



Cabildo de
Gran Canaria

DEPORTES
www.grancanaria.com

CURSO DE SEGURIDAD EN INSTALACIONES Y ACTIVIDADES DEPORTIVAS.

Módulo VI

Protección de datos de carácter personal

por

José Luis Gómez Calvo

2009

CONSUMER EROSKI

Protección de Datos investigará la difusión en la Red de imágenes captadas por cámaras de seguridad

Considera que estos contenidos ponen en peligro el derecho a la imagen y privacidad de las personas

2 de octubre de 2008

La difusión en [Internet](#) de imágenes captadas por cámaras de seguridad instaladas en guarderías, gimnasios, hospitales u oficinas será objeto de una investigación por parte de la Agencia Española de Protección de Datos (AEPD), según anunció ayer su director, Artemi Rallo, que compareció en el Congreso para exponer la Memoria 2007 del organismo.

Jueves 12 de Marzo del 2009

▶ [Inicio](#) | [Contacto](#) | [Música](#) 



GIMNASIO
CENTRAL SALUD

La salud es nuestra prioridad central

Confidencialidad en el tratamiento automatizado de los datos de carácter personal de los Usuarios.

GIMNASIO CENTRAL SALUD, S.L. garantiza la confidencialidad de los datos de carácter personal facilitados por los USUARIOS y su tratamiento automatizado de acuerdo a la legislación vigente sobre protección de datos de carácter personal (Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, así como toda la normativa aplicable a esta materia).



GIMNASIO CENTRO.com
FITNESS & WELLNESS CLUB



GIMNASIO CENTRO, Fitness & Wellness Club

PROTECCION DE DATOS

- Gimnasio Centro garantiza la total confidencialidad en el tratamiento de los datos de carácter personal que se solicitan a través de la web, así como la implementación de las medidas de índoles técnicas y organizativas que garantizan la seguridad de dichos datos.

- En el caso de que los usuarios proporcionen alguna información de carácter personal, los datos recogidos en esta web serán utilizados con la finalidad, en la forma y con las limitaciones y derechos que recoge la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Los datos proporcionados por los usuarios serán incorporados, y conservados con total confidencialidad, a los archivos de carácter personal de los que es responsable Gimnasio Centro.



Santos & Rojas

Nuestro blog sobre Leyes e Internet, LOPD y LSSI

Categoría | **LOPD, Novedad**

“EL LIMBO” DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Publicado el 22 Enero 2009 por José Luis Rojas

Las **FEDERACIONES DEPORTIVAS** son otro campo abonado para la vulneración de la protección de los datos personales de las personas federadas. Son numerosas las federaciones deportivas que todavía no han regularizado su situación. Escasas federaciones territoriales correspondientes a los deportes Ajedrez, Tenis de mesa, Boxeo, etc, han procedido a la inscripción de los ficheros de datos de Federados, Nóminas, Personal y Recursos Humanos, etc. Como sabemos la inscripción del fichero es el primer paso para garantizar el derecho fundamental de los interesados pero no la única acción a realizar, pues también han de garantizarse los principios y derechos de la LOPD y, en consecuencia, la existencia de un **DOCUMENTO DE SEGURIDAD** que recoja las medidas de índole técnica, organizativa y jurídica que evite la pérdida, alteración, tratamiento o acceso no autorizado a los ficheros de datos personales.

SANCIONES



LEVES: De 600 a 60.000 €

GRAVES: De 60.000 a 300.000 €

MUY GRAVES: De 300.000 a 600.000 €



LEGISLACION:

ESTATAL



- Ley Orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal.
- 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.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.



LEGISLACION:

AUTONOMICA

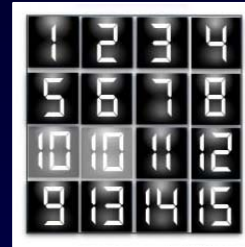


- Decreto 5/2006, de 27 de enero por el que se regulan los ficheros de datos de carácter personal de la Administración de la Comunidad Autónoma de Canarias.
- Orden de 24 de febrero de 2006, por el que se aprueban los modelos de solicitud para ejercer los derechos de acceso, oposición, rectificación y cancelación de los datos de carácter personal contenidos en ficheros e titularidad de la Administración Pública de la Comunidad Autónoma de Canarias.

