, pero… ¿realmente todo está ya escrito?, ¿Cuántas líneas podemos todavía trazar sobre papel blanco para gestionar más datos, más enfoques, en definitiva, más información?

Un nuevo enfoque: ISO 9001:2000 + LOPD

Con motivo de la entrada en vigor de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, surgen una serie de obligaciones para aquellas empresas cuyos ficheros contengan datos de carácter personal susceptibles de tratamiento.

En lo que concierne a las medidas de seguridad de los ficheros informatizados, es aplicable el Reglamento de Medidas de Seguridad aprobado por Real Decreto 994/99, de 11 de Junio, que regula las medidas de índole técnica y organizativa que los responsables de los ficheros deben adoptar para garantizar la protección de los datos personales. Estas medidas afectan a los sistemas informáticos, soportes de almacenamiento, locales, personal, procedimientos operativos, etc.

Pero, vayamos por partes, tomemos como elemento de partida los ingredientes necesarios para definir un nuevo método y… respondamos a una última cuestión: ¿cómo gestionamos los datos personales que tratamos en nuestra Organización? La Ley Orgánica 15/1999 , de 13 de diciembre de Protección de Datos de Carácter Personal y en complemento, el Real Decreto 994/1999, de 11 de junio, que aprueba

el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, son elementos clave para el adecuado tratamiento y la correcta manipulación de los datos de carácter personal.

Nuevos requisitos, nuevos retos. Cada vez son mas los elementos que directa o indirectamente nos invitan a sentarnos ante una pantalla y volcar, una tras otra, todas aquellas notas que más acertadas en unas ocasiones y no tanto en otras muchas, nos conducen a plasmar sobre píxels de luz lo que en la práctica se debe traducir en el planteamiento de nuevos enfoques para el tratamiento de la información.

Nuevos enfoques, por combinar requisitos legales con Sistemas de Gestión no reglamentarios. Nuevas soluciones, por apostar claramente por la unión de diferentes puntos de vista sobre elementos comunes. Nuevas metodologías que nos muestran que en el mundo de la consultoría tan sólo necesitamos la excusa para poder retarnos incluso a nosotros mismos, y así convencernos si cabe, de que si simplificamos al máximo las reglas generales de gestión empresarial, ésta se reduce al tratamiento de la información, a la recopilación de datos, a su tratamiento, su análisis y su estudio para poder así, conducirnos a la toma de decisiones como base para la mejora contínua y el enfoque orientado a la excelencia empresarial.

Con todo esto, hemos visto crecer la posibilidad de integrar dos enfoques: Sistemas de Calidad según Norma UNE-EN ISO 9001:2000 y Sistemas de Protección de Datos de Carácter Personal según el Real Decreto 994/1999, y lo hemos convertido en realidad, con el único objeto de poder simplificar los métodos de control sobre la información que tratamos a diario.

En EuQuality Networks, S.L. les proponemos integrar los requisitos de la Norma ISO 9001:2000 con las medidas de seguridad establecidas por el Real Decreto 994/1999, y poder así, cumplir con la legislación vigente sin multiplicar el número de registros a cumplimentar ni la extensión de los ficheros a custodiar. Para ello, presentamos a continuación una breve introducción a cada modelo como base para establecer los elementos comunes y definir las etapas a desarrollar en un proyecto de implantación integrado.

Introducción a la LOPD

Los ficheros se clasifican en tres niveles: básico, medio y alto (*dependiendo del tipo de datos que contienen*)

- **Básico:** todos los ficheros que contengan cualquier dato de carácter personal
  - nombre
  - apellidos
  - direcciones de contacto
  - teléfono (fijo o móvil)

- **Medio:** los ficheros que contengan datos relativos a
  - comisión de infracciones administrativas o penales
  - información de Hacienda Pública
  - información de servicios financieros
  - solvencia patrimonial
  - crédito

- **Alto:** los ficheros que contengan datos
  - ideología
  - religión
  - creencia
  - Afiliación sindical
  - origen racial
  - salud
  - vida sexual
  - para fines policiales sin consentimiento de las personas afectadas

Medidas de seguridad obligatorias a aplicar para cada tipo de fichero

- **Medidas para ficheros clasificados de nivel Básico:**
  - Documento de Seguridad
  - Régimen de funciones y obligaciones del personal
  - Registro de incidencias
  - Identificación y autenticación de usuarios
  - Control de acceso
  - Gestión de soportes
  - Copias de respaldo y restaurado

- **Medidas para ficheros clasificados de nivel Medio:**
  - Las medidas de seguridad del nivel básico
  - Identificación del responsable de Seguridad

- Auditoría Bianual
- Medidas adicionales de identificación y autenticación de usuarios, gestión de soportes, registro de incidencias
- Control de acceso físico

