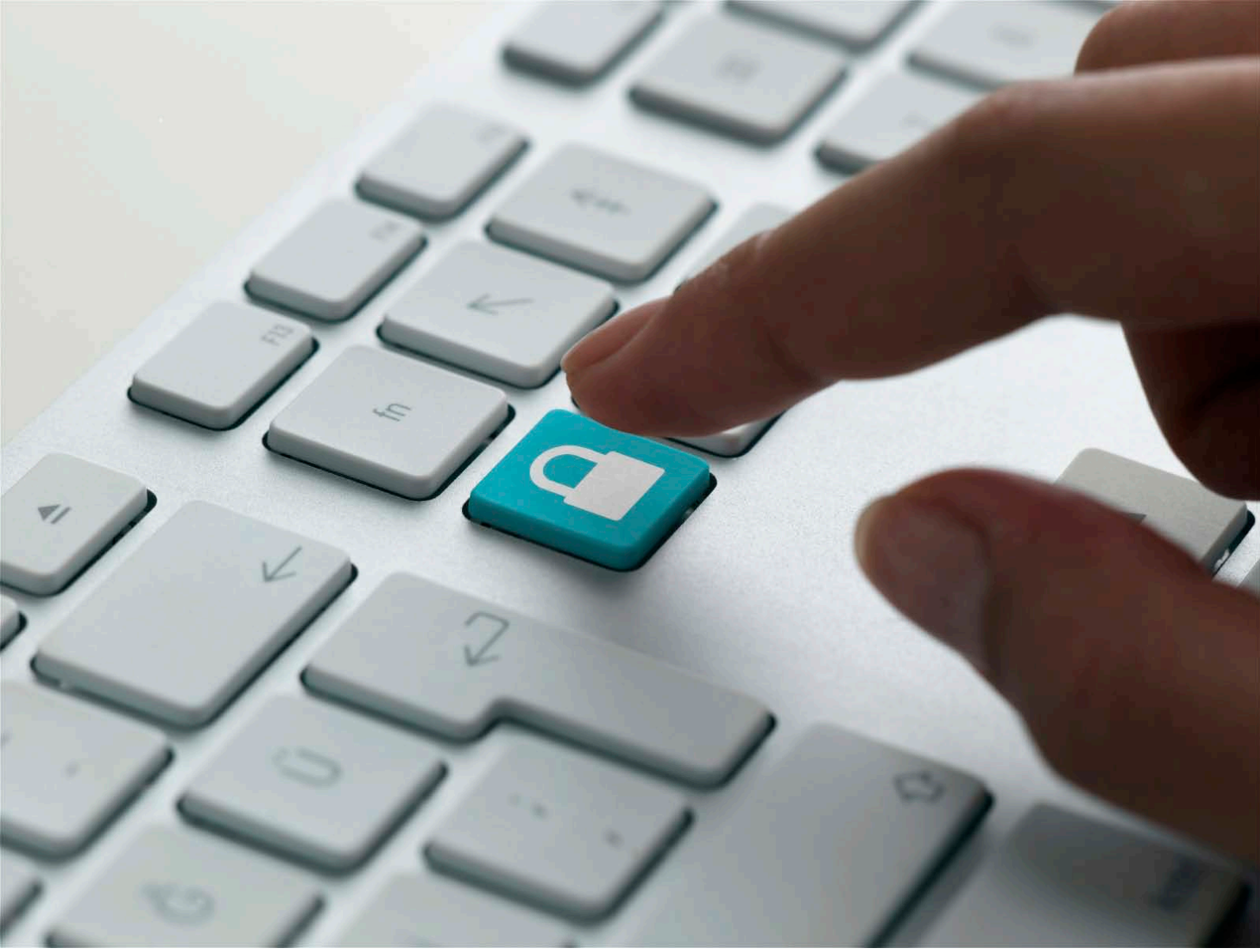

Protección de datos en la Fundación Progreso y Salud

CÓDIGO DE BUENAS PRÁCTICAS PARA LA PROTECCIÓN DE DATOS PERSONALES

Versión 1.0

JUNTA DE ANDALUCIA

Fundación Progreso y Salud
CONSEJERÍA DE IGUALDAD, SALUD Y POLÍTICAS SOCIALES

1. INTRODUCCIÓN

La Fundación Pública Andaluza Progreso y Salud está comprometida con la seguridad en la custodia y tratamiento de la información. Por ello, todas las personas que trabajan o colaboran en la organización, o prestan servicios en alguna de las dependencias de la Fundación Progreso y Salud adquieren el compromiso de cumplir la normativa vigente.

Las medidas y recomendaciones que aparecen a continuación deben ser aplicadas al tratamiento de la información en general y, con especial atención, a lo datos de carácter personal en cumplimiento de la Ley Orgánica 15/1999 de Protección de Datos (LOPD) y su Reglamento (Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD).

Es importante aclarar que las **muestras biológicas se consideran**[1] **también datos de carácter personal en caso de estar codificadas o reversiblemente disociadas**.

A continuación, se adjunta una serie de recomendaciones en materia de protección de datos cuyo cumplimiento considera importante la Fundación. Ante cualquier duda respecto al uso o transferencia de información, puede contactarnos en: lopd.fps@juntadeandalucia.es.

Muchas gracias por su colaboración.

2. BUENAS PRÁCTICAS GENERALES

Todo el personal que acceda a información de la organización está obligado a conocer y observar las medidas, normas, protocolos, reglas y estándares que afecten a las funciones que desarrolla. Cada persona se responsabiliza del puesto de trabajo que tiene asignado y debe cumplir con los procedimientos internos de la entidad con respecto a la protección de datos personales.

- Deberán **guardar el debido secreto y confidencialidad** sobre la información que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aún después de finalizar las relaciones contractuales con la organización.

- Evitar revelar información corporativa, salvo en aquellos casos en que el desempeño de las funciones organizativas así lo requieran. **No sacar información ni datos personales** de la organización salvo en los casos que lo requieran las funciones asignadas y, en su caso, previa autorización.

