SISTEMAS DE SEGURIDAD EN RELACIÓN A ASPECTOS LEGALES, CONTROL DE ACCESOS, SOFTWARE … UNA VISIÓN ESTRATÉGICA

Begoña Arroitajauregi, Jaime Garrido y Aitor Iriarte

EUSKAL ESTATISTIKA ERAKUNDEA
INSTITUTO VASCO DE ESTADISTICA

Donostia-San Sebastián, 1
01010 VITORIA-GASTEIZ
Tel.: 945 01 75 00
Fax.: 945 01 75 01
E-mail: eustat@eustat.es
www.eustat.es

SISTEMAS DE SEGURIDAD EN RELACIÓN A ASPECTOS LEGALES, CONTROL DE ACCESOS, SOFTWARE... UNA VISIÓN ESTRATÉGICA

Begoña Arroitajauregi, Jaime Garrido y Aitor Iriarte

Toledo, junio de 2004

Indice

Capítulo
1

Introducción

La base del trabajo de los diversos Institutos y Servicios Estadísticos está constituida por la recopilación, elaboración y ordenación sistemática de los datos.

Teniendo en cuenta que muchos de estos datos son individuales de carácter personal, las diversas leyes que regulan la estadística oficial en sus ámbitos competenciales establecen como uno de los principios básicos de la actividad estadística pública la preservación del secreto estadístico, es decir, el deber de proteger estos datos, los identificables como propios de personas concretas, sean éstas personas físicas o jurídicas.

Además de los datos individuales obtenidos para la elaboración de estadística oficial, los Institutos y Servicios Estadísticos disponen para el ejercicio de sus labores administrativas de ficheros con datos de carácter personal que, si bien no se hallan protegidos por el deber de secreto estadístico, si se hallan protegidos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Por esta razón la seguridad de los datos facilitados para la elaboración de la estadística oficial así como la seguridad de los datos de las personas físicas incorporadas a ficheros administrativos, se revela como un elemento esencial dentro de la organización.

Capítulo
2

Identificación de los ficheros y régimen jurídico de la protección de sus datos

Los ficheros que contienen datos de carácter personal o datos que posibiliten la identificación individual se pueden dividir en dos grandes grupo: los ficheros que sirven a fines exclusivamente estadísticos y los ficheros administrativos.

El régimen jurídico de la protección de los datos que contienen está compuesto en el caso de los ficheros administrativos por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

En el caso de la protección de los datos que posibiliten la identificación individual que obran en los ficheros que sirven a fines exclusivamente estadísticos, su régimen jurídico está compuesto básicamente por la normativa estadística que regula el deber de secreto estadístico y por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal en los supuestos que esta norma lo prevea. En este sentido, el art. 37 m) de esta Ley, al enumerar las funciones de la Agencia Española de Protección de Datos, establece expresamente, tras indicar que la Agencia velará "por el cumplimiento de las disposiciones que la Ley de Función estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico", que le corresponderá a la propia Agencia, "dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46".

En este sentido, el artículo 6.d) del estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, establece, en relación con las funciones de la misma relacionadas con los ficheros exclusivamente estadísticos, la función de "dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos".

A la vista de lo dispuesto en estos dos preceptos, la Agencia Española de Protección de Datos concluye que le corresponde decidir sobre el nivel de seguridad al que deberán someterse los ficheros de datos de carácter personal que sean objeto de tratamiento para fines exclusivamente estadísticos, no encontrándose estos ficheros excluidos del ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre en lo que se refiere a las medidas de seguridad que sea necesario adoptar sobre los mismos.

Asimismo, considera que las medidas de seguridad que se adopten en desarrollo de lo establecido en la Ley Orgánica serán las que efectivamente vendrán a garantizar un adecuado tratamiento de los datos de carácter personal, de forma que, en caso de no adoptarse tales medidas, el tratamiento resultaría contrario a la Ley, por producirse un nivel insuficiente de protección.

A la vista de estos argumentos la Agencia española de Protección de Datos considera que cualesquiera ficheros que, en lo referente a la seguridad de los ficheros y tratamientos, no se encuentren expresamente excluidos del ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (por ejemplo los enumerados en el artículo 2.2 de la misma) habrán de

someterse a las medidas de seguridad contenidas en el Real Decreto 994/1999, de 11 de junio, dado que sólo en este caso quedará suficientemente garantizada la protección de los datos de carácter personal contenidos en el fichero o tratamiento.

Por ello, la Agencia Española de Protección de datos concluye que, sin perjuicio de la aplicación de su legislación específica en otras materias, los ficheros creados para fines exclusivamente estadísticos que contengan datos de carácter personal habrán de implantar las medidas de seguridad a las que se refiere 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, siendo el nivel de las mismas el que corresponda en atención de lo previsto en el artículo 4 de esta norma.

En conclusión, la normativa por la que se regirá la protección de los datos individuales contenidos en los diversos ficheros que obran en Eustat será:

- **Constitución Española**

- Art. 18: Se garantiza el derecho al honor, a la intimidad personal y familiar.

- La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos

- **Directiva Europea 95/46/CE**

- Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

- **L.O.P.D. 15/1999**

    - Garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas.

