

Universidad de Cádiz
Seguridad y Competencias Profesionales
Curso 2010/2011

Documento de Seguridad de Bodegas San Dionisio, S.A.

Leopoldo Jesús Gutiérrez Galeano

Lidia Lebrón Amaya

Luis Nadal de Mora

Rafael Sánchez Martínez

Jesús Soriano Candón

18 de enero de 2011

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de 11 de Junio), recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

Índice general

Historial de cambios	IX
1. Ámbito de aplicación del documento	1
2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento	3
3. Procedimiento general de información al personal	7
4. Funciones y obligaciones del personal	9
5. Procedimiento de notificación, gestión y respuestas ante las incidencias	11
6. Procedimientos de revisión	13
7. Consecuencias del incumplimiento del Documento de Seguridad	15
A. Aspectos específicos relativos a los diferentes ficheros	17
A.1. Aspectos relativos al fichero de personal	17
A.2. Aspectos relativos al fichero de proveedores	19
A.3. Aspectos relativos al fichero de clientes	21
A.4. Aspectos relativos al fichero financiero	22
A.5. Aspectos relativos al fichero de producción	24
A.6. Aspectos relativos al fichero de informes	26
B. Nombramientos	29
C. Autorizaciones firmadas para la salida o recuperación de datos	31
D. Inventario de soportes ((si se gestiona en papel))	33
E. Registro de incidencias	35

Índice de figuras

Índice de cuadros

C.1. Autorización de salida o recuperación de datos	31
E.1. Impreso de notificación de incidencias	35

Historial de cambios

<i>Fecha</i>	<i>Cambios</i>
18 de enero de 2011	Primera versión del documento.

1. Ámbito de aplicación del documento

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad del Director de GI/TI, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

- *Nivel básico*: Se aplicarán a los ficheros con datos de carácter personal.
- *Nivel medio*: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, (en estos dos casos, deberán ser de titularidad pública), servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).
- *Nivel alto*: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales sin consentimiento (en este último caso, también deberán ser de titularidad pública).

En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

- Fichero de personal: Nivel básico.
- Fichero de proveedores: Nivel básico.
- Fichero de clientes: Nivel básico.
- Fichero financiero: Nivel básico.
- Fichero de producción: Nivel básico.
- Fichero de informes: Nivel básico.

En el Anexo A se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

- Medidas y normas relativas a la identificación y autenticación del personal autorizado a acceder a los datos personales

La identificación y autenticación a la red corporativa está centralizada. Esto quiere decir que cada empleado tiene su nombre de usuario y contraseña que le permite acceder a:

1. El propio sistema operativo.
2. Los datos organizados en forma de archivos del sistema operativo, como cualquiera producido por herramientas de oficina (Textos, Hojas de cálculo, imágenes, etc.), y que sean accesibles a través del sistema de ficheros del sistema operativo.
3. Correo electrónico corporativo.
4. El acceso a las distintas aplicaciones corporativas puestas a disposición por la compañía, cuyo acceso se prohíbe fuera del entorno de seguridad de la red corporativa. El acceso a través de una red privada virtual está autorizado por esta política.

El **nombre de usuario** se obtiene a partir del nombre del empleado. Por ejemplo: para un empleado llamado Juan Pérez Madrid su nombre de usuario será: jperez, que se compone por las iniciales de su nombre seguido de su primer apellido.

En caso de que haya dos empleados con el mismo nombre se puede adoptar cualquier regla que permita identificarlos, por ejemplo: vimmartinez, vicmmartinez, etc.

Las medidas mínimas de seguridad de **contraseña** para usuarios del sistema son:

- Tamaño mínimo de 8 caracteres.
- Utilización de caracteres alfanuméricos.
- Caducidad de las contraseñas a los 2 meses.
- Máximo de 3 intentos de acceso. En el caso de fallar 3 veces se bloquea el usuario y se debe contactar con el Administrador de Sistemas para resetear el usuario.

2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

■ Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones.

Para solicitar un alta, modificación o baja de las autorizaciones de acceso a los datos, uno de los empleados del puesto de trabajo en cuestión (o el empleado particular, si la solicitud no abarca todos los empleados de un puesto concreto) deberá entregar el impreso de solicitud al Administrador del Sistema, o en su caso el de Red, dependiendo del tipo de fichero (la autoridad en cuestión se especifica en cada sección del Anexo A correspondiente a cada fichero), el cual deberá llevarla a cabo si la considera oportuna, y con la supervisión del Director de GI/TI.

