Evaluación de seguridad

? Archivo adjunto desconocido

Proceso: Evaluación de seguridad

Objetivo

Establecer el flujo del proceso de Evaluación de Productos que hace la Unidad de Seguridad TIC del SAS.

Alcance

Este proceso aplica a los productos de tipo aplicación y a los de gestión de proyectos que implantan un producto.

Roles

Los roles que intervienen en este proceso son

Rol	Descripción
Responsable de producto/Responsable de proyecto	Es el máximo responsable del producto/proyecto desde el punto de vista de su gestión.
Unidad de Seguridad STIC	Responsable de la Evaluación del producto / proyecto desde el punto de vista de la seguridad.

Flujo del proceso

Cualquier proyecto de nueva creación o implantación tendrá que ser evaluado desde el punto de vista de la Seguridad por parte de la USTIC de forma previa a su aceptación y puesta en servicio, por lo que será necesario crear una Evaluación de seguridad para que la USTIC proceda a evaluarlo. Esta Evaluación de seguridad desde el punto de vista de la seguridad **NO** se considerará impedimento bloqueante para el desarrollo de una determinada versión de un producto o para el desarrollo normal de un proyecto.

En el momento en el que se cree la evaluación de seguridad, será conveniente que aporte en la misma toda la documentación necesaria (diagrama de flujo de datos, acuerdo de encargado de tratamiento, Certificaciones de Seguridad, documentación funcional y técnica y a ser posible cumplimentando el formulario de recogida de datos) para el buen desarrollo de los diferentes informes por parte de la USTIC, todo ello sin perjuicio de que se solicite ampliación de información al ser considerada insuficiente.

En el caso de los proyectos, independientemente del área TIC al que pertenezcan deberán tener creada la evaluación de seguridad. Los proyectos tienen una propiedad, denominada **Revisión seguridad solicitada** q ue mostrará el valor "Sí" cuando se haya creado la primera evalución de seguridad , de manera que la USTIC podrá controlar aquellos proyectos que no hayan pasado la revisión de seguridad. Existe una segunda propiedad, **Revisión seguridad completada**, que mostratá el valor "Sí" cuando se haya cerrado la primera evaluación de seguridad.

Este tipo de tarea podrán ser creadas por los integrantes del equipo provincial o del área centralizada a la que pertenezca el proyecto. o por el Responsable de producto en el caso de que se trate de una aplicación. En la misma creación se hará hincapié sobre la documentación que la USTIC necesitará (diagrama de flujo de datos, acuerdo de encargado de tratamiento, Certificaciones de Seguridad, documentación funcional y técnica y a ser posible cumplimentando el formulario de recogida de datos así como enlace a su espacio donde pueden puedan consultar la información pertinente a dicho proyecto. En la creación hay que tener en cuenta que:

- Aparecen una serie de preguntas y, en función de su respuesta, el comportamiento del flujo de la tarea es diferente. Las detallamos a continuación
- Si la tarea de seguridad viene con la aprobación de alguien, pierde cualquier prioridad y será atendida por la USTIC cuando queden recursos disponibles para la misma. Si una tarea se crea y sigue su curso habitual pero en cualquier momento se registra que está autorizada, pasará a ese estado "latente" denominado "Pdte. revisión" y será atendida cuando sea posible.

Las preguntas que se hacen en la creación son:

¿Proyecto de nueva implantación?

- Respuesta Sí

Se solicita contestar otras dos preguntas y aportar la documentación pertinente:

¿Dispone de acuerdo de encargado de tratamiento de datos en el contrato?

¿Dispone de certificación de seguridad del sistema?

Independientemente de estas respuestas, la tarea se creará y cualquier miembro de la USTIC podrá asignársela. Podrá pedir información y documentación al Responsable del proyecto /Responsable de producto. El resultado de la evaluación **no constituye la aceptación para la puesta en servicio del proyecto** y sí un asesoramiento sobre las medidas de seguridad a implantar, según el Esquema Nacional de Seguridad y el RGPD.