        - Ámbito de aplicación:

            Objetivo: Datos almacenados en un soporte físico

            Subjetivo: Personas físicas

            Territorial: Responsable del fichero en territorio español

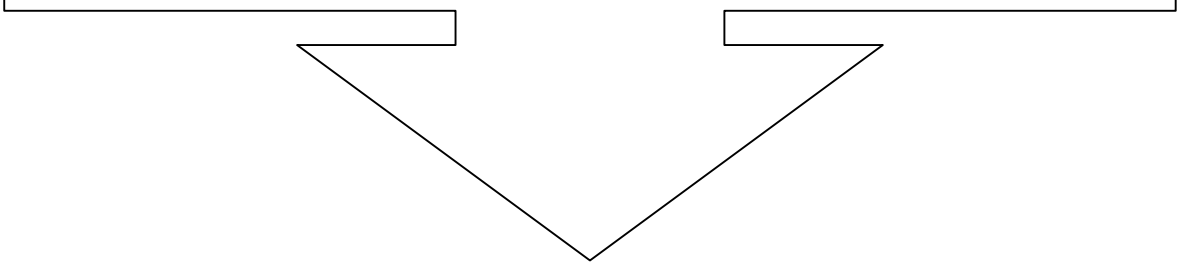
L.O.P.D. 15/1999

Ficheros que se rigen por sus disposiciones específicas y, por lo especialmente previsto en la L.O.P.D.

→ Ficheros amparados por la legislación sobre función estadística pública.

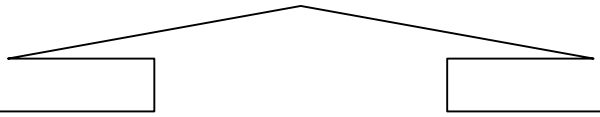
AEPD

→ Ficheros amparados por la legislación sobre función estadística pública.



Reglamento de Medidas de Seguridad 994/1999

Medidas de seguridad de ficheros automatizados que contengan datos de carácter personal



Ley De Estadística de la Comunidad Autónoma de Euskadi (Ley 4/1986)

"Deber de secreto estadístico": protección de datos de personas físicas y jurídicas

Capítulo
3

Clasificación de los datos conforme al reglamento de seguridad

Nivel de seguridad	Naturaleza de la información	Medidas de seguridad a adoptar
BASICO	- Datos Identificativos - Características personales - Datos Académicos - Datos de detalle de empleo - Circunstancias sociales - Datos económico-financieros - Transacciones	- Documento de seguridad - Definición de funciones del personal - Registro de incidencias - Identificación/autentificación - Control de acceso - Gestión de soportes - Copias de respaldo y recuperación
MEDIO	-Infracciones administrativas - Infracciones penales - Hacienda Pública - Servicios financieros - Solvencia patrimonial y de crédito - Suficientes para evaluar la personalidad del individuo	- Medidas del nivel anterior - Responsable de seguridad - Auditoria (mínimo bianual) - Control de acceso físico
ALTO	- Ideología, Religión o Creencias - Origen racial - Salud o vida sexual - Fines policiales	- Medidas del nivel anterior - Distribución de soportes - Registro de accesos - Cifrado de telecomunicaciones

En el reglamento de Seguridad las medidas de seguridad exigibles se clasifican en tres niveles : bajo, medio y alto, atendiendo a la naturaleza de la información tratada. Las medidas de seguridad a adoptar tienen carácter acumulativo debiéndose adoptar, en consecuencia, las medidas correspondientes al nivel del que se trate y las de los niveles inferiores. De esta manera, todos los ficheros deben cumplir con las medidas correspondientes al nivel básico; éstas y las correspondientes al nivel medio han de ser adoptadas en los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, solvencia patrimonial y de crédito y los suficientes para evaluar la personalidad del individuo; y las medidas de nivel alto junto con las de nivel medio y básico han de ser adoptadas en los ficheros que contengan datos sobre ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales.

En este sentido y en lo que a Eustat se refiere, tanto los ficheros que contiene datos de carácter personal y que sirven a fines administrativos como los que tienen información sujeta a secreto estadístico se han clasificado en alguno de los tres niveles indicados en el cuadro anterior en función de la naturaleza de la información que contienen y se han determinado las medidas técnicas y organizativas, articuladas mediante normativas y procedimientos, que garanticen el mantenimiento de un nivel de seguridad acorde con la naturaleza de los datos que sean objeto de tratamiento. Todo esto se ha plasmando en dos documentos de seguridad, uno para los ficheros estadísticos y otro para los ficheros administrativos.

Hasta el momento todos los ficheros incluidos en el Documento de Seguridad de ficheros administrativos con datos de carácter personal se han calificado como nivel básico, aunque las medidas de seguridad adoptadas están preparadas para trabajar con ficheros de nivel medio de seguridad.

En lo que respecta a los ficheros estadísticos, también se les ha asignado el nivel básico de seguridad , si bien las medidas adoptadas están preparadas para un nivel medio. Además, no se descarta que a algún fichero estadístico se le asigne un nivel de seguridad alto cuando se terminen de inventariar todos los existentes.

Capítulo
4

Contenido básico de cada documento de seguridad

El artículo 9 de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal establece cómo el Responsable del Fichero debe adoptar todas aquellas medidas de índole técnica y organizativa necesarias para garantizar la protección de los datos de carácter personal. El legislador fue más allá del concepto de protección y amplió este campo a conceptos como alteración, perdida, tratamiento y/o acceso no autorizado.

Este articulo 9 de la Ley Orgánica 15/1999 emplaza a un desarrollo normativo posterior en donde se establezcan los requisitos y condiciones que deben reunir los ficheros y las personas que intervienen en el tratamiento de los datos de carácter personal. Este desarrollo se hizo mediante la promulgación del Real Decreto 994/1999 de 11 de junio.

Según el artículo 8 del citado Reglamento, el Responsable del Fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados con datos de carácter personal y a los sistemas de información.

Conforme al artículo 8.3 del Real Decreto 994/1999 de 11 de junio, el documento de seguridad deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en los sistemas de información o en la organización del mismo.

