Con el objetivo de garantizar la confidencialidad y seguridad de los datos personales de la Entidad, y dar cumplimiento a la normativa vigente en materia de protección de datos personales y garantía de derechos digitales, la Entidad establece las medidas preventivas siguientes, que ha de cumplir todo el personal contratado o colaborador.

MEDIDAS INFORMÁTICAS

1. Los datos personales a que tiene acceso el personal y colaboradores sólo serán utilizados para las actividades de investigación y docencia inherentes a la finalidad de FIDMAG, garantizando el compromiso de confidencialidad y ética profesional.

2. Cada usuario con acceso informático a las actividades de tratamiento, tendrá cuidado de que los datos que se visualicen por pantalla o que se impriman, no puedan ser visualizados por personas no autorizadas a su acceso.

3. Cuando un empleado o colaborador finalice su jornada laboral o deje su lugar de trabajo durante un período de tiempo determinado, cerrará las aplicaciones con las que ha estado trabajando, finalizará su sesión como usuario y apagará el ordenador.

4. Cada usuario que tiene acceso a datos de carácter personal, cuando acceda a estos datos mediante su clave informática de usuario, deberá procurar que esta clave no sea visualizada por nadie que la pueda utilizar sin autorización.

5. Cada usuario es responsable de la confidencialidad de su clave de acceso. En caso de que esta sea conocida por personas no autorizadas, deberá notificarlo como incidencia, y proceder a su cambio.

6. Cada trabajador/colaborador deberá proceder al cambio de su *password* cuando el sistema así lo requiera. Así mismo, se mantendrá el bloqueo de pantalla que se activará automáticamente y como norma general cada 5 minutos sin actividad.

7. Cuando el usuario de un lugar de trabajo lo abandone temporalmente deberá activar manualmente el bloqueo de sesión (Ctrl+Alt+Supr). La vuelta a su lugar de trabajo implicará la activación de sesión con la introducción del correspondiente *password*.

8. Cualquier modificación en los sistemas de información (SI), se deberá comunicar al Delegado de Protección de Datos, dpd@fidmag.org

9. Es responsabilidad de cada usuario eliminar los ficheros temporales una vez dejen de tener utilidad, así como todas las copias documentales que se tengan. FIDMAG dispone de destructoras para eliminar toda documentación en soporte papel o discos compactos, que contengan datos personales y ya no sean de utilidad.

MEDIDAS RESPECTO DEL USO DEL CORREO ELECTRÓNICO

10. El personal al servicio de FIDMAG, debe hacer un buen uso del correo electrónico que le ha sido atribuido para el ejercicio de sus funciones. Cada persona trabajadora que tiene una cuenta de correo asignada se configura como persona usuaria de estos sistemas y es responsable de estos recursos que tiene asignados y de todas las acciones que se lleven a término en su utilización.

11. En supuestos de envío de datos de nivel alto a través de correo electrónico será requerida la previa disociación de datos identificativos del afectado y si no se pudiesen disociar se dispondrá de sistemas de cifrado en la medida en que acontecería una situación excepcional. Dado que el correo electrónico nos permite enviar los datos encriptados, se podrá hacer uso de este medio cuando así se requiera, siempre siguiendo las indicaciones del Responsable de Seguridad Informática y, en la medida de lo posible, se usará una vía alternativa al correo electrónico para facilitar la contraseña de los documentos encriptados.

MEDIDAS RESPECTO DEL ACCESO A INTERNET

12. El acceso a Internet se limitará a los temas directamente relacionados con la actividad que presta la Entidad y con el lugar de trabajo del usuario.

13. El acceso a páginas web y otras fuentes de información como FTP, etc., se limita a aquellos que tengan información relacionada con la actividad de la entidad o con el lugar de trabajo del usuario.

14. Queda prohibido introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados o sin licencia por parte de la entidad, o cualquier tipo de obra o material donde los derechos de la propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de la autorización pertinente.

15. En todo caso, para cualquier actuación respecto de los anteriores supuestos será requisito indispensable la autorización expresa del Responsable de Seguridad Informática.

MEDIDAS RESPECTO A DATOS EN SOPORTE FÍSICO

16. Se deberá garantizar el destino último del papel inservible o duplicado mediante su destrucción a través de la máquina trituradora de papel o un servicio externo especializado. Esta medida es necesaria para garantizar la confidencialidad y para evitar que exista riesgo de acceso por parte de personal no autorizado.

