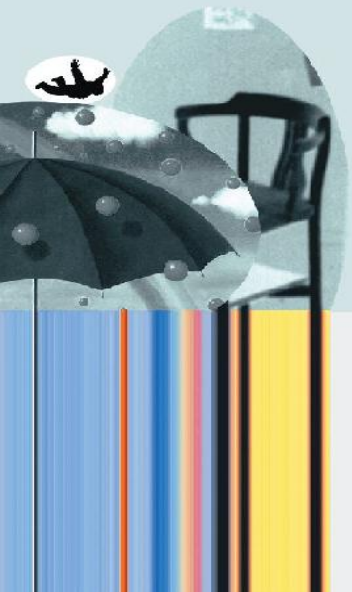
Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

El cumplimiento de las medidas de seguridad, paso a paso



- El Reglamento RD-1720/2007

El cumplimiento de la LOPD, paso a paso

- Documéntese
- Cumpla con los requisitos formales
- Cumpla con las obligaciones materiales
- Vigile y haga vigilar las medidas de seguridad

A.- Documentándose sobre la LOPD

- Como punto de partida, examine nuestra página web (www.avpd.eus).
- Lea la Ley Orgánica de Protección de Datos (LOPD, Ley 15/1999),
- Lea la Ley Autonómica de Creación de la Agencia Vasca de Protección de Datos (LAVPD, Ley 2/2004),
- Lea el nuevo Reglamento (RD-1720/2007), de Desarrollo de la LOPD

B.- Cumpliendo con los requisitos formales:

- Efectuar el inventario más completo posible de los posibles ficheros de datos personales
- Identificar las características necesarias para su declaración, recogidas en el artículo 20 de la LOPD y desarrolladas en el artículo 54 del RD-1720/2007
- Confeccionar la disposición de regulación de ficheros
- Aprobar dicha disposición y publicarla en el Boletín Oficial que corresponda
- Notificar la disposición y los detalles de los ficheros a la AVPD, mediante el programa disponible en: http://www.avpd.eus/erregistro

C.– Cumpliendo con las obligaciones materiales

- Tratar adecuadamente los Datos Personales
  - Recogida de datos
  - Mantenimiento y actualización.
  - Secreto Profesional
- Facilitar a quienes figuren en los ficheros el ejercicio de sus derechos A.R.C.O.
  - (Acceso, Rectificación, Cancelación y Oposición)
- Otras Recomendaciones:
  - Adopción de Códigos Tipo o Manuales de Buenas Prácticas
  - Prestar atención a los contratos con terceros
  - Proporcionar apoyo y formación al personal

D.- Vigilando las medidas de seguridad

- Reguladas en el RD-1720/2007
- Distingue tres niveles de exigencia para las medidas de seguridad
  - Nivel Básico
  - Nivel Medio
  - Nivel Alto
- Medidas específicas según la organización de los ficheros:
  - Ficheros no automatizados
  - Ficheros no automatizados
- Diferentes medidas (“objetivos de control”)

Niveles de seguridad

Resumen medidas nivel Básico

Ficheros automatizados y no automatizados
Art. 89. Funciones y obligaciones del personal Art. 90. Registro de incidencias Art. 91. Control de acceso Art. 92. Gestión de soportes y documentos

Sólo automatizados	Sólo no automatizados
Art. 93. Identificación y autenticación Art. 94. Copias de respaldo y recuperación	Art. 106. Criterios de archivo - posibilitar derechos ARCO Art. 107. Dispositivos de almacenamiento - mecanismos apertura Art. 108. Custodia de los soportes - en el proceso de tramitación

Resumen medidas nivel Medio

Ficheros automatizados y no automatizados
Arts. 95 y 109: Responsable de seguridad Arts. 96 y 110: Auditoria

Sólo automatizados	Sólo no automatizados
Art. 97. Gestión de soportes Art. 98. Identificación y autenticación Art. 99. Control de acceso físico Art. 100. Registro de incidencias	