El contenido básico de cada documento es el que a continuación se indica:

Documento de seguridad de Ficheros con Datos de Carácter Personal

- ✓ Se refiere a ficheros creados mediante una disposición de carácter general publicada en el diario oficial correspondiente, que son:
  - Control de distribución horaria por tareas
  - Control de peticiones externas de información
  - Proveedores (Gestión de expedientes de contratación)
  - Gestión de personal
  - Registro de entradas y salidas
  - Becarios
  - Seminarios
  - Sistema de mensajería
  - Directorio para distribución de publicaciones
- ✓ Estos ficheros deben estar registrados en la Agencia de Protección de Datos.
- ✓ Se indican las medidas de obligado cumplimiento.
- ✓ Se definen las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido.
- ✓ Funciones y obligaciones del personal
- ✓ Supone una superación de los niveles de seguridad exigidos por la legislación vigente (generalización de medidas para todos los niveles de seguridad)

Documento de seguridad de ficheros estadísticos

- ✓ Se refiere a ficheros para fines estadísticos que contienen datos de personas físicas o jurídicas. De momento únicamente se ha trabajado sobre dos ficheros:
  - Subsistema de población
  - Directorio de actividades económicas
- ✓ Se indican las medidas de seguridad de obligado cumplimiento (Reglamento de Seguridad)
- ✓ No contiene normas derivadas directamente de la LOPD (ejercicio de derechos de acceso, rectificación y cancelación de los interesados)
- ✓ Procedimientos comunes semejantes
  - ■ Adecuación a niveles y medidas de seguridad establecidos para los datos de carácter personal
- ✓ Procedimientos específicos: cesión de información sujeta a secreto estadístico.

El listado completo y actualizado de los ficheros protegidos y toda la información relacionada con el contenido de los ficheros y los recursos empleados en su tratamiento se gestiona mediante una aplicación desarrollada con MS Excel.

Capítulo

5

Estructura de los documentos de seguridad

Funciones y obligaciones del personal

El personal con acceso a ficheros con datos de carácter personal y ficheros estadísticos individualizados deberá conocer sus deberes y obligaciones hacia el tratamiento y las medidas de seguridad que versan sobre dichos ficheros.

El Documento de Seguridad distingue las siguientes figuras:

- Responsable del Fichero
- Responsable de Seguridad
- Administradores del Sistema
- Usuarios del Fichero

Funciones y obligaciones del Responsable del Fichero

- Aprobación y Difusión del Documento de Seguridad (Asesorado por el Responsable de Seguridad)
- Nombrar formalmente al responsable de Seguridad
- Notificar los cambios en los ficheros con DCP para su inscripción en la Agencia de Protección de Datos
- Emitir las autorizaciones precisas
- Autorizar las altas, bajas y modificaciones de acceso a los usuarios
- Autorizar los envíos o recepciones de soportes con datos protegidos
- Autorizar a los usuarios que vayan a asumir funciones específicas (gestión de soportes)
- Adoptar medidas para que los usuarios conozcan las normas de seguridad que afectan al desarrollo de sus funciones
- Aprobar la creación, modificación o supresión de los ficheros

- Resolver las peticiones de los interesados para el ejercicio de derechos de acceso, rectificación y cancelación de los datos
- Procurar la inclusión en los formularios de toda la información acerca de la protección de DCP que deba tener el titular

Funciones y obligaciones del Responsable de Seguridad

- Mantener actualizado el Documento de Seguridad
- Verificar el cumplimiento del Documento de Seguridad
- Colaborar en las auditorías de seguridad
- Solicitar al Responsable del Fichero autorizaciones:

  -acceso de usuarios

  -entrada y salida de soportes

  -cesión de datos

  -recuperación de datos
- Analizar las incidencias en los ficheros
- Verificar la realización de copias de respaldo
- Controlar el registro de accesos físicos a locales
- Identificar, junto con el responsable del fichero, las medidas de seguridad para cada aplicación

Funciones y obligaciones de los Administradores del Sistema

- Realización de copias de seguridad
- Gestión de soportes

  -Custodia

  -Identificación/Inventariado

  -Reutilización/Desechado

- Mantenimiento del registro de incidencias
- Gestión del registro de entradas/salidas
- Control de accesos

Funciones y obligaciones de los Usuarios del Fichero

- Proteger la confidencialidad de los datos
- Devolver los soportes utilizados y guardarlos en las dependencias del CPD bajo llave
- Notificar al Responsable de Seguridad cualquier incidencia que pueda afectar a la seguridad de los datos
- No revelar su identificador y contraseña
- No utilizar identificadores ajenos
- No guardar datos protegidos en discos locales
- Utilizar únicamente software autorizado
- Salvaguardar el puesto de trabajo
- Datos identificativos y direcciones de personas sólo se introducirán en Outlook (declarado en la APD)

Recursos protegidos

Los puestos de trabajo desde los que se puede acceder a los ficheros

Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

Esto implica que tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán estar físicamente ubicados en lugares que garanticen esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente o bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

En el caso de las impresoras deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de Fichero, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

Queda expresamente prohibida la conexión a redes o sistemas exteriores de los puestos de trabajo desde los que se realiza el acceso al fichero. La revocación de esta prohibición será autorizada por el responsable del fichero, quedando constancia de esta modificación en el Registro de Incidencias.

Los puestos de trabajo desde los que se tiene acceso al fichero tendrán una configuración fija en sus aplicaciones y sistemas operativos que sólo podrá ser cambiada por los administradores autorizados del anexo F previa de la Dirección (Dirección General y Subdirecciones).

Control de accesos físicos a las dependencias donde están ubicados los datos protegidos

Se establecerá un sistema de control de acceso físico a las dependencias de los CPDs y otras dependencias donde se ubican ficheros con datos protegidos, de modo que se impida el acceso al personal no autorizado por el Responsable del Sistema.

Cuando las personas con permisos temporales de acceso se encuentren en dependencias del CPD, estarán, en todo momento, acompañadas de personal del CPD.

Las puertas de acceso al CPD deberán estar permanentemente cerradas.

Se reducirá, dentro de lo razonablemente posible, el número de personas autorizadas para acceder al CPD.

Se tendrá especial diligencia en anular con prontitud las autorizaciones de acceso a las dependencias de los CPDs a las personas que, habiendo estado autorizadas, ya no necesiten el acceso al mismo.

