

La Protección de Datos Personales ABADIB 2009

La Protección de Datos Personales para los colectivos de ABADIB:

**Impacto del Nuevo Reglamento de Protección de Datos y
responsabilidad de cada asociado**

Contenidos

1. Objetivos
2. Legislación y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Contenidos

1. **Objetivos**
2. Marco Legislativo y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Objetivos

Los objetivos de esta sesión son:

- ▶ Manejar el **concepto de fichero** de datos personales y que datos pueden manejar los colectivos asociados a ABADIB
- ▶ Conocer los **principios de protección de datos**
- ▶ Estar familiarizados con las **medidas** de seguridad establecidas en el Reglamento
- ▶ Conocer los aspectos básicos del **Nuevo REAL DECRETO 1720/2007**
- ▶ Conocer la **solución**, desarrollada por **Ernst & Young**, en materia de protección de datos para las Administraciones Públicas

Contenidos

1. Objetivos
2. Marco Legislativo y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Legislación en materia de Protección de Datos:

LEY ORGÁNICA 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal.

REAL DECRETO 994/1999, del 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal.

REAL DECRETO 195/2000, del 11 de febrero, por el que se establece el plazo para implementar las Medidas de Seguridad de los Ficheros Automatizados previstas por el Reglamento aprobado por el R.D. 994/1999 de 11 de junio.

REAL DECRETO 1332/1994, del 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.

REAL DECRETO 1720/2007, del 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal.

INSTRUCCIÓN 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al Ejercicio de los Derechos de Acceso, Rectificación y Cancelación.

INSTRUCCIÓN 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

INSTRUCCIÓN 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

INSTRUCCIÓN 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.

INSTRUCCIÓN 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

DIRECTIVA 97/66/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 15 de diciembre de 1997, relativa al tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones.

RESOLUCIÓN 22/2001, de 22 de junio, por la que se publica el Acuerdo del Consejo de Ministros que concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información.

Conceptos básicos

¿Cuales son las principales obligaciones de los colectivos de ABADIB en relación con la LOPD?

- ▶ Identificar los tratamientos de información
- ▶ Inscribir en el **Registro General** de Protección de Datos
- ▶ **Informar y obtener el consentimiento** (cuando sea preciso) a los titulares
- ▶ **Guardar secreto** y mantener la confidencialidad de los datos recogidos
- ▶ Adoptar las **medidas de seguridad** exigidas por la legislación
- ▶ Permitir a los titulares de los datos el **ejercicio de sus derechos**
- ▶ Deber de **colaboración** con la Agencia
- ▶ Atención de los **derechos** de los ciudadanos

En las Administraciones Públicas, la declaración de los ficheros, al igual que la modificación o supresión, exige la Publicación en Diario Oficial de los ficheros que se pretende declarar y sus contenidos

Conceptos básicos

¿Qué es la Agencia de Protección de Datos?

- ▶ La Agencia Española de Protección de Datos es un organismo oficial, creado con la finalidad de velar por el cumplimiento de la legislación sobre protección de datos personales y controlar su aplicación
- ▶ Realiza labores de divulgación a ciudadanos, entidades y empresas, centraliza todos los registros de ficheros con datos de carácter personal de todas las compañías que dispongan de éstos y que los hayan declarado a la AEPD
- ▶ Realizan inspecciones en las compañías por denuncias de los afectados o por iniciativa propia
- ▶ Impone sanciones, dependiendo de la gravedad de la infracción:
 - ▶ Infracción leve: multa de 600 a 60.000 euros
 - ▶ Infracción grave: multa de 60.000 a 300.000 euros
 - ▶ Infracción muy grave: multa de 300.000 a 600.000 euros.

