

| | |
|--------------------------------|--|
| EMPRESA | Centro Geriátrico Borja-FONTILLES CIF: G46335097 |
| DOMICILIO | Ctra. Orba - La Vall de Laguar, km 4 |
| AUDITOR/ES | ESTHER SALCEDO HIDALGO |
| ALCANCE DE LA AUDITORIA | GRADO DE CUMPLIMIENTO DE LA LEY 15/1999 Y DEC. 1720/2007 |

El presente informe se ha realizado para dar cumplimiento al Art. 96 del real Decreto 1720/2007, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal. Este informe no es necesario ser remitido a la A.E.P.D, pero si, puesto a su disposición si así ésta lo requiriera.

Las deficiencias detectadas deberán ser subsanadas por el responsable del fichero en el corto plazo y queda bajo su responsabilidad poner en marcha dichas acciones susceptibles de sanción.

PLAN DE TRABAJO

- a. Revisión del documento de seguridad**
- b. CHECKLIST:**
 - Análisis de los sistemas de información de la empresa.
 - Identificación, autenticación y controles de acceso
 - Funciones del responsable de seguridad
 - Soportes de datos
 - Pruebas con datos reales
 - Copias de seguridad
 - Registro de incidencias
 - Control de acceso físico a la sala
 - Registro de accesos
 - Transmisiones
- c. Entrevista usuarios y responsables con acceso a datos**
- d. Recorrida a instalaciones**

CHECKLIST PARA VALORAR EL GRADO DE CUMPLIMIENTO LOPD

| IDENTIFICACIÓN Y NOTIFICACIÓN DE FICHEROS | |
|--|--|
| Clasificación del nivel de seguridad es adecuada respecto a la naturaleza de la información contenida en cada uno de los ficheros y su finalidad | <p>SATISFACTORIO</p> <p>FICHERO 1: DONANTES ENVIO DE INFORMACION SOBRE LAS ACTIVIDADES DE LA ASOCIACION Y PUBLICIDAD PARA LA CAPTACION DE FONDOS Y DONACIONES. N.S.: BÁSICO CÓD.: 2011230052 Nº REG. SALIDA: 472942/2010</p> <p>FICHERO 2: SANATORIO GERIATRICO FINALIDAD SANITARIA GERONTOLOGICA USOS PREVISTOS: ATENCION AL USUARIO USO INTERNO N.S.: ALTO CÓD.: 2052100017 Nº REG. SALIDA: 471438/2010</p> <p>OBSERVACIÓN: Se deberían dar de alta el fichero de PROVEEDORES y EMPLEADOS.</p> |
| La creación, modificación o supresión de ficheros con datos de carácter personal desde la última auditoría se ha comunicado a la AGPD | <p>SATISFACTORIO</p> <p>No se han creado, modificado o suprimido ficheros desde la última auditoría comprobándose que no ha habido cambios sustanciales de la información comunicada.</p> |

| CONTENIDO Y ALCANCE DEL DOCUMENTO DE SEGURIDAD | |
|---|--|
| Existe un Documento de Seguridad (DS) y se dispone del prescrito legalmente | <p>SATISFACTORIO</p> <p>Documento de Seguridad con fecha de noviembre 2012.</p> <p>RECOMENDACIÓN:</p> <p>Se aconseja disponer de un único Documento de Seguridad (ya que ambas sedes tienen el mismo CIF) donde se haga referencia a todos los ficheros (tanto de Valencia como de Fontilles) y que se disponga de una copia del mismo en las dos ubicaciones.</p> |
| Se mantiene actualizado y revisado | <p>SATISFACTORIO</p> <p>Última revisión de noviembre de 2012.</p> |

