ANEXO IV

FUNCIONES Y OBLIGACIONES DEL PERSONAL EN MATERIA DE PROTECCIÓN DE DATOS

1. INTRODUCCIÓN

1.1. ¿QUÉ ES LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES?

Es la normativa que regula la recogida y el tratamiento de los datos personales (dichos datos pueden ser de clientes, trabajadores, solicitantes de empleo, usuarios, etc.).

1.2. ¿QUÉ OBJETO TIENE?

Establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Es decir, limitar el grado de intrusión en nuestra intimidad que pueden generar las nuevas tecnologías, así como el tráfico indiscriminado de datos personales.

1.3. ¿A INCUMBE LA LEY?

La ley obliga a su cumplimiento a todos los profesionales, empresas, organismos públicos y privados que traten con datos personales registrados en soporte físico (soporte papel o informático).

1.4. ¿QUÉ SON LOS DATOS PERSONALES?

Es toda información sobre una persona física identificada o identificable («el interesado»).

Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

- Son datos de carácter personal:
- El nombre y apellidos de una persona.
- Teléfono fijo o móvil.
- Dirección postal.

- Correo electrónico.
- DNI / NIF.
- Dirección IP.
- Una fotografía.
- Una grabación de vídeo.
- Cualquier otra información de la que se desprendan datos personales.

1.5. CLASIFICACIÓN DE LOS DATOS PERSONALES

Los datos de carácter personal se pueden clasificar en:

- **Datos identificativos:** nombre y apellidos, dirección postal, dirección electrónica, teléfono, DNI/NIF, SS/mutualidad, imagen, voz, firma o huella digitalizada, firma electrónica, etc.
- **Datos de características personales:** estado civil, familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricas.
- **Datos de circunstancias sociales:** características de alojamiento, vivienda, situación militar, propiedades y posesiones, aficiones y estilo de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.
- **Datos académicos y profesionales:** formación y titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o a asociaciones profesionales.
- **Datos de empleo:** profesión, puestos de trabajo, datos no económicos de nómina, historial del trabajador.
- **Datos de información comercial:** actividades y negocios, licencias comerciales, suscripciones a publicaciones y medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- **Datos económicos, financieros y de seguros:** ingresos y rentas, inversiones y bienes patrimoniales, créditos, préstamos y avales, datos bancarios, planes de

pensiones, jubilación, datos económicos de nómina, deducciones impositivas, impuestos, seguros, hipotecas, subsidios y beneficios, historial de créditos, tarjetas de crédito.

- **Datos de transacciones de bienes y servicios:** bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones, indemnizaciones.
- **Categorías especiales de datos personales:** son aquellos datos que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como los datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

1.6. MEDIDAS DE SEGURIDAD

No es lo mismo tratar datos meramente identificativos para, por ejemplo, realizar la facturación de un servicio, que tratar el historial médico, o la vida sexual de una persona.

Hay datos mucho más sensibles que otros, y que necesitan de una mayor protección para garantizar la confidencialidad e integridad de los mismos.

En particular, los datos más sensibles (y que deben ser objeto de una mayor protección) son los detallados como categorías especiales de datos personales del apartado anterior.

Deben implantarse medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

1.7. ¿QUÉ ES UN TRATAMIENTO DE DATOS PERSONALES?

Es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

1.8. ¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO?

Es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

1.9. ¿QUIÉN ES EL ENCARGADO DEL TRATAMIENTO?

La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Por ejemplo, la asesoría laboral del responsable, que realiza las nóminas de sus trabajadores, es un encargado del tratamiento.

1.10. OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos. Dichas medidas se revisarán y actualizarán cuando sea necesario.