QUE ES UN DATO DE CARÁCTER PERSONAL

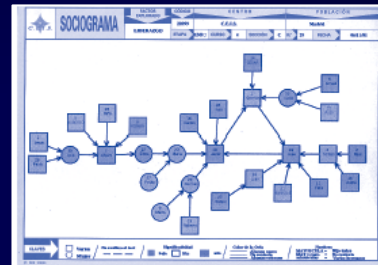
Cualquier información:

• Numérica



• Alfabética

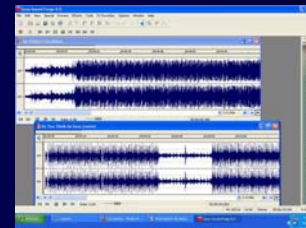
• Gráfica



• Fotográfica



• Acústica



O de cualquier otro tipo concerniente a personas físicas identificadas o identificables

SOPORTES DE DATOS

Automatizados

NO Automatizados

Ficha Empleado - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://localhost:8080/servlet/CapturaEmpleadoServlet?cmd=get&id=1 Ir

Nombre:	Pepe Lopez
Id. empleado:	1
Departamento:	Ventas
e-mail:	pepe@empresa.com

Listo Local intranet

CATEDRA DE _____

E. U. P.

CURSO: 19 97 - 19 98

Especialidad: I.T. En Informática de Sistemas

Asignatura: Téc. de Intel. Artif. en Gest. de Imág. y Docum.

Grupo: _____

Nombre: Mariano Edad: 19


Apellidos: Gutiérrez Iglesias

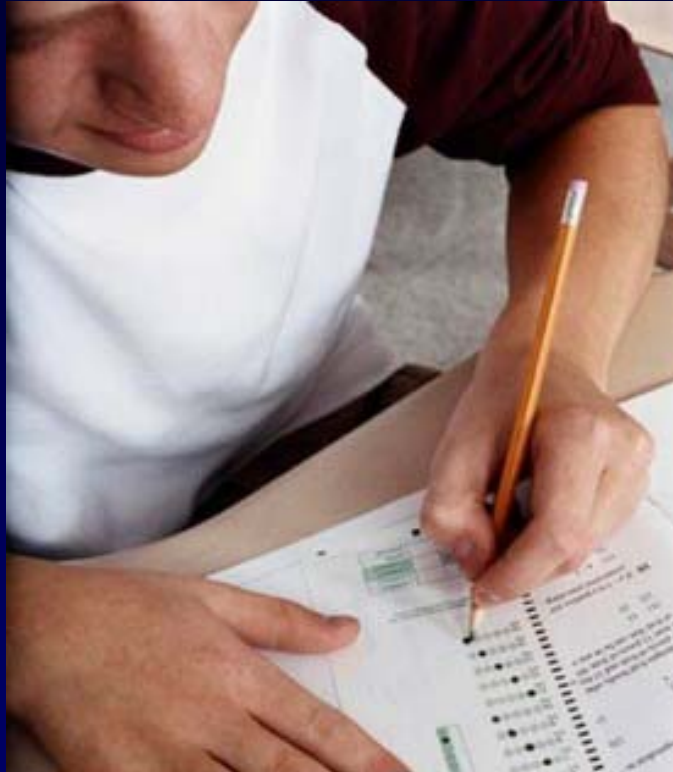
Domicilio en Córdoba: c/ José Mª Martorell, 6 3ª1ª Telf.: 41 38 90

Cursa la asignatura por primera vez

Observaciones: _____

Calificación curso anterior: _____





POSIBLES CONTENIDOS DE LOS DATOS EN EL AMBITO DEPORTIVO

- Datos de identificación personal, domiciliarios, etc.
- Datos de características o de la personalidad de los usuarios, que permitan evaluar ciertos aspectos de la personalidad o del comportamiento **DE LOS MISMOS**
- Datos de salud

