

INSTRUCCIONES DE USO DE LA APLICACIÓN LOPDYENS

1. INTRODUCCIÓN

La normativa vigente en materia de Protección de Datos y Seguridad de la Información exige que los responsables de los tratamientos de datos personales que se realicen en la Universidad de Sevilla observen una serie de principios y garantías, y apliquen las medidas de seguridad necesarias a los sistemas de información en los que se tratan los datos. No adecuarse a ella, implicaría un incumplimiento normativo y una posible vulneración de un derecho fundamental, el derecho a la protección de los datos de carácter personal que sean objeto de tratamiento.

A fin de facilitar la anterior tarea, la Universidad de Sevilla pone a disposición de las distintas unidades administrativas la presente aplicación, LOPDyENS. Se trata de una herramienta diseñada para ir incorporando todos los requerimientos legalmente impuestos a través de los distintos campos que se han habilitado, permitiendo comprobar la trazabilidad del cumplimiento normativo.

Los Responsables Delegados (en adelante RD) y los Responsables Tecnológicos (en adelante RT) de los tratamientos o las personas en las que estos deleguen (Gestores) deben incluir entre sus tareas cotidianas las cuestiones relacionadas con la protección de datos tal como exigen tanto la normativa europea como la de ámbito nacional.

El presente documento pretende servir de guía a las personas encargadas de estas tareas para la correcta utilización de la herramienta LOPDyENS.

2. FUNCIONAMIENTO BÁSICO DE LA APLICACIÓN

La plataforma LOPDyENS está basada en una herramienta de Gestión de Proyectos. Por cada tratamiento de datos que se realiza en la US, existirá un proyecto que será asignado al RD, RT y Gestor/es del mismo para que puedan registrar las tareas de cumplimiento. El proyecto constará de una serie de tareas diseñadas para dar respuesta a las exigencias normativas derivadas de la normativa de Protección de Datos.

Cada tarea incluida en la aplicación incorpora una breve explicación y plantillas para facilitar su cumplimentación por parte del usuario.

2.1. ALTA EN LA APLICACIÓN

El acceso a la aplicación se realiza con el Usuario Virtual de la Universidad de Sevilla (en adelante UVUS). Cuando el usuario entra por primera vez sus datos quedan registrados en la herramienta y los administradores procederán a adjudicarle aquel/los proyecto/s que le corresponda/n. El proceso de alta puede tardar uno o dos días desde que se produce el primer acceso.

Una vez asignados el/los proyecto/s al usuario, éste los verá en la pantalla de inicio de la aplicación cuando entre de nuevo una vez culminado el proceso de alta.

2.2. ENTRADA A LA APLICACIÓN

El acceso a la aplicación se hará a través de la dirección URL <https://lopdyens.us.es/> con el UVUS tal y como se indica en la Figura 1.



Figura 1: Formulario de acceso a lopdyens.us.es

Tras acceder a la aplicación, el usuario se encontrará con la siguiente pantalla de inicio que se observa en la Figura 2.



Inicio

La Universidad de Sevilla, como responsable de los Tratamientos de Datos y de los Sistemas de Información Corporativa en los que se tratan, tiene la obligación de cumplir con la normativa aplicable y poder demostrarlo. Para ello delega la responsabilidad de los tratamientos de información en las siguientes figuras:

Responsables Delegados de tratamiento (RD): son los responsables de implantar las medidas para el cumplimiento del Reglamento General de Protección de Datos (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD) en aquellos tratamientos de datos que le son encomendados en el ejercicio de sus funciones.

Responsables Tecnológicos (RT): son los responsables de implantar las medidas de seguridad requeridas por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y su modificación RD 951/2015 de 23 de octubre (ENS) en los Sistemas de Información que le son encomendados en el ejercicio de sus funciones.

Esta plataforma de Gestión de Proyectos es la herramienta corporativa para el cumplimiento de la responsabilidad proactiva de RD y RT. En ella se incluyen todos los tratamientos aprobados siguiendo el procedimiento establecido para ello (consultar Procedimientos y RATUS en la web sic.us.es).