- Respuesta No

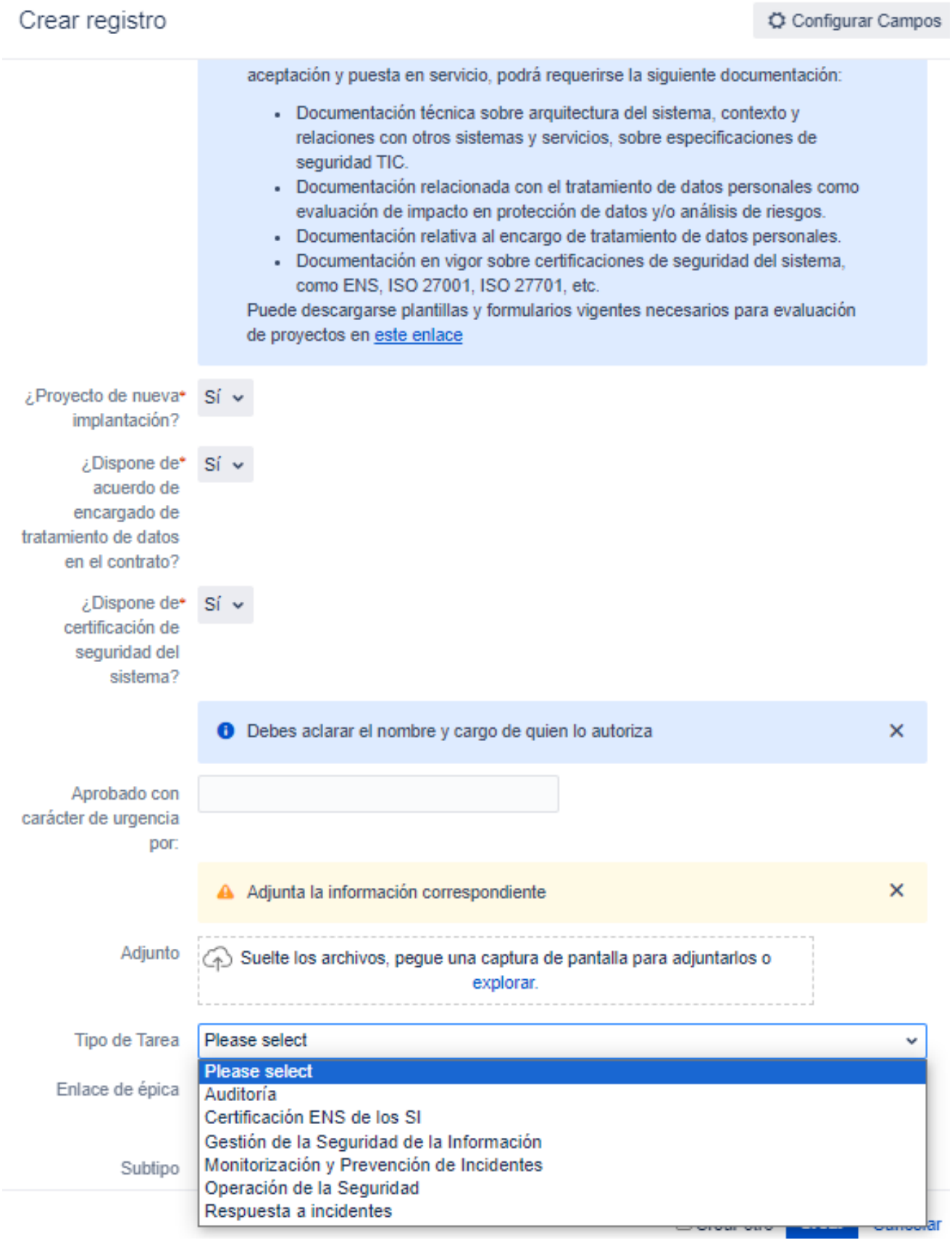
  Se solicita contestar una serie de cuatro preguntas, de manera que si la contestación de alguna de ellas es Sí, el proceso será el mismo que en el caso anterior.