Resumen medidas nivel Alto

Sólo automatizados	Sólo no automatizados
Art. 101. Gestión y distribución de soportes –Cifrado de datos. Evitar dispositivos que no permitan el cifrado Art. 102. Copias de respaldo y recuperación Art. 103. Registro de accesos –Excepción: Responsable persona física y único usuario Art. 104. Telecomunicaciones – Cifrado en redes públicas o inalámbricas	Art. 111. Almacenamiento de la información –Archivadores, áreas restringidas Art. 112. Copia o reproducción –Personal autorizado Art. 113. Acceso a la documentación –Mecanismo identificación accesos por diferentes usuarios Art. 114. Traslado de documentación –Impedir acceso, manipulación

10 Objetivos de Control de medidas de seguridad

- Organización de la Seguridad
- Documentación de Seguridad
- Funciones y obligaciones del personal
- Identificación y autenticación de usuarios
- Controles y registros de accesos
- Accesos a través de redes / Internet
- Soportes y documentos con información
- Copias de respaldo y recuperación
- Gestionar Incidencias de seguridad
- Efectuar Controles y Auditorías

1.- Organización de la Seguridad

Nivel Básico	Nivel Medio	Nivel Alto
	✓ Debe existir uno (o varios) ***Responsables de Seguridad***, designados por el responsable del fichero. ✓ Es el encargado de ***coordinar y controlar*** las medidas de seguridad. ✓ En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero ✓ También ha de gestionar la seguridad de los ***ficheros no automatizados*** (archivística)	
	Aplicable a ficheros automatizados y manuales	

2.- Documento de Seguridad - Requisitos

Nivel Básico	Nivel Medio	N. Alto
Establece y recopila, como mínimo: ✓ El Ámbito de aplicación. ✓ Las medidas, normas, procedimientos y estándares de seguridad. ✓ Las funciones y obligaciones del personal. ✓ La estructura de los ficheros y la descripción de los sistemas de información. ✓ Los procedimientos de gestión y respuesta ante incidencias. ✓ Los procedimientos de realización de las copias de respaldo y recuperación de datos. ✓ Las Medidas para el transporte, destrucción y reutilización de soportes.	Además debe contener: ✓ La Identificación del ***responsable de seguridad***. ✓ Los Controles periódicos del cumplimiento del documento.	
Aplicable a ficheros automatizados y manuales		

2.- Doc. de Seguridad – (...)

Nivel Básico	Nivel Medio	N. Alto

- En función de los sistemas de tratamiento u otros criterios, podrá ser:
  - Único, para todos (o un grupo de) los ficheros, o
  - Individualizado por cada fichero,
- Deberá recoger las situaciones excepcionales relativas a:
  - Prestaciones de servicios (82.1), uso de dispositivos portátiles (86),
  - Medidas compensatorias, imposibilidad aplicación medidas previstas
- Recogerá las delegación de autorizaciones (art. 84)
- Incluirá los ficheros externalizados, indicándolo expresamente
- Puede delegarse la llevanza del Documento de Seguridad en el Encargado de Tratamiento
- Los Encargados de Tratamiento han de incluir los ficheros que tratan por cuenta de terceros, con referencia a las condiciones del encargo
- Carácter Interno. Controlado y actualizado periódicamente

Aplicable a ficheros automatizados y manuales

3.- Funciones y obligaciones del Personal

Nivel Básico	Nivel Medio	Nivel Alto

- ✓ Las funciones y obligaciones relacionadas con el acceso a datos personales habrán de estar claramente definidas y documentadas.
- ✓ Deben definirse las funciones de control y autorizaciones delegadas
- ✓ El personal debe conocer las normas que les afecten
- ✓ El personal debe conocer las consecuencias de su incumplimiento.