Se pretende que sea una herramienta de uso fácil y útil para los RD y RT y que refleje el desarrollo y gestión del tratamiento de datos personales y las medidas de seguridad que aplican a la infraestructura en la que se tratan.

Cada proyecto asociado a un tratamiento de datos se compone de varias pestañas:

- 1. Vistazo:** se describe la finalidad y legitimación del tratamiento según está publicado en el RATUS. Se indica además el nombre del RD y RT y la/s persona/s encargada/s de la cumplimentación de la aplicación en caso de que no sean el RD y el RT (gestores). Esta pestaña viene ya rellena para cada tratamiento con la información del mismo.
- 2. Peticiones:** En este apartado se incluyen por defecto las peticiones mínimas relativas a la gestión del tratamiento y medidas de seguridad aplicables con una descripción de lo que deben incluir. No todos los tratamientos han de cumplimentar todas las peticiones. De igual modo, los RD y RT podrán crear las peticiones que consideren oportunas para el seguimiento de las tareas de cumplimiento. Por ejemplo, en las peticiones relativas a "Encargados de tratamiento" se deberán adjuntar los acuerdos firmados con los encargados en caso de que existan empresas externas que estén tratando los datos por cuenta de la Universidad de Sevilla y deben estar asociados a los contratos de prestación de servicio.

Figura 2: Página de inicio de la aplicación.

NOTA MUY IMPORTANTE: El usuario debe olvidarse de todas las posibilidades que ofrece la aplicación y centrarse únicamente en la pestaña “Proyectos” (ver Figura 3) que se encuentra arriba en el menú con color azul oscuro y las letras en color blanco.



Figura 3: Opciones de acceso a los proyectos.

Una vez que clique en “Proyectos” aparecerá/n un listado de el/los tratamiento/s que le ha/n sido adjudicado/s como se observa en la Figura 4. Insistimos en que pueden ser uno o varios en función de los tratamientos que se hagan en su unidad.



Figura 4: Vista del listado de proyectos de tratamientos asignados.

2.3. ACCESO AL TRATAMIENTO DE DATOS

A cada tratamiento se accede clicando encima de su nombre. Aparecerá la siguiente pantalla de la Figura 5.

Proyecto Tratamiento de datos US

Información general **Actividad** Tareas

Información general

Descripción: Proyecto plantilla RGPD + ENS
Denominación del Tratamiento: Tratamiento de datos de la US
Sistema de información: Sistema de información
Finalidad: Gestión de tratamiento de datos de la US
Legitimación: Cumplimiento de una obligación legal aplicable al responsable del tratamiento. (Art. 6.1.c)RGPD). Ley Orgánica 6/2001, de 21 de diciembre de Universidades (Modificada por Ley Orgánica 4/2007). Estatutos de la Universidad de Sevilla.
Registro Actividades de Tratamiento: [Tratamiento de datos de la US](#)

Tareas

	abiertas	cerradas	Total
Gestión de incidentes	3	0	3
Gestión del tratamiento	4	0	4
Encargado trat./Servicios Ext.	2	0	2
Formación y concienciación	2	0	2
Transparencia	1	0	1
Consentimiento	1	0	1
Derecho de los interesados	1	0	1
Sistemas de Información	3	0	3
Medidas de seguridad	5	0	5

[Ver todas las tareas](#) | [Resumen](#)

Figura 5: Vista información general de un proyecto.

Cómo se puede observar en la Figura 5, un proyecto tiene asociados un conjunto de **Tareas**. Las tareas están agrupadas por tipo o categorías. En la primera columna se indican los “tipos de tareas” con los que vamos a trabajar y dentro de cada tipo aparecerán el conjunto de tareas asociadas. El usuario se centrará en esta pantalla para realizar su trabajo. En concreto, deberá trabajar sobre las tareas “abiertas” dentro de cada tipo. Las columnas “cerradas” y “Total” son sólo informativas. Cada una de las filas se corresponde con las actuaciones que el usuario debe tener al día para el adecuado cumplimiento de las medidas técnicas y organizativas exigidas por la normativa para su tratamiento de datos personales.