En el Anexo A, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para cada uno de ellos. Esta lista se actualizará cada vez que se produzca un cambio (alta, baja o modificación) en las autorizaciones de acceso a los datos, ya sea por parte de un solo empleado o de la totalidad de los empleados de un puesto concreto.

■ Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en un armario ignífugo dedicado expresamente a ello, dentro de la organización de la empresa, en una sala del edificio de oficinas, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación:

El Director de GI/TI, el Responsable de Seguridad, el Jefe de TI y la persona asignada para realizar las copias de seguridad, si no es el propio Jefe de TI, son las personas autorizadas a acceder al lugar destinado al almacenado de soportes que contengan datos de carácter personal, dentro de la organización de la empresa.

Para autorizar a nuevos miembros al acceso, o desautorizar a los existentes se consta de un formulario que deberá ser aceptado por los tres cargos mencionados anteriormente (Director de GI/TI, Responsable de Seguridad y Jefe de TI) -siempre que el emisor del formulario no sea uno de ellos; en este caso firmarían los dos restantes-, facilitando así al nuevo miembro, u obligando a la devolución en su caso, de los medios (llaves y/o tarjetas) necesarios para dicho acceso a los soportes en cuestión.

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas:

Las copias diarias se almacenarán en el lugar mencionado anteriormente. Se utilizarán 6 cintas para este tipo de copias, una para cada día de la semana, ya que el séptimo día se realizará una copia completa, por lo que la diaria no sería necesaria. Las cintas se reutilizarían en cada ciclo de copias, siendo estas reemplazadas por nuevas cada cierto periodo de tiempo que puedan empezar a deteriorarse por su uso. Este periodo de tiempo será estimado por el responsable del mantenimiento de las copias de seguridad.

Al igual que las copias diarias, las semanales se tratarán con el mismo método, constando este ciclo con 4 cintas que se graban semanalmente. Al final de cada mes se realizará una copia completa, por lo que las cintas podrán ser reutilizadas como se ha explicado anteriormente.

La copia completa mensual se tratará de diferente forma, ya que será trasladada a un edificio ajeno a la ubicación actual del equipamiento de la empresa, para evitar la pérdida de los datos originales y copias por catástrofes como incendios, terremotos, inundaciones, etc. Estarán en un lugar con las medidas de seguridad adecuadas y seguras de amenazas como las que hemos nombrado, en una caja fuerte o armario a prueba de fuego.

Todas las copias serán almacenadas siguiendo un orden cronológico, tanto las diarias y semanales en su correspondiente sala, como las copias completas mensuales fuera de las instalaciones principales de Bodegas San Dionisio, S.A. Este orden lógico facilitará la búsqueda de alguna determinada copia de una fecha específica.

Todo el formato físico de copias quedaría correctamente etiquetado. Esto significa que dicha etiqueta estaría cifrada mediante un código interno a la organización. Por ejemplo, se podrían usar 7 caracteres alfanuméricos, de forma que el primero se establezca para indicar a qué departamento pertenecen los datos:

- 1: Departamento Administrativo
- 2: Departamento Comercial
- 3: Departamento de Producción
- 4: Departamento de GI/TI
- 5: Departamento Financiero

el segundo caracter indicaría qué tipo de backup es:

- D: Diario
- S: Semanal
- M: Mensual

y el resto para la fecha en que se ha realizado la copia, también debidamente encriptada, pudiendo usar indistintamente letras o números para referirse al día, mes y año; por ejemplo, el mes de la A (letra 1 del abecedario) hasta la L (letra 12), y el año el número de años que ha transcurrido desde 1990. Así, la etiqueta 5S03J21 correspondería a una copia semanal que contiene datos del departamento financiero, realizada el 03 de octubre de 2011.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento:

La autorización deberá ser aprobada por el Director de GI/TI -o el Jefe de TI si

2. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento

está delegado a hacerlo en su defecto-. Esta deberá indicar el soporte en cuestión, la finalidad y destino, la forma de envío y la persona que autoriza.