Las Entidades Públicas no reciben sanciones pecuniarias, sólo Administrativas

El coste de una denuncia es mucho más alto y se valora en términos de imagen pública y depuración de responsabilidades políticas

Conceptos básicos

Plazos de Implantación

- ❑ Según Reglamento 994/1999
 - ▶ Expirados todos los plazos

- ❑ Según Nuevo Reglamento de Desarrollo de la LOPD 1720/2007
 - **Ficheros automatizados existentes**
 - Medidas de nivel medio: un año
 - Medidas de nivel alto: 18 meses
 - **Ficheros no automatizados existentes**
 - Nivel básico: un año
 - Nivel medio: 18 meses
 - Nivel alto: dos años
 - **Ficheros de nueva creación**
 - De forma inmediata a la entrada en vigor

Contenidos

1. Objetivos
2. Antecedentes y conceptos básicos
3. **Ficheros**
4. Principios de protección de datos
5. Medidas de seguridad
6. Trabajos desarrollados en TSRS
7. Documentación

Ficheros

Ficheros típicos de colectivos de ABADIB:

- ▶ **Usuarios bibliotecas**
- ▶ **Empleados**

El concepto de fichero con datos de carácter personal es un concepto “lógico”

Lo MÁS IMPORTANTE que hay que identificar es:

- Tipo de información que se maneja
- Origen
- Finalidad
- Destinatarios: Personal propio, otras entidades públicas, proveedores de servicios, etc.
- Modalidades de tratamiento: Informático, papel...

Ficheros

Clasificación de ficheros de acuerdo a los datos que contengan:

- ▶ **Nivel Básico** = datos de carácter personal
- ▶ **Nivel Medio** = infracciones administrativas o penales, Hacienda Pública, servicios financieros, solvencia patrimonial y crédito, evaluación de la personalidad del afectado o interesado
- ▶ **Nivel Alto** = ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual, policiales

Los ficheros de cada nivel deben tener implantadas una serie de medidas de seguridad organizativas y técnicas, de carácter acumulativo.

Cambios en los Niveles según el Nuevo Reglamento de Desarrollo

- ▶ **Nivel Básico** = Desde el nivel alto pasan a ser nivel bajo:
 - ▶ Datos especialmente protegidos cuando sólo se utilicen para **pago de cuotas** a entidades de las que los titulares sean miembros
 - ▶ Datos de discapacidad o invalidez cuando tengan como única finalidad cumplir una **obligación legal**
- ▶ **Nivel Medio** = Se añaden a la definición anterior los siguientes ficheros:
 - ▶ Pertenecientes a las Entidades Gestoras y Servicios Comunes de la **Seguridad Social** que tengan relación con sus competencias
 - ▶ **Mutuas** de accidentes de trabajo y de enfermedades profesionales de la Seguridad Social
- ▶ **Nivel Alto** = Se añaden a la definición anterior los siguientes ficheros:
 - ▶ Todos los datos derivados de **violencia de género**
 - ▶ Pertenecientes a operadores de servicios de comunicaciones, sobre datos de **tráfico y localización**

No es de aplicación a ficheros con datos de carácter personal de personas jurídicas, ni de las personas físicas que presten sus servicios para aquellas (nombre, apellidos, las funciones o puestos desempeñados, así como dirección, teléfono, e-mail y fax profesionales)

No es de aplicación a los datos referidos a personas fallecidas

Los productos software comerciales **deberán especificar el nivel de seguridad** que permiten alcanzar

Contenidos

1. Objetivos
2. Antecedentes y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Principios de protección de datos

Calidad de los datos

- ▶ Adecuados, pertinentes y no excesivos, en relación a la finalidad para la que se recogieron
- ▶ Exactos y puestos al día
- ▶ Cancelación cuando dejen de ser necesarios

Nuevo reglamento:

- ▶ Cancelación del dato en diez días en caso de resultar inexactos
- ▶ Notificar al cesionario de los datos la cancelación o rectificación
- ▶ Se pueden mantener los datos, previa disociación
- ▶ Para fines históricos o estadísticos, previa solicitud a la AEPD

Principios de protección de datos

Derecho de información

- Se debe informar de modo expreso, preciso e inequívoco al interesado de lo siguiente:
 - ▶ Existencia del fichero, finalidad y destinatario
 - ▶ Obligatoriedad o carácter facultativo de las respuestas
 - ▶ Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición
 - ▶ Identidad y dirección del responsable del tratamiento

Nuevo reglamento:

- ▶ Forma de recabar el consentimiento del interesado: medio sencillo
- ▶ Obtención del consentimiento a menores de edad: <14 años, padres o tutores
- ▶ Se exige la acreditación del cumplimiento del “deber de informar” por parte del Responsable
- ▶ Se podrá dar por cumplido si en el plazo de 30 días, no se obtiene respuesta del afectado
- ▶ No será necesario el consentimiento del afectado cuando se recaben los datos para el ejercicio de las funciones propias de la Administración Pública para el ámbito de las competencias que se le atribuya

Principios de protección de datos

Datos especialmente protegidos

◆ Datos de nivel alto

- ▶ Consentimiento expreso y por escrito
- ▶ Excepciones:
 - ▶ Prestación de asistencia médica
 - ▶ Ficheros partidos políticos, sindicatos, iglesias, fundaciones y asociaciones sin ánimo de lucro



Nuevo reglamento:

- ▶ Ahora se incluye el consentimiento expreso y por escrito para datos de violencia de género

Principios de protección de datos

Seguridad de los datos

- ▶ El responsable del fichero (o responsable del tratamiento) deberá adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos

Nuevo reglamento:

- ▶ Nuevas Medidas especificadas en el Reglamento de desarrollo
- ▶ Medidas para ficheros no automatizados (papel)

Principios de protección de datos

Deber de secreto

- ▶ El personal que trate datos de carácter personal deberá guardar secreto profesional sobre los mismos
- ▶ Secreto profesional que subsistirá aún después de finalizar la relación laboral



Principios de protección de datos

Comunicación de datos a terceros

- ▶ Únicamente para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario, con el previo consentimiento del interesado
- ▶ Excepciones:
 - ▶ Art. 12: No se considera comunicación de datos el acceso a los datos, cuando dicho acceso sea necesario para la prestación de un servicio al responsable del fichero = acceso a los datos por cuenta de terceros
 - ▶ Destrucción o devolución una vez terminada la prestación
- ▶ Este acceso a los datos por cuenta de terceros, deberá estar regulada por contrato (finalidad, datos, prohibición de comunicarlos, medidas de seguridad técnicas)

Principios de protección de datos

Comunicación de la cesión de los datos

- ▶ Obligación de informar al afectado, indicando la finalidad, la naturaleza de los datos cedidos y el nombre y dirección del cesionario

Nuevo reglamento:

- ▶ No será necesario el consentimiento para la comunicación de datos sobre salud, 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 la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud

Principios de protección de datos

Derecho de acceso, rectificación y cancelación

- ▶ **Acceso:** obtener gratuitamente información de sus datos de carácter personal, el origen y las comunicaciones realizadas o que se prevén realizar
- ▶ **Rectificación:** modificación de los datos cuando éstos resulten ser inexactos o incompletos
- ▶ **Cancelación:** supresión de los datos que resulten inadecuados o excesivos o para revocar el consentimiento otorgado
- ▶ Obligación, del responsable del tratamiento, de hacerlo efectivo en el plazo de **diez días**
- ▶ En el caso de haberlos cedido, el responsable del tratamiento deberá **notificarlo al cesionario**

Principios de protección de datos

Procedimiento de oposición, acceso, rectificación o cancelación

- ▶ No se exigirá contraprestación alguna por el ejercicio de esos derechos
- ▶ Las actuaciones contrarias a esta Ley pueden ser objeto de reclamación ante la AEPD

Nuevo reglamento:

- ▶ Se especifica cómo cual debe ser el procedimiento a seguir para que el interesado pueda ejercer sus derechos
- ▶ En cualquier caso, se deberá atender la solicitud del afectado aún en el caso de que éste no haya utilizado los medios previstos por la Entidad

Principios de protección de datos

Transferencias internacionales

- ▶ No se podrán realizar transferencias de datos de carácter personal a países que no proporcionen un nivel de protección equiparable al que presta la LOPD
- ▶ El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la AEPD
- ▶ Existe una lista de países los cuales la AEPD considera que ofrecen un nivel adecuado para la protección de datos personales
- ▶ En caso de transferir datos a un país distinto, se requiere la autorización previa del Director de la AEPD