FICHA DEPORTIVA

- Datos de identificación
- Historial deportivo
- Ficha técnica
- Objetivos de la temporada
- Situación laboral

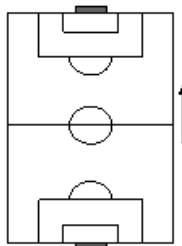
Temporada ____ - ____			
DATOS PERSONALES			
Nombre: _____			
Dirección: _____			
Telf.: _____			
Fecha nac.: _____ Lugar: _____			
Estado civil: _____			
		ALTURA Y PESO:	
		ROPA	
		Calzado nº: _____	
		Talla: _____	
		Nº camiseta: _____	
HISTORIAL			
Equipos anteriores y categoría:			

Resultados a destacar:			

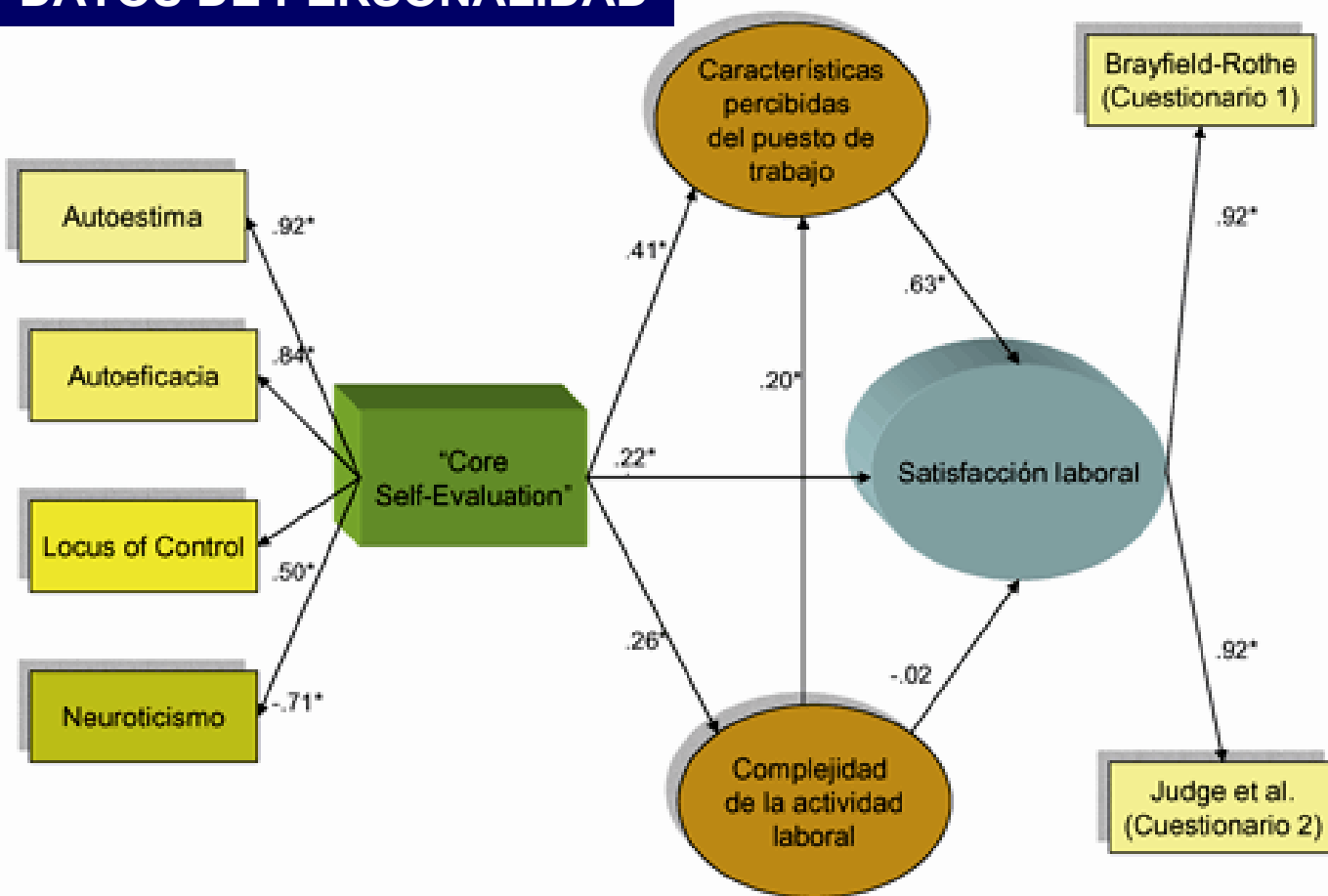
FICHA TÉCNICA			
Lateralidad: _____		Ocupación en el campo:	