| CONTENIDO Y ALCANCE DEL DOCUMENTO DE SEGURIDAD | |
|--|--|
| El documento está formado por los apartados mínimos requeridos por la norma | <p>NO SATISFACTORIO</p> <p>No incluye ejercicio de derechos ARCO ni Tratamiento por cuenta de terceros.</p> |
| Están definidos los controles periódicos en el Documento de Seguridad para verificar el cumplimiento del mismo | <p>NO SATISFACTORIO</p> <p>En el Documento de Seguridad no están definidos los controles periódicos para verificar el cumplimiento del mismo.</p> |
| Están definidos en el Documento de Seguridad el tratamiento de datos por cuenta de terceros | <p>NO SATISFACTORIO</p> <p>El Documento de Seguridad no incluye el tratamiento de datos por cuenta de terceros.</p> |

| AUDITORIAS | |
|--|--|
| En el caso en que sea necesario, ¿se han sometido los sistemas de información a la preceptiva auditoría bienal en materia de protección de datos? | <p>NO SATISFACTORIO</p> <p>Última auditoría realizada en 2009 por personal externo de la organización.</p> <p>OBSERVACION:</p> <p>Se deben realizar auditorías cada dos años.</p> |
| Si han realizado modificaciones sustanciales del sistema de información ¿se ha realizado la Auditoría extraordinaria para verificar la adaptación, adecuación y eficacia de las nuevas medidas de seguridad implantadas? | <p>SATISFACTORIO</p> <p>No se han realizado cambios sustanciales en el sistema de información que requieran de auditoría extraordinaria.</p> |
| El informe de auditoría contempla los aspectos requeridos por la normativa | <p>SATISFACTORIO</p> |
| En el caso de que se haya realizado anteriormente alguna auditoría: ¿Ha analizado el informe de auditoría con el fin de adoptar las medidas correctoras adecuadas? | <p>NO SATISFACTORIO</p> <p>No se han tomado todas las acciones correctivas necesarias para corregir las desviaciones detectadas en la última auditoría. Algunas desviaciones se mantienen hasta la fecha de realización de la presente auditoría.</p> |

| FUNCIONES Y OBLIGACIONES DEL PERSONAL | |
|--|---|
| Se han documentado y definido las funciones y obligaciones del personal | SATISFACTORIO Apartado d) del Documento de Seguridad y Anexo I. |
| ¿En éstas se hace referencia tanto a ficheros automatizados como no automatizados? | SATISFACTORIO |
| ¿Conoce el personal de una manera comprensible las normas de seguridad que les afectan para sus funciones y han suscrito el alta con sus funciones y obligaciones? | NO SATISFACTORIO Se dispone de Compromiso de confidencialidad escrito firmado por todo el personal de la Residencia. No se dispone para el personal del Hospital. No hay evidencia de que se haya notificado al personal sus funciones en materia de protección de datos. No obstante el personal realizó un curso de formación en materia de protección de datos en mayo-junio 2013. |
| Han suscrito el alta de Responsable de Seguridad el/los Responsable/s de Seguridad? | SATISFACTORIO En el Documento de Seguridad se nombra como Responsable de Seguridad a Raquel Miró y Marisol Sendra. (apartado a). OBSERVACIÓN: No hay un nombramiento para el Hospital, únicamente para el Centro Geriátrico. |

| IDENTIFICACIÓN Y AUTENTICACIÓN | |
|--|---|
| ¿El sistema de información (Sistema operativo y aplicaciones) está configurado de manera que se pueda identificar a todo aquel usuario de forma inequívoca y personalizada que intente acceder y la verificación de que está autorizado? | SATISFACTORIO Acceso a equipos informáticos con usuario y contraseña. |
| La organización ha establecido un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantice su confidencialidad y autenticidad? Únicamente aplicable cuando el mecanismo de autenticación se base en la existencia de contraseñas. | SATISFACTORIO Informático organización |

