NIVEL BÁSICO

MEDIDAS DE SEGURIDAD PARA PARA EL TRATAMIENTO DE DATOS DEL FICHERO WWW.DIMENSIS.COM (versión: 2009)
Nº INSCRIPCIÓN REGISTRO GENERAL DE PROTECCIÓN DE DATOS: 2051780197

Objeto del Documento de Medidas de Seguridad

El presente documento se enmarca en el artículo 8 del Real Decreto 994/1999 de 11 de junio, mediante el cual se regulan las medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

DIMENSIS GLOBAL COMMUNICATIONS, S.L., provista del CIF B-62.166.244, es titular y responsable del fichero de datos "WWW.DIMENSIS.COM" inscrito en la Agencia de Protección de Datos con número de inscripción 2051780197 en el Registro General de Protección de Datos.

El fichero de datos: "WWW.DIMENSIS.COM" (en adelante el FICHERO, ver Anexo 0 a), Inventario de Ficheros) se clasifica en el Nivel de Seguridad Básico, según se desprende de las estipulaciones del artículo 4 del Real Decreto 994/1999 en función del tipo de datos almacenado, por lo que el presente documento de Medidas de Seguridad recogerá cuantas medidas sean necesarias para lograr el nivel de garantía exigido. Las presentes Medidas de Seguridad también serán de aplicación en los sistemas de información que tratan los datos de los ficheros inventariados (ver Anexo 0 b), Inventario de Recursos Informáticos).

Responsable de los Ficheros

Este documento de Medidas de Seguridad ha sido elaborado bajo la responsabilidad de DN. JORGE FLORES DOMÍNGUEZ (en adelante RESPONSABLE DE LOS FICHEROS), en su calidad de administrador de la empresa, DIMENSIS GLOBAL COMMUNICATIONS, S.L. titular y responsable del FICHERO. En su condición de Responsable del FICHERO, DN. JORGE FLORES DOMÍNGUEZ se compromete a implantar y actualizar el presente documento de Medidas de Seguridad con el fin de poder aplicar siempre las garantías suficientes y exigidas de nivel básico. Por otra parte, el Responsable de los Ficheros se asegurará de que todo el personal profesional que entre en contacto con los ficheros reste sujeto al presente documento y se le obligará a su cumplimiento.

Conocimiento del documento de Medidas de Seguridad

El Responsable de los ficheros entregará una copia del documento a toda persona con acceso a los datos protegidos o a los sistemas que faciliten el acceso a los mismos. En el momento de la entrega del presente documento, la persona que lo reciba firmará un ACUSE DE RECEPCIÓN (Anexo 1) y restará sujeta a las medidas que se recogen en él.

Personal sujeto al Documento de Medidas de Seguridad

Las personas que tengan acceso a los datos de los ficheros o a los sistemas de los mismos deberán regir su actuación según las presentes normas. El personal se puede subdividir en:

a) administradores del sistema: es el personal encargado de administrar o mantener el entorno operativo de los ficheros. Este personal deberá estar explícitamente relacionado en la LISTA DE PERSONAL CON ACCESO AL SISTEMA (Anexo 2).

b) usuario del sistema: son las personas que realizan parte de su función laboral a partir de los datos recogidos en los ficheros. Este personal deberá estar explícitamente relacionado en la LISTA DE PERSONAL CON ACCESO A LOS DATOS (Anexo 3).

Responsable de la Seguridad de los Ficheros

El Responsable de los Ficheros podrá también asumir el cargo de RESPONSABLE DE SEGURIDAD, o bien podrá delegar está función a otra persona. En todo caso, las funciones propias del RESPONSABLE DE SEGURIDAD serán las de coordinar y controlar las medidas definidas en el presente documento y de tratar las incidencias con la diligencia suficiente que garantice la integridad de la información contenida en los ficheros. La delegación de esta parcela, no priva que el Responsable de los Ficheros continue siendo el responsable último.

Procedimientos para la creación, modificación y supresión de ficheros

Para la creación, modificación y supresión de ficheros con datos de carácter personal por las personas empleadas en DIMENSIS GLOBAL COMMUNICATIONS, S.L. será necesario el cumplimiento de determinados requisitos los cuales se especifican a continuación.