17. Los soportes informáticos que tengan datos personales, (por ejemplo: en discos duros, USB o CD) deberán de estar claramente identificados con una etiqueta externa que informe de los datos contenidos y la fecha en que se guardaron en el soporte informático.

18. Todos los soportes con datos de nivel medio/alto que salgan del centro se deberán anotar en el "Registro de Entradas y Salidas de Soportes".

MEDIDAS RESPECTO DE LOS DATOS CLÍNICOS

19. Los archivos donde estén ubicados los Datos Clínicos han de estar cerrados con llave. Deberá tenerse cuidado de la llave, no hacer copia sin autorización expresa ni dejarla en lugar accesible para personas no autorizadas.

20. Cada empleado/colaborador con acceso a los Datos Clínicos en soporte papel deberá de indicar el registro de entradas y salidas (informático o papel) de los Datos Clínicos del archivo. Durante el período en que los Datos Clínicos se encuentran fuera del archivo, todo el personal ha de velar para evitar cualquier acceso por parte de personas no autorizadas.

21. La devolución de los Datos Clínicos al archivo ha de realizarse inmediatamente después de la circunstancia que motivó su salida.

22. Está absolutamente prohibido extraer Datos Clínicos fuera del centro sin autorización expresa del Responsable de Tratamiento.

23. El acceso a los datos identificativos de los participantes en los proyectos de investigación está restringido al equipo de investigación del proyecto en el que participan.

24. Los datos clínicos recogidos mediante soportes móviles (ordenador portátil o USB) se mantendrán encriptados y con contraseña, y se trasladarán a los servidores de FIDMAG a la mayor brevedad posible, eliminándolos de los soportes móviles.

25. FIDMAG dispone de un registro de accesos y trazabilidad de los mismos. Mensualmente se emite un informe y se revisan los accesos producidos.

26. Si se detectan accesos no autorizados a los Datos Clínicos o un mal uso de los datos a que tienen acceso los trabajadores/colaboradores de FIDMAG, siempre será necesaria la presencia del afectado para justificar o no el que en principio es un acceso no autorizado o incumplimiento del régimen interno de la seguridad de la información. En todo caso, si el acceso acontece como no autorizado o una violación de la normativa de protección de datos de la entidad, FIDMAG, podrá adoptar las medidas disciplinarias convenientes de acuerdo con lo que establezca el convenio laboral de aplicación y en función de las circunstancias concurrentes en cada caso. El Convenio SISCAT prevé diversos "tipos" infractores que permitirían calificar las conductas relacionadas como infracción leve, menos grave, grave y muy grave.

MEDIDAS RESPECTO DEL USO DE USB

Los puertos para los dispositivos USB se encuentran cerrados. Si dadas las funciones del usuario su uso fuese necesario, el usuario está obligado a una solicitud expresa al DPD y a tomar las medidas oportunas: registro de la salida y cifrando los datos de los dispositivos, o disociando los mismos. Se dispone de formulario y registro de solicitud de acceso a escritura a los puertos USB. Ver ***Anexo 8 – Modelo solicitud derecho de uso de USB.*** El usuario deberá tener en cuenta las siguientes cautelas:

27. Estos tipos de dispositivos serán utilizados única y exclusivamente con la finalidad de la prestación de los servicios y tareas del centro, garantizando el compromiso de confidencialidad y ética profesional.

28. Los dispositivos USB que tengan datos personales confidenciales deberán estar claramente identificados, por ejemplo, a través de un código, con el cual se pueda saber cuáles son los datos contenidos en el mismo y la fecha en que fueron guardados. Los criterios de identificación de la información que contienen han de impedir la identificación para el personal no autorizado.

29. En el caso de que resulte necesario emplear este tipo de soportes, el Responsable de Tratamiento ha designado al DPD para que sea el encargado de autorizar la idoneidad de su uso. El encargado de controlar las entradas y salidas de los mismos será el Responsable de Seguridad Informática.

30. Estos movimientos de USB deberán de quedar anotados en el "Registro de Entradas y Salidas de Soportes".

31. Los dispositivos de almacenaje de los soportes que contengan datos de carácter personal deberán de disponer de mecanismos que obstaculicen su apertura. **Sólo se utilizarán USB suministrados por la entidad, y siempre serán encriptados y con contraseña de acceso**.

32. De la misma manera, se deberán cifrar los datos que contengan los dispositivos portátiles, mediante una contraseña, cuando estos se encuentren fuera de las instalaciones que están bajo el control del Responsable de Tratamiento.