En el Anexo C se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

- Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

- Régimen de trabajo fuera de los locales de la ubicación del fichero

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. Para ello, existirá una o varias personas autorizadas en el centro o local donde se almacenan los soportes que contengan los datos de carácter personal, que cuiden de la seguridad del transporte y el correcto almacenamiento de los mismos en las instalaciones para ello dedicadas. La autorización deberá contener claramente el tipo de soporte a almacenar, las personas autorizadas al tratamiento de los mismos, el destino donde se almacenarán y la persona que autoriza (en este caso el Director de GI/TI -o el Jefe de TI si está delegado a hacerlo en su defecto-). Esta autorización, como se ha mencionado, se realiza para el tratamiento de los soportes, y no autoriza acceso a la información que contienen.

- Ficheros temporales

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

- Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En el Anexo A se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

3. Procedimiento general de información al personal

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo A correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con el siguiente procedimiento:

La organización consta de información específica para cada puesto de trabajo acerca de las normas de seguridad y las consecuencias de su incumplimiento, que son facilitadas en el momento que se contrata al empleado, estando este obligado a firmar un documento que indica que el mismo ha leído y entiende estas normas. El empleado recibirá una copia de este documento, siendo su responsabilidad el entendimiento y cumplimiento de estas, así como de las consecuencias del incumplimiento de las mismas.

4. Funciones y obligaciones del personal

- Funciones y obligaciones de carácter general.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla.

Constituye una obligación del personal notificar al responsable del fichero (de acuerdo al Anexo A), o de seguridad en su caso, las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo V.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

- Funciones y obligaciones del Director de GI/TI.

Como responsable de los ficheros, es el encargado jurídicamente de la seguridad de los mismos y de las medidas establecidas en el presente documento, implantará las medidas de seguridad establecidas en él y adoptará las medidas necesarias para que el personal afectado por este documento conozca las normas que afecten al desarrollo de sus funciones.

Además, debe asegurar el buen funcionamiento de copias, almacenado y transporte de los soportes físicos que contengan las copias. Para ello, cuenta con:

- La opción de delegar al Jefe de IT como autorizado al cumplimiento de algunas funciones que se deben llevar a cabo.
- El apoyo del Administrador del Sistema y de Red, que son los responsables de asignar, modificar o anular los distintos niveles de accesos a los ficheros de datos por parte de los empleados de la organización. En el Anexo A se especifica quién de cada uno de ellos es el responsable del acceso a cada fichero.
- El Responsable de Seguridad, encargado de coordinar y controlar las medidas definidas en el presente documento.

5. Procedimiento de notificación, gestión y respuestas ante las incidencias

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal.

El procedimiento a seguir para la notificación de incidencias será:

Cuando ocurra una incidencia, el usuario o administrador deberá registrarla en el Libro de Incidencias o comunicarla al Responsable de Seguridad para que a su vez proceda a su registro.

En la notificación se hará constar :

- Tipo de incidencia
- Fecha y hora en que se produjo
- Persona que realiza la notificación
- Persona a quien se comunica
- Efectos que puede producir la incidencia
- Descripción detallada de la misma

En el Anexo E se adjunta el impreso de notificación manual que podrá ser utilizado para la notificación de incidencias.

El registro de incidencias se gestionará mediante el Libro de Incidencias mencionado, que mantendrán las incidencias registradas de los 12 últimos meses, con los datos anteriormente listados.

En el Anexo C se incluirán los documentos de autorización por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

6. Procedimientos de revisión

- Revisión del Documento de Seguridad.

<Especificar los procedimientos previstos para la modificación del documento de seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal >

7. Consecuencias del incumplimiento del Documento de Seguridad

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a <indicar la normativa sancionadora aplicable>

A. Aspectos específicos relativos a los diferentes ficheros

A.1. Aspectos relativos al fichero de personal

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Personal.
- Unidad/es con acceso al fichero o tratamiento: Director de Administración, Jefe de Personal y Administradores de Personal.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>
 - Identificador: <código de inscripción>
 - Nombre: <nombre inscrito>
 - Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador del Sistema.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:

- Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
- Procedencia de los datos: <indicar quien suministra los datos>
- Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
- Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>
- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.
<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.

- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

A.2. Aspectos relativos al fichero de proveedores

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Proveedores.
- Unidad/es con acceso al fichero o tratamiento: Director de Administración, Jefe de Logística, Inspector de Mantenimiento y Administradores de Logística.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>
 - Identificador: <código de inscripción>
 - Nombre: <nombre inscrito>
 - Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador del Sistema.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:
 - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
 - Procedencia de los datos: <indicar quien suministra los datos>
 - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>

- Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>
- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

A.3. Aspectos relativos al fichero de clientes

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Clientes.
- Unidad/es con acceso al fichero o tratamiento: Director Comercial, Jefe de Ventas, Jefe de Marketing, Comerciales de Marketing, Jefe de Productos Terminados, Administradores de Venta, Comerciales de Venta y Administradores de Terminados.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>
 - Identificador: <código de inscripción>
 - Nombre: <nombre inscrito>
 - Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador del Sistema.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:
 - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
 - Procedencia de los datos: <indicar quien suministra los datos>
 - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
 - Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>

- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>
- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

A.4. Aspectos relativos al fichero financiero

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Finanzas.
- Unidad/es con acceso al fichero o tratamiento: Director Financiero, Jefe Contabilidad, Comptroller y Contables.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>
 - Identificador: <código de inscripción>
 - Nombre: <nombre inscrito>
 - Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador del Sistema.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:
 - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
 - Procedencia de los datos: <indicar quien suministra los datos>
 - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
 - Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>

- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.
<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

A.5. Aspectos relativos al fichero de producción

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Producción.
- Unidad/es con acceso al fichero o tratamiento: Director de Producción, Jefes del Departamento de Producción, Coordinador de Producción, Inspector de Calidad, Técnicos de Laboratorio, Capataces y Operarios.

- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>
 - Identificador: <código de inscripción>
 - Nombre: <nombre inscrito>
 - Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador de Red.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:
 - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
 - Procedencia de los datos: <indicar quien suministra los datos>
 - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
 - Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>
- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.

- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.
- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.
<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

A.6. Aspectos relativos al fichero de informes

Actualizado a: 18 de enero de 2011

- Nombre del fichero o tratamiento: Informes.
- Unidad/es con acceso al fichero o tratamiento: Directores de departamentos y miembros de GI.
- Identificador y nombre del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección de Datos (RPGD)>

- Identificador: <código de inscripción>
- Nombre: <nombre inscrito>
- Descripción: <descripción inscrita>
- Nivel de medidas de seguridad a adoptar: básico.
- Administrador: Administrador de Red.
- Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>
- Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el artículo 32 de la LOPD>.
- Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.
- Información sobre el fichero o tratamiento
 - Finalidad y usos previstos:
 - Personas o colectivos sobre los que se pretenda obtener o que resulten obligados a suministrar los datos personales:
 - Cesiones previstas:
 - Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>
 - Procedencia de los datos: <indicar quien suministra los datos>
 - Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>
 - Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>
- Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>
- Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.
- Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.

- Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.
- Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.
- Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.
- Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.
- Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.
- Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

B. Nombramientos

<Adjuntar original o copia de los nombramientos que afecten a los diferentes perfiles incluidos en este documento, como el del responsable de seguridad>

C. Autorizaciones firmadas para la salida o recuperación de datos

AUTORIZACIÓN DE SALIDA O RECUPERACIÓN DE DATOS	
Fecha: _____	
SOPORTE	
Identificación	
Contenido	
Fichero de donde proceden los datos	
Fecha de creación	
FINALIDAD Y DESTINO	
Finalidad	
Destino	
Destinatario	
FORMA DE ENVÍO	
Medio de envío	
Remitente	
Precauciones para el transporte	
AUTORIZACIÓN	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

Cuadro C.1.: Autorización de salida o recuperación de datos

D. Inventario de soportes ((si se gestiona en papel))

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el Capítulo II, punto “Gestión de soportes” de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento >

E. Registro de incidencias

Incidencia nº: _____ (A ser rellenado por el responsable de seguridad)
Fecha de notificación: _____
Tipo de incidencia: (Anotar todos los detalles de interés de la incidencia)
Descripción detallada de la incidencia:
Fecha y hora en que se produjo la incidencia:
Persona(s) que realiza(n) la notificación: (Especificar sin son usuarios o no del fichero)
Persona(s) a quien(es) se comunica:
Efectos que puede producir: (En caso de no subsanación o incluso independientemente de ella)
Persona que realiza la comunicación:
Fdo.: _____

Cuadro E.1.: Impreso de notificación de incidencias

