5. Medidas, normas, procedimientos, reglas y estándares de seguridad

5.1. Centros de tratamiento y locales

Los locales donde se encuentran los equipos informáticos que contienen los ficheros objeto de tratamiento deben disponer de las medidas de seguridad necesarias para garantizar la confidencialidad de los datos de carácter personal y su disponibilidad.

El tratamiento de datos fuera de los locales o centros de tratamiento habituales del responsable deberá realizarse, en la medida de lo posible, con idénticas garantías y medidas de seguridad que resultan aplicables en ellos.

En este sentido, el responsable adoptará las medidas oportunas para evitar el acceso a los datos por parte de terceros o la violación de seguridad de los mismos. Como mínimo, para todos aquellos casos en que los datos se trasladen a través de dispositivos portátiles se procederá a su encriptación o a la exigencia de contraseñas personales e intransferibles para el acceso a los archivos y carpetas informáticos en que se encuentren almacenados.

En aplicación de lo previsto en el artículo 33 del Reglamento Europeo de Protección de Datos, cualquier violación de la seguridad de los datos como consecuencia de la pérdida o sustracción de los dispositivos de almacenamiento (USB, ordenador portátil, etc.), o cualquier otra incidencia sobre estos o cualquier otro dispositivo que los contenga, tanto en la sede o local habitual del responsable como en su traslado o durante su uso en otros locales que no constituyan sede o local del responsable, deberá ser comunicado a la autoridad de control a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas titulares de dichos datos.

5.1.1. Régimen de trabajo fuera de los locales del responsable o del encargado del tratamiento.

Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable o del encargado del tratamiento, el responsable deberá garantizar que se siguen aplicando todas las medidas de seguridad necesarias en cada caso para salvaguardar la confidencialidad de los datos y evitar el acceso a los mismos por parte de terceros.

La encriptación de datos, la seudonimización o el acceso a través de contraseñas de acceso de diferentes niveles, diseñadas siguiendo parámetros de contraseña segura, son medidas de seguridad que se utilizarán siempre que sea posible para evitar riesgos y para limitar las consecuencias negativas provocadas por situaciones de riesgo inevitables en que los datos puedan ser objeto de acceso no permitido.

En la relación de personal autorizado, se recogen las autorizaciones y el período de validez de las mismas.

5.2. Puestos de trabajo

Se considera como puestos de trabajo todo ordenador personal, terminal u otro dispositivo desde el que se pueda acceder a los datos en las situaciones siguientes:

- Cuando los datos personales se encuentren almacenados directamente en el equipo.
- Cuando los datos personales se encuentren almacenados en el servidor y desde el equipo correspondiente al puesto de trabajo se pueda acceder al servidor y a los datos.
- Cuando los datos personales se encuentren almacenados "en la nube" y se acceda a los mismos desde el equipo mediante la utilización de claves de acceso y contraseñas seguras.

Cada una de las personas autorizadas tendrá asignado un puesto de trabajo desde el que acceder a los datos por alguna de las vías indicadas o cualquier otra. El usuario asignado al puesto de trabajo será responsable de garantizar que la información a la que accede no podrá ser visualizada o comunicada a personas no autorizadas. Cualquier dispositivo conectado al puesto de trabajo tales como impresoras o pantallas deberán de estar ubicadas de forma que se garantice la confidencialidad de la información y que ésta no pueda ser visualizada o comunicada a personas no autorizadas.

El usuario responsable del puesto de trabajo, cuando finalice su turno o cuando se ausente temporalmente, deberá dejar los equipos y dispositivos en un estado que impida el acceso o la visualización de los datos protegidos a personas no autorizadas. Esto se podrá realizar mediante un protector de pantalla, la suspensión de la sesión de trabajo o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora, el reinicio de la sesión o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos de carácter personal. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso a los datos sólo podrá ser cambiada con la autorización del Responsable de las Actividades de Tratamiento, el Delegado de Protección de Datos o el administrador del sistema designado.

Para reducir los niveles de riesgo sobre los datos, estas medidas de seguridad (cierre de sesión, desconexión, ...) deberán ser aplicadas por todo el personal del responsable muy especialmente cuando el acceso a los datos se realice a través de sistemas de almacenamiento en la nube a los que se acceda mediante conexión a internet desde cualquier equipo informático portátil o fijo, que no sea titularidad del

responsable, y esté ubicado fuera de sus locales, por lo que resulte más difícil comprobar si se han producido violaciones de seguridad o si son susceptibles de producirse en el futuro.

5.3. Identificación y autenticación del personal autorizado.

El responsable de las actividades de tratamiento establecerá un procedimiento que garantice la correcta identificación y autenticación de los usuarios autorizados a acceder a los sistemas de información.

Los accesos a los sistemas de información se realizarán mediante un mecanismo que permita la identificación de forma inequívoca y personalizada del usuario. Cada identificación deberá pertenecer a un único usuario.

Todos los usuarios autorizados para acceder a los datos personales, relacionados en el Anexo Relación de personal autorizado, deberán tener un código o nombre de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

5.3.1. Procedimiento de asignación y cambio de contraseñas.

El responsable de las actividades de tratamiento o la persona con autorización delegada por el responsable asignará un nombre de usuario y propondrá una contraseña para cada uno de los usuarios que, tras el primer acceso, vendrán obligados a cambiarlas.

Las contraseñas deberán constar de un mínimo de 8 dígitos y con una combinación de caracteres alfanuméricos. Se deberá evitar la utilización de nombre o cifras o su combinación que sean fácilmente deducibles.