| IDENTIFICACIÓN Y AUTENTICACIÓN | |
|--|--|
| Las contraseñas se cambian con la periodicidad establecida en el DS | NO SATISFACTORIO Se cambian contraseñas cada 6 meses en el programa informático. De los equipos informáticos no se cambian nunca las contraseñas. Hay equipos compartidos que no almacenan datos de carácter personal. |
| Ha establecido algún mecanismo que limite la posibilidad de intentos reiterados de acceso no autorizado al Sistema de Información? | SATISFACTORIO Establecido máximo 3 intentos. |

| CONTROL DE ACCESOS | |
|--|--|
| ¿Los accesos de los usuarios están configurados de tal manera que sólo (únicamente) tengan acceso autorizado a aquellos datos y recursos necesarios para el desarrollo de sus funciones, tanto para ficheros automatizados como no automatizados? | SATISFACTORIO |
| ¿Está actualizada la relación de usuarios con acceso autorizado al sistema de información? | NO SATISFACTORIO El listado de personal autorizado no está actualizado. |
| ¿Los mecanismos de accesos están configurados para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados? | SATISFACTORIO |
| ¿Se han establecido las medidas técnicas para que únicamente los responsables del sistema informático (responsables, administradores) puedan conceder, alterar o anular el acceso autorizado, según los criterios establecidos por el responsable del fichero? | SATISFACTORIO El Responsable de Seguridad controla el módulo de seguridad del programa informático. El Responsable de Seguridad junto con el informático gestiona el acceso a la información de los equipos informáticos. |

| CONTROL DE ACCESOS | |
|---|----------------------|
| ¿Se han establecido las medidas oportunas para que únicamente el personal autorizado en el Documento de Seguridad acceda a los locales donde están ubicados los equipos que dan soporte al sistema de información? | SATISFACTORIO |
| REGISTROS DE ACCESOS | |
| ¿Los ficheros descritos en el DS como de nivel alto tienen activado un registro de accesos de manera que se guarde, como mínimo: identificación del usuario, fecha y hora en que se realizó, fichero accedido, tipo de acceso y si ha sido autorizado o denegado? | SATISFACTORIO |
| ¿El registro de accesos graba la información que permita identificar el registro accedido? | SATISFACTORIO |
| ¿Los mecanismos que permiten el registro de los datos detallados anteriormente están bajo el control directo del responsable de seguridad, sin que se permita en ningún caso la desactivación de los mismos? | SATISFACTORIO |
| ¿Se conservan los datos registrados en el registro de accesos durante dos años? | SATISFACTORIO |
| ¿Ha revisado mensualmente el registro de accesos y ha elaborado el informe de revisiones realizadas y los problemas detectados? | SATISFACTORIO |

| COPIAS DE SEGURIDAD | |
|---|--|
| ¿Se están realizando las copias con la periodicidad establecida en el Documento de seguridad y existe un procedimiento de actuación para la realización de dichas copias de respaldo? | SATISFACTORIO Copias de seguridad diarias por diferencial. Copias semanales totales. Procedimiento descrito en apartado g) del Documento de Seguridad. |
| ¿Está establecido un procedimiento para la recuperación de los datos? | SATISFACTORIO Procedimiento descrito en apartado g) del Documento de Seguridad. |
| ¿Ha verificado semestralmente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos? | SATISFACTORIO |
| En caso de realizar pruebas con datos reales, ¿Ha realizado una copia de seguridad con carácter previo? | SATISFACTORIO No se realizan pruebas con datos reales. |
| ¿Conserva una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar distinto a aquél donde están los equipos informáticos que los tratan? | SATISFACTORIO |

| GESTION DE SOPORTES Y DOCUMENTOS | |
|--|--|
| ¿Los soportes informáticos y documentos se hallan inventariados en el documento de seguridad, permiten ser identificados y solo es accesible al personal autorizado? | SATISFACTORIO Se dispone de inventario de hardware. OBSERVACIONES: Adjuntar dicho inventario como un anexo al Documento de Seguridad. |