- a) El mecanismo de acceso y cumplimentación por parte del usuario será siempre el mismo sea la tarea que sea: el usuario clicará sobre un tipo de tarea concreta o sobre el número de tareas abiertas que le llevará a la pantalla de la Figura 6.



Figura 6: Listado de tareas del tipo Gestión de incidentes

- b) Una vez dentro clicará sobre la tarea concreta en la que desee trabajar y aparecerá una pantalla similar a la de la Figura 7.

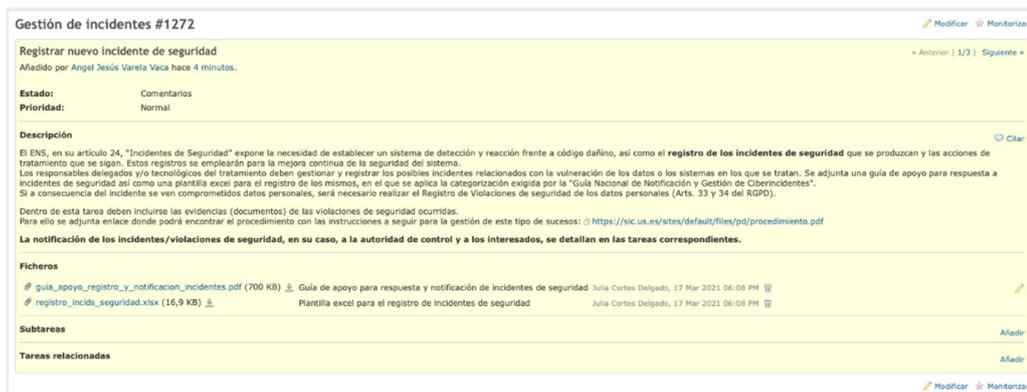


Figura 7: Tarea de Registrar nuevo incidente de seguridad.

- c) Para modificarla tarea se pinchará sobre la imagen de un lápiz situada arriba a la derecha como se observa en la Figura 8.



Figura 8: Opción de modificación de tarea.

- d) A continuación, se abrirá en la misma vista a mitad de pantalla con un formulario a fin de que pueda escribir lo que proceda y/o adjunte la documentación necesaria tal y como se observa en la Figura 9. En la caja de texto "Modificar" se podrá adjuntar el texto que crea conveniente.

Figura 9: Formulario de modificación de la tarea.

Si se desea **subir un documento** a la aplicación, una vez pulsado y se haya accedido a la pantalla de modificar, el usuario tendrá en la parte baja sección llamada “Ficheros”, si pulsa el botón “Seleccionar archivos”, se le abrirá una ventana que le permitirá elegir el documento desde su PC como se observa en la Figura 10.