Las contraseñas se almacenarán de forma ininteligible. El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

Las contraseñas son de carácter personal e intransferible y no serán visibles en pantalla cuando son introducidas.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

Con una periodicidad de cada 6 meses y de forma automática, se propondrá a los usuarios, que cambien su contraseña por una nueva, volviendo a quedar almacenada de forma ininteligible.

El responsable de las actividades de tratamiento o el Administrador del sistema, en su caso, podrá cambiar los requisitos de acceso, las condiciones, modos sistemas y formas de tratamiento o de lectura cuando lo crea oportuno, notificando la decisión a los usuarios y dejando constancia de tal modificación en este documento y en el Registro de incidencias.

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos, y deben por tanto estar especialmente protegidas. Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al responsable de las actividades de tratamiento, o a la persona con autorización delegada por el responsable, y subsanada en el menor plazo de tiempo posible.

Para las Actividades de Tratamiento:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores
- Asociados Potenciales

Quedará limitada la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información. Tras 3 intentos fallidos de acceso quedará bloqueada la contraseña.

5.4. Control de Acceso

5.4.1. Control de acceso lógico

Para reducir al nivel mínimo los riesgos de acceso y tratamiento no permitido de datos personales, el responsable ha establecido un sistema de acceso a datos en que los miembros de la organización tendrán acceso única y exclusivamente a aquellos datos que les resulten imprescindibles para el desarrollo de sus funciones.

En el Anexo Relación de personal autorizado, se incluye una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

Si la aplicación informática que permite el acceso a los datos personales no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante la restricción y disponibilidad de recursos en la sesión del usuario con el control de acceso lógico mediante usuario y contraseña.

Queda prohibido que un usuario acceda a recursos con derechos distintos de los que ha sido autorizado.

En el caso de personal ajeno al responsable de las actividades de tratamiento que tenga acceso a los recursos estará sometido a las mismas condiciones y obligaciones de seguridad que el personal propio, constando en el Anexo Relación de personal autorizado.

Exclusivamente la persona con autorización delegada del responsable de las actividades de tratamiento podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por el Responsable.

Para el caso de nuevas altas de accesos, se comunicará al Responsable por la persona con autorización delegada del responsable de las actividades de tratamiento, con la propuesta de acceso, código de acceso y listado de las funciones del nuevo autorizado. De todo ello se deberá dejar constancia en este Registro de Actividades de Tratamiento en el Anexo Relación de personal autorizado.

5.4.2. Control de acceso físico

Exclusivamente el personal autorizado podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información correspondientes a las actividades de tratamiento siguientes:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores
- Asociados Potenciales

El personal que tiene acceso a los lugares donde se hallan instalados los equipos físicos que dan soporte a los sistemas de información que tratan los datos personales, constan relacionados en el Anexo Relación de personal autorizado como personal afecto a las citadas actividades de tratamiento.

Para el personal del responsable de las actividades de tratamiento, distinto de los usuarios con acceso a los sistemas de información, como pueden ser de mantenimiento, limpieza, seguridad, etc., serán autorizados por el responsable, quien expedirá autorización o credencial que acredite su acceso autorizado.

Para el personal ajeno al responsable de las actividades de tratamiento, que le preste servicios sin acceso a datos personales, en el contrato de prestación de servicios deberá constar expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que pueda conocer con motivo de la prestación de servicios.

5.4.2.1. Registro de accesos

Para aquellos tratamientos sobre datos de carácter personal especialmente protegidos, clasificados con riesgo elevado o muy alto:

- Asociados
- Asociados Potenciales

Deberá registrarse cada intento de acceso, la identificación del usuario, la fecha y hora en que se realizó, el tratamiento accedido, el tipo de acceso y si ha sido autorizado o denegado. Si el acceso fue autorizado, se guardará la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable sin que se deba permitir, en ningún caso, la desactivación ni la manipulación de los mismos.

El período mínimo de conservación de los datos del registro de accesos será de dos años.

El responsable revisará al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

Este registro de accesos no será necesario cuando concurran las siguientes circunstancias:

a) Que el responsable de las actividades de tratamiento sea una persona física.
b) Que el responsable de las actividades de tratamiento garantice que sólo él tiene acceso y trata los datos personales.

La concurrencia de estas dos circunstancias debe hacerse constar expresamente en este registro de actividades de tratamiento.

5.4.2.2. Acceso a la documentación

Para aquellos tratamientos que contienen datos de carácter personal especialmente protegidos, clasificados con riesgo elevado o muy alto:

- Asociados
- Asociados Potenciales

El acceso a la documentación se limita exclusivamente al personal autorizado que consta en el Anexo Relación de personal autorizado.

Para los documentos que puedan ser utilizados por múltiples usuarios, se establecerán mecanismos que permitan identificar los accesos realizados.

El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en este registro de actividades de tratamiento.

5.5. Entorno de Sistema Operativo y de Comunicaciones

Al estar los datos ubicados en un ordenador (o con funciones de servidor) con un sistema operativo determinado y poder contar con unas conexiones que le comunican con otros ordenadores, es posible, para las personas que conozcan

estos entornos, acceder a los datos protegidos sin pasar por los procedimientos de control de acceso con los que pueda contar la aplicación. Se trata de un riesgo de seguridad para los datos.

El sistema operativo y de comunicaciones debe tener al menos un responsable o administrador.

En el caso más simple, cuando los datos se encuentren ubicados en un ordenador personal y se acceda mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente a dichos datos.