La normativa también establece los requisitos documentales necesarios para poder cumplir con la citada normativa y poder ser capaz de demostrar dicho cumplimiento

Entre la documentación mínima que debe dispone la entidad se encuentra:

- El Registro de Actividades de Tratamiento, tanto como responsable del tratamiento, como encargado del tratamiento, en su caso.
- Documentación del análisis de riesgos realizado.
- La/s Evaluación/es de Impacto relativa/s a la Protección de Datos, en su caso.
- Las medidas de seguridad implantadas.
- Las funciones y obligaciones del personal con acceso a datos personales.
- El registro de incidencias y el registro de las notificaciones de las violaciones de la seguridad a la Autoridad de Control, en su caso.
- Los protocolos de atención a los derechos de los interesados.

- Los compromisos de confidencialidad con los trabajadores.
- Los contratos de acceso a datos por cuenta de terceros.
- La documentación relativa a las transferencias internacionales de datos, así como las garantías apropiadas obtenidas o las excepciones utilizadas como base jurídica para su realización.
- Toda la documentación adicional que sea necesaria para demostrar el cumplimiento de la normativa de protección de datos en la entidad (cláusulas legales, consentimientos otorgados por los interesados, autorizaciones para la contratación de subencargados del tratamiento, ponderaciones del interés legítimo, etc.).

Esta documentación debe mantenerse en todo momento actualizada y debe ser revisada siempre que se produzcan cambios que puedan repercutir en el cumplimiento de la normativa de protección de datos o en las medidas de seguridad implantadas, como son cambios relevantes en:

- la organización
- el contenido de la información incluida en los tratamientos
- los tratamientos de datos personales realizados
- los sistemas de tratamiento empleados

Debe mantenerse adecuada, en todo momento, a las disposiciones vigentes en materia de protección de los datos de carácter personal.

1.11. LOS DERECHOS DE LOS INTERESADOS

Los derechos que los interesados pueden solicitar al responsable del tratamiento son los siguientes:

- Derecho de acceso.
- Derecho de rectificación.
- Derecho de supresión («el derecho al olvido»).
- Derecho a la limitación del tratamiento.

- Derecho a la portabilidad de los datos.
- Derecho de oposición.
- Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.

El protocolo, los plazos y la forma de actuación está detallada en el ANEXO X, "Protocolos de atención a los derechos". El personal podrá solicitar una copia del mismo en cualquier momento.

Cualquier usuario que reciba una solicitud por parte de un interesado, deberá rellenar el formulario "GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS", que se encuentra en el APÉNDICE II, y remitirlo cuanto antes al Delegado de Protección de Datos o al responsable de gestionar los derechos de los interesados.

2. FUNCIONES Y OBLIGACIONES DE LOS USUARIOS

Usuario es todo el personal autorizado que accede a los datos de carácter personal para el desempeño de las funciones propias de su puesto de trabajo.

Todos los usuarios tienen la obligación de colaborar con el responsable del tratamiento para velar por el cumplimiento de la legislación vigente sobre protección de datos personales.

Los usuarios deben respetar los procedimientos definidos para gestionar la seguridad de la información personal que se detallan a continuación.

2.1. OBLIGACIONES GENERALES

- Guardar secreto y confidencialidad de la información tratada. Quienes intervienen en cualquier fase del tratamiento de los datos personales, está obligado al secreto profesional respecto a los datos y al deber de guardarlos, obligaciones que continúan incluso después de finalizar las relaciones con el responsable del tratamiento.
- La vulneración del deber de secreto respecto a los datos personales tratados, será considerado una falta grave, lo cual dará lugar al inicio de acciones disciplinarias, si proceden.
- Proteger los datos personales que esté tratando y custodiarlos para que personal no autorizado no tenga acceso a ellos.
- Los sistemas de información, recursos, y la información personal a la que se accede, sólo se debe utilizar para las labores estrictamente profesionales que el usuario tiene asignadas.
- Facilitar a los interesados el ejercicio de sus derechos. Para ello, recogerá la solicitud escrita y la trasladará al responsable correspondiente para su atención según el protocolo establecido.