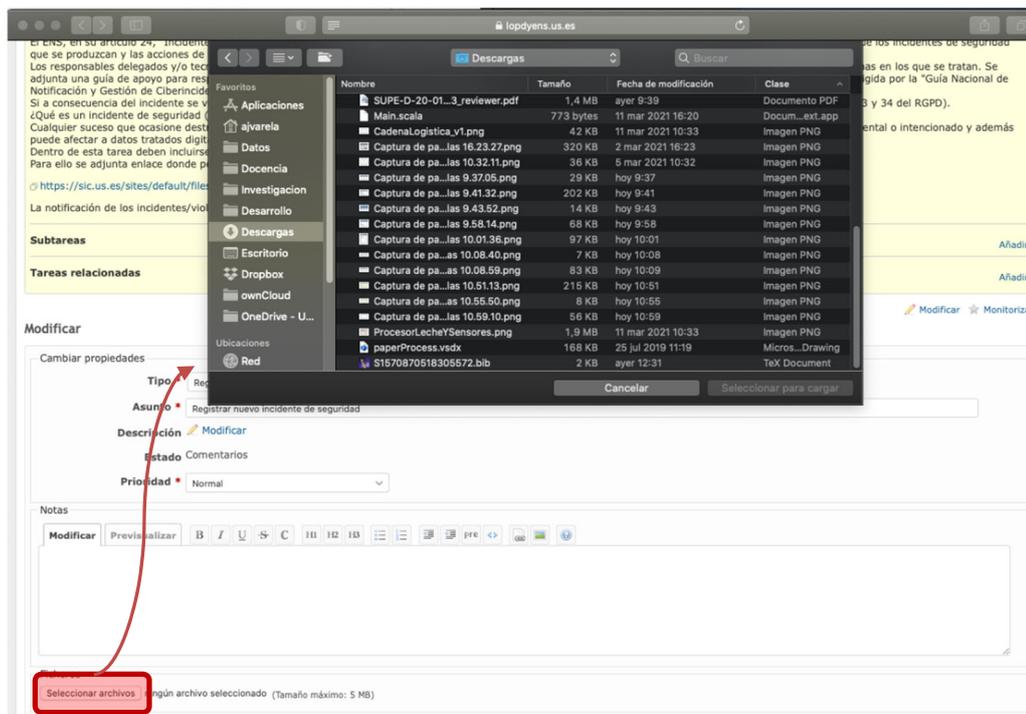


Figura 10: Ventana para seleccionar documento desde el PC.

- e) Una vez incluido el texto y adjuntados los documentos, a continuación, se pulsará el botón aceptar y la modificación quedará registrada en la aplicación.

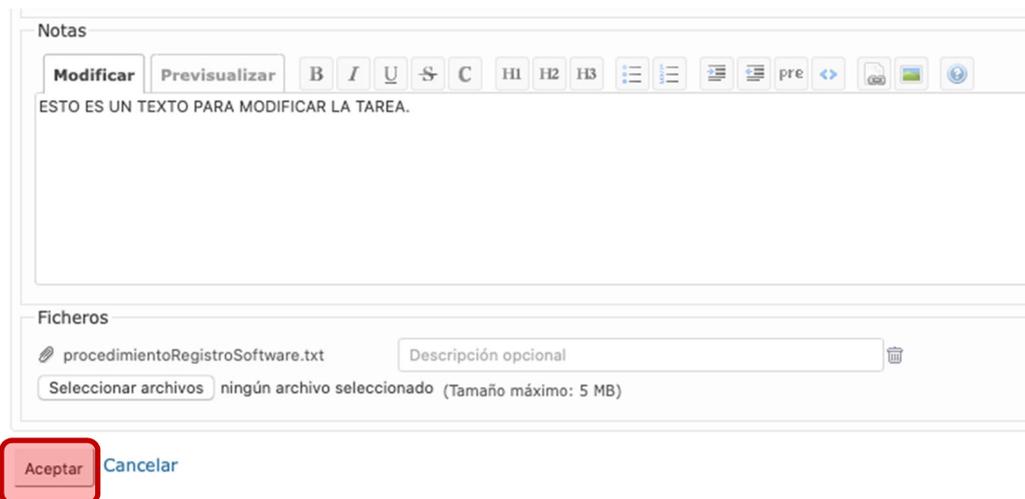


Figura 11: Modificación de texto y documento adjuntado a la tarea.

Tras pulsar “Aceptar” (ver Figura 11) la aplicación de manera automática volverá a una pantalla anterior habiendo dejado constancia de la modificación realizada. De esta forma, en cualquier momento se estará en disposición de saber todas las anotaciones que se han ido realizando por el usuario de la aplicación, ya que en la pestaña “Histórico” quedarán reflejadas todas las modificaciones realizadas sobre cada tarea tal y como se observa en la Figura 12.

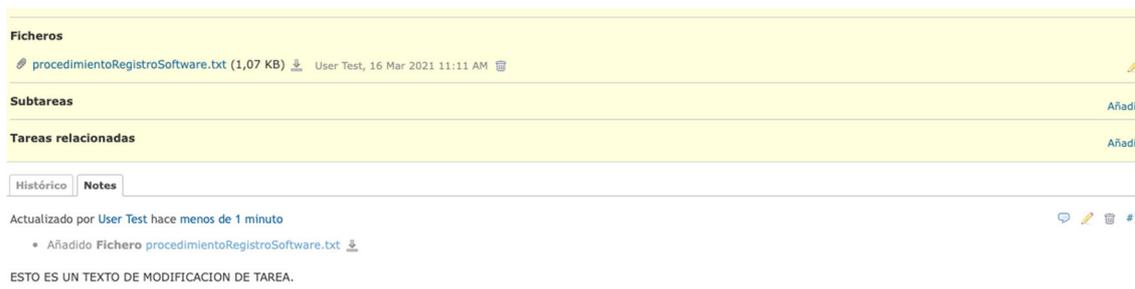


Figura 12: Histórico de modificación actualizado con los cambios realizados.