OBJETIVOS en la temporada :			

SITUACIÓN LABORAL o ESTUDIO:			
_____		Lugar: _____	
Horario: _____			



DATOS DE PERSONALIDAD



*: valor significativo en el umbral de probabilidad $p < .01$

¿QUE ES UN FICHERO?

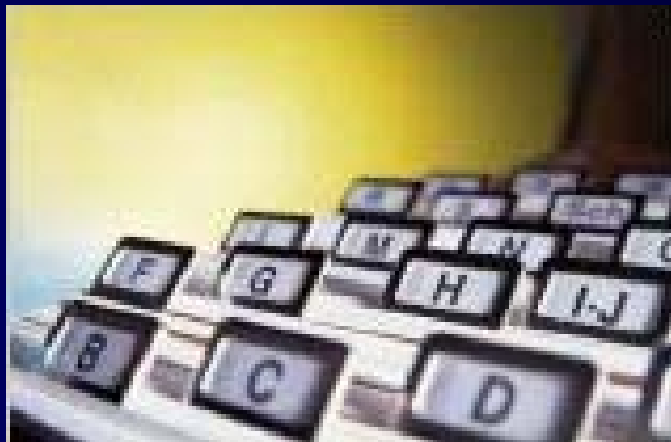
Todo conjunto organizado de datos e carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.



INSCRIPCION DE FICHEROS

Todo fichero que contenga datos de carácter personal debe ser inscrito en el Registro General de Protección de Datos, conforma al formulario disponible de forma gratuita en la web de la Agencia de Protección de Datos (www.agpd.es)

El formulario electrónico de **NO**tificaciones **T**elemáticas a la **A**EPD (**NOTA**) permite la presentación de notificaciones a través de Internet con certificado de firma electrónica reconocido



FUENTES ACCESIBLES AL PUBLICO

Son fuentes accesibles al público.

- a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999.
- b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
- c) Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
- d) Los diarios y boletines oficiales.
- e) Los medios de comunicación social

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.

ENCARGADO DE TRATAMIENTO

La persona física o jurídica, pública o privada, u órgano administrativo, que sólo 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.

.

FICHEROS DE TITULARIDAD PRIVADA

Son 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.

NOTIFICACION E INSCRIPCIÓN DE LOS FICHEROS DE TITULARIDAD PRIVADA.

Los ficheros de datos de carácter personal de titularidad privada, serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación.

La notificación deberá indicar:

- 1. La identificación del responsable del fichero.**
- 2. La identificación del fichero.**
- 3. Sus finalidad y los usos previstos.**
- 4. El sistema de tratamiento empleado en su organización.**
- 5. El colectivo de personas sobre el que se obtienen los datos.**
- 6. El procedimiento y procedencia de los datos.**
- 7. Las categorías de los datos**
- 8. El servicio o unidad de acceso.**
- 9. La indicación del nivel de medidas de seguridad básico, medio o alto exigible.**
- 10. En su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero.**
- 11. Los destinatarios de cesiones y transferencias internacionales de datos**



DERECHOS DE LOS CIUDADANOS

1. Deber de información al interesado
2. Consentimiento para el tratamiento de datos
3. Derechos de acceso, oposición, rectificación y cancelación

update '09 - turismo

El necesario cruce de ideas para afrontar la crisis en la nueva sociedad del ocio

Auténticos expertos en el arte de hacer aflorar y compartir los principales vectores de cambio y tendencias que afectarán también a nuestra industria.