Ninguna herramienta o programa de utilidad que permita el acceso a los datos deberá ser accesible a ningún usuario o administrador no autorizado. Esto incluye cualquier medio de acceso en bruto no elaborado o editado a los datos que deberán estar bajo el control del administrador autorizado.

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

Si el ordenador en el que se ubican los datos está integrado en una red de comunicaciones de forma que desde otros ordenadores conectados a la misma sea posible el acceso a los datos, el administrador responsable del sistema deberá asegurarse de que este acceso no se permite a personas no autorizadas.

5.6. Gestión de soportes y documentos

5.6.1. Etiquetado e Inventario de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, conocer de qué actividad de tratamiento se trata y el tipo de información que contienen y la fecha de creación.

Los soportes han de ser inventariados y almacenados en el almacén o almacenes de soportes que constan relacionados en el apartado *Almacenes* del Anexo Recursos protegidos. El acceso al almacén o almacenes estará restringido al personal autorizado para ello y que consta relacionado en el Anexo Relación de personal autorizado.

El inventario de soportes y su mantenimiento se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización y puede ser impreso en cualquier momento. El inventario deberá estar permanentemente actualizado.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el registro de actividades de tratamiento.

La identificación de los soportes que contengan datos de carácter personal que la organización considere especialmente sensibles se podrá realizar utilizando sistemas de etiquetado que serán comprensibles y con significado para los usuarios con acceso autorizado a los citados soportes y documentos y que dificulten la identificación para el resto de personas.

5.6.2. Salida de soportes y documentos

Es previsible que en el proceso de tratamiento de los datos personales llevado a cabo en esta organización, se produzca la salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anexos a un correo electrónico, fuera de los locales del responsable o encargado y bajo el control del responsable de las actividades de tratamiento.

Para evitar riesgos sobre los datos deberán aplicarse las medidas de seguridad necesarias para garantizar su confidencialidad y evitar accesos no permitidos a los mismos. En este sentido, los datos se transmitirán encriptados siempre que sea posible, o sólo podrán visualizarse mediante el acceso a través de nombre de usuario y contraseña.

En caso de producirse alguna incidencia sobre los datos el sistema debería detectarla lo antes posible para evitar el uso indebido de los mismos.

Con respecto a los documentos también se consideran incluidos en la salida de documentos los siguientes supuestos:

- Envío por correo electrónico en el cuerpo del mensaje o como adjuntos datos objeto de tratamiento.
- Los faxes cuando incorporan datos objeto de tratamiento.
- Cualquier otro procedimiento electrónico como ftp, descargas desde la web o carpetas compartidas, sistemas de almacenamiento en la nube, etc.

Como medida de seguridad preventiva, el responsable incorporará en este documento toda la información necesaria para conocer quiénes son las personas que tienen acceso a las diferentes formas de tratamiento y las medidas de seguridad que están obligadas a aplicar en cada una de ellas. En la medida de lo posible, el sistema almacenará como mínimo los últimos accesos para detectar irregularidades lo antes posible y prevenir riesgos en el acceso no autorizado a los datos así como su limitación lo antes posible en caso de producirse.

En el caso del correo electrónico para garantizar la trazabilidad de los datos que salen materialmente del sistema de información, puede servir como registro el propio sistema de indexación del gestor del correo electrónico.

5.6.3. Traslado de soportes y documentación

En el traslado de la documentación se adoptarán las medidas y procedimientos apropiados para evitar la sustracción, pérdida o acceso indebido a la información durante su transporte. En este sentido, se utilizarán sistemas de encriptado siempre

que sea posible, o como mínimo, la exigencia de contraseñas seguras para el acceso a los datos.

En el caso de la documentación, las personas encargadas de su custodia extremarán al máximo las medidas de prevención para evitar accesos no autorizados. Sólo será objeto de transporte la documentación en que figuren datos personales cuando sea imprescindible. Como medida de prevención de riesgos, y siempre que ello sea posible, se recurrirá a la seudonimización como garantía de confidencialidad de los datos durante su traslado en papel.

5.6.3.1. Traslado de documentación

El traslado de la documentación de las actividades de tratamiento:

- Asociados
- Asociados Potenciales

Siempre que se proceda al traslado físico de la documentación, deberán adoptarse las medidas apropiadas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

5.6.4. Destrucción y borrado de documentos o soportes

Los documentos y soportes que vayan a ser desechados correspondientes a los tratamientos:

- Asociados - (Riesgo Elevado o Muy Alto, Trat. Mixto)
- Voluntarios - (Riesgo Moderado, Trat. Mixto)
- Personal - (Riesgo Bajo, Trat. Mixto)
- Proveedores - (Riesgo Bajo, Trat. Mixto)
- Cursos de Formación para Educadores - (Riesgo Moderado, Trat. Mixto)
- Asociados Potenciales - (Riesgo Elevado o Muy Alto, Trat. Mixto)
- Colaboradores - (Riesgo Bajo, Trat. Mixto)
- Registro diario de jornada laboral del personal empleados - (Riesgo Bajo, Trat. Mixto)

Aquellos soportes que se vayan a reutilizar deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables de ningún modo. No será válido el borrado lógico o rápido que impide el acceso a la información pero no la elimina físicamente hasta que ha sobrescrito sobre la misma.

Los soportes que se vayan a eliminar deberán ser borrados físicamente antes de su eliminación, que consistirá en un proceso de destrucción mecánica del soporte, trituración o incineración.

Los documentos en formato papel que vayan a desecharse, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos en formato papel.

Los procesos de reutilización y eliminación descritos han de ser previos a la preceptiva baja de los soportes en el inventario.