Primera.- Antes de proceder a la creación, modificación y supresión de un fichero, la persona empleada de la empresa que vaya a llevar a cabo esta función tendrá de comunicarlo de forma previa al Responsable de Seguridad.

Segunda.- El Responsable de Seguridad decidirá donde debe almacenarse el nuevo fichero, controlará y limitará los accesos, proporcionará las medidas de seguridad adecuadas, realizará la notificación pertinente ante la Agencia Española de Protección de Datos. Realizará las actualizaciones del Documento de Seguridad y los procedimientos de seguridad si estuvieran afectados por la creación, modificació o supresión del fichero.

Procedimiento de creación de ficheros

La información que maneje el personal con acceso a los ficheros de datos y los sistemas tiene que quedar almacenada en Carpetas de Red, siendo el Responsable de Seguridad la persona encargada de controlar y limitar los accesos y proporcionar las medidas de seguridad adecuadas.

El personal con acceso a los ficheros de datos y a los sistemas donde se almacenen y traten los datos de carácter personal debe cumplir con los puntos del procedimiento anterior. Así mismo, tiene que tener presente que está totalmente prohibida la creación y/o almacenamiento de ficheros con datos de carácter personal en su disco duro.

Las extracciones puntuales realizadas sobre ficheros preexistentes no son creaciones de ficheros, sino que serán ficheros temporales. La creación de ficheros temporales seguirá el mismo procedimiento que el de la creación de un fichero normal. Una vez que la finalidad del fichero temporal se haya extinguido, previa comunicación al Responsable de Seguridad se suprimará el fichero.

Procedimiento de Modificación de Ficheros

Es necesario cumplir con este procedimiento con el fin de controlar en todo momento los cambios producidos en los ficheros existentes y proceder a la verificación de las actualizaciones. Por modificación se entederá todo cambio sustancial producido en ellos.

Procedimiento de Supresión de Ficheros

Para proceder a la supresión o cancelación de un fichero deberá concurrir el hecho que haya desaparecido la finalidad por la cual fue creado -cuando los datos hubieran dejado de ser necesarios o pertinentes. Por consiguiente los datos deberán ser bloqueados.

LAS MEDIDAS DE SEGURIDAD

1ª.- Proceso de obtención de los datos que se incorporan en los ficheros

Cada vez que DIMENSIS GLOBAL COMMUNICATIONS, S.L. recabe datos de carácter personal informará de manera clara y precisa al titular de éstos de:

a) la existencia de unos ficheros con datos de carácter personal que archivan datos de información relativa a la persona. Igualmente, se informará de la finalidad de los ficheros y de los destinatarios de la información que dimana de ellos
b) el carácter obligatorio o facultativo de la respuesta a las preguntas
c) las consecuencias del suministro de los datos o de la negativa a no facilitarlos
d) la posibilidad de ejercer el derecho de acceso, rectificación, cancelación y oposición
e) la identidad y dirección del responsable del fichero

La información anteriormente expuesta aparecerá a modo de advertencia en los formularios utilizados para la recogida de los datos de los ficheros.
En caso de la incorporación de datos obtenidos por otros medios que no sean por el proceso normal de inscripción, se informará de forma expresa, precisa e inequívoca, en el periodo máximo de tres (3) meses posteriores al registro de los datos.
Por otra, en caso de que la fuente de los datos fuese de carácter "público", se informará también al afectado del origen de los mismos, así como de los derechos que le corresponden respecto al "consentimiento inequívoco". El consentimiento puede ser revocado por el interesado si existe una causa justificada. La revocación no tendrá efectos retroactivos.

2ª.- Ubicación de los Sistemas de Información

Los locales donde se ubiquen los ordenadores que contengan los ficheros tendrán las garantías suficientes de confidencialitad y disponibilidad de los datos protegidos.

3ª.- Puestos de Trabajo

Los puestos de trabajo que tengan dispositivos que permitan el acceso a los datos para su consulta (terminales y ordenadores personales) tendrán también un acceso restringido. Se considerarán personas con derecho de acceso a los puesto de trabajo con acceso a los datos, las que se recojan en el Anexo 3. En el momento de la consulta de los datos, tanto el Responsable de los Ficheros, como el personal con acceso a éstos, se aseguran de que la información que se puede visualizar en la pantalla no puede ser vista por otras personas que no sean las estrictamente autorizadas. Por ello, las medidas en este sentido serán:

a) Tanto las pantallas como las impresoras estarán ubicadas en lugares que garanticen la confidencialidad de los datos.
b) Si el responsable del puesto de trabajo abandona temporalmente su puesto, deberá siempre dejarlo de tal modo que se impida la visualización de los datos.
c) También deberá tomarse la precaución de no dejarse documentos en la impresora.