  Si todas las preguntas tienen como respuesta No, la tarea de seguridad se cerrará directamente y el proyecto quedará registrado con la Revisión seguridad informada a Sí.

Una vez que la USTIC realiza la evaluación, resuelve la tarea indicando las posibles vulnerabilidades a corregir. En el caso de proyectos el usuario de la USTIC decidirá quién debe validar el resultado de esa evalución y si decide corregir los posibles fallos o asumirlos en el caso de que los hubiera. Para las aplicaciones esa validación se hace siempre por parte del Responsable de producto.

Ciclo de vida de las evaluaciones de seguridad

Además de los campos habituales al crear cualquier tarea, deben tenerse en cuenta los campos específicos que determinarán el ciclo de vida de la evalución de seguridad


Crear registro
Configurar Campos
aceptación y puesta en servicio, podrá requerirse la siguiente documentación:
Documentación técnica sobre arquitectura del sistema, contexto y relaciones con otros sistemas y servicios, sobre especificaciones de seguridad TIC.
Documentación relacionada con el tratamiento de datos personales como evaluación de impacto en protección de datos y/o análisis de riesgos.
Documentación relativa al encargo de tratamiento de datos personales.
Documentación en vigor sobre certificaciones de seguridad del sistema, como ENS, ISO 27001, ISO 27701, etc.
Puede descargarse plantillas y formularios vigentes necesarios para evaluación de proyectos en este enlace
¿Proyecto de nueva implantación?
Sí
¿Dispone de acuerdo de encargado de tratamiento de datos en el contrato?
Sí
¿Dispone de certificación de seguridad del sistema?
Sí
Debes aclarar el nombre y cargo de quien lo autoriza
Aprobado con carácter de urgencia por:
Adjunta la información correspondiente
Adjunto
Suelte los archivos, pegue una captura de pantalla para adjuntarlos o explorar.
Tipo de Tarea
Please select
Enlace de épica
Subtipo
Please select
Auditoría
Certificación ENS de los SI
Gestión de la Seguridad de la Información
Monitorización y Prevención de Incidentes
Operación de la Seguridad
Respuesta a incidentes

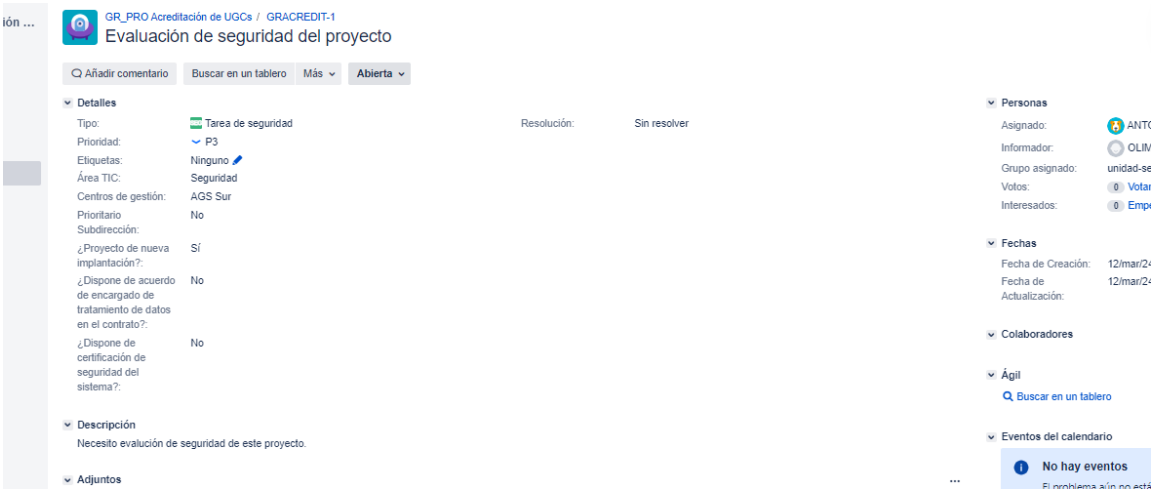
Los tipos de tarea sirven a la USTIC para organizar su trabajo. No es necesario por el solicitante de la evaluación de seguridad que sea informado el tipo de tarea.