5.6.5. Registro de Entrada y Salida de soportes

Deberán ser registradas las salidas y entradas de soportes correspondientes a las actividades de tratamiento:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores
- Asociados Potenciales

El registro de entrada de soportes indicará el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

El registro de salida de soportes indicará el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

El procedimiento de registro de entradas y salidas de soportes se gestiona mediante el programa por persona autorizada y puede ser impreso o no como Anexo de este registro de actividades de tratamiento.

5.6.6. Gestión y distribución de soportes

La gestión y distribución de soportes que contengan datos de carácter personal de las actividades de tratamiento:

- Asociados
- Asociados Potenciales

La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido y que dificulten la identificación para el resto de personas.

La distribución de los soportes se realizará cifrando los datos que contengan o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Los dispositivos portátiles cuando se encuentren fuera de las instalaciones que están bajo control del responsable de las actividades de tratamiento, deberán cifrar los datos que contengan.

En caso que se requiera el uso de **dispositivos portátiles que no permiten el cifrado**, debe especificar el motivo de su uso y adoptar las medidas de seguridad necesarias que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

5.7. Ficheros temporales o copias de trabajo de documentos

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir igualmente con las medidas de seguridad que correspondan.

Como medida de prevención de riesgos, los ficheros temporales o copias de documentos así creados serán borrados o destruidos una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Lo anterior, incluye los ficheros temporales que utilicen y generen las aplicaciones de acceso al Fichero.

Las copias de trabajo de documentos en formato papel, deberá procederse a su destrucción mediante la trituradora de papel. Está prohibida la reutilización de documentos o copias de trabajo en formato papel.

El Responsable de las Actividades de Tratamiento o, en su caso, el Delegado de Protección de Datos, deberá asegurarse de que los ficheros temporales o copias de trabajo de documentos no son accesibles por personal no autorizado.

5.8. Transmisión de datos por redes de Telecomunicaciones

- Asociados
- Asociados Potenciales

La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

5.9. Copias de seguridad

Es obligatorio establecer procedimientos de actuación para la realización de copias de respaldo periódicas, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción como vía para restaurar su disponibilidad y el acceso a los datos personales de forma rápida en caso de incidencia física o técnica, de acuerdo con los previsto en el artículo 32 del Reglamento Europeo de Protección de Datos.

5.9.1. Procedimiento de realización de copias de respaldo.

Las copias de seguridad deben de realizarse como mínimo con una periodicidad semanal, cada viernes o último día laborable de la semana. El soporte magnético que las almacena dispondrá de toda la información del sistema.

Las copias han sido planificadas de tal manera que no habrá una intervención de ningún operador para esta rutina. La misión del operador de copias tendrá como trabajo principal:

- Comprobación de la copia semanal.
- Cambio de soporte.
- Verificación de la copia semanal.

La copia se entregará al Responsable o persona designada por éste, quien deberá entregar la más antigua que tenga, estableciendo así un sistema de rotación de soportes.

En caso de que cualquiera de las copias no se efectuara correctamente, se debería de editar el informe que genera la aplicación de backup y proceder a repetir la copia manualmente o informar al responsable del sistema.

5.9.2. Recuperación de datos

Los procedimientos para la recuperación de los datos deben garantizar en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En caso de fallo del sistema con pérdida total o parcial de los datos existirá un procedimiento, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos del Fichero al estado en que se encontraban al tiempo de producirse la pérdida o destrucción. De esta manera se reducen los efectos negativos generados por las incidencias que puedan afectar a los datos.

Únicamente respecto de los tratamientos parcialmente automatizados siguientes:

- Asociados
- Voluntarios
- Personal
- Proveedores
- Cursos de Formación para Educadores
- Asociados Potenciales
- Colaboradores
- Registro diario de jornada laboral del personal empleados

Siempre que exista documentación que permita alcanzar la recuperación de los datos al estado en que se encontraban al tiempo de producirse la pérdida o destrucción, se procederá a grabar manualmente los datos quedando constancia motivada de este hecho en el registro de incidencias.

5.9.3. Verificación de los procedimientos de copia y recuperación de datos

El responsable o la persona con autorización delegada del responsable de las actividades de tratamiento verificará cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos.

5.9.4. Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten datos de carácter personal no se realizarán con datos reales, salvo que previamente se haya realizado una copia de seguridad y se aseguren las medidas de seguridad correspondientes al tratamiento realizado y se anote su realización en este registro de actividades de tratamiento.

De las pruebas realizadas conforme al párrafo anterior, deberá quedar constancia en el registro de incidencias.

5.9.5. Almacenamiento de las copias de respaldo

Las copias de respaldo y recuperación se encuentran almacenadas en el almacén o almacenes que constan relacionados en el apartado *Almacenes* del Anexo Recursos Protegidos.

Sobre estos almacenes se aplicarán las medidas de seguridad necesarias para evitar riesgos de accesos no autorizados y disminuir al mínimo las consecuencias de éstos en caso de producirse.

5.9.6. Copia de respaldo en lugar diferente

Se conservará una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir las medidas de seguridad, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

5.10. Criterios de archivo

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición.

En aquellos casos en los que no exista norma aplicable, el responsable de las actividades de tratamiento deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

5.11. Dispositivos de almacenamientos

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquellos no permitan adoptar esta medida, el responsable de las actividades de tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

5.11.1. Custodia de soportes

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento indicados en el apartado anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

5.11.2. Almacenamiento de la información

Los armarios, archivadores u otros elementos en los que se almacenan los ficheros no automatizados con datos de carácter personal se encuentran en el almacén o almacenes que constan relacionados en el apartado *Almacenes* del Anexo Recursos Protegidos, en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos.