Aplicable a ficheros automatizados y manuales

4.- Identificación y Autenticación

Nivel Básico	Nivel Medio	Nivel Alto
✓ Se identificará ***univoca y personalmente*** a cada usuario ✓ Procedimiento de asignación y gestión de ***contraseñas*** ✓ Periodo de caducidad para las contraseñas ***inferior a un año***. ✓ Se almacenarán de forma ***ininteligible***.	✓ Existirá un ***límite al número de intentos*** reiterados de acceso no autorizado.	
Aplicable solo a ficheros automatizados		

5.a- Control y Reg. de Accesos en ficheros automatizados

Nivel Básico	Nivel Medio	Nivel Alto
✓ Acceso únicamente a los datos y recursos necesarios ***para sus funciones***. ✓ Relación actualizada de ***usuarios*** y ***perfiles*** y sus accesos autorizados. ✓ Mecanismos para evitar el acceso con distintos derechos. ✓ Concesión de derechos por personal autorizado.	✓ Existirán controles de ***acceso físico a los locales*** donde se encuentren ubicados los sistemas de información.	✓ Existirá un ***Registro de Accesos*** donde figurará: ✓ usuario, hora, ✓ fichero, tipo acceso ✓ registro accedido. ✓ Bajo el control del responsable de seguridad. ✓ Se hará un ***informe mensual***. ✓ Se conservará al menos durante 2 años. ✓ ***Excepción***: ✓ Accede una única persona física
Aplicable a ficheros automatizados y manuales	***Aplicable solo a ficheros automatizados***	

5.b- Control y Reg. de Accesos para ficheros manuales

Nivel Básico	Nivel Medio	Nivel Alto
✓ Acceso únicamente a los datos y recursos necesarios para sus funciones. ✓ Relación actualizada de usuarios y perfiles y sus accesos autorizados. ✓ Mecanismos para evitar el acceso con distintos derechos. ✓ Concesión de derechos por personal autorizado.		✓ El acceso se limitará al ***personal autorizado***. ✓ Habrá mecanismos para ***identificar los accesos*** a documentos disponibles para múltiples usuarios ✓ Procedimiento en el Documento de Seguridad para registrar los ***accesos de otras personas***
Aplicable a ficheros automatizados y manuales		***Aplicable solo a ficheros manuales***

6.- Acceso y transmisión mediante Telecomunicaciones

Nivel Básico	Nivel Medio	Nivel Alto
✓ Las medidas de seguridad exigibles a los accesos mediante redes de comunicaciones, ***sean públicas o privadas***, deberán de garantizar un nivel de seguridad ***equivalente*** al los accesos en ***modo local***		✓ La transmisión de datos a través de redes de telecomunicaciones ✓ ***Públicas (Internet)*** ✓ ***Inalámbricas (WiFi)*** se realizará ***cifrando los datos*** o mediante cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros
Aplicable solo a ficheros automatizados		

7.a- Gestión de Soportes para ficheros automatizados

Nivel Básico	Nivel Medio	Nivel Alto
✓ ***Inventario*** de soportes ✓ Acceso restringido. ✓ ***Salida autorizada*** de soportes, incluso eMail. ✓ Medidas en el traslado para impedir pérdidas, … ✓ Medidas para ***impedir la recuperación*** de datos de soportes desechados o reutilizado. ✓ Debe identificarse el tipo de datos que contienen.	✓ Habrá un registro de ***entrada y salida*** de soportes.	✓ "Cripto-Etiquetado" ✓ Distribuir soportes ***cifrando*** los datos u otro mecanismo que impida el acceso. ✓ Cifrado de ***dispositivos portátiles***. ✓ Excepciones, al DS
Aplicable a ficheros automatizados y manuales	***Aplicable solo a ficheros automatizados***	