4ª.- El Sistema de Contraseñas para el personal

Tanto el personal con acceso a los datos como el personal con acceso al sistema, tendrán asignadas unas contraseñas que tan sólo conocerán ellos y el Responsable de los Ficheros quien en determinadas circunstancias o incidencias las facilitará al Responsable de la Seguridad del Sistema, con el fin de arreglar el problema surgido.
Las contraseñas se renovarán periódicamente, y se guardarán en un sistema seguro al que sólo tendrá acceso el Responsable de los Ficheros.

5ª.- Gestión de las Incidencias

Se entiende por incidencia cualquier hecho que pueda alterar el normal desarrollo de la gestión de los ficheros así como también de la normal consulta de sus datos y que pueda suponer poner en peligro la integridad de la información. Se podría calificar de incidencia: la caída del sistema de seguridad informática que facilitara el acceso de los datos personales a personas no autorizadas, el intento no autorizado de salida de un soporte, la destrucción parcial o total o la pérdida de equipos informáticos, la recuperación de datos de carácter personal a partir de copias de salvaguarda, los accesos no autorizados a las salas donde se ubiquen los sistemas de soportes informáticos, incendio, inundación, ... Con el fin de hacer frente a estas circunstancias, se creará un REGISTRO DE INCIDENCIAS (Anexo 4), en los siguientes términos:

a) El Registro de Incidencias será creado por el propio Responsable de Seguridad del Sistema y estará a la disposición de los usuarios y administradores del sistema. En él se recogerán todas las incidencias que pueden suponer un peligro para la seguridad del sistema y por lo tanto de los datos.
b) Los usuarios que tengan conocimiento de una incidencia son responsables de registrarla en el Registro de Incidencias o en su defecto comunicarlo al Responsable de Seguridad del Sistema. En caso de no proceder de esta manera, se considerará la conducta del usuario como una falta grave contra la seguridad del fichero.
c) La incidencia será comunicada a la persona responsable de solventar la incidencia por parte del Responsable de Seguridad del Sistema. El Responsable de solventar la incidencia clasificará la incidencia en un archivo de control. A continuación deberá buscar una solución. Una vez solucionada la incidencia, la solución también quedará guardada. Además se informará a las personas que hubieran detectado la incidencia y a las que hubieran estado involucradas en ella.

6ª.- Gestión de Soportes

Se consideran soportes informáticos los medios de grabación y recuperación de datos que se utilizan para realizar copias y pasos intermedios en los procesos de aplicación de gestión de los ficheros. Estos soportes informáticos debe estar inventariados y controlados (Anexo 6 a) según los siguientes parámetros:
a) Todos los soportes deberán llevar una etiquetas que identifiquen claramente el nombre del fichero, el contenido de los mismos y la fecha de su realización.
b) Mientras, los soportes sean útiles, éstos deberán almacenarse en lugares en los que sólo se permita el acceso a personas debidamente autorizadas.
c) La salida de soportes deberá estar siempre gestionada y autorizada por el Responsable de los Ficheros (Anexo 5 y Anexo 6).
d) Una vez que los soportes ya no sean útiles, deberán tomarse todas las medidas que garanticen un borrado total de los datos, con el fin de que no sea posible la recuperación de los mismos y se les dará de baja del inventario.

7ª.-Copias de Seguridad y de Recuperación

El Responsable de los Ficheros preve procesos que garanticen la conservación y recuperación de los datos en caso de que el sistema fallara o tuviera alguna pérdida. Por ello, el Responsable de los Ficheros asignará a una persona la tarea de realizar copias de periodicidad fijada (al menos semanalmente, salvo que en dicho periodo no se haya producido ninguna actualización) de los datos del fichero. A partir de las copias, debe ser posible recuperar los ficheros y el estado de los datos de éstos según se encontraban en el momento de la pérdida o la incidencia. El Responsable de los Ficheros se encargará de guardar en una ubicación segura los soportes que contengan las copias de seguridad y sólo él o la persona asignada bajo su autorización, podrán acceder a las mismas.