Si, atendidas las características de los locales de que dispusiera el responsable de las actividades de tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, se adoptarán las medidas alternativas que, debidamente motivadas, se incluirán en el registro de actividades de tratamiento.

5.11.3. Copia o reproducción

La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el registro de actividades de tratamiento.

Las copias o reproducciones desechadas deberán ser destruidas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior. Se procederá a su destrucción mediante la trituradora de papel.

5.12. Procedimiento de notificación, registro, gestión y respuesta ante las incidencias

5.12.1. Definición

Una incidencia es “cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos”, es decir, a la confidencialidad, integridad y disponibilidad de los datos. Cualquier situación o hecho que pueda poner en peligro la confidencialidad o integridad de los datos durante su tratamiento o durante el almacenamiento que posibilite su tratamiento se considera una incidencia.

5.12.2. Procedimiento

Todo usuario que tenga conocimiento de una incidencia será responsable del registro de la misma en el registro de Incidencias o en su caso de la comunicación por escrito a FEDERACIÓ D'ESCOLTISME VALENCIÀ o a la persona con autorización delegada del responsable de las actividades de tratamiento.

El conocimiento y la no notificación o registro de una incidencia por parte de un usuario será considerado como una falta contra la seguridad del tratamiento por parte de ese usuario.

La notificación o registro de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, en su caso, detectado, la persona que realiza la notificación, persona a quien se le comunica, efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Junto a esa gestión interna, y en cumplimiento de la obligación impuesta por el artículo 33 del Reglamento Europeo de Protección de Datos, en caso de violación de la seguridad de los datos personales, el responsable de tratamiento lo notificará a la autoridad de control sin dilación indebida, y siempre antes de que transcurran 72 horas de que haya tenido constancia de la misma. En caso de incumplirse este plazo, la notificación incorporará además las causas justificantes de este retraso.

El Reglamento excluye de la obligación de notificar esta violación únicamente en el caso de que sea improbable que la misma constituya un riesgo para los derechos y las libertades de las personas físicas.

Cuando el encargado de tratamiento tenga conocimiento de la existencia de violaciones de seguridad de datos personales, deberá ponerlo en conocimiento del responsable lo antes posible.

De acuerdo en el apartado 3 del artículo 33 del Reglamento Europeo, la notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles

consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si además el responsable observa que esta violación de seguridad de los datos entraña un alto riesgo para los derechos y libertades de las personas físicas, deberá comunicarle a los interesados la incidencia producida lo antes posible, de manera que éstos puedan adoptar las medidas necesarias para reducir los riesgos de uso indebido o transmisión a terceros de los datos sobre los que se ha producido el acceso.

Según lo previsto en el artículo 34 del Reglamento Europeo, esta comunicación al interesado no será necesaria si concurre alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado; c) la comunicación suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

A pesar de que el responsable pueda considerar que no es necesaria la comunicación de la incidencia al interesado por concurrir alguna de estas condiciones, la comunicación será necesaria de acuerdo con el artículo 34.4 si así lo ordena la autoridad de protección de datos competente a la que se le ha comunicado previamente.

5.12.3. Registro de incidencias

El registro de incidencias se gestiona mediante la aplicación informática de gestión de protección de datos personales de la organización, concretamente en el módulo o apartado de "Gestión de Incidencias".

5.12.4. Registro de incidencias

En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los tratamientos:

- Asociados
- Voluntarios
- Cursos de Formación para Educadores
- Asociados Potenciales

Cuando para la resolución de la incidencia se requiera realizar una recuperación de datos, deberá consignarse, además:

- Los procedimientos realizados de recuperación de los datos.
- La persona que ejecutó el proceso.
- Los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
- Autorización para la ejecución de los procedimientos de recuperación de los datos de FEDERACIÓ D'ESCOLTISME VALENCIÀ o de la persona con autorización delegada del responsable de las actividades de tratamiento.

5.13. Revisión del documento

Este documento deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información objeto de tratamiento o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

El responsable o la persona con autorización delegada del responsable de las actividades de tratamiento, junto con el delegado de protección de datos, si es el caso, mantendrán una reunión cada vez que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información objeto de tratamiento, con el objetivo de coordinar los cambios a introducir en el Registro de Actividades de Tratamiento, elevando conclusiones al responsable de las actividades de tratamiento.

Igualmente el presente documento deberá actualizarse cada vez que se detecten nuevos riesgos en el tratamiento de los datos o se modifique su nivel de probabilidad o gravedad, de manera que se hayan de reflejar igualmente las nuevas medidas de seguridad implementadas para eliminar dichos riesgos o reducir su incidencia o consecuencias negativas sobre los derechos y libertades de los interesados.

5.14. Procedimiento de control del cumplimiento

Deben establecerse controles periódicos para verificar el cumplimiento de lo dispuesto en el Registro de Actividades de Tratamiento.

- Verificar el inventario de hardware y software.
- Cumplimiento de la política general de seguridad.
- Registro de incidencias.
- Variaciones en el conjunto de actividades de tratamiento.
- Cumplimiento de la política de protección de datos.
- Verificar clasificación de datos.
- Comprobar configuración del sistema.
- Comprobar la relación de personal y accesos autorizados.