Apúntese y descubrirá nuevas ideas para su negocio.

> Formalice su inscripción pinchando aquí <

Convoca:

editurinfo
Información turística profesional



SEGITTUR
turismo e innovación

Turismo2020

Conduce:

infonomia

Organiza:

LABELTUR

1. DEBER DE INFORMACIÓN AL INTERESADO

> Lugar

Auditorio Mapfre
Avda General Perón, 40
28020 MADRID

> Aforo limitado

> Inscripción gratuita
Por estricto orden de recepción

Información sobre el cumplimiento de la Ley de Protección de Datos.

De acuerdo con la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, le informamos que sus datos forman parte de un fichero automatizado propiedad de LABELTUR (C/ Major, 3 - 17473 Ventalló (Girona)) con la finalidad de promoción y difusión de nuestras actividades y servicios. Así mismo le informamos sobre la posibilidad de ejercer sus derechos de acceso, rectificación, cancelación y oposición, dirigiendo dicha petición según los términos y condiciones que establece la ley a secretaria@labeltur.com.



2. CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS

El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes (Ejemplo un censo)



2. CONSENTIMIENTO PARA EL TRATAMIENTO DE LOS DATOS **DE MENORES DE EDAD**

Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, 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

2. FORMA DE RECABAR EL CONSENTIMIENTO

El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículo 5 de la Ley Orgánica 15/1999 y 12.2 del Reglamento, advirtiéndole de que en caso de **no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.**

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.

2. MEDIO DE RECABAR EL CONSENTIMIENTO

Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos.





2. REVOCACIÓN DEL CONSENTIMIENTO

El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

3. Derechos de **A**cceso, **R**ectificación, **C**ancelación y **O**posición.



DERECHO DE **ACCESO**

Es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal :

- Están siendo objeto de tratamiento,**
- La finalidad del tratamiento que, en su caso, se esté realizando.**
- La información disponible sobre el origen de dichos datos.**
- Las comunicaciones realizadas o previstas de los mismos.**

DERECHO DE RECTIFICACIÓN

Es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

DERECHO DE CANCELACIÓN

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 al Reglamento.

DERECHO DE OPOSICION

Es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o el cese en el mismo en los siguientes supuestos:

- a) Cuando no sea necesario su consentimiento para el tratamiento.**
- b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.**
- c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado.**



**MEDIDAS DE
SEGURIDAD EN
EL
TRATAMIENTO
DE DATOS DE
CARÁCTER
PERSONAL**

Niveles de protección

- **Bajo**
- **Medio**
- **Alto**

Aplicación de los niveles en el caso del deporte

- **Bajo:** Todos los ficheros o tratamientos de datos de carácter personal, deberán adoptar las medidas de seguridad calificadas de nivel básico.
- **Medio:** 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 o del comportamiento de los mismos.
- **Alto:** Datos de salud

¿QUÉ SON DATOS DE SALUD?

“Las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo”.

Pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido.

Debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o el consumo de drogas

Fuente: Apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa



DOCUMENTO DE SEGURIDAD

**Objetivo: medidas de índole
técnica y organizativa
acordes a la normativa de
seguridad**

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS.

Medidas de seguridad de nivel básico

1. Funciones y obligaciones del personal
2. Registro de incidencias
3. Control de acceso
4. Gestión de soportes y documentos
5. Identificación y autenticación.
6. Copias de respaldo y recuperación

Medidas de seguridad de nivel medio

1. Responsable de seguridad
2. Auditoria.
3. Gestión de soportes y documentos
4. Control de acceso físico

Medidas de seguridad de nivel alto

1. Gestión y distribución de soportes
2. Copias de respaldo y recuperación
3. Registro de accesos
4. Telecomunicaciones

Las medidas de seguridad aplicables en los » **ficheros automatizados** se encuentran reguladas en los artículos 89 a 104 del reglamento que desarrolla la Ley Orgánica de Protección de Datos (Real Decreto 1720/2007) y son las siguientes:

	Medidas de seguridad	Nivel Básico	Nivel Medio	Nivel Alto
1	» Funciones y obligaciones del personal	Si	Si	Si
2	» Registro de incidencias	Si	Si	Si
3	» Control de acceso	Si	Si	Si
4	» Gestión de soportes y documentos	Si	Si	Si
5	» Identificación y autenticación	Si	Si	Si
6	» Copias de respaldo y recuperación	Si	Si	Si
7	» Responsable de seguridad	-----	Si	Si
8	» Auditoria	-----	Si	Si
9	» Gestión de soportes y documentos	-----	Si	Si
10	» Identificación y autenticación	-----	Si	Si
11	» Control de acceso físico	-----	Si	Si
12	» Registro de incidencias	-----	Si	Si
13	» Gestión y distribución de soportes	-----	-----	Si
14	» Copias de respaldo y recuperación	-----	-----	Si
15	» Registro de accesos	-----	-----	Si
16	» Telecomunicaciones	-----	-----	Si

- **Nivel básico:** Las medidas correspondientes al nivel básico (1-6) se aplican a todos los ficheros.» [\[+info\]](#)
- **Nivel medio:** Las medidas del nivel básico más las de nivel medio (1-12) se aplican a aquellos ficheros que requieren de un nivel medio de seguridad. » [\[+info\]](#)
- **Nivel alto:** Todas las medidas de seguridad (1-16) se aplican a aquellos ficheros que requieren de un nivel alto de seguridad.» [\[+Info\]](#)

DESTRUCCION DE DATOS AUTOMATIZADOS

Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá proceder 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

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS **NO** AUTOMATIZADOS.

Medidas de seguridad de nivel básico

1. Funciones y obligaciones del personal
2. Registro de incidencias
3. Control de acceso
4. Gestión de soportes
5. Dispositivos de almacenamiento
6. Custodia de soportes

Medidas de seguridad de nivel medio

1. Responsable de seguridad
2. Auditoría.

Medidas de seguridad de nivel alto

1. Almacenamiento de información
2. Copia o reproducción
3. Acceso a la documentación
4. Traslado de documentación

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS.

Medidas de seguridad de nivel alto

Almacenamiento de información

Los armarios, archivadores i otros elementos en los que se almacenen los ficheros con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS.

Medidas de seguridad de nivel alto

Copia o reproducción

Únicamente podrán ser realizadas bajo el control del personal autorizado en el documento de seguridad.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS.

Medidas de seguridad de nivel alto

Acceso a la documentación

Se limitará exclusivamente al personal autorizado.

Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS.

DESTRUCCION DE DATOS NO AUTOMATIZADOS

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

DESTRUCTORAS DE PAPEL



NIVELES DE DESTRUCCIÓN DE DOCUMENTOS

La Norma DIN 32757 establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de ese nivel

Nivel	Tamaño	
1	Tiras de un máximo de 12 mm de ancho	Documentos generales que deben hacerse ilegibles
2	Tiras de un máximo de 6 mm de ancho	Documentos internos que deben hacerse ilegibles
3	Tiras de un máximo de 2 mm. de ancho Partículas de un máximo de 4x80 mm.	Documentos confidenciales
4	Partículas de un máximo de 2 x 15 mm.	Documentos de importancia vital para la organización que deben mantenerse en secreto
5	Partículas de un máximo de 0,8 x 12 mm.	Documentos clasificados, para los que rigen exigencias de seguridad muy elevadas.

DEBER DE SECRETO

**Art. 10 de la Ley Orgánica 15/1999,
de Protección de Datos de Carácter
Personal**

**El responsable del fichero y quienes
intervengan en cualquier pase del
tratamiento de los datos de carácter
personal, están obligados al secreto
profesional respecto de los mismos
y al deber de guardarlos,
obligaciones que subsistirán aun
después de finalizar sus relaciones
con el titular del fichero o , en su
caso, con el responsable del mismo.**



INFRACCIONES DEBER DE SECRETO

Infracciones leves:

Incumplir el deber de secreto de cualquier datos de carácter personal.