Nuevo reglamento:

- ▶ Se regulan los supuestos para autorizar la transferencia de datos dentro de grupos de empresas multinacionales

Contenidos

1. Objetivos
2. Antecedentes y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Medidas de seguridad

- ▶ Documento de Seguridad
- ▶ Funciones y Obligaciones del Personal
- ▶ Registro de Incidencias
- ▶ Identificación y Autenticación de Usuarios
- ▶ Control de Acceso (Lógico y Físico)
- ▶ Gestión de Soportes
- ▶ Copias de Respaldo y Recuperación
- ▶ Responsable de Seguridad
- ▶ Auditoría
- ▶ Pruebas con Datos Reales
- ▶ Telecomunicaciones



Medidas de seguridad

Novedades en Medidas de Seguridad

Nuevo reglamento:

- ▶ Organización del Documento de Seguridad
- ▶ Inclusión de las relaciones con proveedores en el Documento de Seguridad
- ▶ **Medidas de seguridad en ficheros automatizados:**
 - ▶ Nivel Básico
 - ▶ No se permiten usuarios genéricos
 - ▶ Caducidad de contraseña < 1 año
 - ▶ Cada 6 meses se revisará los procedimientos de copias de respaldo y recuperación
 - ▶ Realizar una copia de seguridad antes de hacer una prueba con datos reales
 - ▶ Nivel Medio:
 - ▶ Ampliación del alcance de la auditoría a apartados legales conexos con RD 1720/2007 y se deberán realizar auditorías cuando se produzcan modificaciones sustanciales de información
 - ▶ La medida de pruebas con datos reales se extiende a ficheros de nivel básico
 - ▶ Nivel Alto:
 - ▶ Cifrado de dispositivos portátiles
 - ▶ El Registro de acceso no será necesario si el responsable del fichero es una única persona y únicamente accede ella

Medidas de seguridad

Nuevo reglamento:

Medidas de seguridad en ficheros no automatizados (PAPEL):

- ▶ Nivel Básico
 - ▶ Obligaciones comunes (Documento de Seguridad, Funciones y Obligaciones, Registro de Incidencias, Control de Acceso y Gestión de Soporte)
 - ▶ Archivo:
 - ▶ Garantizar la conservación, localización y consulta
 - ▶ Ejercicio de derechos (acceso, rectificación, cancelación y oposición)
 - ▶ Almacenamiento:
 - ▶ Mecanismos que obstaculicen la apertura de dispositivos de almacenamiento
 - ▶ Custodia:
 - ▶ Documentación en proceso de revisión o tratamiento custodiada por la persona a cargo e impedir acceso no autorizado
- ▶ Nivel Medio
 - ▶ Responsable de seguridad
 - ▶ Auditoría