| GESTION DE SOPORTES Y DOCUMENTOS | |
|--|--|
| En el caso de que se hayan producido salidas de soportes, incluidos los comprendidos o anejos a un correo electrónico, fuera de los locales del Responsable del Fichero: ¿se han autorizado por el Responsable del Fichero o se ha dejado constancia de ello en el Documento de Seguridad? | NO SATISFACTORIO No se han realizado las autorizaciones correspondientes para las salidas de soportes. |
| En el traslado de la documentación, ¿se adoptan las medidas adecuadas para evitar la sustracción, pérdida o acceso indebido? | SATISFACTORIO |
| ¿Se han adoptado las medidas para impedir cualquier recuperación posterior de la información que contenían los soportes desechados o reutilizados? | SATISFACTORIO |
| ¿Están etiquetados los soportes de forma que solo el personal autorizado sepa el contenido de dicho soporte cuando los datos son sensibles para la organización? | SATISFACTORIO No se disponen de soportes como USB's, discos duros, etc. |
| ¿Se han etiquetado de forma comprensible para que los usuarios con acceso autorizado identifiquen el contenido y dificulten la identificación para el resto de usuarios? | SATISFACTORIO |
| ¿Se mantiene actualizado el Registro de entrada y salida de soportes y documentos? | NO SATISFACTORIO No se lleva a cabo el registro de entrada y salida de soportes. |
| ¿Se han adoptado las medidas técnicas y organizativas para que la distribución de soportes se haya hecho cifrando los datos o usando otro mecanismo que garantice que la información no sea inteligible ni manipulada durante su transporte? | SATISFACTORIO |

| GESTION DE INCIDENCIAS | |
|---|--|
| <p>¿Existe un procedimiento de notificación y gestión de incidencias que indique el tipo, fecha-hora, persona que notifica, a quién se comunica y efectos que produzca, tanto para ficheros automatizados como no automatizados?</p> <p>En el caso de que se hayan producido pérdidas de datos de <u>nivel medio</u> y haya sido necesaria su recuperación: ¿Ha consignado en el registro de incidencias, además de los datos requeridos, los procedimientos realizados de recuperación de datos, indicando 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?</p> | <p>SATISFACTORIO</p> <p>Apartado f) del Documento de Seguridad.</p> <p>NO SATISFACTORIO</p> <p>No se ha registrado la incidencia referente a pérdida de datos.</p> |
| <p>En caso de que se hayan producido pérdidas de datos: ¿Se ha autorizado debidamente la recuperación de datos por el responsable del fichero?</p> | <p>NO SATISFACTORIO</p> <p>Ante una pérdida de datos no se ha autorizado debidamente la recuperación de datos por parte del responsable del fichero (no hay evidencia escrita).</p> |

| ACCESO Y TRANSMISIÓN A TRAVÉS DE REDES DE COMUNICACIONES | |
|---|-----------------------------|
| <p>¿Los accesos a los datos realizados a través de redes de comunicaciones garantizan un nivel de seguridad equivalente al correspondiente a los accesos en modo local?</p> <p>¿Se han adoptado las medidas técnicas y organizativas para que la transmisión de datos a través de redes de telecomunicaciones se haya hecho cifrando los datos o usando otro mecanismo que garantice que la información no sea inteligible ni manipulada?</p> | <p>SATISFACTORIO</p> |

| FICHEROS TEMPORALES | |
|--|--|
| ¿Los ficheros temporales creados por la organización cumplen con el nivel de seguridad correspondiente a la naturaleza de los datos que contienen? | SATISFACTORIO |
| ¿Los ficheros temporales han sido destruidos una vez que han dejado de ser necesarios para los fines que motivaron su creación? | SATISFACTORIO Se dispone de 1 destructora de papel en la residencia. RECOMENDACIÓN Se debería de disponer de destructora de papel también en el Hospital. |