Existirá una relación actualizada de personas autorizadas para acceder al CPD.

Cuando se detecte la presencia, en las dependencias del CPD, de una persona no autorizada o indicios de que se ha producido un acceso no autorizado, se hará constar este hecho como incidencia de seguridad.

Administración de usuarios

Para controlar que los usuarios sólo acceden a los datos y recursos protegidos que necesitan para su trabajo cotidiano es necesario definir las siguientes normas:

- Perfiles de usuarios

    - El Responsable del Sistema, en colaboración con el Responsable de Seguridad y los administradores del sistema, creará unos perfiles de usuarios donde se

especificarán con detalle las opciones y modo de acceso (actualización o consulta) a los recursos protegidos.

- Todos los usuarios estarán asignados a un perfil concreto, que les permita acceder única y exclusivamente a los datos y recursos protegidos determinados.

- Administración de usuarios

  - Cualquier modificación o nueva necesidad detectada dentro del área de administración de usuarios debe ser comunicada al Responsable de Seguridad.

  - Es el Responsable del Sistema quien tiene la potestad de conceder, anular o modificar los accesos autorizados a los recursos protegidos.

  - Control de accesos. Existe un sistema de control de accesos que permite identificar al usuario que accede al sistema, de tal forma que le permita o deniegue el acceso según disponga o no de la autorización oportuna y registra el acceso de forma que quede constancia del mismo.

  - El sistema de control de accesos contabiliza el número de intentos de accesos fallidos. El número máximo para estos intentos es tres.

- Identificador de usario y contraseñas

  - El usuario y contraseña son personal e intransferibles.

  - Los usuarios temporales tendrán una vida útil determinada, desactivándose tras cumplir este periodo .

  - La contraseña tendrá una longitud mínima de cinco caracteres, y estará compuesta por una combinación de letras y números que no sean fácilmente identificables.

  - Las contraseñas de los usuarios se almacenan cifradas en el sistema.

  - Al realizar un nuevo alta de un usuario se le asignará una contraseña temporal que tendrá que cambiar obligatoriamente al acceder por primera vez al sistema.

  - La comunicación de esta contraseña temporal se realizará de forma personal al usuario por el responsable correspondiente .

  - Las contraseñas tienen un tiempo de vida de cuatro meses, a partir del cual es necesario realizar un cambio obligatorio.

  - El usuario tiene la posibilidad de cambiar su contraseña de acceso en cualquier momento.

Entrada/salida de soportes

Distinguimos las siguientes fases:

- Emisión de autorización

- Inscripción en el Registro
- Entrada o Salida del soporte
- Gestión del soporte

Emisión de autorización

- Anualmente, el Responsable del Sistema emitirá un escrito elaborado por el Responsable de Seguridad que contendrá las autorizaciones para Entradas o Salidas de soportes programadas durante el periodo considerado solicitadas previamente por los usuarios.

  Este escrito contendrá los siguientes aspectos:

  - Autorizaciones para enviar/recibir soportes. Por cada operación se establecerán uno o varios técnicos autorizados.

  - Destino del soporte. En el caso de operaciones de entrada de soportes, se recogerá el destino del soporte una vez se carguen los datos (inventariarlo, devolverlo al origen, desecharlo, reutilizarlo)

- Si fuera necesario, el Responsable del Sistema podrá emitir autorizaciones complementarias de entradas o salidas programadas que modifiquen la anterior.

- El Responsable del Sistema autorizará para cada operación considerada las entradas o salidas de soportes excepcionales.

- La determinación de las personas autorizadas para la entrada o salida de carácter excepcional podrá derivarse a las subdirecciones.

- Con carácter general, serán técnicos estadísticos las personas autorizadas para recibir o enviar soportes con datos protegidos.

- Podrá excepcionalmente autorizarse a técnicos informáticos, siempre que la naturaleza de la operación así lo aconseje (pruebas de aplicaciones,...)

- Las autorizaciones que se emitan serán comunicadas al CPD.

- La relación de personas autorizadas para proceder a la recepción o envío de soportes con datos protegidos constará en un anexo de este Documento de Seguridad.

Inscripción en el Registro

- El CPD será la unidad encargada de la gestión del Registro de entrada y salida de soportes.

- Cuando un técnico vaya a recibir/enviar un soporte lo comunicará inmediatamente al CPD y esperará la confirmación de la autorización y del registro del envío/recepción del soporte facilitando para ello la información que sea necesaria.

- Si la recepción/envío de ficheros con datos protegidos se produce a través de correo electrónico, o de otro medio telemático que no conste en soporte físico, se informará al CPD e igualmente esperará la confirmación de la autorización y del registro del envío/recepción facilitando para ello la información que sea necesaria.

- El CPD comprobará que existe la autorización precisa, anotará la operación, si procede, en el Registro la E/S y se lo comunicará al técnico.

Entrada o Salida del Soporte

- Producida la inscripción en el Registro, la persona autorizada procederá al envío o la recepción.

- Si el CPD verificase la inexistencia de autorización para la operación solicitada, comunicará esta circunstancia al solicitante, así como la persona autorizada para la operación de que se trate.

- La persona encargada de recepcionar todos los envios en Eustat, Secretaria de Dirección, trasladará al CPD todos los soportes recibidos que estén dentro del ámbito de este procedimiento para su registro. El CPD comunicará al técnico estadístico correspondiente la llegada de los soportes.

- En el caso de envío de soportes, el técnico correspondiente entregará los soportes objeto de envío al CPD, quien los registrará y trasladará a la Secretaria de Dirección para su envío efectivo.

- Si el envío se produjera por correo electrónico o por cualquier otro medio telemático que no conste en soporte físico, será el técnico quien proceda a su envío una vez reciba del CPD comunicación de haberse procedido a la inscripción.