8.-Descripción de la estructura de los sistemas utilizados

· Sistema operativo FreeBSD
· Sistema operativo Microsoft IIS
· Servidor web Apache Web Server
· Servidor web Microsoft IIS
· Panel de control ISPmanager
· Panel de control PLESK
· Acceso mediante protocolo HTTPS en todas las aplicaciones de acceso desde web
· Encriptación MD5, SASL v2.0
· Lenguajes soportados: HTML, PHP, JAVA, Perl, C/C++
· Bases de datos en MySQL con acceso desde PhpMyAdmin, mediante protocolo HTTPS y con identificación de usuario y contraseña encriptada
· Servidores de correo: Sendmail, Qpopper, MailEnable, OpenWebMaill, SquirrelMail
· OpenSSH, OpenSSL, SAMBA
· Servidor DNS: bind
· Servidor FTP: ProFTPD

9ª.-Descripción del Sistema Informático que permite el acceso al fichero

· Acceso desde la red troncal de IBERCOM.
· Acceso desde Internet mediante autentificación de clave encriptada, en servidor seguro (HTTPS) por medio de protocolo SSH.
· Protección de la red mediante proxy de seguridad con Firewall instalado
· Protección de cada máquina mediante configuración de reglas Firewall

10ª.- Obligaciones del Responsable de los Ficheros

El Responsable de los Ficheros tiene la responsabilidad jurídica de la seguridad de los ficheros y de garantizar la correcta aplicación de las Medidas de Seguridad.

a) El Responsable de los Ficheros tomará cuantas medidas crea oportunas con el fin de garantizar en todo momento la integridad y confidencialidad de los datos que se almacenan en los ficheros. Por ello, se encargará de mantener actualizado el presente documento de Medidas de Seguridad, comunicándolo al personal que tiene a su cargo y facilitando la versión actualizada del documento.
b) La actualización de este documento se hará mediante la introducción de nuevos procedimientos que ofrezcan mayores garantías de seguridad o mediante la actualización según los preceptos de la nueva normativa de protección de datos de carácter personal.

c) El Responsable de los Ficheros estará informado de todo cuánto suceda en referencia al estado de los ficheros y revisará con periodicidad diaria el Registro de Incidencias que le facilitará y mantendrá siempre actualizado el Responsable de Seguridad del Sistema.
d) El Responsable de los Ficheros se encargará de la Asignación de las contraseñas que permiten el acceso al sistema que almacena los ficheros, así como también las contraseñas que permiten el acceso a los datos del fichero (Anexo 7).
e) El Responsable de los Ficheros se responsabilizará de la Gestión de los soportes y toda salida y entrada de éstos restará siempre bajo su autorización.
f) El Responsable de los Ficheros velará porque la cesión puntual y temporal de ficheros a terceros con el fin de realizar actividades reguladas por contrato de prestación de servicios se haga siempre según lo estipulado en las presentes Medidas de Seguridad y en los conceptos previstos en el contrato.
g) El Responsable de los Ficheros se responsabilizará de la gestión de las copias de seguridad y de respaldo, asegurándose que todas las tareas relacionadas con esta actividad se realizan simpre bajo los preceptos de la cláusula 7ª.
h) Inscripción de los ficheros en la Agencia Española de Protección de Datos.

12ª.- Obligaciones del Responsable de Seguridad del Sistema

El Responsable de la Seguridad del Sistema asumirá las tareas de coordinar y controlar la aplicación de las Medidas de Seguridad en cooperación con el Responsable de Seguridad.

a) El Responsable de Seguridad del Sistema se encargará del control del Registro de Incidencias y lo mantendrá siempre a disposición del personal autorizado. Ante las incidencias, el Responsable de Seguridad del Sistema junto con el Responsable de los Ficheros tomarán las medidas oportunas para subsanar la situación y garantizar la integridad de los datos.