2.2. PUESTOS DE TRABAJO

- Cada usuario es responsable de la confidencialidad de la contraseña que tiene para acceder a los sistemas de información. En caso que de forma accidental o intencionada esta contraseña sea conocida por personas no autorizadas, deberá

registrarlo como incidencia y proceder al cambio de la misma.

- El usuario deberá cambiar la contraseña inicial asignada en el primer acceso que realice al sistema, o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de una tercera persona para realizar el proceso. Las contraseñas deberán ser lo suficientemente complejas para no ser adivinadas de forma sencilla por un tercero. Para ello, se deberán seguir las siguientes normas para elegir la contraseña:
    - Deberán tener una longitud mínima de 8 caracteres alfanuméricos.
    - No deberán coincidir, ni siquiera en parte, con el código de usuario.
    - No deberán estar basados en cadenas de caracteres que sean fácilmente asociadas al usuario (nombre, apellidos, ciudad y fecha de nacimiento, nombres de familiares, matrícula del coche, etc.).
- El usuario deberá aplicar las reglas nemotécnicas para poder construir una contraseña lo suficientemente compleja como para que no pueda ser adivinada por terceros y a la vez sean muy fáciles de recordar por él.
- Los puestos de trabajo estarán bajo la responsabilidad de algún usuario autorizado que garantizará que la información que muestran no pueda ser visible a personas no autorizadas.
- Los puestos de trabajo deberán estar físicamente ubicados en lugares que garanticen la confidencialidad, así como las pantallas, impresoras y cualquier otro dispositivo conectado al puesto de trabajo y desde el que sea posible tener acceso a datos de carácter personal.
- Cuando el responsable del 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 datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. Para reanudar el trabajo será necesaria la introducción de una contraseña que desactive el protector de pantalla. Deberá retirar también cualquier soporte, como documentos, fichas, discos, u otros que contengan datos del fichero, y proceder a guardarlos en su ubicación protegida habitual.

- En el caso de las impresoras, deberá asegurarse que no quedan documentos con datos personales en la bandeja de salida. Si las impresoras son compartidas, el usuario que ha mandado la impresión deberá retirar los documentos conforme vayan siendo impresos.

- Queda expresamente prohibido cualquier cambio de la configuración de la conexión de los puestos de trabajo a sistemas o redes exteriores, que no esté autorizada previamente por el responsable del tratamiento.

- Se deberá evitar el guardar copias de los datos personales en ficheros temporales. En caso de que el tratamiento haga imprescindible realizar dichas copias, se deberán adoptar las siguientes precauciones: realizar siempre las copias sobre un mismo directorio de nombre TEMP o similar, de forma que no queden dispersas por el disco duro, y siempre sea posible conocer donde están los datos temporales. Tras realizar el tratamiento que ha requerido estos datos temporales, proceder a su inmediata eliminación.

- Los ficheros temporales creados exclusivamente para la realización de trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda en función de los datos que contienen.

- El trabajo fuera de los locales del responsable del tratamiento, solo se podrá realizar cuando exista una autorización previa del responsable del tratamiento o del encargado del tratamiento, en todo caso, deberá garantizarse la seguridad de esos datos.

- No deberá copiarse, ni transportar información en portátiles, o equipos que se encuentren fuera de las oficinas sin la correspondiente autorización del responsable del tratamiento. Especial consideración deberán tener los puestos de trabajo portátiles, como ordenadores portátiles o PDA. Estos dispositivos portátiles, cuando puedan almacenar datos personales, deberán contar con una autorización especial por parte del responsable del tratamiento.

2.3. GESTIÓN DE SOPORTES

Se entiende por soporte todo objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden

grabar y recuperar datos.

Ejemplos de soportes: disquetes, cd-rom, dvd-rom, memoria usb, disco duro, etc.

