DOCUMENTACIÓN Y REQUISITOS A SATISFACER POR LOS SUMINISTRADORES DE SOFTWARE QUE GESTIONEN DATOS PERSONALES SOBRE PACIENTES O PERSONAL DEL HOSPITAL PARA ELABORAR EL DOCUMENTO DE SEGURIDAD

1. Introducción

En general las aplicaciones con las que se gestiona la actividad hospitalaria, ya sean aplicaciones que soportan sistemas de información que se alimentan desde teclados de terminales o aplicaciones asociadas a equipos de instrumentación clínica, quirúrgica, o de laboratorio, que se alimentan desde dichos equipos, utilizan los datos de identificación de los pacientes para asociarles la actividad.

La Ley Orgánica de Protección de Datos 15/1999 establece que los datos de salud, son datos personales que requieren nivel de seguridad ALTA y según el Reglamento de Medidas de Seguridad RD 1720/2007 hay que aplicarles una serie de medidas, entre otras, la obligatoriedad de disponer de forma actualizada del Documento de Seguridad.

El Reglamento de Medidas de Seguridad en su artículo 88 apartado 3, establece que tiene que estar formalizada la estructura del "fichero" (ver definiciones en artículo 5) y los sistemas de información que lo tratan. Este requisito se concreta en que tiene que ser conocida y tiene que estar documentada la estructura de almacenamiento de los datos y la estructura de las aplicaciones informáticas que los tratan.

Lo que viene a continuación es la concreción de los requisitos, entre otros, del citado artículo 88, apartado 3 y las implicaciones que tiene en materia de documentación sobre los suministradores de software que gestiona datos personales.

2. Objetivo del documento

La documentación y requisitos que son imprescindibles para formalizar la recepción de las aplicaciones que gestionan datos personales sobre pacientes o personal del hospital, es la necesaria para cubrir lo establecido en el Reglamento de Medidas de Seguridad en su conjunto, publicado como R.D. 1720/2007 de 21 de diciembre, en particular los requisitos que se derivan del Título III sobre derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), del "Artículo 88" y "Disposición adicional única Productos de software", aplicando las definiciones contenidas en el "Artículo 5", con el fin de elaborar el "DOCUMENTO DE SEGURIDAD", condición necesaria para poder efectuar la recepción de cualquier aplicación que gestiona datos personales sobre pacientes o personal del hospital. Dicha documentación se suministrará en un CD-ROM, etiquetado con el texto "Documentación de administración y sistemas para elaboración del DOCUMENTO DE SEGURIDAD del sistema (poner nombre del sistema), aaaa/mm/dd", en fichero o ficheros con formato PDF.

Cualquier discrepancia que pudiera surgir en la interpretación del R.D.1720/2007 se resolverá exclusivamente mediante consulta a la Agencia Española de Protección de Datos.

El CD-ROM Incluirá un fichero de nombre "Inventario_de_ficheros.pdf" que incluya una tabla con dos columnas, la primera contendrá el nombre de cada uno de los ficheros en formato PDF que se suministran en el CD-ROM, la segunda contendrá una descripción explícita del contenido de dichos ficheros.

3. Requisitos de documentación mínima a entregar para formalizar la recepción

En cumplimiento del Reglamento de Medidas de Seguridad, se suministrará como mínimo la documentación altamente detallada que se refiere a continuación:

1. Diccionario de datos.
2. Diccionario de procesos.
3. Diccionario de Interfaces de programación (API) para aplicaciones
4. Modelo analítico de crecimiento de la base de datos
5. Procedimiento para recuperación de contraseñas de administración, caso de pérdida u olvido.
6. Documentación para formalizar la instalación, configuración y operación.
7. Artificios y artefactos para activación del software
8. Garantía y soporte
9. Certificado de los niveles de seguridad que permite alcanzar el software

3.1. Diccionario de datos de las bases de datos y ficheros de las aplicaciones

Para cada una de las aplicaciones servidor o cliente se proporcionará como mínimo:

1. Inventario de tablas que conforman la base de datos completa que utiliza.
2. Para cada tabla, inventario de todos los campos que la conforman.
3. Diagrama entidad-relación.
4. Script en lenguaje SQL con el que generar la BD completa, incluidos usuarios y restricciones. El citado script incluirá líneas de comentarios que faciliten la interpretación de su contenido.
5. Ficheros de configuración y parametrización del sistema objeto de documentación, incluidos sus nombres, ubicación y descripción completa del contenido.
6. Procedimiento para importar/exportar los datos a formato plano posicional o con separadores para datos textuales y a formatos estándar de imagen JPEG o vídeo H.264 para imagen vídeo.
7. En el caso en que los datos no sea posible obtenerlos directamente en modo nativo desde el almacén que los contiene y se requiera de procesos adicionales para el acceso a los mismos, se aportarán los algoritmos de descodificación, incluida su descripción en lenguaje coloquial.