- El escrito que contenga las autorizaciones de entrada, determinará el destino correspondiente a los distintos soportes.

- La persona responsable de la recepción entregará el soporte a la unidad o persona que corresponda para proceder según se haya indicado en el escrito de autorización.

- Recibido el soporte y cargados, en su caso, los datos, el soporte podrá recibir uno de los siguientes tratamientos:

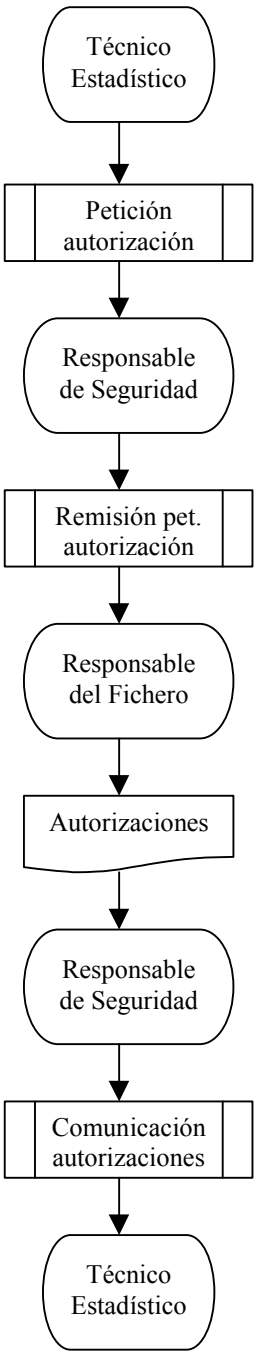
    - Inventariarlo

    - Devolverlo al origen

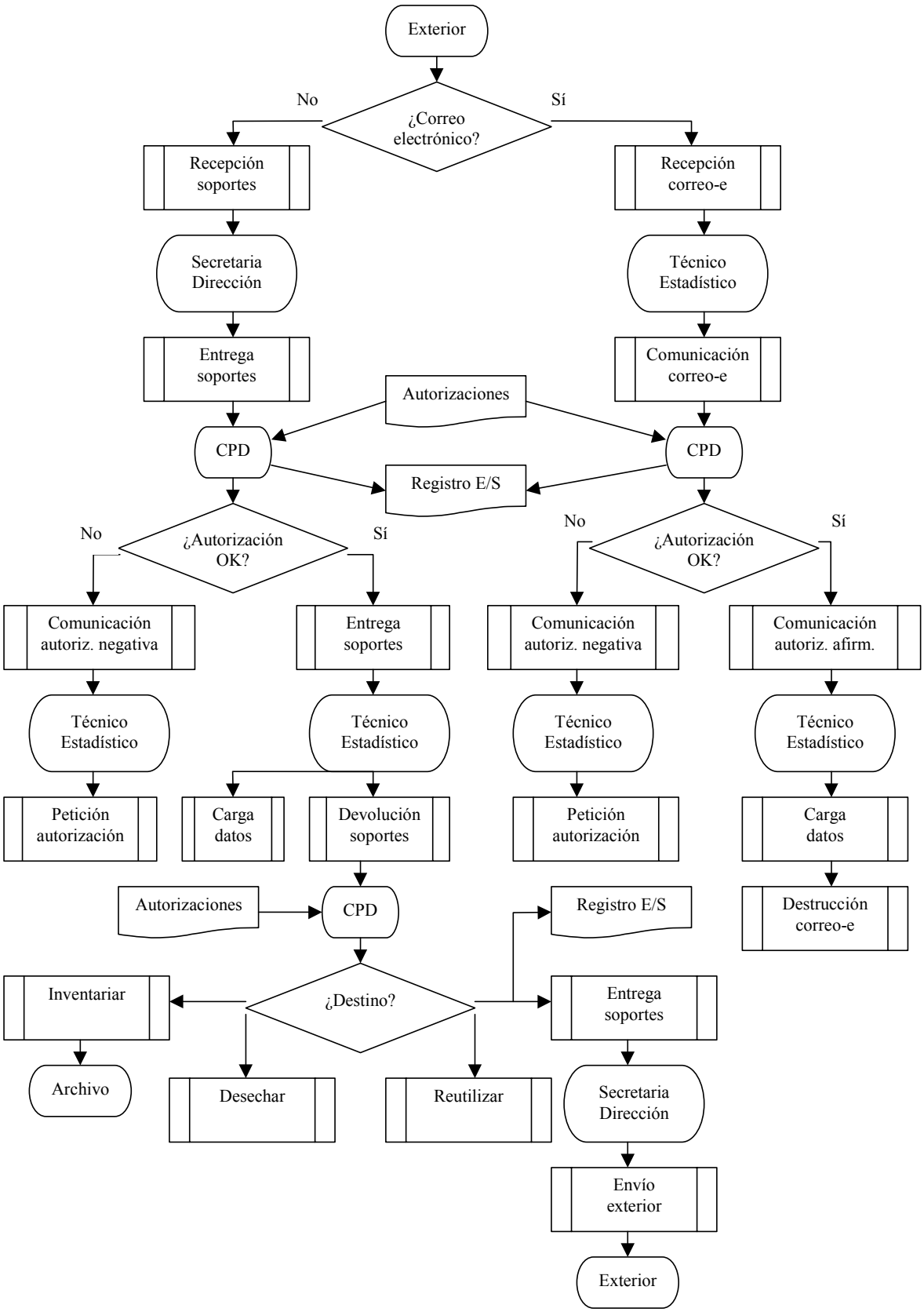
    - Desecharlo

    - Reutilizarlo

Organigrama de Emisión de Autorizaciones



Organigrama de Entrada de Soportes



Eustat

Soportes

Identificación e inventariado

El Responsable del Sistema emitirá una autorización en favor del CPD para la identificación, inventariado, reutilización y desechado de soportes que contengan datos protegidos, dejando a las subdirecciones la determinación de las personas.