Los usuarios deben observar las siguientes medidas de seguridad en relación con los soportes que contengan datos de carácter personal:

- Los usuarios que traten los soportes o documentos con datos de carácter personal, son los encargados de custodiarlos y vigilar para que personas no autorizadas no accedan al soporte físico o documentos a su cargo.
- Cuando un usuario gestione o produzca soportes que contengan datos de carácter personal, estos deberán estar claramente identificados con una etiqueta externa y, en su caso, inventariados según el protocolo establecido.
- Los soportes que contengan datos personales, deberán ser almacenados en lugares a los que no tenga acceso el personal no autorizado.
- La salida de soportes que contengan datos de carácter personal de las instalaciones bajo control del responsable del tratamiento, deberá ser autorizada previamente.
- La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o añejos a un correo electrónico, fuera de los locales bajo el control del responsable fichero o tratamiento, deberá ser autorizada previamente.
- El traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación.
- Cuando deban ser enviados datos personales sensibles fuera de las ubicaciones del responsable del tratamiento, ya sea mediante soporte físico de grabación de datos o bien a través de correo electrónico o FTP, deberán ir cifrados o utilizar cualquier otro mecanismo que asegure que la información no es accesible ni manipulada durante su transporte.

2.3.1. DESTRUCCIÓN Y REUTILIZACIÓN DE SOPORTES

Uno de los mayores peligros para la confidencialidad de los datos son los soportes desechados.

Todos los desechos informáticos de cualquier tipo que puedan contener información de carácter personal, como CDs, cintas, discos removibles, o incluso los propios ordenadores obsoletos que contengan discos de almacenamiento, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general, ningún desecho informático debe ser nunca dejado para retirar sin ser destruido o depositado en el contenedor de la empresa encargada de la destrucción de los datos.

- Aquellos CDs que contengan datos de carácter personal deberán ser destruidos en una destructora o por cualquier otro medio que haga imposible extraer ningún dato posteriormente.

- Todos los disquetes y otros soportes removibles desechados deberán ser eliminados sus datos previamente con alguna aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos y entregados para su reutilización al responsable del tratamiento.

- Si se trata de ordenadores obsoletos, antes de su donación, venta o entrega a otras organizaciones, deberá comunicarse al responsable del tratamiento para que pase una aplicación de borrado seguro que haga imposible la recuperación posterior de los datos contenidos. Si el ordenador estuviese estropeado y no se pudiese realizar la operación de limpiado, se deberán desmontar los discos duros y proceder a su destrucción o encomendar a una empresa de reciclaje especializada la destrucción de los mismos.

2.4. FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

- Los ficheros temporales o copias de documentos creados exclusivamente para trabajos temporales o auxiliares, deberán cumplir las medidas de seguridad que les corresponda y serán borrados o destruidos una vez hayan dejado de ser necesarios para los fines que motivaron su creación.

2.5. DOCUMENTACIÓN EN PAPEL (NO AUTOMATIZADA)

- En tanto los documentos con datos personales no se encuentren archivados en los dispositivos de almacenamiento indicados en el punto anterior, por estar en

proceso de tramitación, las personas que se encuentren a su cargo deberán custodiarlos e impedir el acceso de personas no autorizadas.

- Siempre que se proceda al traslado físico de documentación que contenga datos personales (especialmente si son sensibles), deberán adoptarse las medidas que impidan el acceso indebido, manipulación, sustracción o pérdida de la información objeto del traslado durante el transporte de la misma. Para ello, el traslado del soporte fuera de las instalaciones, debe realizarse siempre en un maletín o contenedor similar y que disponga de mecanismo que para su apertura precise de una llave o el conocimiento de una combinación y en todo momento el maletín o contenedor debe estar controlado, bajo supervisión de la persona que lo custodia.

2.5.1. DESTRUCCIÓN DE DOCUMENTACIÓN

Uno de los mayores peligros para la confidencialidad de los datos son los documentos desechados.