- Cuando se abandona el puesto de trabajo, bien temporalmente o bien al finalizar el turno, se debe dejar en un estado que **impida la visualización de los datos protegidos: bloqueando el equipo** con contraseña o desconectándose de las aplicaciones y la red, y **apagando el monitor**.

[1] Ley 14/2007, de 3 de julio, de Investigación Biomédica

- **Inmediatamente reenviar** a la dirección de correo lopd.fps@juntadeandalucia.es cualquier **solicitud de ejercicio de derecho de acceso, rectificación, cancelación u oposición** de los datos por parte de su titular. Existen unos plazos legales ajustados para responder a dichas solicitudes.

- Con respecto a los **ordenadores portátiles y resto de dispositivos de almacenamiento móviles (teléfonos móviles, memorias USB, etc.)**, se debe cumplir:
  - Mantenerlos siempre controlados, (no dejar en lugares públicos, taxis, etc.) para evitar su sustracción.
  - Reducir y/o eliminar la información que no vaya a ser utilizada.

- En caso de **pérdida o robo de un dispositivo** de almacenamiento móvil (portátil, teléfono, memoria USB, etc.) se **notificará inmediatamente como incidencia de seguridad**.

- Se debe proporcionar la ayuda que se requiera en lo que se refiere a **mantener la calidad de los datos**, lo cual implica controlar:
  - Que la **información** contenida en los ficheros únicamente sea **tratada en relación con las finalidades** para las que se haya obtenido.
  - Que los datos sean **exactos**, estén **actualizados** y sean **cancelados cuando éstos hayan dejado de ser necesarios.**

3. BUENAS PRÁCTICAS CON INFORMACIÓN EN SOPORTE AUTOMATIZADO

Considerar la información como un activo fundamental de la organización cumpliendo las siguientes medidas:

- En caso de detectar **cualquier indicio de problema de seguridad,** inmediatamente debe **poner el mismo en conocimiento del responsable de sistemas de información** de su centro de trabajo o por correo electrónico a lopd.fps@juntadeandalucia.es. Entre otras, son incidencias frecuentes las pérdidas de contraseñas o la recuperación de datos por borrado accidental.