El campo "Aprobado con carácter de urgencia por" no debe informarse. En el caso de que se informe, la evaluciaón de seguridad quedará "aparcada" por la USTIC puesto que el proyecto no depende para nada del resultado de la evaluación puesto que alguien ha autorizado su puesta en marcha. Ese estado al que van las tareas que tienen informado ese campo es "Pdte. revisión".

- **Proyecto de nueva implantación =Sí**

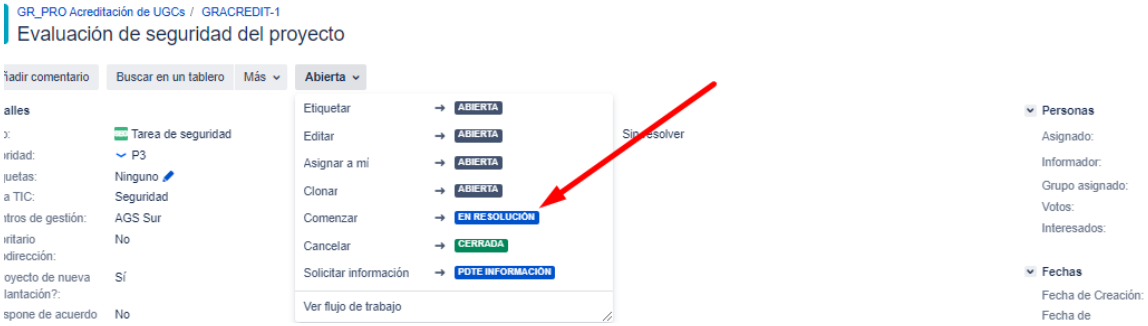
  Independientemente de lo que se conteste en las otras dos preguntas, la evaluación de seguridad siempre se va a hacer. Se creará en estado ABIERTA , sin asignar nominalmente pero asignada al grupo unidad-seguridad.

  El usuario de la USTIC que vaya a llevar a cabo la evaluación deeb asignarse la tarea, de manera que los usuarios sepan quién es el responsable de evaluar su proyecto.



  Si la USTIC tiene a su disposición toda la información necesaria, comenzará la evaluación. En caso contrario solicitará información a quien pueda proporcionársela. En ese caso, la tarea pasará al estado PDTE. INFORMACIÓN asignada a quien debe aportar lo que se le solicita. Al completar la información, volverá de nuevo a asignarse al miembro de la USTIC que había solicitado la información.

  Una vez que la USTIC tiene toda la información disponible para comenzar la evalucuación, la pasa a EN RESOLUCION accediendo a Comenzar.



Una vez que la tarea esté en estado EN RESOLUCION, es posible que pueda necesitarse más información que volvería a pedirse exactamente igual que antes.

Normalmente, la USTIC descompone el trabajo que tiene una evaluación de seguridad en fases, de manera que crea subtareas de la tarea padre. Estas subtareas (que son registros del tipo "Subtarea seguridad") conllevan las tareas definidas por la USTIC para una determinada fase.