| EJECUCIÓN DE TRABAJOS FUERA DE LOS LOCALES DEL RESPONSABLE DEL FICHERO | |
|--|--|
| ¿El Responsable del Fichero o tratamiento ha autorizado previamente la realización de trabajos fuera de los locales? | NO APLICA Durante la auditoría el interlocutor declara que no se realizan trabajos fuera del centro. |
| ¿Se ha dejado constancia en el Documento de Seguridad de la autorización para la realización de trabajos fuera de los locales, determinando un periodo de validez para las mismas? | NO APLICA Durante la auditoría el interlocutor declara que no se realizan trabajos fuera del centro. |

| ENCARGADOS DE TRATAMIENTO | |
|--|--|
| ¿Se consignan en el Documento de Seguridad los supuestos de encargados de tratamiento a quienes se presta o quienes prestan servicios? | NO SATISFACTORIO En el Documento de Seguridad no se hace referencia a los encargados de tratamiento. |
| ¿Se contienen respecto de cada uno de ellos la siguiente información: la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o | SATISFACTORIO |

| ENCARGADOS DE TRATAMIENTO | |
|--|--|
| documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo? | |

| PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES | |
|--|---|
| ¿Se han adoptado las medidas necesarias para limitar al personal sin acceso a datos pueda tratar con ellos? | SATISFACTORIO |
| Si es personal ajeno, ¿existe el contrato de prestación de servicios sin acceso a datos donde se prohíbe acceder a datos personales? | SATISFACTORIO Informático, personal de limpieza interno. OBSERVACIÓN: Tener en cuenta posibles prestadores de servicio sin acceso a datos como por ejemplo: empresas de mantenimiento. |

| DELEGACIÓN DE AUTORIZACIONES | |
|--|-------------------------|
| ¿Consta en el documento de seguridad las personas autorizadas para otorgar autorizaciones? | NO SATISFACTORIO |

| OBLIGACIONES RELATIVAS A FICHERO NO AUTOMATIZADOS | |
|---|--|
| CRITERIOS DE ARCHIVO | |
| ¿Mantiene los soportes y documentos archivados de forma que se garantice la correcta conservación, localización y consulta, posibilitando el ejercicio de los derechos de acceso, rectificación, cancelación y oposición? | SATISFACTORIO Despachos y armarios bajo llave. |

| DISPOSITIVOS DE ALMACENAMIENTO | |
|--|----------------------|
| ¿Ha adoptado las medidas que obstruyan la apertura de los dispositivos de almacenamiento de documentos que contengan datos de carácter personal? | SATISFACTORIO |
| ALMACENAMIENTO DE LA INFORMACIÓN | |
| El acceso a las áreas donde se encuentran los armarios y archivadores que contienen información con datos personales de nivel alto ¿está protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente y permanecen cerradas cuando no sea preciso el acceso a los documentos que contienen? | SATISFACTORIO |
| CUSTODIA DE LOS SOPORTES | |
| Mientras la documentación no se encuentre archivada, ¿está custodiada y se impide el acceso por personal no autorizado? | SATISFACTORIO |
| COPIA Y REPRODUCCIÓN DE DOCUMENTOS | |
| ¿Está controlando que únicamente las personas autorizadas en el documento de seguridad realicen copias de los documentos que contengan datos personales de nivel alto? | SATISFACTORIO |
| ¿Ha procedido a la destrucción de las copias desecharadas de forma que se evite el acceso a la información contenida? | SATISFACTORIO |

| ACCESO A LA DOCUMENTACIÓN | |
|---|----------------------|
| ¿Ha comprobado que el acceso a la documentación que contiene datos de nivel alto solo se produce por personal autorizado? | SATISFACTORIO |
| ¿Existen mecanismos que permitan identificar los accesos realizados en caso de documentos que puedan ser utilizados por múltiples usuarios? | SATISFACTORIO |
| ¿Queda registrado el acceso de personas no incluidas en el personal autorizado? | SATISFACTORIO |

