Requisitos

* Registro de usuarios. Una persona debe registrarse en el sistema como usuario. Debe contener la siguiente información: Nombre, Apellidos, email, usuario y contraseña
* Herramienta de autodiagnóstico. Cada usuario puede hacer uso de la encuesta de autodiagnóstico para diagnosticar si es necesario la realización de una EIPD (Análisis de necesidad)
* Análisis de necesidad. El usuario debe de indicar si el tratamiento a analizar esta incluida dentro de la lista de tipos de tratamientos de datos publicados por la AEPD requieren una EIPD, la sensibilidad de los datos, las finalidades de tratamiento, las tecnologías empleadas para el tratamiento, los encargados de tratamiento, cesiones de datos y transferencias internacionales de datos, la percepción del riesgo por el responsable del tratamiento y DPO y la base jurídica del tratamiento
* Consulta, creación, edición y eliminación de EIPD. Un usuario puede consultar, crear, editar y eliminar su propia EIPD

Pasos de una EIPD:

* + Una EIPD contiene un ciclo de vida, un análisis de necesidad y proporcionalidad del tratamiento, gestión de riesgos (identificar, evaluar y tratar los riesgos) y conclusión de validación (plan de acción y conclusiones)
  + Un ciclo de vida recoge toda la información que permite una adecuada identificación de amenazas y valoración de riesgos a los que están expuestos los datos. El ciclo de vida tiene 5 etapas: captura de datos, clasificación/almacenamiento, uso/tratamiento, cesión de los datos a un tercero para su tratamiento y destrucción.
  + Para cada una de las etapas del ciclo de vida, Se deben de identificar todos los elementos involucrados en cada una de las etapas. Dichos elementos pueden clasificarse en las siguientes categorías:
    - Actividades u operaciones
    - Datos
    - Tecnología
    - Intervinientes
  + Análisis de la necesidad y proporcionalidad del tratamiento: En este paso el usuario debe de indicar la legitimación del tratamiento para que le tratamiento sea lícito (consentimiento, relación contractual, intereses vitales del interesados u otras personas, obligación legal para el responsable, interés publico o ejercicio de poderes público o intereses legítimos prevalentes del responsable o de terceros) , e indicar la evaluación de la necesidad y proporcionalidad de las operaciones del tratamiento)
  + Gestión de riesgos: Identificación y Evaluación de riesgos para la protección de datos.

Para realizar el proceso de gestión de riesgos, es necesario que el usuario realice los siguientes pasos:

1.- Gestión de riesgos: debe seleccionar todas aquellas amenazas que considere, para ello debe marcar la opción SI. Las amenazas se presentan en un listado de dos pantallas.

2. Gestión de riesgos: Una vez seleccionadas las amenazas, y avanzando a la siguiente pantalla, se mostrarán las amenazas seleccionadas con las posibles medidas de control asociadas a cada una de ellas.

3. El usuario debe seleccionar aquellas medidas que sean necesarias para mitigar el riesgo de la amenaza. Además, deberá seleccionar la probabilidad y el impacto de que ocurra dicha amenaza.

4. Una vez seleccionadas las medidas de control, se debe evaluar la probabilidad y el impacto calculando nuevamente el riesgo residual. Este proceso es necesario realizarlo para cada una de las amenazas seleccionadas.

5. Cuando se hayan rellenado todas las medidas de control, probabilidades e impactos de las amenazas y se avance en la pantalla, se mostrará el resultado Aceptable o No Aceptable de dicha gestión de riesgos que, en última instancia, deberá ser validado por el responsable.

* + Tras la gestión de riesgos, se podrá generar un informe de riesgos y generar el informe final en el que contendrá un resumen de la gestión de riesgos y una muestra gráfica de los riesgos.

Si el resultado de la gestión de riesgos sale No aceptable se puede revisar los riesgos con el fin de disminuir el riesgo residual. En todo caso después se ha de realizar un plan de acción en la que se describe todas las medidas de control definidas para tratar los riesgos identificados y sacar una conclusión con respecto al resultado obtenido.

* + Un plan de acción es el conjunto de iniciativas que se deben de llevar a cabo para implantar los controles que ayudan a reducir el riesgo de una actividad de tratamiento hasta conseguir un nivel aceptable.
* Un plan de acción debe incluir al menos los siguientes campos de información:
  + Control
  + Descripción de control
  + Responsable de implantación
  + Plazo de implantación.
* Para la ejecución del plan de acción, se ha de considerar dos posibilidades:
  + Si la EIPD se ha hecho sobre un nuevo tratamiento
  + Si la EIPD se ha hecho sobre un tratamiento ya existente.

En caso de que se haya hecho sobre un nuevo tratamiento, el plan de acción hay que plantearlo durante la fase de definición de requerimientos de la actividad. Y en caso de que se haya realizado sobre un tratamiento ya existente, entonces se habría que lanzar un proyecto para implantar las medidas incluidas en el plan de acción sobre el tratamiento actual. En este caso el responsable del tratamiento tendría que establecer un plazo máximo en el que se han de implantar las medidas de control incluidas en el plan de acción. Si se supera el plazo establecido, dado que el riesgo residual actual no sería aceptable, el responsable podría exigir la suspensión del tratamiento hasta que se implanten las medidas correspondientes.

La conclusión de la EIPD se saca basándose en el riesgo residual conseguido durante la fase de gestión de riesgo, en el que se valora si dicho nivel es aceptable o si supera los limites razonables. Si la conclusión de la EIPD no sea favorable, se habría que evaluar la posibilidad de añadir nuevas medidas de control para reducir el nivel de riesgo hasta que se consiga un nivel aceptable. En caso de que no fuera posible, el tratamiento no se podría llevar a cabo y se tendría que activar el procedimiento de consulta previa a la autoridad de control. En caso de que sea favorable, pues la actividad de tratamiento se llevará a cabo siempre que las medidas de control hayan sido implantadas. Dichas conclusiones se añadirían en el Informe final del tratamiento.

Tras todo esto, se realizaría un proceso de supervisión durante la fase de implantación para garantizar y validad que las medidas de control se han llevado a cabo correctamente. También se implantaría un sistema de revisión de y realimentación del tratamiento con el fin de comprobar la efectividad de la EIPD y verificar si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estos resultados se usarían para realimentar la EIPD y actualizarla cada vez que sea necesario.