7.b- Gestión de Soportes y Docs. para ficheros manuales

Nivel Básico	Nivel Medio	Nivel Alto
✓ Se aplicarán ***criterios de archivo*** que permitan la conservación, localización y consulta ✓ Los dispositivos de almacenamiento tendrán ***mecanismos que obstaculicen su apertura*** ✓ Cuando la documentación no se encuentre archivada, su depositario ***deberá custodiarla*** e impedir accesos no autorizados		✓ El acceso a armarios, archivadores, etc. estará protegido mediante ***puertas con cerradura***. Cuando no se acceda, permanecerán cerradas. ✓ Soluciones alternativas, ***motivadas*** en el Documento de Seguridad ✓ Siempre que se proceda al ***traslado físico de documentación***, deberán adoptarse medidas para impedir su acceso o manipulación
Aplicable solo a ficheros manuales		

8.- Procedimientos de Respaldo y Recuperación

Nivel Básico	Nivel Medio	Nivel Alto
✓ Procedimientos de copia para respaldo y recuperación, al menos semanalmente ✓ Garantizar la reconstrucción de los datos al mismo estado en que se encontraban en el momento de la pérdida o destrucción. ✓ Verificación semestral de su definición, funcionamiento y aplicación ✓ Pruebas con ***datos reales*** con mismo nivel de seguridad y con copia de seguridad		✓ Las copias de respaldo y los procedimientos de recuperación se conservarán en un ***lugar diferente*** de donde se encuentren los equipos.
Aplicable solo a ficheros automatizados		

9.- Procedimiento de Gestión de Incidencias

Nivel Básico	Nivel Medio	Nivel Alto
✓ Debe existir un Registro de Incidencias con: ✓ tipo de incidencia, ✓ cuándo se ha producido, ✓ persona que la notificia, ✓ persona a quien se comunica ✓ efectos derivados.	✓ Además, debe contener: ✓ Procedimientos efectuados para recuperación de los datos, ✓ persona que lo ejecuta, ✓ datos restaurados ✓ datos grabados manualmente. ✓ Es necesaria la autorización por escrito del responsable del fichero para su recuperación.	
Aplicable a ficheros automatizados y manuales	***Aplicable solo a ficheros automatizados***	

10.- Controles del Documento de Seguridad y Auditorías

Nivel Básico	Nivel Medio	Nivel Alto
✓ Realizar controles periódicos ✓ Mantener actualizado el Documento de Seguridad		

	✓ Al menos una auditoría cada dos años.
	✓ Cuando se realicen modificaciones sustanciales
	✓ Puede ser interna o externa.
	✓ Debe dictaminar sobre:
	  ✓ Adecuación de medidas y controles.
	  ✓ Deficiencias identificadas
	  ✓ Medidas correctoras necesarias.
	✓ El responsable de seguridad debe:
	  ✓ Analizar el informe de Auditoría
	  ✓ Elevar sus conclusiones al responsable del fichero
	✓ A disposición de la APD	

Aplicable a ficheros automatizados y manuales		

Quién hace qué?

Medidas de Seguridad	Respons. Fichero	Respons. Seguridad	Personal
Organización de la Seguridad	***Designar***	**Participar**	
Documento de Seguridad	***Decidir políticas***	***Elaborar Aplicar***	Conocer
Funciones y obligaciones del personal	**Definir *Actuar***	**Documentar**	***Cumplir***
Identificación y autenticación de usuarios		***Definir pol.*** **Implantar**	***Cumplir***
Controles y registros de accesos		**Implantar *Gestionar***	Conocer
Accesos a través de la redes de comunicaciones		***Implantar Gestionar***	Conocer
Soportes y documentos con información		**Definir pol. *Gestionar***	***Cumplir***
Copias de respaldo y recuperación		**Definir pol. *Supervisar***	
Incidencias de seguridad	***Actuar***	**Anticipar *Gestionar***	**Cooperar**
Efectuar Auditorías y Controles periódicos	**Decidir**	**Encargar *Gestionar***	**Cooperar**