| TRASLADO DE LA DOCUMENTACIÓN | |
|--|----------------------|
| ¿Ha implantado un procedimiento para impedir el acceso a los datos contenidos en los ficheros cuando se lleve a cabo un traslado físico de la documentación? | SATISFACTORIO |

| OTROS ASPECTOS | |
|--|---|
| La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato. ¿Ha procedido a recoger la firma de todos los contratos requeridos por la norma? | NO SATISFACTORIO No se disponen de algunos contratos con prestadores de servicios (Mutua, Farmacia...). |
| Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: ¿Se han establecido las cláusulas pertinentes? | SATISFACTORIO |

| OTROS ASPECTOS | | | |
|---|---|--|--|
| ¿Existe un procedimiento documentado para garantizar a los interesados que lo soliciten poder ejercer alguno de los derechos de Acceso, Rectificación, Cancelación y Oposición? | NO SATISFACTORIO No se dispone del procedimiento de ejercicio de derechos ARCO. | | |

| COMPROBACIONES A REALIZAR EN LA VISITA A INSTALACIONES | | | |
|---|--|--|---|
| Existencia y funcionamiento de un Sistema de Alimentación Ininterrumpida (SAI) | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| RECOMENDACIÓN: Sería recomendable disponer de SAI en todas las instalaciones. | | | |
| Servidor con perfiles de usuarios definidos y no generales (nombres de usuarios y contraseña – único) | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Antivirus en los dos equipos informáticos con base de datos actualizada | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Fireware (cortafuegos) activo | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Protector de pantalla en puestos informáticos protegido por contraseña. | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Descarga de software. Desde cualquier ordenador con acceso a internet se puede descargar software de manera libre. | <input type="checkbox"/> SÍ | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Red Local para uso de periféricos con retención de impresión de documentos | <input type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input checked="" type="checkbox"/> N/A |
| Existen programas con riesgo potencial (Kaza, Ares, Emule). En caso afirmativo, ¿está especificada correctamente la carpeta donde se descargan? | <input type="checkbox"/> SÍ | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Acceso al servidor bajo llave | <input type="checkbox"/> SÍ | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Videocámaras (cartel y nota informativa) | <input type="checkbox"/> SÍ | <input checked="" type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Destructoras de papel | <input checked="" type="checkbox"/> SÍ | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |

| COMPROBACIONES A REALIZAR EN LA VISITA A INSTALACIONES | | | |
|--|--|-----------------------------|---|
| <u>Medidas de seguridad en instalaciones</u> | | | |
| Puertas con apertura sin llave – barra de emergencia – únicamente desde dentro de las instalaciones. | <input type="checkbox"/> Sí | <input type="checkbox"/> NO | <input checked="" type="checkbox"/> N/A |
| Rejas en ventanas de zonas restringidas | <input checked="" type="checkbox"/> Sí | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |
| Detectores de humo, Extintores, BIEs. | <input checked="" type="checkbox"/> Sí | <input type="checkbox"/> NO | <input type="checkbox"/> N/A |

**RESULTADO DE LA AUDITORIA LOPD
CONFORME A LOS REQUISITOS DE LA LEY 15/99 Y DEC. 1720/2007**

TOTAL DE DESVIACIONES: 12

Nota: se entiende por desviación a un incumplimiento del reglamento LOPD o del documento de seguridad de la empresa, susceptibles de sanción. Debería subsanarse en el menor plazo posible.

TOTAL DE OBSERVACIONES/ RECOMENDACIONES: 7

Nota: se entiende por observaciones/recomendaciones como oportunidades de mejora que se irán incorporando durante un período razonable.