Medidas de seguridad

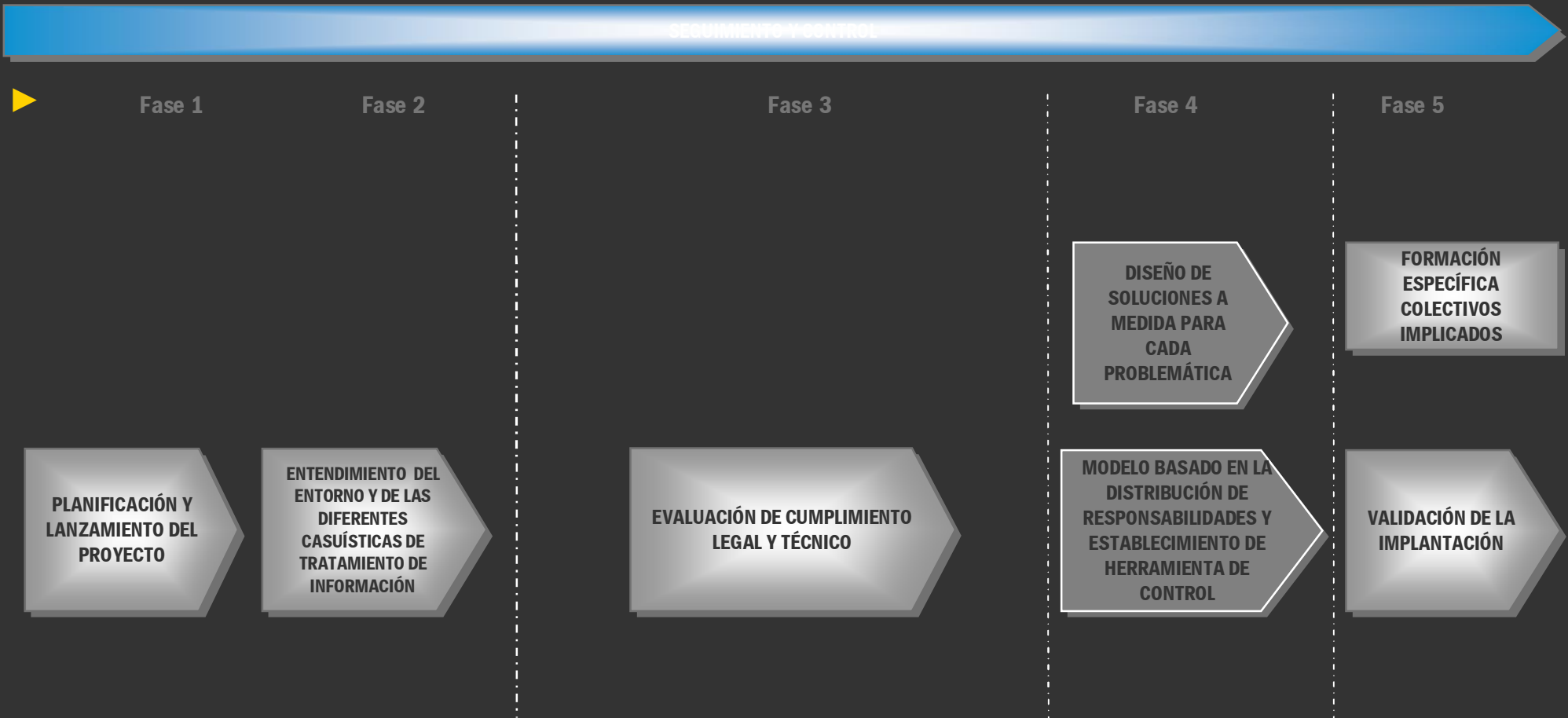
Nuevo reglamento:

- ▶ Nivel Alto
 - ▶ Almacenamiento:
 - ▶ Acceso protegido mediante llave u otro dispositivo
 - ▶ Áreas cerradas cuando no sea preciso el acceso
 - ▶ Copia:
 - ▶ La generación de copias o reproducción de documentos controlados por personas autorizadas
 - ▶ Destrucción de copias que impida acceso o recuperación
 - ▶ Acceso:
 - ▶ Limitación estricta al personal autorizado
 - ▶ Establecer mecanismos que permitan identificar los accesos realizados
 - ▶ Traslado:
 - ▶ Adoptar medidas que impidan el acceso a la información durante su traslado

Contenido

1. Objetivos
2. Antecedentes y conceptos básicos
3. Ficheros
4. Principios de protección de datos
5. Medidas de seguridad
6. Solución LOPD E&Y para Administraciones Públicas

Solución LOPD E&Y para Administraciones Públicas



Implantación Herramienta Gestión LOPD

- ▶ A lo largo de los más de 10 años que Ernst & Young ha prestado servicios de asesoramiento y auditoría relacionados con la legislación sobre protección de datos personales, nos hemos encontrado con diferentes casuísticas en diversas Entidades que han implicado un análisis exhaustivo de cada una de ellas, diseñando una solución específica condicionada por los aspectos específicos que las caracterizan
- ▶ Gracias a esta larga experiencia sectorial se han venido desarrollando verticales específicos para la mayoría de sectores que nos hemos encontrado
- ▶ A continuación se presentará como ejemplo, el modelo de solución diseñado para las Administraciones Públicas, en comunidades autónomas, corporaciones locales, ayuntamientos y entidades públicas

Preguntas