- Verificar procedimiento de gestión de soportes.
- Verificación procedimientos de identificación y autenticación.
- Se cumple el proceso de copias de respaldo y recuperación.
- Verificar prestaciones de servicios con acceso y sin acceso a datos.
- Verificar contratos de encargo de tratamiento.
- Verificar contratos de confidencialidad y prestación servicios sin acceso a datos.
- Variaciones en la legislación.

6. Funciones y obligaciones del personal

Todas las personas que tienen acceso a los datos se encuentran obligadas por ley a cumplir lo establecido en este documento. El personal afectado por esta normativa lo podemos clasificar como sigue:

1. **Administradores**, disponen de los máximos privilegios y están encargados de administrar o mantener el entorno operativo del Fichero.

2. **Personal Informático**, encargados de mantener los sistemas de información y resolver las incidencias en máquinas y programas.

3. **Usuario**, Todo sujeto autorizado para acceder a datos o recursos.

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información han de estar claramente definidas y documentadas. En el Anexo Relación de personal autorizado se relacionan.

6.1. Funciones y obligaciones con carácter general

Todo el personal interno o externo de la empresa 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 de las actividades de tratamiento o al delegado de protección de datos 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 apartado Medidas, normas, procedimientos, reglas y estándares de seguridad.

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

6.2. Funciones y obligaciones del Responsable

El responsable de las actividades de tratamiento es el encargado jurídicamente de la seguridad de los datos y de las medidas establecidas en el presente documento. El responsable 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.

El responsable de las actividades de tratamiento es FEDERACIÓ D'ESCOLTISME VALENCIÀ en la persona de David Baldoví Sánchez en calidad de representante legal de la empresa.

6.2.1. Ámbito

Decide sobre la finalidad, contenido, usos y aplicaciones de las actividades de tratamiento: Asociados, Voluntarios, Personal, Proveedores, Cursos de Formación para Educadores, Asociados Potenciales, Colaboradores, Registro diario de jornada laboral del personal empleados y responde de su legalidad y legitimación, de acuerdo con lo dispuesto en el Reglamento Europeo 2016/679, relativo al tratamiento de datos personales, la Ley Orgánica de Protección de Datos, y las instrucciones y recomendaciones de la Agencia de Protección de Datos y normativa relacionada. Es el responsable de cumplir los requisitos exigidos en la legislación vigente para garantizar los derechos de los afectados (acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición). Responde frente al afectado, frente a terceros y frente a la Administración de todos los daños y perjuicios que se deriven del mal uso de los datos.

Coordinará la puesta en marcha de las medidas de seguridad y cuidará de la difusión de las mismas entre todos los miembros de la organización, controlando su cumplimiento por los usuarios.

De acuerdo con el artículo 24 del Reglamento Europeo de Protección de Datos, 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 del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

En aplicación de las obligaciones que le impone el artículo 25 del mismo texto legal, el responsable, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, diseñará las medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, o como la minimización de datos, de manera que queden integradas las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados.

En concreto, también impone el Reglamento al responsable del tratamiento en ese artículo 25 la obligación de aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

6.2.2. Finalidad del Tratamiento

El Responsable de las Actividades de Tratamiento decide sobre la finalidad del tratamiento.

6.2.3. Usos de los Datos

El uso es confidencial e intransferible. Los datos en él contenidos serán utilizados por FEDERACIÓ D'ESCOLTISME VALENCIÀ, a través de su personal designado propio o externo, cumpliendo en todo momento las medidas de seguridad y los requisitos exigidos para su legitimación y legalidad en su tratamiento.

6.2.4. Funciones

- Decidir sobre la finalidad, contenido y uso del tratamiento.
- Diseñar e implementar las medidas técnicas y organizativas en materia de protección de datos tendentes de eliminar o reducir los riesgos de uso o acceso indebido a los mismos, así como a reducir las consecuencias negativas que puedan producirse como consecuencia de un uso o acceso indebido a los mismos.
- Realizar el control del tratamiento, calidad y seguridad de los datos.
- Controlar la gestión de soportes informáticos que contienen datos de carácter personal.
- Gestionar y dirigir los procedimientos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición de los afectados y resolverlos en el plazo legalmente previsto.
- Proceder al bloqueo de los datos en los casos en que, siendo procedente su cancelación, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado.
- Elaborar el Registro de Actividades de Tratamiento.
- Encargarse de que exista una relación actualizada de usuarios con acceso autorizado a los sistemas de información.
- Establecer los procedimientos de identificación y autenticación para dicho acceso.
- Establecer los mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
- Establecer los procedimientos de realización de copias de respaldo y recuperación de datos.
- Encargarse de forma directa o por delegación del cumplimiento efectivo de la normativa sobre Protección de Datos en la organización, garantizando la difusión y conocimiento de este Documento entre todo el personal.
- Implantar las medidas de seguridad establecidas en este documento.
- Mantener este Documento actualizado en todo momento, debiendo revisarse siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo y adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos.
- Garantizar los bienes jurídicos y recursos protegidos.
- Notificar a la autoridad de protección de datos competente, y en su caso, también al interesado, de las violaciones de seguridad de los datos que se hayan producido, cuando sea obligatorio de acuerdo con lo previsto por el artículo 33 del Reglamento Europeo de Protección de Datos.

6.2.5. Obligaciones

6.2.5.1. Legitimación para el tratamiento de los datos

Cumplir todos los requisitos legales y reglamentarios para **obtener el consentimiento del afectado** para que los datos puedan ser ingresados, tratados, guardados, transmitidos, manipulados, cedidos y/o cancelados por el responsable de las actividades de tratamiento o aquel a quien se haya destinado para cada forma de tratamiento.