El inventario de tablas se proporcionará formalizado en una tabla de 4 columnas, con los siguientes nombres:

1. Nombre de la tabla.
2. Descripción de su contenido.
3. Reglas de validación para incorporación de nuevas ocurrencias.
4. Reglas de validación para eliminación de ocurrencias existentes.

"***Nombre de la tabla***", se tiene que proporcionar el nombre de todas y cada una de las tablas físicas que conforman cada una de las bases de datos del sistema de información a recepcionar.

"***Descripción de su contenido***" se tiene que proporcionar un texto que describa de forma detallada y sin ambigüedad el propósito y contenido de cada tabla.

"***Reglas de validación para incorporación de nuevas ocurrencias***" se tienen que proporcionar párrafos que describan sin ambigüedad todas las reglas que identifiquen las condiciones (escenarios), bajo las cuales se incorporan nuevas filas (en términos informáticos) u ocurrencias (en términos de información) a la tabla.

"***Reglas de validación para eliminación de ocurrencias existentes***" se tienen que proporcionar párrafos que describan sin ambigüedad reglas que identifiquen filas con contenido inconsistente y por tanto, que tienen que ser eliminadas, incluyendo las eliminaciones en cadena a que este hecho de lugar, tal que se garantice la integridad referencial en todas las bases de datos.

El inventario de campos para cada tabla se proporcionará formalizado en tantas tablas de 4 columnas, como tablas físicas contenga la base de datos, con los siguientes nombres para las mismas:

1. Nombre del campo
2. Descripción de su contenido
3. Reglas de validación sintáctica para representación de su contenido, incluido el tipo de dato
4. Reglas de validación semántica para validación de su contenido, incluido las referencias externas

"***Nombre del campo***", se tiene que proporcionar el nombre que tengan todos y cada uno de los campos que conforman cada tabla de la base de datos.

"***Descripción de su contenido***" se tiene que proporcionar un texto que describa de forma detallada y sin ambigüedad el propósito y contenido del campo.

"***Reglas de validación sintáctica para representación de su contenido, incluido el tipo de dato***" se tienen que proporcionar párrafos que describan sin ambigüedad todas y cada una de las reglas de validación sintáctica (sobre formato, caracteres permitidos para su representación y tipo de dato) que condicionen la representación del valor del campo y que están programadas internamente en las aplicaciones.

"***Reglas de validación semántica para validación de su contenido, incluido las referencias externas***" se tienen que proporcionar párrafos que describan sin ambigüedad todas y cada una de las reglas de validación semántica (contenido) que condicionan la asignación del valor al campo y que están

programadas internamente en las aplicaciones. Si es una referencia externa, indicar la tabla que aloja la variable categórica contra la que se tiene que contrastar dicho valor. Si el valor es numérico, el intervalo en que puede tomar valores (definido por los dos extremos o por la función o algoritmo de como se determinen estos). Si el valor es codificado, el algoritmo de codificación de cada uno de sus campos.

3.2. Diccionario de procesos:

Para cada una de las aplicaciones servidor o cliente se proporcionará como mínimo:

1. Esquema con la arquitectura de la aplicación
2. Inventario de módulos.
3. Estructura de directorios del sistema de ficheros para la aplicación correctamente instalada.
4. Esquema de navegación entre módulos

El inventario de módulos se proporcionará formalizado en una tabla de 4 columnas, con los siguientes nombres:

1. Nombre del módulo (nombre del fichero que lo contiene visto desde el sistema de ficheros)
2. Descripción de la funcionalidad del módulo
3. Módulos a los que llama (tantos nombres en la misma columna como módulos a los que llama)
4. Tabla/s de la BD a las que accede (tantos nombres en la misma columna como tablas)
5. Proceso que realiza sobre las tablas en el acceso (alta, baja, consulta, actualización)

Para el caso de aplicaciones que controlen equipos de instrumentación clínica (procesos en tiempo real), quirúrgica o de laboratorio, el esquema de navegación se facilitará mediante la matriz de conmutación de estados, modelado el sistema mediante máquina de estados finitos, formalizada en una tabla de 4 columnas, de nombres:

1. Estado actual
2. Eventos (tantas filas como eventos puedan ocurrir en dicho estado)
3. Acciones (tantas filas como eventos con las acciones que se desencadenen para tratar cada evento)
4. Nuevo estado que alcanza después de ejecutar las acciones (tantas filas como eventos)

Para el caso de aplicaciones interactivas o de proceso por lotes (o mezcla de ambos) se proporcionará el esquema de navegación de izquierda a derecha al estilo de un explorador.