Los soportes que vayan a ser utilizados para contener datos protegidos deberán ser debidamente etiquetados.

Todos los soportes que contengan datos protegidos serán inventariados y almacenados en un lugar seguro de acceso restringido al personal autorizado. En el CPD existirá un inventario de soportes que contienen los backups, que facilite su control, almacenamiento y localización.

Se mantendrá un inventario de soportes que contienen datos protegidos. Cuando un soporte se prepare para ser reutilizado, la información que contiene será eliminada. Si el soporte va a ser desechado, se borrará la información contenida y se destruirá físicamente. Además, en ambos casos:

a) Para soportes propios inventariados, se actualizará el inventario.
b) Para soportes recibidos y no inventariados (porque no se almacenan), se actualizará el registro de entrada de soportes marcándolos con el indicador apropiado.
c) Para soportes recibidos e inventariados (porque se han guardado para su tratamiento posterior), se actualizarán el registro de entrada y el inventario.

Reutilización y desechado de soportes

Cuando la información que contiene un soporte ya no sea necesaria para el fin para el que se guardó, el soporte será desechado o, en su caso, preparado para ser reutilizado.

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información.

Cuando finalice la vida útil de un soporte, éste no podrá ser reutilizado.

El Responsable del Sistema emitirá una autorización en favor del CPD para la reutilización y desechado de soportes que contengan datos protegidos, dejando a las subdirecciones la determinación de las personas.

Tratamiento de ficheros temporales

Los ficheros temporales que se creen tendrán las mismas medidas de seguridad que correspondan a los ficheros maestros de los que proceden sus datos.

Las unidades usuarias sólo podrán generar ficheros temporales cuando sean para su uso exclusivo en procesos específicos y relacionados con el trabajo de la unidad. Estos

ficheros no podrán ubicarse en unidades locales de PCs, ni se permitirá su salida fuera de la unidad usuaria, ni podrán ser copiados en soportes informáticos (ni siquiera para ser almacenados). Una vez que estos ficheros hayan dejado de ser útiles para la finalidad con la que se crearon, serán borrados por el usuario que los creó.

Los procesos internos deben estar diseñados para que los ficheros temporales creados durante su ejecución se eliminen a la finalización de ésta. Si por causas accidentales, el proceso falla durante su ejecución, los ficheros temporales permanecerán creados hasta que se analice y conozca la causa que motivó el fallo. Posteriormente se procederá al borrado de los ficheros temporales existentes.

Ficheros temporales generados por los administradores de sistemas:

a) Este tipo de ficheros se generan mediante acciones específicas ejecutadas por los administradores de sistemas, a petición de las áreas usuarias y con autorización del Responsable del Sistema.
b) Estos ficheros son depositados en un directorio del servidor de red, en una carpeta de acceso restringido a un usuario o grupo concreto de usuarios.
c) Una vez hayan dejado de ser útiles, deberán ser borrados físicamente por el usuario que los solicitó o por el Administrador del Sistema, a petición de aquél.
d) Estos ficheros temporales no podrán ser copiados en soportes externos, ni se permitirá su salida fuera de la unidad usuaria, salvo autorización expresa y por escrito del Responsable del Fichero.

Control para verificar lo dispuesto en el Documento de Seguridad

Bajo coordinación del Responsable de Seguridad, se establecerán controles esporádicos para verificar el cumplimiento de las normativas y procedimientos establecidos en este Documento de Seguridad.

Se realizarán los siguientes controles y auditoría:

- Comprobación del conocimiento y aceptación de las normas de seguridad por parte de los usuarios que acceden a los Sistema de Información.
- Control de las actividades del registro en el Instituo Vasco de Estadística:
- Registro de entrada/salida de soportes.
- Control de autorizaciones de entrada/salida de soportes:
- Verificación de la existencia actualizada de autorizaciones para las entradas/salidas de soportes.
- Verificación de la existencia actualizada de autorizaciones a los usuarios.
- Una vez realizado el control, el Responsable de Seguridad realizará un análisis y un informe contemplando los siguientes aspectos:

- Evaluación del grado de conocimiento del Documento de Seguridad por parte de los usuarios del Fichero.

- Evaluación del número y gravedad de las incidencias de seguridad registradas durante el periodo que abarque el análisis.

- Evaluación del grado de cumplimiento de la actividad del registro.

- Evaluación del grado de cumplimiento de las autorizaciones para la entrada y salida de soportes.

- Anomalías y fallos detectados.

Realización de auditorias periódicas

Los ficheros a los que se les haya asignado un nivel de seguridad medio o alto, deberán someterse a auditorías periódicas para verificar el cumplimiento de las medidas establecidas.

La auditoria actuará en estos puntos:

- Aplicación del Documento de Seguridad.

- Sistema de identificación y autenticación de acceso a los Sistema de Información.

- Sistema de control de acceso lógico.

- Sistema de control de acceso físico.

- Procedimientos de gestión de soportes.

- Control Antivirus.

- Procedimientos de copias de respaldo (backups) y recuperación de datos.

- Control de la notificación y gestión de incidencias.

Aunque hasta el momento todos los ficheros incluidos en el Documento de Seguridad son de nivel básico, EUSTAT se está planteando la posibilidad de someterse a una auditoría cuando todas las medidas de seguridad lleven un período de tiempo implantadas.

Utilización de datos protegidos en pruebas

El entorno de explotación y el de pruebas y desarrollo se mantendrán totalmente diferenciados. No se podrá acceder, de modo directo, a explotación desde el entorno de desarrollo. En caso de que sea necesario acceder al entorno de explotación, por parte

de desarrollo, para realizar tareas de mantenimiento o de otro tipo, se precisará la autorización del Responsable del Sistema.