Sanción entre 601,01 y 60.101,21 €

Infracciones graves:

Vulnerar el deber de secreto sobre los datos de carácter personal incorporados relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros prestación de solvencia patrimonial y crédito, así como aquellos que sean suficientes para obtener una evaluación de la personalidad de un individuo.

Sanción entre 60.101,21 y 300.506,05 €

Infracciones muy graves:

La vulneración de los datos de ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, así como los que3 hayan sido recabados confines policiales sin consentimiento de las personas afectadas.

Sanción entre 300.506,05 y 601.012,10 €



Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras



Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999.

A tal fin deberán:

- a) Colocar en las zonas videovigiladas, al menos un distintivo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados.
- b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999

ZONA VIDEOVIGILADA



LEY ORGANICA 15/1999, DE PROTECCIÓN DE DATOS

PUEDE EJERCITAR SUS DERECHOS ANTE:

ZONA VIDEOVIGILADA



**LEY ORGANICA 15/1999,
DE PROTECCIÓN DE DATOS**

PUEDE EJERCITAR SUS DERECHOS ANTE:

GREEN CANAL GOLF, S.A.

Av. Islas Filipinas esq. Av. Pablo Iglesias - 28003 Madrid



**LES RECORDAMOS QUE LAS BOLAS PERTENECEN
GREEN CANAL GOLF,
SU SUSTRACCIÓN IMPLICA UN DELITO.**

ZONA VIDEOVIGILADA



LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS

PROHIBIR E IGNORAR SU EXISTENCIA ANTE
REAL MADRID CLUB DE FÚTBOL

ESTADO SANTIAGO BERNABEU

AVENIDA CONCHA ESPINOSA, 1, 28002 MADRID



PREVENCIÓN DE LA VIOLENCIA EN LOS ESPECTÁCULOS DEPORTIVOS
Ley 10/2015 (Ley Orgánica) y normativa derivada

LO QUE SE ADVIERTE PARA PÚBLICO CONCIENTE Y ESTRICTO CUMPLIMIENTO

Queda prohibida la introducción y posesión de pistolas, revólveres, bombas, o cualquier otro tipo de arma de fuego, así como cualquier tipo de arma blanca, así como cualquier tipo de arma de fuego, así como cualquier tipo de arma blanca, así como cualquier tipo de arma de fuego, así como cualquier tipo de arma blanca.

Queda prohibida la introducción y posesión de cualquier tipo de explosivos, dinamita, pólvora, o cualquier otro tipo de explosivo, así como cualquier tipo de explosivo, así como cualquier tipo de explosivo.

Queda prohibida la introducción y posesión de cualquier tipo de explosivos, dinamita, pólvora, o cualquier otro tipo de explosivo, así como cualquier tipo de explosivo, así como cualquier tipo de explosivo.



SECURITY MEASURES TO PREVENT VIOLENCE AT SPORT EVENTS
Sport Act 10/2015 and related regulations

FOR PUBLIC INFORMATION AND COMPLETE STRICT COMPLIANCE

It is forbidden to bring into another stadium inside the stadium any kind of firearm, weapons, knives, bombs or any other type of weapon, as well as any other type of weapon, as well as any other type of weapon.

It is forbidden to bring into the stadium, arena, or any other type of sports venue any kind of explosive, dynamite, powder, or any other type of explosive, as well as any other type of explosive.

www.rfef.es

EVITE INFORMAR EN LOS ACCESOS A LAS INSTALACIONES DEL CLUB

IMÁGENES CAPTADAS POR CIRCUITO CERRADO DE TELEVISIÓN PARA SU SEGURIDAD



Madrid Fútbol Club

ATENCIÓN

Recordamos a los que abandonan el estadio o entrada en el estadio para este sistema de seguridad.