Normalmente hay cuatro fases:

- Fase 1: Especificación

  En esta **Fase 1 de Especificación**, del que se emitirá el **Informe de Evaluación de Seguridad** , se detallarán los tratamientos de datos personales implicados en el proyecto y el *Análisis de los riesgos de privacidad asociados*, de conformidad al marco normativo de Protección de Datos Personales (**RGPD y LOPDGDD**), evaluando las posibles limitaciones y riesgos para los derechos y libertades fundamentales de los interesados y la necesidad de la realización de una *Evaluación de Impacto en la Protección de Datos (EIPD*).

  En el mencionado Informe de Evaluación de Seguridad, además vendrá reflejado un *Análisis de Riesgos* conforme al *Esquema Nacional de Seguridad (**ENS**)*, identificando las vulnerabilidades y los controles necesarios para garantizar la integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad de la información; aportando la *Declaración de Aplicabilidad* donde se formalizará la relación de medidas de seguridad que resultan de aplicación al sistema de información de que se trate, conforme a su categoría, siendo esta Unidad la que establecerá una propuesta de *Categorización preliminar del sistema de información*, cuya determinación se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de **la información** tratada o de los **servic ios** prestados para:

  i. Alcanzar sus objetivos.
  ii. Proteger los activos a su cargo.
  iii. Garantizar la conformidad con el ordenamiento jurídico.

- Fase 2:

Acuerdo de Encargado de Tratamiento de datos personales

Las relaciones entre el responsable y el encargado deben formalizarse en un contrato o en un acto jurídico que vincule al encargado respecto al responsable.

El responsable del tratamiento debe elegir un encargado del tratamiento que **ofrezca garantías suficientes** respecto a la implantación y el mantenimiento de las medidas técnicas y organizativas apropiadas, de acuerdo con lo establecido en el RGPD, y que **garantice la protección de los derechos** de las personas afectadas. Existe, por tanto, un *deber de diligencia en la elección del responsable*.

En este documento se regula de forma minuciosa el contenido mínimo de los contratos de encargo, debiendo preverse aspectos como:

- Objeto, duración, naturaleza y la finalidad del tratamiento
- Tipo de datos personales y categorías de interesados
- Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
- Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
- Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

Puede ser necesrio a nivel de fase que se solicite información. tanto antes como una vez comenzada la fase. Una vez acabada, la USTIC la resolverá indicando quién debe ser el validador de la misma. Esto implica que como resultado de esa fase de la evalución, es posible que los usuarios de los equipos provinciales o los responsables de aplicaciones acepten esas recomendaciones o correcciones prOpuestas y una vez corregidas, pidan de nuevo que sean revisadas por la USTIC. Esto implicaría la no aceptación de la subtarea para que la USTIC vuelva a evaluar.

- Fase 3: Puebas de seguridad en PRE
- Fase 4: Despliegue

En el caso de aceptar la evaluación de la STIC la subtarea se cerrará.

Como siempre que haya subtareas, éstas deberán estar cerradas para poder cerrar la tarea padre,