- No realizar acciones que puedan poner en peligro la seguridad de la información (introducción de software ilegal, envío de información a través de correo electrónico sin las suficientes medidas de seguridad, etc.). Se debe respetar la configuración de aplicaciones corporativas (ofimática, antivirus, etc.) de los puestos de trabajo y sólo podrá ser cambiada bajo la autorización del responsable de seguridad o de los administradores informáticos autorizados.

- Se debe **cumplir la política de contraseñas establecida**, especialmente la **periodicidad de cambio (al menos una vez al año)**, y utilizar contraseñas de al menos ocho caracteres que combinen números, letras (mayúsculas y minúsculas) y caracteres especiales.

- Es muy importante que los profesionales **no almacenen ni traten datos de carácter personal en el disco duro** del equipo debido al alto riesgo de pérdida de datos y de accesos no autorizados. Dichas acciones deberán realizarse en los entornos provistos al efecto (carpetas de los servidores, aplicaciones, etc.) protegidos mediante identificadores de usuario con los permisos correspondientes.

- No se permite el acceso a los sistemas de información con un identificador de usuario que no sea el propio, así como comunicarlo o cederlo con su contraseña a cualquier otra persona. Las **contraseñas no deberán anotarse o guardarse en lugares visibles** o fácilmente accesibles.

- **Cada usuario se responsabiliza de la confidencialidad de sus contraseñas** y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarlo como incidencia de seguridad al personal de sistemas de información de la FPS según el procedimiento establecido y proceder a su cambio inmediato.

- Se recomienda reducir al máximo el almacenamiento de información confidencial y eliminarla cuando haya dejado de ser necesaria. En caso de crear **archivos para uso temporal debe asegurarse su eliminación cuando estos hayan dejado de utilizarse**.

- Respecto al **correo electrónico e Internet,** se debe prestar atención al envío de datos de carácter personal por medio del correo electrónico, tanto en el cuerpo del mensaje como en anexos y, si se realiza, tratar esos mensajes y anexos como temporales y borrarlos en cuanto dejen de ser necesarios. **El correo electrónico no es un gestor documental**, los ficheros enviados o recibidos deben estar almacenados en los sistemas y carpetas correspondientes protegidos por las credenciales de usuario correspondientes.

  Además, se deben evitar realizar las siguientes acciones si el usuario tiene asignada una dirección personal de la Fundación:

  

  - Que un empleado haga uso de una cuenta de correo ajena o permitir a un tercero el uso de la suya propia.
  - El envío de mensajes difamatorios, calumniadores, amenazantes o abusivos transmitiendo cualquier mensaje que puede interpretarse como tal.
  - Transmitir material de la organización a menos que esté adecuadamente protegido y autorizado.
  - Transmitir identificadores, contraseñas, configuraciones de las redes locales o direcciones a través de Internet.
  - No abrir correos procedentes de direcciones desconocidas o que no estén relacionados con motivos de trabajo y ofrezcan las suficientes garantías, para evitar la entrada de virus, troyanos o código malicioso.
  - No abrir adjuntos a correos o pulsar en enlaces a menos que sea conocido y de confianza el origen del correo y del enlace.

- Evitar en los puestos de trabajo la descarga de ficheros e instalaciones de ejecutables procedentes de Internet que no ofrezcan las suficientes garantías sobre su origen e integridad y que no hayan sido debidamente autorizadas.
- No se pondrán utilizar cuentas de correo personales para el envío de información profesional del organismo excepto en situaciones inevitables como por ejemplo cuando exista una urgencia y el sistema esté caído.
- No se podrá utilizar el correo corporativo para finalidades distintas a las corporativas.
- No realizar reenvío masivo de correos y siempre que se haga, utilizar CCO (enviar con copia oculta), cuando se envía a diferentes destinatarios con el fin de ocultar la visualización de las diferentes direcciones de correo.
- El uso de Internet no deberá interferir en sus obligaciones o degradar el servicio a otros trabajadores.
- Los trabajadores no podrán realizar vistas a sitios web con páginas que promuevan actividades ilegales.