➢ **Medidas para ficheros clasificados de nivel Alto:**
- Las medidas de seguridad del nivel básico y medio
- Seguridad en la distribución de soportes
- Registro de accesos
- Medidas adicionales de copias de respaldo y restauración
- Cifrado de telecomunicaciones

Obligaciones previstas en la Ley

Todo responsable de fichero debe:

➢ **Confeccionar el Documento de Seguridad:** el responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento, cuyo contenido mínimo viene legalmente establecido, de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información

➢ **Efectuar la inscripción de los ficheros en el RGPD:** los ficheros que contengan datos de carácter personal deberán ser inscritos en el Registro General de Protección de Datos

➢ **Someterse a una Auditoría bienal** (en caso de ficheros calificados de nivel medio y alto): los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos cada dos años

➢ **Otras obligaciones:** el responsable del fichero deberá dar cumplimiento a todas las obligaciones que la Ley va fijando a lo largo de su articulado (deberes de información, de calidad de datos, contrato regulador del acceso por cuenta de terceros….)

Introducción a UNE-EN ISO 9001:2000

La Norma se estructura en cinco grandes bloques:

- **Sistema de Gestión de la Calidad**
  - Requisitos Generales
  - Control de la Documentación y registros
- **Responsabilidades de la Dirección**
  - Compromiso, Enfoque, Política y Organización
  - Planificación
  - Responsabilidad, Autoridad y Comunicación
  - Revisión por la Dirección
- **Gestión de los Recursos**
  - Recursos Materiales
  - Recursos Humanos
- **Realización del Producto**
  - Planificación
  - Procesos relacionados con el cliente
  - Diseño y desarrollo
  - Compras
  - Control de las Operaciones del Producción
  - Control de los Equipos
- **Medición, Análisis y Mejora**
  - Medición y Seguimiento
  - Control del Producto No Conforme
  - Análisis de Datos
  - Mejora

Requisitos Generales

Toda Organización debe establecer, documentar, implementar y mantener el sistema de gestión de la calidad y mejorar continuamente su eficacia de acuerdo a los requisitos establecidos por la propia Norma, para lo cual, toda la Organización que implante un Sistema de Calidad debe,

- **Identificar los procesos de su sistema de gestión de la calidad y la interacción.**
- **A partir de los procedimientos referenciados en el Manual de Calidad, definir:**

- Los criterios y métodos de control tanto de las operaciones como de los procesos para asegurar su eficacia.
- Asegurar la disponibilidad de recursos e información necesarios para apoyar la operación y el seguimiento de los procesos.
- Realizar el seguimiento, la medición y la comparación de los procesos.
- Implementar las acciones necesarias para alcanzar los resultados planificados y la mejora continua de estos procesos.

Sistema Integrado - ISO*PD*

Elementos Comunes

Si tomamos como punto de partida y base de nuestra propuesta el Artículo 8, Capítulo II del Reglamento de Medidas de Seguridad en el Supuesto de Ficheros de Nivel Básico y el artículo 15 para Niveles Medio y Alto, observamos que la base para garantizar la adaptación a la LOPD es el desarrollo del "Documento de Seguridad", el cual, contiene los aspectos que como mínimo debe cumplir la Organización en materia de Seguridad en ficheros con Datos Personales. Del mismo modo, la Norma UNE-EN ISO 9001:2000 delega en el "Manual de Calidad" la responsabilidad de establecer el alcance del Sistema y sus documentos relacionados. Ambos son de obligado cumplimiento para el personal de la Organización y deben mantenerse en todo momento actualizados, debiéndose ser revisados cuando se produzcan cambios que puedan afectar a su integridad.

Los elementos comunes de ambos documentos nos permiten darles un enfoque que permita cumplir con ambos sistemas, para que, en un único Manual sinteticemos la información relevante y facilitemos su entendimiento y difusión a todo el personal.

NORMA UNE-EN ISO 9001:2000	
1	INTRODUCCIÓN
2	OBJETO Y CAMPO DE APLICACIÓN
3	TÉRMINOS Y DEFINICIONES
4	SISTEMA DE GESTIÓN DE CALIDAD
4.1.	requisitos generales
4.2.	requisitos de documentación
5	RESPONSABILIDADES DE LA DIRECCIÓN
5.1.	compromiso de la dirección
5.2.	enfoque al cliente
5.3.	política de calidad
5.4.	planificación
5.5.	responsabilidad, autoridad y comunicación
5.6.	revisión por la dirección
6.	GESTION DE RECURSOS
6.1.	provisión de recursos
6.2.	recursos humanos
6.3.	infraestructura
6.4.	ambiente de trabajo
7.	REALIZACIÓN DEL PRODUCTO
7.1.	planificación de la realización del producto
7.2.	procesos relacionados con el cliente
7.3.	diseño y desarrollo
7.4.	compras
7.5.	producción y presatción del servicio
7.6.	control de los dispositivos de seguimeitno y medición
8.	MEDICIÓN, ANÁLISIS Y MEJORA
8.1.	generalidades
8.2.	segumiento y medición
8.3.	control del producto no conforme
8.4.	análisis de datos
8.5.	mejora