13ª.- Obligaciones del Personal con Acceso a los Datos de los Ficheros

Los puestos de trabajo que permitan el acceso a los datos con el fin de llevar a cabo tareas de carácter profesional con ellos, sólo serán desarrollados por personas que dispongan de la autorización previa y expresa del Responsable del Fichero (ver Anexo 3).

a) Las personas que ocupen puestos de trabajo con acceso a los datos, se asegurarán de que durante el tiempo que dure la consulta de los datos, ninguna otra persona puede consultar o visualizar estos datos.
b) Durante su ausencia en el transcurso de una consulta, estas personas tomararán cuantas medidas estén a su alcance para evitar cualquier consulta o visualización no autorizada.
c) También tomarán todas las precauciones con el fin de evitar cualquier olvido de documentos en las impresoras.
d) El personal de un puesto de trabajo con acceso a los datos, se responsabiliza de la confidencialidad de la contraseña que le ha sido asignada, la cual es intransferible. Igualmente se compromete a utilizarla exclusivamente dentro del marco profesional.
e) El personal de un puesto de trabajo con acceso a los datos tiene la obligación de declarar cualquier incidencia que detecte y de dar parte de la misma en el Registro de Incidencias.

14ª.- Derecho de Acceso, Rectificación, Revocación del Consentimiento y Cancelación de los Datos por parte de los afectados

El Responsable de los Ficheros se asegurará de que cualquier persona que acredite ser afectada en referencia a los datos recogidos en los ficheros pueda ejercer sus derechos de acceso, rectificación, revocación del consentimiento y cancelación de los datos.

Con el fin de gestionar este tipo de situación, el Responsable de los Ficheros pondrá a disposición de los afectados el DOCUMENTO DE SOLICITUD DE EJERCICIO DE LOS DERECHOS DE LOS AFECTADOS (Anexo 8). A partir de la presentación de la solicitud, el Responsable de los Ficheros deberá:

a) El Responsable del Fichero deberá resolver la petición de acceso a los datos en el plazo máximo de un mes desde la recepción de la solicitud. Transcurrido este periodo, el Responsable de los Ficheros no hubiera dado ninguna respuesta, el afectado podrá presentar la oportuna reclamación a la Agencia Española de Protección de Datos.
b) Una vez realizada la consulta por parte del afectado, en el plazo de diez días, previa petición del afectado, el Responsable de los Ficheros deberá proceder a la rectificación o cancelación de los datos que hubieran sido considerados incorrectos o incompletos.
c) Previa petición del afectado, el Responsable de los Ficheros dejará de almacenar los datos por los cuales el afectado haya retirado su consentimiento.
d) El Responsable de los Ficheros deberá comunicar al afectado las medidas aplicadas con el fin de satisfacer su petición.
e) El Responsable del fichero podrá denegar el acceso a datos de carácter personal cuando el derecho se haya ejercitado en un intervalo inferior a doce meses y no se acredite un interés legítimo. El acceso también podrá denegarse si lo solicita una persona distinta al afectado.

15ª.- Cesión de los datos

La cesión temporal y puntual de los datos cuando sea necesaria para poder realizar la prestación de servicios de los ficheros será regulada mediante un contrato entre la entidad prestadora de los servicios y Dimensis Global Communications, S.L. En el contrato de prestación de servicios se establecerán claramente las instrucciones de tratamiento de la información y la imposibilidad de proceder a una subcontratación. Las condiciones fijadas en el contrato de prestación de servicios serán coherentes en todo lo estipulado en las presentes Medidas de Seguridad.
Una vez finalizada la relación contractual, el prestador de los servicios se compromete a devolver todos los soportes y otro material que haya precisado para la ejecución de sus servicios, y en destruir los datos que hayan podido quedar en su sistema de información.
El Responsable de los Ficheros supervisará los extremos y condiciones de esta cesión profesional.

16ª Actualización del Documento de Medidas de Seguridad

Como Medida de Seguridad última, el Responsable de los Ficheros llevará a cabo una revisión periódica del presente Documento de Medidas de Seguridad con aras a actualizarlo a las innovaciones técnicas que se consideren que ofrecen mayores garantías de seguridad dentro del nivel básico e igualmente con respecto a la Normativa de Protección de Datos.
Por ello, cada versión nueva actualizada que surja de la presente (1era), deberá ir numerada con el número de versión que le corresponda y su fecha de edición.