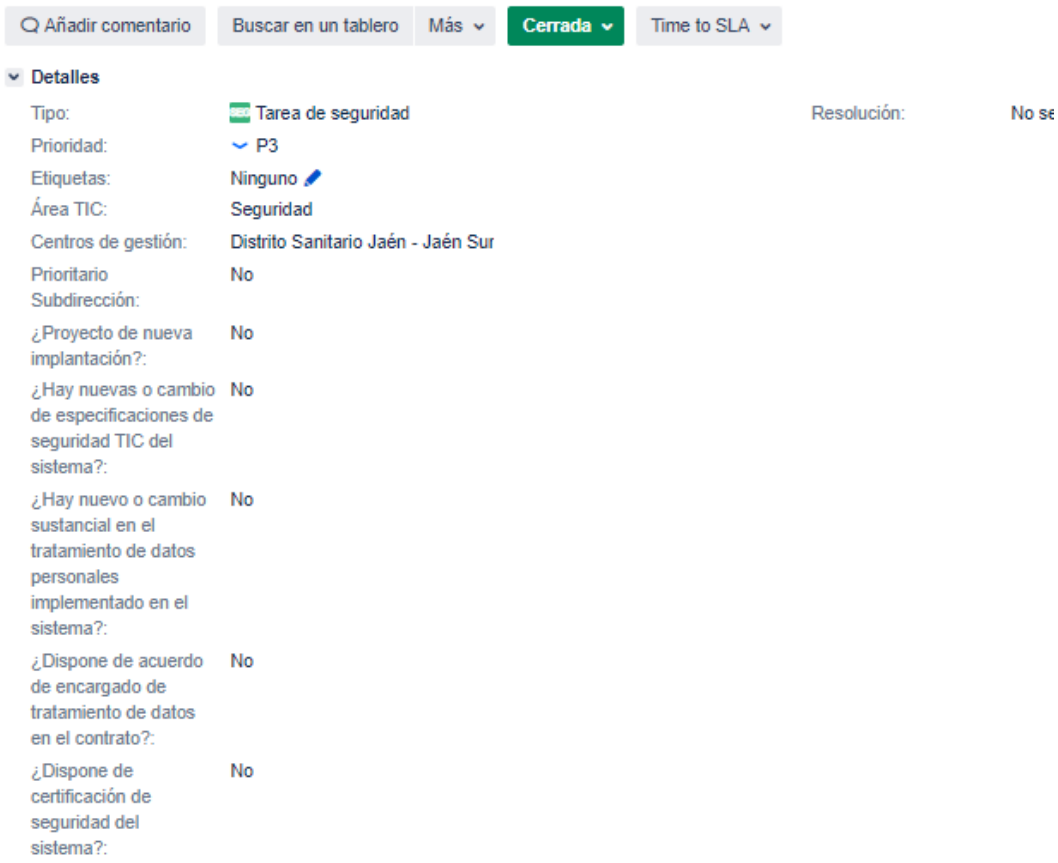
Cuando se accede a resolver la tarea padre (sin subtareas o con todas las subtareas cerradas), el flujo es idéntico al descrito para las subtareas, es decir, la USTIC indica quién es el validador y este puede, o aceptar la evaluación de la USTIC y no hacer nada (se cerrará la tarea) o bien corregir esas vulnerabilidades y que la USTIC vuelva a evaluar (No aceptar solución técnica para pasar de nuevo a estado EN RESOLUCION).

- **Proyecto de nueva implantación= No**

  En este caso, las preguntas que aparecen al crear la evaluación de seguridad son diferentes


Crear registro
Configurar Ca
evaluación de impacto en protección de datos y/o análisis de riesgos.
Documentación relativa al encargo de tratamiento de datos personales.
Documentación en vigor sobre certificaciones de seguridad del sistema, como ENS, ISO 27001, ISO 27701, etc.
Puede descargarse plantillas y formularios vigentes necesarios para evaluación de proyectos en este enlace
¿Proyecto de nueva implantación?
No
¿Hay nuevas o cambio de especificaciones de seguridad TIC del sistema?
Sí
¿Hay nuevo o cambio sustancial en el tratamiento de datos personales implementado en el sistema?
Sí
¿Dispone de acuerdo de encargado de tratamiento de datos en el contrato?
Sí
¿Dispone de certificación de seguridad del sistema?
Sí
Debes aclarar el nombre y cargo de quien lo autoriza
Aprobado con carácter de urgencia por:
Adjunta la información correspondiente
Adjunto
Suelte los archivos, pegue una captura de pantalla para adjuntarlos o explorar.
Crear otro
Crear
Ca

- Si todas las respuestas son No: la USTIC considera que no debe hacer evaluación de seguridad de ese proyecto. Por tanto, la tarea se cierra automáticamente nada más crearse indicando en su resolución No se hará



- Si al menos una de las respuestas es Sí: el flujo de la tarea es el mismo descrito para el proyecto de nueva implantación.

Ayuda relacionada:

- Enlace
- Enlace