RD 994/1999 REGLAMENTO MEDIDAS DE SEGURIDAD	
CAP. 1	DISPOSICIONES GENERALES
Art. 1	ámbito de aplicación y fines
Art. 2	Definiciones
Art. 3	niveles de seguridad
Art. 4	aplicación de los niveles de seguridad
Art. 5	acceso a datos a través de redes de comunicaciones
Art. 6	regimen de trabajo fuera de los locales de la ubicación del fichero
Art. 7	ficheros temporales
CAP. 2	MEDIDAS DE SEGURIDAD DE NIVEL BÁSICO
Art. 8	documento de seguridad
Art. 9	funciones y obligaciones del personal
Art. 10	registro de incidencias
Art. 11	identificación y autenticación
Art. 12	control de acceso
Art. 13	gestión de soportes
Art. 14	copias de respaldo y recuperación
CAP. 3	MEDIDAS DE SEGURIDAD DE NIVEL MEDIO
Art. 15	documento de seguridad
Art. 16	responsable de seguridad
Art. 17	Auditoria
Art. 18	identificación y autenticación
Art. 19	control y acceso físico
Art. 20	gestión de soportes
Art. 21	registro de incidencias
Art. 22	pruebas con datos reales
CAP. 4	MEDIDAS DE SEGURIDAD DE NIVEL ALTO
Art. 23	distribución de soportes
Art. 24	registro de accesos
Art. 25	copias de respaldo y recuperación
Art. 26	Telecomunicaciones
CAP.5	INFRACCIONES Y SANCIONES
Art. 27	Infracciones y Sanciones
Art. 28	Responsables
CAP. 6	COMPETENCIAS DEL DIRECTOR DE LA AGENCIA DE PROTECCIÓN DE DATOS
Arf. 29	competencias del director de la APD

Etapas del Proyecto

Un Proyecto de Adaptación a la LOPD para una empresa con un Sistema de Gestión de Calidad implantado, requiere del desarrollo de las siguientes etapas:

- **Fase 0:** Detallar y aprobar la propuesta de servicios a realizar. Definir la Política Marco de Actuación en relación con la Política de Calidad establecida. Definir las Funciones y responsabilidades asociadas[1]

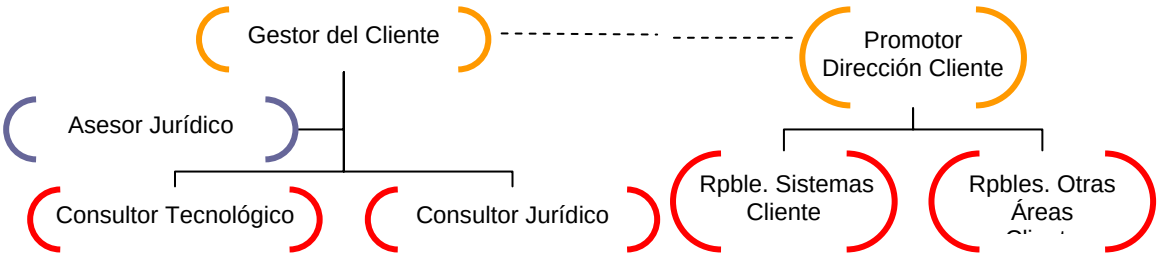
- **Fase 1:** Recogida de información, entrevistas con los responsables del sistema y servicios jurídicos, análisis de los procesos de la empresa en relación a la toma de información automatizada y no automatizada y clasificación de los ficheros.

- **Fase 2:** Revisión del manual de Calidad y de los procedimientos relacionados a continuación de conformidad a lo establecido en el reglamento:
  - Control de documentación
  - Control de Registros
  - Auditoria Interna
  - Control del Producto No Conforme

- **Fase 3:** Revisión y elaboración de los documentos necesarios para garantizar la confidencialidad de la información en los circuitos internos de la propia empresa y en su relación con terceros. Confección de recomendaciones jurídicas, organizativas y técnicas. Redacción de los contratos, formularios y cláusulas necesarias para la recogida de datos, los tratamientos por cuenta de terceros y las cesiones y comunicaciones de datos

- **Fase 4:** Notificación e inscripción de los ficheros en el Registro General de Protección de Datos

- **Fase 5:** Programación y realización de una auditoria interna al Sistema Integrado. Emisión de las Acciones Correctivas necesarias ante no conformidades detectadas.



[1] Desarrollo del Proyecto – Organización