A N E X O S

ANEXO 0 a) INVENTARIO DE FICHEROS

FICHEROS DE TITULARIDAD DE DIMENSIS GLOBAL COMMUNICATIONS, S.L

Fichero Físico	Fichero Lógico	Núm. RGPD del Fichero lógico	Nivel Medidas Seguridad

ANEXO 0 b) INVENTARIO DE RECURSOS INFORMÁTICOS

Sistema operativo que tienen instalados los equipos

- FREEBSD
- WINDOWS

Páginas web

- www.dimensis.com

Bases de Datos que almacenan datos de carácter personal

- MySql (en servidor remoto)
- Hojas de cálculo Excel (en ordenador local, con conexión a Internet, protegido por firewall y contraseña de acceso).

Conexiones Remotas

- Internet
- Intranet

Aplicaciones Remotas

- VDSmanager (panel de control para gestión de servidores)
- ISPmanager (panel de control para gestión de dominios)
- Plesk (panel de control para gestión de dominios)

Centros de Tratamiento y Locales

- Domicilio de trabajo en España:

Dimensis Global Communications, SL
Jorge Flores Domínguez
C/ Arquitecte Vives, 65
43800 Valls (Tarragona)

- Datacenter en España:

World Wide Web Ibercom, S.L.
Parque Empresarial Zuatzu
Edificio Easo 2º
20018 San Sebastián
GUIPÚZCOA (SPAIN)
CIF: B-20609459
Autorizado por la CMT con Licencia tipo C

- Datacenter en Bruselas:

ISPsystem Belgium
PoBox 74, 1410 - Waterloo, Belgium
Tel: (+32) 04 74 38 73 49

ANEXO 1 ACUSE DE RECEPCIÓN

Declaración de Recepción

En Barcelona, a _____ de _____ de 2009

Don _____, mayor de edad, provisto/a del DNI con núm. _____ expedido en _____, en _____, actuando en nombre y representación propios, en su calidad de _____ de la empresa .....,

declara

que en la fecha del presente documento le ha sido entregada una copia del Documento de Medidas de Seguridad mediante el cual se rige la gestión, consulta y mantenimiento de los ficheros automatizados de datos de carácter personal de la empresa DIMENSIS;
Teniendo conocimiento de la existencia de las Medidas de Seguridad, Don _____, acepta y se compromete a regir su conducta con respecto todo aquello que afecta a los ficheros objeto de las presentes Medidas de Seguridad, según lo estipulado en su articulado.
Y para que así conste, firma el presente acuse de recepción, como prueba de que una copia actualizada de las Medidas de Seguridad obra en su poder y conoce el contenido de las mismas.

_____
nombre y apellidos

_____
firma

ANEXO 2 LISTA DE PERSONAL CON ACCESO AL SISTEMA

Las personas con acceso a los sistemas de información que almacenan los datos de los ficheros y que permiten su actualización, han sido designadas por el Responsable de los Ficheros y son:

- JORGE FLORES DOMÍNGUEZ: en su calidad de Responsable de los Ficheros
- JORGE FLORES DOMÍNGUEZ: en su calidad de Responsable de Seguridad del Sistema
- JORGE FLORES DOMÍNGUEZ: en calidad de Webmaster

ANEXO 3 LISTA DE PERSONAL CON ACCESO A LOS DATOS

Las personas con acceso a las unidades desde las que se puede proceder a la consulta de los ficheros que contienen datos de carácter personal con el fin de poder trabajar con ellos, han sido designadas por el Responsable de los Ficheros y son:

- Acceso al Datacenter en Bruselas:

    - Igor Chekushkin: en su calidad de administrador de sistemas y programador
    - Didier Windmeulen: en su calidad de administrador de sistemas y programador
    - Dmitry Sidorov: en su calidad de administrador de sistemas y programador
    - John Lepikhin: en su calidad de administrador de sistemas y programador
    - Alexey A. Chekushkin: en su calidad de administrador de sistemas y programador
    - Sergey Redin: en su calidad de administrador de sistemas y programador

- Acceso remoto desde España:

    - Diego Gil Mesa: en su calidad de programador
    - Héctor Iván Tamayo Caroca: en su calidad de diseñador gráfico
    - David Martín Fernández: en su calidad de programador y webmaster