Como regla general, en los entornos de pruebas y desarrollo se deberán realizar las pruebas de los programas y procesos utilizando bases de datos y ficheros con datos ficticios. No obstante podrán tomarse datos de explotación para la realización de pruebas, siempre que lo autorice el Responsable del Sistema, adoptando las siguientes medidas de seguridad:

a) Los datos reales provenientes de explotación serán sometidos a un proceso que permita la disociación de los datos, de tal modo que se imposibilite la asociación de la información obtenida con una persona.

b) Si los datos no se disocian, deberá asegurarse el nivel de seguridad correspondiente a la naturaleza de los datos que se van a manejar.

Las pruebas con datos reales solamente se realizarán en el entorno de pruebas y desarrollo de EUSTAT y no en otro lugar, salvo que como excepción y de forma expresa y justificada medie petición del usuario responsable de la operación estadística relacionada y autorización expresa del Responsable del Fichero para ceder una copia a una empresa externa. En este caso el Responsable de Seguridad tomará las mayores medidas legales, contractuales y organizativas para asegurar el correcto uso y posterior destrucción de los datos reales cedidos.

En EUSTAT el entorno de pruebas y desarrollo tiene el mismo nivel de seguridad que el entorno de explotación.

Control de accesos físicos a las dependencias donde están ubicados los datos protegidos

Se establecerá un sistema de control de acceso físico a las dependencias de los CPDs y otras dependencias donde se ubican ficheros con datos protegidos, de modo que se impida el acceso al personal no autorizado por el Responsable del Sistema.

Cuando las personas con permisos temporales de acceso se encuentren en dependencias del CPD, estarán, en todo momento, acompañadas de personal del CPD.

Las puertas de acceso al CPD deberán estar permanentemente cerradas.

Se reducirá, dentro de lo razonablemente posible, el número de personas autorizadas para acceder al CPD.

Se tendrá especial diligencia en anular con prontitud las autorizaciones de acceso a las dependencias de los CPDs a las personas que, habiendo estado autorizadas, ya no necesiten el acceso al mismo.

Existirá una relación actualizada de personas autorizadas para acceder al CPD.

Cuando se detecte la presencia, en las dependencias del CPD, de una persona no autorizada o indicios de que se ha producido un acceso no autorizado, se hará constar este hecho como incidencia de seguridad.

Actualización del Documento de Seguridad

Los motivos que pueden propiciar la actualización del Documento de Seguridad son los siguientes :

- Creación, supresión o modificación de ficheros en el ámbito de aplicación del documento de seguridad.
- Cambios en la organización de seguridad.
- Cambios en las normativas o procedimientos.
- Cambios relevantes en los sistemas de información.
- Cambios en las disposiciones legales.
- Cambios de Responsable del Sistema.

Corresponde al Responsable del Sistema la aprobación del Documento de Seguridad. No obstante, el Responsable de Seguridad mantendrá actualizada la información de los anexos que lo acompañan.

La modificación y actualización del documento de seguridad será también aprobada por el Responsable del Sistema, previa consulta al Responsable de Seguridad.

Las actividades que componen el procedimiento de actualización del documento de seguridad son las siguientes:

- Aprobar/Comunicar actualización. El Responsable del Sistema aprobará la modificación o nueva versión del documento de seguridad y trasladará al Responsable de Seguridad el contenido de la decisión.
- El Responsable del Sistema aprobará también la creación, modificación y supresión de los ficheros con datos estadísiticos protegidos del Instituto Vasco de Estadística.
- Actualizar el documento de seguridad. Cuando el Responsable del Sistema autorice la creación, modificación o la baja un fichero, trasladará la decisión al Responsable de Seguridad, que actualizará los anexos del Documento de Seguridad recabando, si fuera necesario, la información para ello del CPD.
- Difundir el Documento de Seguridad. Corresponde al Responsable de Seguridad la difusión del documento o de sus modificaciones entre las personas obligadas a lo dispuesto en él.

Notificación y gestión de incidencias

Se entiende por incidencia cualquier anomalía que afecta o pudiera afectar a la seguridad de los datos. A los efectos de su registro, se distinguen entre otros los siguientes tipos de incidencias:

- Olvido de la contraseña.

- Sospecha de uso indebido de la contraseña.
- Pérdida de soportes informáticos.
- Accesos no autorizados a dependencias que contienen sistemas de información con datos protegidos.
- Petición de recuperación de datos.

Cada vez que un usuario detecte una incidencia que pudiera afectar a la seguridad de los datos, lo notificará a través de la aplicación de Avisos al Centro de Asistencia a Usuarios. En caso de urgencia, además de notificarlo a través de dicha aplicación, se pondrá en contacto con telefónico con el CPD. El CPD se encargará del mantenimiento del registro de incidencias de seguridad que afecten a datos protegidos.

Cuando un usuario le comunique una incidencia, el CPD registrará toda la información relevante relacionada con la misma.

Copias de respaldo y recuperación de datos

Actualmente se cuenta con una infraestructura para copias de seguridad compuesta por cuatro servidores dispuestos del siguiente modo:

- Titan es el Servidor Networker (Networker Server y Storage Node), y realiza los backups de información en entorno Windows más las exports de las bases de datos Oracle (entorno Unix).
- Virgo es nodo de almacenamiento (Storage Node) y gestiona el salvado de Rman a cinta (Rman: Permite la recuperación de los datos en cualquier momento de la vida de la BD).
- El host OpenVMS (Libra) dispone de su propio sistema de backups en cintas TK-s.
- El servidor web Piscis realiza backups de su contenido y del banco de datos (Ilargi) sobre cinta DAT.

Estos 4 servidores se encargan de realizar las copias de seguridad de los 11 servidores que contienen datos cruciales para EUSTAT.

La frecuencia y tipo de las copias de seguridad depende de la importancia de los datos y de los cambios que se produzcan en ellos en cada servidor. Como ejemplo decir que sobre el servidor que contiene los datos de explotación se realizan 2 tipos diferentes de backups completos diariamente.