Todos los documentos en papel desechados que contengan datos de carácter personal, deberán ser eliminados o destruidos de acuerdo al siguiente procedimiento:

- Como norma general ningún documento debe ser nunca dejado para retirar sin ser destruido o depositado en un contenedor de la empresa encargada de la destrucción de los datos si la hubiera, o destruido por otros medios que impidan la recuperación de la información.

- Aquellos soportes en papel o material blando, y que no sean demasiado voluminosos, deberán ser destruidos en una destructora de papel.

- En caso de no existir máquina destructora de papel o en el caso de que los listados o documentos sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una empresa encargada de la destrucción de los datos, que garantice mediante contrato la destrucción de los mismos.

- El responsable del tratamiento deberá exigir a la empresa encargada de la destrucción de los datos un contrato en el que se comprometan bajo penalización a la completa destrucción de todo el material retirado.

2.6. GESTIÓN DE INCIDENCIAS

Se considerarán como “incidencias de seguridad”, entre otras, cualquier incumplimiento de la normativa de protección de datos personales, así como cualquier anomalía o evento que afecte o pueda afectar a la seguridad de los datos personales en sus tres vertientes de confidencialidad, integridad y disponibilidad.

Se deberán tener en cuenta, entre otras, las siguientes incidencias:

- Pérdida de información personal.
- Modificación de datos personales por personal no autorizado o desconocido.
- Existencia de sistemas de información sin las debidas medidas de seguridad.
- Los intentos de acceso no autorizados a ficheros de carácter personal.
- El conocimiento por terceros de la clave de acceso al sistema.
- El intento no autorizado de salida de un soporte.
- La existencia de soportes sin control que contengan datos personales.
- La destrucción total o parcial de un soporte que contenga datos de carácter personal.
- La caída del sistema de seguridad informática, que posibilite el acceso a datos personales por personas no autorizadas.
- Cualquier incidencia que pueda afectar a la confidencialidad, integridad y/o disponibilidad de los datos personales.

Todos los usuarios, administradores, responsables, así como cualquier persona que tenga acceso a datos de carácter personal, deben tener conocimiento de este procedimiento para actuar en caso de incidencia que se detalla a continuación:

Cuando una persona tenga conocimiento de una incidencia que afecte, o pueda afectar, a la confidencialidad o integridad de los datos contenidos en los ficheros de la organización, deberá comunicarla inmediatamente al responsable del registro de incidencias a través del formulario GESTIÓN DE INCIDENCIAS, del que se le ha hecho entrega a cada trabajador. Deberá especificar el tipo de incidencia producida y su descripción detallada,

indicando las intervenciones de las personas que hayan podido tener relación con la producción de la incidencia, así como la fecha y hora en que se ha producido o detectado, la persona que realiza la notificación, a quién se comunica y los efectos que se pueden haber derivado de la incidencia.

Una vez rellena la plantilla, se obtendrán 2 copias y se entregarán inmediatamente al responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, solicitándole el acuse de recibo en una de las copias. Esta copia se guardará como resguardo de la notificación.

El responsable del tratamiento, Delegado de Protección de Datos, o a la persona en quien haya delegado la gestión de las incidencias, quedará encargo de la gestión, coordinación y resolución de la misma, así como al registro de la incidencia en el registro habilitado para ello.

El conocimiento y no notificación de una incidencia por parte de un usuario, será considerado como una falta de seguridad por parte de ese usuario.