Todas las tareas deben seguir el mismo ciclo de modificación, en ellas se debe recoger información, documentación o anotaciones que ayuden para la posterior comprobación del cumplimiento de la normativa.

3. DESCRIPCIÓN DE LOS TIPOS DE TAREAS A CUMPLIMENTAR

Las tareas en cada proyecto asociado al tratamiento no se han incluido casualmente si no que responden a exigencias derivadas en la normativa de aplicación en materia de protección de datos personales. Como ya vimos, las tareas están agrupadas por tipo en diferentes categorías, que son los recogidos en la Figura 13.

Tareas			
	abiertas	cerradas	Total
Gestión de incidentes	3	0	3
Gestión del tratamiento	7	0	7
Encargado trat./Servicios Ext.	6	0	6
Formación y concienciación	2	0	2
Transparencia	1	0	1
Consentimiento	1	0	1
Derecho de los interesados	1	0	1
Sistemas de Información	3	0	3
Medidas de seguridad	5	0	5

Figura 13: Listado de tipos de tareas de un proyecto.

Se puede observar que, junto al nombre de cada categoría, aparece un número. Éste se corresponde con el número de actuaciones concretas (tareas) que deben cumplimentarse, en su caso, dentro de cada categoría. Así, por ejemplo, “Gestión de incidentes” contiene 3 tareas a cumplimentar, o “Gestión de tratamiento” contiene 7 tareas a cumplimentar.

A continuación, se detalla cada una de las categorías o tipos de tarea contenidos en un proyecto. La descripción de cada una de las tareas incluidas en las distintas categorías se incluye en cada tarea dentro de la plataforma lopyens.us.es.

3.1. GESTIÓN DE INCIDENTES

Un incidente de seguridad es cualquier suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a los datos personales de un tratamiento de datos. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. La normativa en protección de datos impone al responsable del tratamiento, RD y/o RT la obligación de realizar una serie de actuaciones cuando ocurre un incidente, que se recogen en las tareas que se relacionan a continuación.

#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado
1272	Gestión de incidentes	Comentarios	Normal	Registrar nuevo incidente de seguridad		19 Mar 2021 10:02 AM
1250	Gestión de incidentes	Nueva	Normal	Comunicación de violación de seguridad a los interesados		19 Mar 2021 10:02 AM
1249	Gestión de incidentes	Nueva	Normal	Notificación de violaciones de seguridad a las Autoridades de Control competentes		19 Mar 2021 10:02 AM

Figura 14: Listado de tareas de Registro y Aviso de Incidentes.

Si clicamos en la categoría de “Gestión de Incidentes”, aparecerá la lista de tareas de la Figura 14:

- Registrar nuevo incidente de seguridad.
- Comunicación de violación de seguridad a los interesados.
- Notificación de violaciones de seguridad a las Autoridades de Control competentes.

3.2. GESTIÓN DEL TRATAMIENTO

Si clicamos en esta categoría, aparecerá el listado de tareas asociadas.

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1263	Gestión del tratamiento	En curso	Normal	Identificación y registro del tratamiento concreto de datos personales		19 Mar 2021 10:11 AM	...
<input type="checkbox"/>	1262	Gestión del tratamiento	En curso	Normal	Gestión de la seguridad de datos personales basada en los riesgos		19 Mar 2021 10:11 AM	...
<input type="checkbox"/>	1261	Gestión del tratamiento	En curso	Normal	Políticas internas de la aplicación de las medidas de seguridad		19 Mar 2021 10:11 AM	...
<input type="checkbox"/>	1257	Gestión del tratamiento	En curso	Normal	Aplicación de medidas técnicas y organizativas para la seguridad del tratamiento		19 Mar 2021 10:11 AM	...