Velar para que la recogida de datos de carácter personal se realice cumpliendo con todos los requisitos legales, especialmente el derecho de información y la obtención del consentimiento inequívoco del afectado.

6.2.5.2. Control de las entradas

Consiste en mantener el sistema de archivo de las fichas o formularios con los datos personales del afectado y su consentimiento, bajo control exclusivo del Responsable de las Actividades de Tratamiento.

Sólo se incluirán en el tratamiento los datos obtenidos mediante las fichas o formularios que estén amparados por la firma del interesado. En la documentación de la aplicación de gestión de protección de datos de la organización vienen diversos modelos que deberán adaptarse previamente.

6.2.5.3. El mantenimiento actualizado de los datos

Los datos de carácter personal deben de estar siempre actualizados, deben ser exactos y responder con veracidad a la situación actual del afectado. Si los datos registrados son o devienen inexactos en todo o en parte, o incompletos han de ser cancelados o sustituidos de oficio por los correspondientes rectificados o completados. Tampoco han de mantenerse datos que hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados.

6.2.5.4. Encargados de tratamiento externos

En el caso de que existan encargados de tratamiento externos, se deberá formalizar la relación con éstos de acuerdo con lo establecido en el artículo 28 del Reglamento Europeo de Protección de Datos y en la Ley Orgánica de Protección de Datos. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito.

6.2.5.5. Entorno de Sistema Operativo y de Comunicaciones

Designar al administrador que se responsabilizará del sistema operativo y de comunicaciones que deberá estar relacionado en el Anexo Relación de personal autorizado.

En el caso más simple, como es que los datos están ubicados en un ordenador personal y accedidos mediante una aplicación local monopuesto, el administrador del sistema operativo podrá ser el mismo usuario que accede usualmente a dichos datos.

6.2.5.6. Sistema Informático o aplicaciones de acceso

Se encargará de que los sistemas informáticos de acceso a los datos personales tengan su acceso restringido mediante un código de usuario y una contraseña.

Asimismo cuidará que todos los usuarios autorizados para acceder a los datos, relacionados en el Anexo Relación de personal autorizado, tengan un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

6.2.5.7. Salvaguarda y protección de las contraseñas personales

El responsable de las actividades de tratamiento deberá mantener actualizada la relación de usuarios con acceso autorizado al sistema de información y establecer los procedimientos de identificación y autenticación para este acceso.

El responsable de las actividades de tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Sólo las personas relacionadas en el Anexo Relación de personal autorizado podrán tener acceso a los datos.

6.2.5.8. Gestión de incidencias

Habilitará un Libro de Incidencias a disposición de todos los usuarios y administradores con el fin de que se registren en él cualquier incidencia que pueda suponer un peligro para la seguridad de los datos.

Analizará las incidencias registradas, tomando las medidas oportunas en cada caso.

En caso de incidencia que pueda suponer una violación de seguridad de los datos, el responsable deberá comunicarlo a la autoridad de control a la mayor brevedad, y como máximo en el plazo de 72 horas desde que tuvo conocimiento de la misma, salvo que considere que es improbable que dicha violación de seguridad constituya un riesgo para los derechos y libertades de las personas físicas.

También se deberá notificar esta incidencia al interesado cuando sea probable que la violación de seguridad de los datos entrañe ese alto riesgo para los derechos y libertades de las personas físicas.

El responsable viene obligado a documentar cualquier violación de seguridad de los datos personales en el registro de incidencias, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

6.2.5.9. Gestión de soportes

La salida de soportes informáticos que contengan datos personales fuera de los locales del Responsable deberá ser comunicada al Responsable de las Actividades de Tratamiento.

6.2.5.10. Procedimientos de respaldo y recuperación

El responsable de las actividades de tratamiento se encargará de verificar la definición y correcta aplicación de las copias de respaldo y recuperación de los datos.

6.3. Funciones y obligaciones que afectan a todo el personal

6.3.1. Con carácter general

Tratar los datos de carácter personal de conformidad con lo que se establece en la legislación vigente y en este Registro de Actividades de Tratamiento, accediendo a estos únicamente cuando sea necesario para el desarrollo de sus funciones.

Mantener el secreto profesional respecto de los datos de carácter personal que conozcan y custodiarlos. Esta obligación perdurará después de finalizar las relaciones con el responsable de las actividades de tratamiento.

Conocer la normativa interna en materia de seguridad, y especialmente la referente a protección de datos de carácter personal.

Cumplir lo dispuesto en la normativa interna vigente en cada momento.

Conocer las consecuencias que se pudieran derivar y las responsabilidades en que pudiera incurrir en caso de incumplimiento, que podrían derivar en sanciones.

Comunicar al responsable de las actividades de tratamiento, en el mismo día, cualquier solicitud de ejercicio por parte de los afectados de los derechos de acceso, rectificación, supresión, limitación de tratamiento, portabilidad y oposición, así como cualquier incidencia que conozca sobre la confidencialidad e integridad de los datos.

6.3.2. Puestos de trabajo

El usuario autorizado será el responsable de su puesto de trabajo, garantizando que la información que disponga o muestre su equipo no podrá ser accesible o visible por personas no autorizadas.

Procurará que la disposición de pantallas e impresoras u otros dispositivos de su puesto de trabajo se ubiquen de forma que garanticen la confidencialidad y no sea accesible o visible su contenido por personas no autorizadas.