3.3. Diccionario de Interfaces de programación (API) para aplicaciones

Para cualquier aplicación, ya sea servidor o cliente, se aportará:

1. Inventario de Interfaces de programación para comunicación con otras aplicaciones
2. Descripción de cada interfaz, incluyendo la descripción detallada de los parámetros
3. Inventario de mensajes

El inventario de interfaces se proporcionará formalizado en una tabla de 2 columnas, con los siguientes nombres:

1. Aplicación con la que se comunica
2. Descripción de la funcionalidad del interfaz

La descripción de los parámetros de cada interfaz se proporcionará en una tabla de 3 columnas, con los siguientes nombres:

1. Nombre del parámetro
2. Descripción de la funcionalidad del parámetro
3. Valores que puede tomar el parámetro

El inventario de mensajes se proporcionará en una tabla de 5 columnas, con los siguientes nombres:

1. Identificador del mensaje
2. Propósito del mensaje
3. Aplicación/es destinataria/s del mensaje
4. Descripción del mensaje
5. Formato detallado del mensaje

3.4. Modelo analítico de crecimiento de la base de datos

Se facilitarán las expresiones analíticas o algorítmicas mediante las cuales se pueda predecir la ocupación en bytes de las bases de datos que generen las distintas transacciones o procesos.

3.5. Procedimiento para recuperación de contraseñas de administración de las aplicaciones

Se proporcionará un procedimiento, ya sea para ejecutar directamente sobre la aplicación, ya sea para ejecutar con software adicional, que permita restablecer la contraseña del usuario de administración, para cualquier sistema o subsistema que soporte el sistema de información. En particular permitirá:

1. Recuperación de contraseña de administrador para sistema operativo de servidores
2. Recuperación de contraseña de administrador para sistema operativo de estaciones de trabajo
3. Recuperación de contraseña de administrador para aplicaciones servidor.
4. Recuperación de contraseña de administrador para aplicaciones cliente.

Se suministrarán los nombres de todos los usuarios para propósito de configuración y administración de las aplicaciones y sus contraseñas asociadas. Así mismo se suministrará un procedimiento para restablecer las contraseñas de los usuarios de configuración y administración, caso de pérdida de las mismas, accediendo por los puertos de consola de administración.

3.6. Documentación para formalizar la instalación, configuración y operación

La información requerida en el presente apartado se suministrará en un CD-ROM, etiquetado con el texto "Documentación de instalación y operación del sistema (nombre del sistema), fecha", en fichero o ficheros con formato PDF.

Adicionalmente a la documentación requerida para elaboración del DOCUMENTO DE SEGURIDAD, con las aplicaciones que soporten el sistema de información objeto de recepción y como parte integrante de las mismas, se facilitará un manual, visualizable en pantalla e imprimible, con al menos los siguientes apartados:

- Instalación de todos los componentes hardware y software
- Configuración comentada de todos los componentes hardware y software
- Operación de las aplicaciones
- Esquema de flujos de datos en la operación
- Inventario de eventos que quedan configurados y tratan las aplicaciones
- Esquema de conexión final de todos los componentes que conforman el sistema
- Configuración de cada uno de los componentes adecuadamente comentada

Para cada uno de los ítems anteriores Incluirá un esquema y una foto incrustadas en cada uno de los apartados del documento que ilustren la conexión lógica y física de todos sus componentes

3.7. Artificios y artefactos para activación del software

Con el fin cubrir los requisitos que establece el "Título III. Derechos (ARCO) de acceso, rectificación, cancelación y oposición" del Reglamento de Medidas de Seguridad, cuando para recuperar los datos sobre personas o su actividad (de pacientes o personal del hospital), independientemente de su tipo, sea requiera utilizar la aplicación con la que se han almacenado, no se aceptará como parte de su instalación, la incorporación de artificios o artefactos que impidan moverla de máquina, en caso de avería o disfunción de la misma.

Se entiende por artificio, impedir o restringir el funcionamiento de la aplicación mediante identificador hardware de la máquina sobre la que se ha instalado, tal como Identificador del procesador, dirección MAC, etc.

Se entiende por artefacto, la incorporación de cualquier componente hardware orientado a impedir el funcionamiento de la aplicación si no está instalado, tal como llaves USB, etc. susceptibles de pérdida o sustracción.

3.8. Garantía y soporte
El proveedor del software proporcionará, en concepto de garantía, el soporte necesario, incluidas cuantas modificaciones se requieran para resolver tanto las disfunciones como los problemas de estabilidad de funcionamiento que planteen las aplicaciones. El periodo de garantía en ningún caso será inferior a un año a contar desde la recepción de las aplicaciones.

3.9. Certificado de los niveles de seguridad que permite alcanzar el software
Los sistemas de información sobre los que se requiere esta documentación, contienen datos personales. Consecuencia de ello y en cumplimiento de la "Disposición adicional única. Productos de Software" del citado Reglamento de Medidas de Seguridad, se proporcionará certificado del nivel de seguridad que permite alcanzar, emitido con los requisitos que establece dicha disposición. Alternativamente, en caso de no poder facilitar dicho certificado emitido por Organo competente, se acepta la entrega del código fuente, siempre que esté adecuadamente documentado, lo que requiere informe favorable previo, emitido por quien efectúe la recepción.

4. Condiciones de recepción
Será condición suficiente para rechazar la documentación que se requiere y por tanto la recepción, no facilitar parte de la misma o de forma incompleta, por tanto será condición necesaria para la recepción, la emisión de informe vinculante, en el que conste de forma explícita los componentes de documentación que se han entregado y que los mismos están redactados en los términos exigidos en el presente documento.