Todas las cintas se reutilizan cuando llega la fecha de caducidad de su contenido.

Las cintas tienen una vida útil de 3 años. Una vez rebasado este período de tiempo la cinta se desecha y se sustituye por otra.

La destrucción de soportes se realiza por medio de una empresa externa que previamente asegura la inviolabilidad del contenido. Así mismo, una vez destruidos los soportes emite un certificado con los siguientes datos:

- Fecha de recepción de los soportes

- Peso del envío

- Fecha de destrucción

Las cintas se almacenan en la caja fuerte ignífuga de la sala de servidores del CPD. En el caso de que se realice un clon bajo petición, ésta se almacena en la cámara ignífuga de EUSTAT del sótano. Las cintas cuya vida útil ha expirado se guardan hasta su destrucción en la cámara ignífuga de EUSTAT del sótano.

El transporte de la sala de servidores al sótano de Lakua2 se realiza en mano por parte de los Administradores de backup. El transporte del material a destruir al lugar donde se reciclan los soportes se realiza por parte de la empresa contratada.

Se realizan pruebas de recuperación durante el primer mes del año. Cada uno de los Administradores de backup recuperará una copia de seguridad de los distintos servidores de copias de seguridad.

El análisis de los registros de actividad de las copias programadas se hace diariamente por parte de los Administradores de backup. En caso de ocurrir alguna incidencia, se anota en el Registro de Incidencias.

Creación, modificación y supresión de ficheros que contengan datos protegidos

- Corresponde al Responsable del Sistema la creación, modificación o supresión de ficheros que contengan datos protegidos.

- La creación de un fichero se llevará a cabo por escrito en el que habrán de constar los siguientes datos:

  - Nombre del fichero o subsistema
  - Organo Responsable
  - Ficheros o subsistemas afectados
  - Descripción detallada de la estructura del fichero
  - Nivel de seguridad asignado: básico, medio o alto

- La modificación o supresión de un fichero se efectuará por escrito en el que constarán los aspectos que se modifican y el destino de los datos, respectivamente.

- No se registrarán datos protegidos en ficheros que no reúnan las condiciones de seguridad expresadas en este documento.

Creación de ficheros

- En el desarrollo de aplicaciones, el responsable del proyecto deberá velar para que se tengan en cuenta las medidas de seguridad a considerar en el desarrollo de aplicaciones que manejan datos protegidos.

- Al final del desarrollo de una aplicación, el Responsable de Seguridad junto al responsable del proyecto, validará que se han cumplido las normas de seguridad correspondientes al nivel de los datos que se vaya a tratar.

- Al final de la fase de desarrollo de la aplicación, Responsable de Seguridad actualizará el inventario de ficheros, dando de alta de manera provisional los nuevos ficheros. El fichero o ficheros quedan registrados en el inventario de ficheros en el estado de "provisional". Adicionalmente introducirá en el inventario de ficheros, todos los datos asociados al fichero, el Responsable del Sistema, usuarios, administradores, soportes, etc.

- Tras la aceptación de la aplicación por parte del Instituto Vasco de Estadística, el Responsable de Seguridad actualiza de nuevo el inventario de ficheros para introducir si es necesario, los cambios que hayan podido producirse y pasar el estado de las altas de ficheros a "aceptado".

- Tras la formación de los usuarios en el manejo de la nueva aplicación y cuando ésta vaya a pasar a producción, el Responsable de Seguridad debe realizar las siguientes actuaciones:

- Completar, si es necesario, la información del fichero registrada en el inventario de ficheros (Por ejemplo los usuarios que van a acceder al mismo o la descripción de los Sistema de Información).

- Antes de que la aplicación pase a producción, la empresa que ha desarrollado la aplicación facilitará al Jefe de Proyecto y al Responsable de Seguridad la información sobre los ficheros que maneja la aplicación para su registro en el Inventario de Ficheros antes del paso a producción de la aplicación.

Modificación de ficheros

- En la modificación de aplicaciones, el responsable del proyecto deberá velar para que se tengan en cuenta las medidas de seguridad a considerar en la modificación de aplicaciones que manejan datos protegidos.

- En las pruebas que se realicen de las modificaciones de aplicaciones que manejan datos protegidos, el Responsable de Seguridad debe velar para que se cumpla la normativa de utilización de datos reales en pruebas.

- Al final de la fase de desarrollo de las modificaciones de la aplicación, el Responsable de Seguridad actualizará el inventario de ficheros, dando de alta de manera provisional los ficheros modificados. El fichero o ficheros quedan registrados en el inventario de ficheros en el estado de "modificación provisional". Adicionalmente introducirá en el inventario de ficheros, todos los datos correspondientes al fichero que se hayan podido modificar, Responsable de Seguridad, usuarios, Sistema de Información, campos de la base de datos, etc.

- Tras la aceptación de las modificaciones, el Responsable de Seguridad actualizará de nuevo el inventario de ficheros para introducir si es necesario los cambios que hayan podido producirse y pasar el estado de las modificaciones de ficheros a "aceptado".

Supresión de ficheros

- Cuando un fichero deba ser suprimido, el Responsable de Seguridad debe actualizar el inventario de ficheros con la baja del fichero, esta baja queda registrada como "provisional".

- Tras la aceptación de la baja del fichero por parte de Responsable del Sistema, el Responsable de Seguridad realiza las siguientes tareas:

- Actualiza de nuevo el inventario de ficheros para introducir si es necesario, los cambios que hayan podido producirse y pasar el estado de la baja a "aceptado".

- En los casos en que la supresión de un fichero suponga la eliminación definitiva de la información estadística, deberá incorporarse al documento de seguridad el informe del Consejo Vasco de Estadística o, en su caso, referencia que lo identifique.