ANEXO 4 REGISTRO DE INCIDENCIAS

Declaración de Incidencia

Fecha: _____ Hora:_____Minutos:_____
Ubicación: _____ Incidencia nº:_____/2009

Usuario declarante de la incidencia:
Nombre:_____ Apellidos:_____. Cargo:_____
Persona a quien se le ha comunicado la incidencia:
Nombre: ---------- Apellidos: ---------- Cargo:----------
Descripción de la incidencia:
_____
_____
_____

Tipificación de la incidencia:
□ *Modificaciones no autorizadas de información*
□ *Acceso a ficheros de datos por personal no autorizado*
□ *Copias indebidas de datos en puestos de trabajo*
□ *Mal funcionamiento durante la realización de copias de seguridad*
□ *Errores del sistema/transacciones/bases de datos*
□ *Accesos no autorizados a los lugares donde se ubiquen los sistemas*
□ *Otras*
Unidades afectadas por la incidencia:
_____

Efectos producidos por la incidencia:
_____

Medidas aplicadas inmediatamente después de la incidencia:
_____

_____
Firma

ANEXO 5 REGISTRO SALIDA/ENTRADA DE SOPORTES

Declaración de Movimiento de Soporte

Fecha: _____ *Hora:_____Minutos:_____*
Tipo de soporte: _____ *Salida nº:_____/2009*
Entrada nº: _____/2009
Procedencia del soporte:_____
Contenido:
_____
Motivo del movimiento: _____
Destino:
_____
Forma de envío: _____ Tiempo de envío: _____
Incidencias durante el envío:
_____

Persona autorizada:
Nombre: _____ Apellidos _____ Cargo: _____
Emisión de la autorización:
Fecha: _____
Responsable de la autorización:
Nombre: _____ Apellidos _____ Cargo: _____

ANEXO 6 AUTORIZACIÓN DE MOVIMENTO DE SOPORTES

Autorización

En Barcelona, a _____ de _____ de 2009

Don JORGE FLORES DOMÍNGUEZ, provisto del DNI núm.43.528.994-E en su calidad de Responsable de la Seguridad de los Ficheros de DIMENSIS, extiende el presente documento con el fin de autorizar a

Don/ Doña _____, provisto/a del DNI núm. _____ en su calidad de _____, el movimiento del soporte _____ que contiene datos referidos a _____de su ubicación actual _____ al destino de _____, debido a _____. La presente autorización deberá llevar el número correspondiente al Registro de Salida/Entrada de Soportes.

Y para que así conste, firmo la presente autorización en la fecha y lugar que figuran en el encabezamiento.

_____
firma

ANEXO 7 ASIGNACIÓN DE CONTRASEÑAS

Notificación cambio del password de acceso a los ficheros

Sr./ Sra._____
Función _____

Como responsable del fichero de Base de Datos: _____ le comunico que el nuevo PASSWORD de acceso al mismo es _____

Recibido

_____
Sr./Sra.

El responsable del fichero

_____
Sr./Sra.

con la firma de este comunicado me comprometo a guardar confidencialidad sobre la clave de acceso al fichero, así como a utilizar siempre los datos de la misma de acuerdo con el Documento de Medidas de Seguridad para los ficheros de .....

ANEXO 8 DOCUMENTO DE SOLICITUD DE EJERCICIO DE LOS DERECHOS DE LOS AFECTADOS

Solicitud

En _____, a _____ de _____ 2009

El abajo firmante, Don/Doña _____ provisto/a del DNI núm. _____ que habiendo otorgado mi consentimiento a ..... en fecha de ___ de _____ de 2009 para que incorporará mis datos personales en el fichero _____, mediante el presente

solicito

poder consultar los datos en su día cedidos con el fin de ejercer los derechos contemplados en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, y ejercer si fuera preciso, mi derecho a la rectificación, cancelación de los datos que afectan a mi persona. También si fuera preciso, podré revocar mi consentimiento.

Ruego que se proceda a dar curso a mi solicitud y me emplacen en fecha y hora para poder llevar a cabo la consulta solicitada.

_____
nombre y apellidos

_____
firma

ANEXO 6 a) INVENTARIO DE SOPORTES INFORMÁTICOS

Inventario de Soportes Informáticos del Fichero: .....

Localización:

Identificación	Contenido	Núm. Soporte	Fecha Grabación	Hora de Grabación