- **Ficheros temporales**: los ficheros temporales creados extrayendo datos de las aplicaciones corporativas para la ejecución de una determinada tarea o proceso (ejemplo: listados en Word o Excel) no deben mantenerse indefinidamente ni en el ordenador ni en un directorio de red y una vez finalizada dicha tarea o proceso **hay que eliminarlos**.

4. BUENAS PRÁCTICAS PARA TRATAR INFORMACIÓN EN SOPORTE NO AUTOMATIZADO (PAPEL Y MUESTRAS BIOLÓGICAS)

La confidencialidad de la información se consigue también a través del cuidado del entorno de trabajo, evitando que la misma pueda ser de fácil acceso por cualquiera. Para ello se establecen varias actuaciones de obligado cumplimiento:

- **Mesas limpias**: cada usuario, cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella información que contenga información que pudiera ser de carácter confidencial.

- **Utilización de fotocopiadoras, escáneres e impresoras**: Al utilizar impresoras o fotocopiadoras, debe asegurarse de recoger los originales al finalizar y de que no quedan documentos con datos sensibles en la bandeja de salida. Si las impresoras son compartidas con otros usuarios sin acceso a los datos que están siendo impresos, se deberán retirar los documentos conforme vayan siendo impresos.

  De forma análoga, al utilizar los escáneres debe asegurarse de recoger los documentos originales y, si la carpeta de destino se comparte con usuarios sin acceso a esos datos personales, eliminar el archivo cuanto antes de esa carpeta y trasladarlo a otra carpeta con un nivel de seguridad acorde a los datos que contienen.

- **Utilización de fax**: cuando se vaya a enviar un fax siempre se debe avisar al destinatario para que esté pendiente de la recogida de la información. Cuando se espera recibir información con datos personales por este medio es importante solicitar a la persona que lo envía que nos avise para estar atentos a la llegada de la documentación.

- **Eliminación de documentos**: utilizar los dispositivos destinados al efecto para desechar el material correspondiente, es decir, depositarla en los contenedores destinados al efecto o en las destructoras de papel. Si se elimina documentación en las papeleras, ésta deberá romperse previamente de forma que la información en ella contenida quede ininteligible.

- **Distribución de la documentación**: adoptar medidas cautelares que eviten accesos no autorizados. Se pueden producir diferentes situaciones en el movimiento de los ficheros en papel:

  - Envíos fuera de la sede de trabajo: siempre debe salir en sobre cerrado o dispositivo de seguridad similar que evite accesos de terceros, de manera que no se pueda realizar consulta, copia o reproducción de la misma. También puede utilizarse un servicio de valija interna pues cuenta con el correspondiente acuerdo de confidencialidad.

  - Envíos dentro de la sede de trabajo: para envíos dentro del mismo edificio donde se encuentra nuestro puesto de trabajo, se deben utilizar los medios implantados en la organización de manera que se eviten accesos no deseados.

    - Verificar que las personas a las que se entrega la documentación original o una copia de la misma la han recibido.

    - No retirar de las dependencias soportes o ficheros no automatizados sin la debida autorización.

5. CONSECUENCIAS DEL INCUMPLIMIENTO

El personal que intervenga en cualquier fase del tratamiento de la información y que incumpla lo descrito en el presente documento, o en su caso en los documentos, normas o procedimientos relacionados con la seguridad y con la protección de datos de carácter personal, deberá saber que podrá ser sometido al régimen sancionador/disciplinario existente en la organización, así como a Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal respecto a la comisión de delitos informáticos. Todo ello sin perjuicio de las posibles consecuencias civiles y penales a las que hubiera lugar en su caso.