Tratamiento de datos personales en el Laboratorio de Anatomía Patológica.

Dr. José Santos Salas Valién.
Servicio de Anatomía Patológica Hospital de León. León jsalas@hleo.sacyl.es

Introducción:
Todos somos conscientes de la privacidad con la que deben tratarse los datos personales y sobretodo los relativos a la historia clínica, siendo revelados únicamente, con nuestro consentimiento, a personas o entidades determinadas.
Con la tecnología actual existe una gran facilidad en copiar y distribuir bases de datos, que usamos en nuestro ámbito social o profesional y que contienen datos personales que al final pueden ser usados por terceros sin nuestro consentimiento.
Con objeto de proporcionar una protección y regulación de estos datos se crea en 1993 la Agencia Española de Protección de Datos (AEPD) a raíz de promulgarse la ley orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE 262 del 31 octubre 1992).
La AEPD se encarga de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
Esta Agencia, con el fin de ayudar a aplicar la legislación, publica en abril del 2005 un modelo genérico de documento de seguridad que contiene 7 apartados y 7 anexos.
En este documento de seguridad, donde se recogen las principales características y actuaciones con respecto a la seguridad de nuestros archivos, se definen los distintos ficheros y su nivel de seguridad

Modelo documento de seguridad: El modelo de documento de seguridad propuesto por la AEPD desarrolla los siguientes capítulos y anexos:
Capitulo I: Ámbito de aplicación del documento.
Capitulo II: Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento:

- -Identificación y autentificación de usuarios.
- -Control de acceso.
- -Gestión de soportes.
- -Acceso a datos a través de redes de comunicación.
- -Régimen de trabajo fuera de los locales de la ubicación del fichero.
- -Ficheros temporales.
- -Copias de seguridad.

Capitulo III: Procedimiento general de información al personal.
Capitulo IV: Funciones y obligaciones del personal.
Capitulo V: Procedimiento de notificación, gestión y respuesta ante las incidencias.
Capitulo VI: Procedimientos de revisión.
Capitulo VII: Consecuencias del incumplimiento del documento de seguridad.

Anexo I: Aspectos relativos al fichero.
Anexo II: Nombramientos.
Anexo III: Autorizaciones salida o recuperación de datos.
Anexo IV: Inventario de soportes.
Anexo V: Registro de incidencias.
Anexo VI: Encargados de tratamiento.
Anexo VII: Registro de entrada y salida de soportes.

Con este documento se pretende especificar el nivel de seguridad que aplicamos a nuestro archivo, así como su contenido, los procesos que le afectan y un registro de todas las incidencias.
Estos ficheros de datos deben estar registrados en la AEPD, pudiéndose consultar este registro de forma libre a través de su página Web. Figurará la identificación y finalidad de fichero, su responsable, dónde ejercitar los derechos de oposición, acceso, rectificación y cancelación, la disposición general de creación, modificación o supresión, los tipos de datos, estructura y organización del fichero, el origen y procedencia de los datos y una parte muy importante que es a quién está previsto ceder o comunicar los datos.

Errores frecuentes en sistemas de protección de datos de carácter personal y de seguridad de la información:
Antes de adecuar nuestros archivos a la normativa con el documento de seguridad, es interesante repasar los errores más frecuentes que se cometen en este proceso:

-Desconocimiento de los textos reguladores de obligado cumplimiento. Suele suceder por encargar a un miembro del propio servicio, que a tiempo parcial se responsabiliza de la protección de datos, sin tener la formación ni el tiempo suficiente.

-Abandono progresivo del compromiso de la dirección. La dirección puede iniciar con ganas este proceso y perder rápidamente el interés, abandonando su supervisión.

-Medidas de seguridad no aplicadas. Se elaboran los documentos iniciales pero se dejan de emitir los informes periódicos.

-Ausencia de mantenimiento. Se contrata la implantación a través de una consultoría externa y luego se abandona el mantenimiento.

-Aislamiento del sistema. Cuando no lo integramos con el resto de los sistemas, porque estos no cumplan los criterios de protección o porque tengamos miedo a desproteger nuestro archivo.

Podemos decir que es fundamental, en este proceso, la implicación de la dirección a la vez que debe existir una correcta delegación en el resto de estamentos.
Estos sistemas serán útiles si todo el proceso se realiza correctamente, si tenemos dudas de nuestra capacidad, en tiempo o conocimientos, para llevarlo a cabo es preferible externalizar el proceso.
Debemos tener en cuenta, a la hora de implantar un sistema de estas características, que debemos ser graduales, necesitándose un tiempo y una planificación escalonada.
No debemos pretender únicamente cumplir con la obligatoriedad del documento de seguridad o con conseguir la certificación como finalidad, debemos estar convencidos de su utilidad y así aprovecharnos de ella.

Bibliografía:
1.- Agencia Española de Protección de Datos (AEPD):
https://www.agpd.es/index.php
2.- Modelo documento de seguridad:
https://www.agpd.es/upload/Informa%20AEPD/modelo_doc_seguridad_v1.pdf
3.- Hernando Westerheide S. Los diez errores más frecuentes en Sistemas de Protección de Datos y de Seguridad de la Información:
http://www.hispasec.com/corporate/papers/diez_errores_sistemas_gestion.pdf