Real Madrid

Artículo 5.1 de la Ley Orgánica 15/1999

Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
 - a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
 - b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
 - c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
 - d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
 - e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

MODELO CLAUSULA INFORMATIVA

FICHERO PÚBLICO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado "....." del que es responsable ese organismo, creado por Resolución..... (BOE.....) y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.
2. Que el destinatario de sus datos personales es la empresa de seguridad.....
3. Que puede ejercitar sus derechos de acceso, cancelación y oposición ante el responsable del fichero.
4. Que el responsable del fichero tratamiento es ".....(nombre o razón social)....." ubicado en C/

MODELO CLAUSULA INFORMATIVA

Art. 3, apartado B. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

FICHERO PRIVADO

De conformidad con lo dispuesto en el art. 5.1 LO 15/1999, de 13 de diciembre, de Protección de Datos, se informa:

1. Que sus datos personales se incorporarán al fichero denominado “.....“ y/o serán tratados con la finalidad de seguridad a través de un sistema de videovigilancia.
2. Que el destinatario de sus datos personales es:
 - a. La empresa de seguridad.....
 - b. El dueño del establecimiento.....
3. Que puede ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante el responsable del fichero.
4. Que el responsable del fichero tratamiento es “ (.....nombre o razón social.....)” o su representante D./D^a.”.....” ubicado en C/
.....

CANCELACIÓN

Los datos serán cancelados en el plazo máximo de un mes desde su captación.

NOTIFICACION DE FICHEROS

La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.



SEGURIDAD Y SECRETO

El responsable deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Asimismo cualquier persona que por razón del ejercicio de sus funciones tenga accesos a los datos, deberá de observar la debida reserva, confidencialidad y sigilo en relación con las mismas.

El responsable deberá informar a las personas con acceso a los datos del deber de secreto a que se refiere el apartado anterior.



INFRACCIONES Y REGIMEN SANCIONADOR



INFRACCIONES



1. No atender por motivos formales, la solicitud del interesado de rectificación y cancelación
2. No proporcionar la información que solicite la AEPD
3. No solicitar la inscripción de un fichero
4. Recoger datos de carácter personal sin proporcionar la información debida a los afectados.
5. **Incumplir el deber de secreto**

SANCIONES LEVES:

De 600 a 60.000 €

INFRACCIONES



1. Crear ficheros de titularidad pública, sin autorización publicada en el BOE
2. Crear ficheros de titularidad privada con finalidad distinta al objeto legítimo de la empresa o entidad.
3. **Recoger datos de carácter personal sin consentimiento de los afectados**
4. Tratar los datos con conculcación de principios y garantías.
5. Impedir u obstaculizar el ejercicio de los derechos ARCO
6. Mantener datos inexactos o no efectuar rectificaciones o cancelaciones
7. **Vulnerar el deber de secreto de datos de nivel medio**
8. No remitir a la AEPD las notificaciones previstas en la Ley
9. Obstruir la función inspectora
10. No inscribir un fichero cuando haya sido requerido para ello.
11. Incumplir el deber de información cuando los datos hayan sido recabados de persona distinta del afectado

SANCIONES GRAVES:

De 60.000 a 300.000 €

INFRACCIONES



SANCIONES MUY GRAVES:

De 300.000 A
600.000 €

1. La recogida de datos de forma engañosa y fraudulenta.
2. La comunicación o cesión de los datos, fuera de los casos permitidos.
3. Recabar y tratar sin consentimiento expreso del afectado, datos que revelen ideología, afiliación sindical, religión y creencias.
4. Recabar y tratar datos que hagan referencia al origen racial, a la salud y a la vida sexual, cuando no lo disponga una Ley, o sin consentimiento expreso de los afectados
5. Violentar la prohibición de crear ficheros con la finalidad exclusiva de almacenar datos de ideología, afiliación sindical, religión, creencias. Origen racial o étnico o vida sexual
6. No cesar en el uso ilegítimo de los tratamientos de datos cuando sea requerido para el ello por el Director de la AEPD
7. La transferencia de datos a países que no proporcionen un nivel de protección equiparable a España.
8. Tratar los datos de forma ilegítima, cuando con ello se atente a los principios fundamentales
9. **La vulneración del deber de secreto respecto a los datos de ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual.**
10. No atender u obstaculizar de forma sistemática el ejercicio de los derechos ARCO
11. No atender forma sistemática el deber legal de notificación de la inclusión de datos en un fichero.

GRACIAS
POR
LA ATENCION PRESTADA