Figura 15: Listado de tareas de Gestión de tratamiento

Este apartado se ha concebido para que el usuario de la aplicación introduzca diferentes aspectos del tratamiento que vienen impuestos normativamente. Son los siguientes:

- Identificación y registro del tratamiento concreto de datos personales.
- Gestión de la seguridad de datos personales basada en los riesgos.
- Aplicación de medidas técnicas y organizativas para la seguridad del tratamiento.
- Políticas internas de la aplicación de las medidas de seguridad.

3.3. ENCARGADOS DE TRATAMIENTO

El tratamiento de datos personales responsabilidad de unidad puede realizarse directamente por esta o contratando a un tercero ajeno a la organización que colabore en el desarrollo del tratamiento. Aquí aparece la figura del “encargado de tratamiento” que se define como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (la Universidad de Sevilla).

Estas tareas no deberán ser cumplimentada en el caso de que no exista la figura del encargado en un determinado tratamiento, es decir, si éste se realiza íntegramente por la propia unidad de la Universidad de Sevilla sin ninguna intervención externa.

Si clicamos en la categoría de Encargados de Tratamiento, aparecerá la siguiente lista de tareas de la Figura 16.

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1256	Encargado trat./Servicios Ext.	En curso	Normal	Selección informada de los encargados de tratamiento	Angel Jesús Varela Vaca	19 Mar 2021 10:02 AM	...
<input type="checkbox"/>	1255	Encargado trat./Servicios Ext.	En curso	Normal	Contratos y revisiones de los contratos con los encargados de tratamiento y sus subcontratados	Angel Jesús Varela Vaca	19 Mar 2021 10:02 AM	...

Figura 16: Lista de tareas sobre Encargados de tratamiento.

En este apartado de la aplicación, deberán consignarse una serie de cuestiones exigidas por la normativa de protección de datos relacionadas con la figura del encargado de tratamiento:

- Selección Informada de los encargados de tratamiento.
- Contratos y revisiones de los contratos con los encargados de tratamiento y sus subcontratados.

3.4. FORMACIÓN Y CONCIENCIACIÓN

Se recogerán todas las actividades de formación/concienciación en materia de protección de datos y seguridad de la información que realicen las personas adscritas a la unidad que desarrolla el tratamiento concreto.

Si accedemos a Formación y Concienciación, nos encontramos con las siguientes dos tareas observadas en la Figura 17.

✓ Aceptar 🗑 Anular

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1219	Formación y concienciación	En curso	Normal	Actividades de formación		16 Mar 2021 02:58 PM	...
<input type="checkbox"/>	1218	Formación y concienciación	En curso	Normal	Actividades de concienciación		16 Mar 2021 02:58 PM	...

Figura 17: Lista de tareas de Formación y Concienciación.

Tareas:

- Actividades de concienciación.
- Actividades de formación.

3.5. TRANSPARENCIA

En este tipo de tareas se recogerá toda la información que debe proporcionarse a los interesados (es decir, a los titulares de los datos personales que son objeto de tratamiento) en virtud del principio de transparencia, de conformidad con lo dispuesto en la normativa sobre protección de datos (Clausula Informativa).

En la categoría de Transparencia tendremos una sola tarea como se observa en la Figura 18.

✓ Aceptar 🗑 Anular

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1217	Transparencia	En curso	Normal	Transparencia de la información relativa al tratamiento		16 Mar 2021 09:56 AM	...

Figura 18: Lista de tareas en Transparencia.

Tareas:

- Transparencia de la información relativa al tratamiento.

3.6. CONSENTIMIENTO

En los casos en que, para realizar un tratamiento de datos personales, o alguna operación del tratamiento dentro del mismo se requiera el consentimiento del interesado como base legitimadora, el responsable delegado, debe ser capaz de demostrar que cuenta con el mismo.

En esta categoría sólo aparece una tarea cómo se observa en la Figura 19.

✓ Aceptar Anular

#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
1216	Consentimiento	En curso	Normal	Recogida del consentimiento de los interesados o base legítima establecida conforme a derecho		16 Mar 2021 03:23 PM	...