Al abandonar su puesto de trabajo, aún temporalmente, deberá dejarlo en un estado que impida el acceso o la visualización de los datos protegidos, mediante un protector de pantalla o la salida del sistema y apagado del equipo. La reanudación del trabajo implicará la desactivación de la pantalla protectora o el encendido del equipo con la introducción del nombre de usuario y contraseña correspondiente en cada caso.

No deberá dejar en la impresora documentos impresos en la bandeja de salida que contengan datos protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, el responsable de cada puesto de trabajo deberá retirar los documentos conforme vayan siendo impresos.

La configuración de los puestos de trabajo desde los que se tiene acceso a los datos sólo podrá ser cambiada con la autorización del Responsable de las Actividades de Tratamiento.

6.3.3. Salvaguarda y protección de las contraseñas personales

Todo usuario es responsable de mantener la confidencialidad de su contraseña. Si la contraseña es conocida por otra persona, el usuario deberá registrarlo como incidencia y notificarlo al Responsable de las Actividades de Tratamiento, para proceder a su cambio.

6.3.4. Gestión de incidencias

El usuario que tenga conocimiento de una incidencia deberá de ponerlo en conocimiento del Responsable de las Actividades de Tratamiento y registrarla siguiendo el procedimiento establecido para el registro de incidencias.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad de los Datos por parte de ese usuario.

Todos los miembros de la organización deben conocer la obligación del responsable de notificar las violaciones de seguridad de los datos a la autoridad de control, por lo que han de ser conocedores de su obligación de comunicar a la mayor brevedad al responsable de cualquier incidencia sobre los datos que llegue a su conocimiento y que pueda poner en peligro los derechos y libertades de los ciudadanos en este ámbito.

6.3.5. Gestión de soportes

Los soportes informáticos que contengan datos personales han de estar claramente identificados con una etiqueta externa que indique la actividad de tratamiento, tipo de datos y fecha de creación.

Los soportes que sean reutilizables, y que hayan contenido copias de datos personales, deberán ser borrados físicamente antes de su reutilización, de forma que los datos que contenían no sean recuperables.

Los soportes que contengan datos personales deberán ser almacenados en lugares a los que no tengan acceso personas que no figuren relacionadas en el Anexo Relación de personal autorizado.

La salida de equipos o soportes fuera de las instalaciones requiere la autorización del Responsable de las Actividades de Tratamiento.

Seguir los procedimientos establecidos de gestión y distribución de soportes y observar las autorizaciones precisas en cada caso.

6.3.6. Correo electrónico

No utilizar el correo electrónico u otros medios de comunicación interna o con el exterior para transmitir mensajes que contengan o lleven adjuntos datos de carácter personal que por sus características, volumen o destinatarios puedan poner en peligro la confidencialidad o la integridad de los datos.

Atenerse a los procedimientos establecidos y observar las autorizaciones precisas.

6.3.7. Transferencias de datos

No realizar transferencias con datos de carácter personal entre sistemas o descargas en equipos salvo en aquellos casos expresamente autorizados, y protegiendo después los contenidos para evitar la difusión o copias no autorizadas.

6.3.8. Tratamiento fuera de los locales del responsable

Proteger la confidencialidad e integridad de los datos personales de la entidad que excepcionalmente tuvieran que almacenarse o usarse fuera del lugar de trabajo: en casa del cliente, en el propio domicilio o en otras instalaciones alternativas tanto en sistemas fijos como en portátiles.

Siempre que sea posible, se encriptarán los datos personales o se protegerán mediante contraseña segura.

6.4. Funciones y obligaciones del administrador del sistema y personal informático.

Siempre será posible conocer el personal que intervino con posterioridad a la intervención, dejando constancia de ello, identificando al personal técnico, anotándolo en el Registro de Incidencias.

6.4.1. Funciones

Administradores: Tienen acceso con el máximo privilegio al software del sistema y a las herramientas necesarias para ello, así como al fichero. Resuelven las incidencias que surjan y gestionan los permisos y accesos.

Personal Informático: Resolver las incidencias que surjan en las redes y comunicaciones corporativas y efectuar el mantenimiento de máquinas y

programas.

Usuario: Las labores propias del cargo de Usuario.

6.4.2. Obligaciones

6.4.2.1. Entorno de sistema operativo y de Comunicaciones

Cuidar de que ningún usuario no autorizado en el Anexo Relación de personal autorizado disponga de herramienta o programa que le permita el acceso a los datos.

Guardar en lugar protegido las copias respaldo y recuperación, evitando el acceso a las mismas de persona no autorizada.

Asegurarse de que personal no autorizado pueda tener acceso a los datos protegidos.

Impedir el acceso remoto de personas no autorizadas al equipo donde estén ubicados los datos, especialmente si se encuentra integrado en una red de comunicaciones.

6.4.2.2. Sistema Informático o aplicaciones de acceso a los datos

Si la aplicación informática que permite el acceso a los datos no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de código de usuario y contraseña.

6.4.2.3. Salvaguarda y protección de las contraseñas personales

Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad que se determina en el punto *Identificación y autenticación del personal autorizado* del Apartado Medidas, normas, procedimientos, reglas y estándares de seguridad. Este mecanismo de asignación y distribución de las contraseñas deberá garantizar la confidencialidad de las mismas, y será responsabilidad del administrador del sistema.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del administrador del sistema.

6.4.2.4. Procedimientos de respaldo y recuperación

Obtener periódicamente una copia de seguridad del fichero, que garantice su reconstrucción en el estado en que se encontraba al tiempo de producirse la pérdida o destrucción.

Realizar la copia de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

Comprobar y actualizar el procedimiento, informático o manual, que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos al estado en que se encontraban en el momento del fallo.