3. FUNCIONES Y OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Deberá:

- Elaborar el Registro de Actividades de Tratamiento.
- Realizar el análisis de los riesgos y guardar la documentación del mismo, así como, en su caso, la evaluación de impacto relativa a la protección de datos.
- Implantar y hacer cumplir las medidas de seguridad establecidas.
- Garantizar la difusión y formación al personal que trate con datos personales de las medidas de seguridad y requisitos que deben cumplir para realizar el tratamiento de datos personales.
- Mantener actualizada la documentación siempre que se produzcan cambios relevantes en:
    - El sistema de información.
    - Es sistema de tratamiento.
    - La organización.
    - El contenido de la información incluida en los tratamientos.
    - Como consecuencia de los controles periódicos realizados.
        - Se considera que un cambio es relevante cuando pueda afectar al cumplimiento de las medidas de seguridad implantadas.
- Nombrar uno o varios responsables delegados para el correcto cumplimiento de la normativa de protección de datos.
- Verificar periódicamente la eficacia de las medidas de seguridad establecidas.
- Analizar las incidencias registradas e implantará las medidas correctivas necesarias para evitar ese tipo de incidencias en el futuro.

4. FUNCIONES Y OBLIGACIONES DEL DELEGADO DE PROTECCIÓN DE DATOS O FIGURA EQUIVALENTE

El Delegado de Protección de Datos tiene las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben;

b) supervisar el cumplimiento de lo dispuesto en la normativa de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier asunto relacionado con el cumplimiento de la normativa de protección de datos. Para ello:

1. Coordinará la puesta en marcha de las medidas de seguridad, colaborará con el responsable del tratamiento en su difusión y cooperará con el responsable del tratamiento controlando el cumplimiento de las mismas.

2. Analizará las incidencias registradas, tomando las medidas oportunas en colaboración con el responsable del tratamiento.

3. Comprobará, periódicamente, la existencia de copias de respaldo que permitan la recuperación de los datos, realizando una prueba de restaurado que verifique la correcta definición de los procedimiento y proceso de recuperación, y enviando evidencias de esta comprobación al responsable del tratamiento.

4. A su vez, también periódicamente, comunicará el responsable del fichero cualquier cambio que se haya realizado en los sistemas de información, como cambios en el hardware o software, bases de datos, aplicaciones de acceso al fichero, etc., procediendo a la actualización de la documentación pertinente.

5. Verificará, periódicamente, la veracidad del inventario de soportes.
6. Tendrá el control directo de los mecanismos que permiten el registro de accesos, sin que se deba permitir, en ningún caso, la desactivación de los mismos.
7. Se encargará de revisar, en su caso y de forma periódica, la información de control registrada en el registro de accesos y elaborará un informe que entregará al responsable del tratamiento para su revisión y archivo.
8. Periódicamente realizará una auditoría de la eficacia de las medidas de seguridad implantadas.
9. Los resultados de los controles periódicos, así como de las auditorías, serán adjuntados a la documentación acreditativa del cumplimiento de la normativa de protección de datos.

APÉNDICE I

GESTIÓN DE INCIDENCIAS			
FECHA		HORA	
TIPO DE INCIDENCIA			
DESCRIPCIÓN:			
EFECTOS DERIVADOS:			
PERSONA QUE COMUNICA LA INCIDENCIA			
PERSONA QUE RECIBE LA NOTIFICACIÓN			
ACUSE DE RECIBO			
FECHA		HORA	
FIRMA:			

APÉNDICE II

GESTIÓN DE SOLICITUDES DE DERECHOS DE LOS INTERESADOS			
FECHA		HORA	
NOMBRE DEL SOLICITANTE			
APELLIDOS DEL SOLICITANTE			
NIF DEL SOLICITANTE			
DOMICILIO DEL SOLICITANTE			
DERECHO QUE DESEA EJERCER	[ ] ACCESO [ ] RECTIFICACIÓN [ ] SUPRESIÓN [ ] LIMITACIÓN DEL TTO [ ] OPOSICIÓN [ ] PORTABILIDAD [ ] DECISIONES INDIVIDUALES AUTOMATIZADAS		
OBSERVACIONES:			
[ ] FOTOCOPIA DEL NIF INCLUIDA			
[ ] OTROS DOCUMENTOS APORTADOS:			
PERSONA QUE RECIBE LA SOLICITUD			