Figura 19: Lista de tareas sobre Consentimiento.

Sólo deberá cumplimentarse en aquellos tratamientos en los que se requiera, bien para realizar un tratamiento o bien en alguna operación del tratamiento dentro del mismo, el consentimiento del interesado como base legitimadora, el responsable delegado, debe ser capaz de demostrar que cuenta con el mismo.

Tareas:

- Recogida del consentimiento

3.7. DERECHOS DE LOS INTERESADOS

En esta tarea se recogerán los procedimientos mediante los cuales se facilita al interesado el ejercicio de sus derechos (acceso, supresión, oposición...) en virtud de los artículos 15 a 22 del RGPD.

En esta categoría sólo aparece una tarea como se observa en la Figura 20.

✓ Aceptar Anular

#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
1215	Derecho de los interesados	En curso	Normal	Publicar y facilitar el ejercicio de los derechos de los interesados		16 Mar 2021 03:26 PM	...

Figura 20: Lista de tareas sobre Derechos de los interesados.

- Publicar y facilitar el ejercicio de los derechos de interesados.

En esta tarea se recogerán los procedimientos mediante los cuales se facilita al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22 del RGPD.

3.8. SISTEMAS DE INFORMACIÓN

Un Sistema de Información es un conjunto de elementos que nos permite prestar uno o varios servicios digitales. El Sistema incluye la información que se trata digitalmente, los recursos tecnológicos, las personas que lo gestionan, los procedimientos, etc. es obligatorio disponer de un inventario de los activos que tratan la información (elementos del Sistema de Información). Los elementos del Sistema de Información deben valorarse en función del impacto que tendría un incidente que afectara a la seguridad. Esta valoración es la que determina las medidas de seguridad que deben aplicarse al sistema.

En esta categoría tendremos tres tareas como las que se observan en la Figura 21.

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1237	Sistemas de Información	Nueva	Normal	Declaración de aplicabilidad		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1236	Sistemas de Información	Nueva	Normal	Categoría del sistema		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1235	Sistemas de Información	Nueva	Normal	Inventario de activos		16 Mar 2021 09:56 AM	...

Figura 21: Listado de tareas de las categorías de Sistemas de Información.

Las tareas necesarias para mantener un Sistema de Información seguro son:

- Inventario de activos
- Categoría del Sistema
- Declaración de aplicabilidad

3.9. MEDIDAS DE SEGURIDAD

Las medidas de seguridad incluidas en este grupo de tareas están seleccionadas de la lista de medidas que aparecen en la Declaración de Aplicabilidad y son proporcionales a la categoría del sistema de información a proteger.

Son las medidas mínimas necesarias para lograr el cumplimiento de los principios básicos y requisitos mínimos de seguridad establecidos por el Esquema Nacional de Seguridad. El Responsable Delegado, asesorado por el Responsable Tecnológico, podrá decidir si es necesario aplicar alguna otra medida no incluida en el listado siguiente. El conjunto de tareas de la categoría Medidas de Seguridad son las aparecen en la Figura 22.

<input type="checkbox"/>	#	Tipo	Estado	Prioridad	Asunto	Asignado a	Actualizado	
<input type="checkbox"/>	1242	Medidas de seguridad	Nueva	Normal	Desarrollo seguro y puesta en producción		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1241	Medidas de seguridad	Nueva	Normal	Gestión del cambio		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1240	Medidas de seguridad	Nueva	Normal	Bastionado de equipos		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1239	Medidas de seguridad	Nueva	Normal	Mecanismos de acceso local y remoto		16 Mar 2021 09:56 AM	...
<input type="checkbox"/>	1238	Medidas de seguridad	Nueva	Normal	Personas con acceso y permisos asignados		16 Mar 2021 09:56 AM	...

Figura 22: Lista de tareas de la categoría de Medidas de Seguridad.

A continuación, se listan las medidas de seguridad que debemos aplicar a los activos que componen el Sistema de Información:

- Personas con acceso y permisos asignados
- Mecanismos de acceso local y remoto
- Bastionado de equipo
- Gestión del cambio
- Desarrollo seguro y puesta en producción