En el cuadro adjunto se indican las desviaciones (DE) y observaciones / recomendaciones (OB) detectadas en la auditoria. Estas anotaciones van seguidas de un número que indica su orden correlativo.

| CÓDIGO | DESCRIPCIÓN |
|--------|--|
| DE01 | <p>En cuanto al contenido y alcance del Documento de Seguridad:</p> <ul style="list-style-type: none">a) En el Documento de Seguridad no están definidos los controles periódicos para verificar el cumplimiento del mismo.b) No incluye procedimiento de ejercicio de derechos ARCO ni el Tratamiento de datos por cuenta de terceros. |
| DE02 | <p>En cuanto a auditorías:</p> <ul style="list-style-type: none">a) La organización no se ha sometido a las correspondientes auditorías bienales. La última auditoría se realizó en 2009 por personal interno.b) No se han tomado todas las acciones correctivas necesarias para corregir las desviaciones detectadas en la última auditoría. Algunas desviaciones se mantienen hasta la fecha de realización de la presente auditoría. |
| DE03 | <p>No se dispone de compromiso de confidencialidad para el personal del Hospital.</p> <p>No hay evidencia de que se haya notificado al personal (Hospital y Residencia) sus funciones y obligaciones en materia de protección de datos.</p> |
| DE04 | Para los equipos informáticos que sí que almacenan datos de carácter personal no se realiza el cambio de las contraseñas. |
| DE05 | El listado de personal autorizado no está actualizado. |

| CÓDIGO | DESCRIPCIÓN |
|--|--|
| DE06 | <p>En cuanto a la gestión de soportes y documentos:</p> <p>a) No se han realizado las autorizaciones correspondientes para las salidas de soportes.</p> <p>b) No existe un registro de entrada y salida de soportes y documentos.</p> |
| DE07 | <p>En cuanto a la gestión de incidencias:</p> <p>a) No se ha registrado la incidencia ocurrida referente a pérdida de datos.</p> <p>b) Ante la pérdida de datos no se ha autorizado debidamente la recuperación de datos por parte del responsable del fichero (no hay evidencia escrita).</p> |
| DE08 | El Responsable del Fichero no ha autorizado previamente la realización de trabajos fuera del centro. |
| DE09 | En el Documento de Seguridad no consta las personas autorizadas para otorgar autorizaciones. |
| DE10 | No se dispone de contratos firmados con todos los prestadores de servicios (Mutua, Farmacia....). |
| DE11 | El acceso al servidor (ubicado en la desde de Valencia) no se encuentra bajo llave. |
| OB01 | Se debería de dar de alta el fichero de PROVEEDORES y EMPLEADOS. |
| OB02 | Se debería de nombrar a un Responsable de Seguridad para el Hospital, ya que únicamente existe esta figura para el Centro Geriátrico. |
| OB03 | El inventario de hardware se debería adjuntar como un anexo al Documento de Seguridad. |
| RECOMENDACIONES: | |
| <ul style="list-style-type: none"> ▪ Se recomienda realizar actividades formativas periódicas para el reciclado de los conocimientos del personal en materia de protección de datos. ▪ Se debería de disponer de destructora de papel también en el Hospital. ▪ Se aconseja disponer de un único Documento de Seguridad (ya que ambas sedes tienen el mismo CIF) donde se haga referencia a todos los ficheros (tanto de Valencia como de Fontilles) y que se disponga de una copia del mismo en las dos ubicaciones. ▪ Sería recomendable disponer de SAI en todas las instalaciones. | |

COMPROBATO FINAL

- 1.- Gerencia se queda con el original de este informe, entregando copia al auditor, quien se compromete a mantener la confidencialidad del mismo.
- 2.- Las desviaciones han sido aclaradas y entendidas.
- 3.- Todas las desviaciones se refieren a incumplimientos de las exigencias de la LOPD, establecidas en las normativas vigentes.

4.- Observaciones

- a) El/los auditor/es ha/n sido objetivo/s e imparcial/es.
- b) Se ha auditado todo el a través de un muestreo, por lo que pueden existir otras desviaciones no detectadas y por lo tanto no identificadas en este informe.

Firma del auditor



Firma Representante del Resp. de Seguridad

Nombre: Esther Salcedo Hidalgo

Nombre: Miguel Giménez