33. Cuando se dejen de utilizar estos soportes o se borre la información que contienen, se deberán adoptar medidas que eviten el acceso a la información contenida o su recuperación posterior.

MEDIDAS RESPECTO DEL USO DE TABLETS Y TELÉFONOS MÓVILES

34. Únicamente el personal autorizado podrá tener estos dispositivos. La Entidad dispone de registro.

35. Estos tipos de dispositivos serán utilizados única y exclusivamente con la finalidad de la prestación de los servicios y tareas del centro, garantizando el compromiso de confidencialidad y ética profesional.

36. En el caso de que resulte necesario emplear estos tipos de soportes, el Responsable de Tratamiento ha dado instrucciones al DPD para que sea el encargado de autorizar la idoneidad de su uso.

37. Estos soportes deberán de disponer de contraseña o código de acceso.

38. Se debe evitar la descarga de documentos que contengan datos de carácter personal en estos soportes. Para el caso de que resultase necesario hacer la descarga, un vez realizada y finalizada la necesidad que la motivó se deberá proceder a eliminar los datos de carácter personal del dispositivo.

39. Cuando se dejen de utilizar estos soportes o se borre la información que contengan, se deberán adoptar medidas que eviten el acceso a la información contenida o su recuperación posterior.

MEDIDAS RESPECTO DEL USO DEL MATERIAL

40. Todo trabajador, ya sea personal interno contratado, así como personal colaborador externo como estudiantes en prácticas, especialistas en formación en el período de rotación, becarios, adscritos a otras Instituciones, personal de otros centros de Hermanas Hospitalarias, o de otros, que en cumplimiento de las funciones que tienen atribuidas tenga que realizar una salida de documentos, ya sea en soporte manual o automatizado, deberá de ser registrada en el "Registro de Entrada y Salida de Soportes", y ser autorizada de forma expresa por el DPD de acuerdo con el cumplimiento de las medidas de seguridad, entre ellas el cifrado del soporte portátil si hablamos de memorias USB o dispositivos portátiles, tomando las medidas de seguridad que eviten la sustracción, pérdida o acceso indebido.

41. El responsable de la salida queda igualmente comprometido al retorno obligado de la documentación, una vez finalizado el motivo que la motivó.

PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENCIAS Y VIOLACIONES DE SEGURIDAD

42. Se considerarán como "Incidencias de Seguridad", entre otras, cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de FIDMAG. Podemos definir como

incidencia cualquier suceso que pueda dar lugar a las siguientes situaciones: pérdida de privacidad de la información, acceso y/o uso no autorizado de servicios y sistemas, bloqueo/desbloqueo de identificadores de usuario, modificaciones no autorizadas de información, denegación de servicio, incidencias en la gestión de red (caídas de red, servidores, comunicaciones...), errores del sistema, transacciones, bases de datos, o usuarios, mal funcionamiento durante la realización de copias de seguridad, recuperación de datos a partir de copias de seguridad.

43. Una violación de seguridad es una brecha de datos personales que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

44. FIDMAG dispone de un registro de las incidencias que afectan a la seguridad de los datos, así como un procedimiento para la notificación y tramitación de incidencias y/o violaciones de seguridad.

45. Todo trabajador o colaborador tiene la obligación de comunicar cualquier incidencia y/o violación de seguridad de forma inmediata al Delegado de Protección de Datos (dpd@fidmag.org), cumplimentando el ***Anexo 10 - Procedimiento de gestión de incidencias*.**

46. El procedimiento a seguir para la notificación de incidencias, incluirá los siguientes requisitos: usuario que comunica la incidencia, momento en que se produjo la incidencia, tipo de incidencia, equipamiento informático afectado y descripción del suceso.

47. Una vez cumplimentado el formulario con todos aquellos detalles de la incidencia que se conozcan, se ha de entregar a la máxima celeridad posible al DPD. La incidencia se tramitará en formato electrónico, se firmará también en formato electrónico y se entregará al **Delegado de Protección de Datos** por correo electrónico en la dirección dpd@fidmag.org

Ante el incumplimiento de las funciones y obligaciones que corresponden a los usuarios, en materia de protección de datos de carácter personal y garantía de derechos digitales, resultaran de aplicación las consecuencias previstas en el Convenio Laboral aplicable por el incumplimiento de las obligaciones laborales.