Manual µCeENS y Requisitos Esenciales

µCe ens

Certificación esencial en el ENS

Área de Normativa y Servicios de Ciberseguridad

1. **¿Qué es µCeENS?**
   - Definición
   - Actuaciones principales derivadas de la Metodología.
   - Desarrollo de la Metodología: Herramientas de Gobernanza y Soluciones ABS.
2. **¿Quién puede beneficiarse de µCeENS?**
3. **¿Cómo se aplica µCeENS?**
   - Fases de la metodología.
   - Entregables.
4. **Actividades de adopción de µCeENS**
   - **4.1. Cómo acceder a µCeENS – Portal de Gobernanza**
   - **4.2. Cómo crear un sistema**
   - **4.3. Cómo acceder al sistema**
   - **4.4. Secciones de µCeENS**
     - Diagnóstico de Cumplimiento
     - Gobierno
     - Plan de adecuación
     - Implantación
     - Conformidad

µCe ens
Certificación esencial en el ENS

1. ¿Qué es µCeENS?

Definición:

- Es un **modelo, una metodología** que facilita la obtención de la Certificación de Conformidad en el ENS.
- Tiene en cuenta los **Requisitos de Seguridad definidos en un Perfil de Cumplimiento Específico** validado por el Centro Criptológico Nacional.

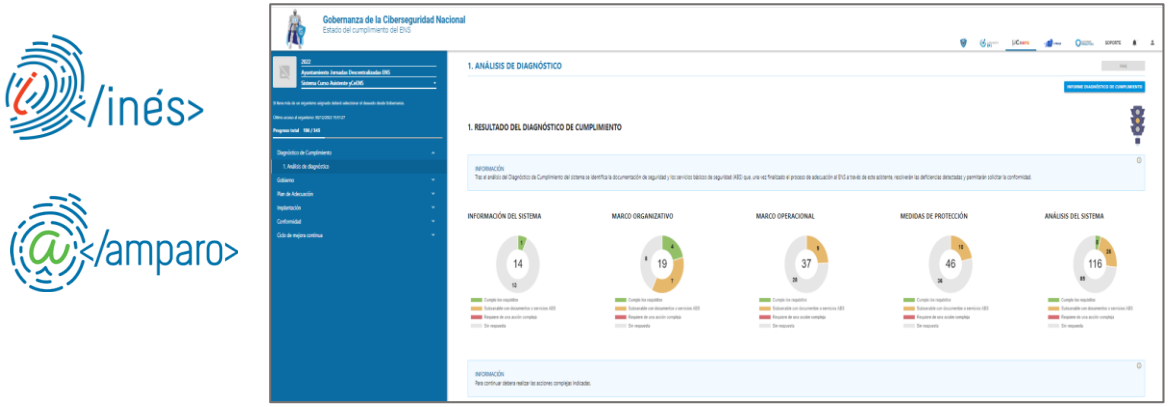
Acompañamiento en base a fases y actuaciones durante el proceso de la Certificación de Conformidad:

1. **Definición de un Modelo mínimo viable**.
2. **Diagnóstico de cumplimiento** en base a **Perfiles de Cumplimiento Específicos**.
3. **Gobierno**: Política de Seguridad, Gobernanza y Marco Normativo necesario.
4. **Herramientas de perfilado básico de seguridad (soluciones ABS)** como apoyo a la implementación técnica de seguridad, tareas de mantenimiento y recogida de evidencias.
5. **Mejor Continua** al propiciar el progreso y avance del nivel de implantación de la seguridad en las Organizaciones.

Desarrollo de la Metodología:

- **Automatización de los procesos en las herramientas de Gobernanza** para obtener la adecuación y la correspondiente Certificación de Conformidad en el ENS, conforme a un **Perfil de Cumplimiento Específico**, que se complementa con los servicios básicos de seguridad proporcionados por las soluciones del CCN en la modalidad ABS:.

Herramientas de Gobernanza:



Soluciones ABS:

2. ¿Quienes puede beneficiarse de µCeENS?

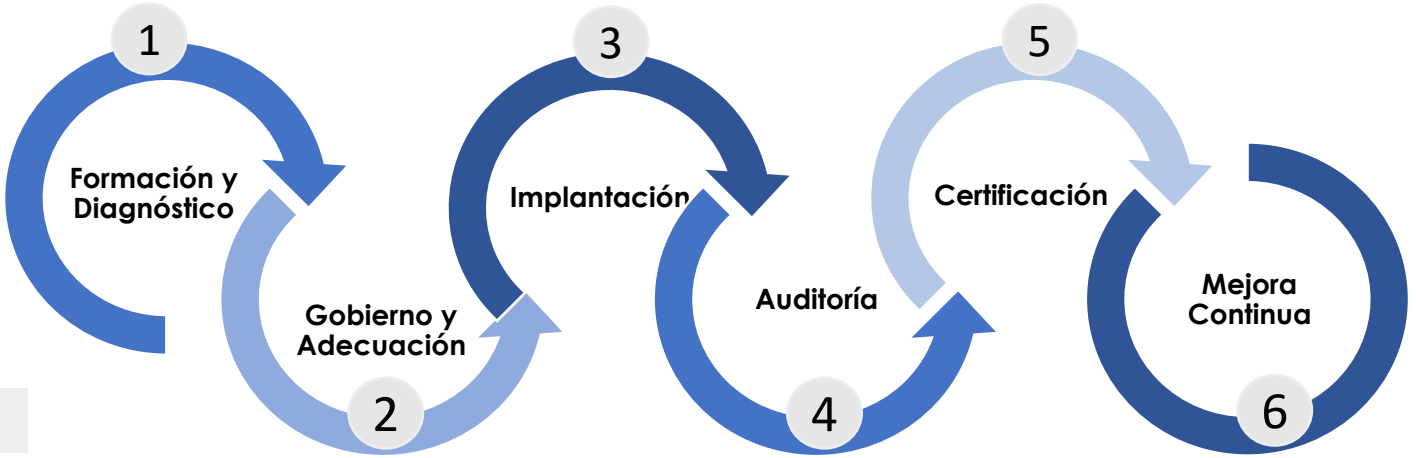
Alcance determinado para Entidades u Organizaciones con las siguientes características:

- **Dificultades para abordar la Adecuación al ENS**, tras analizar los riesgos y amenazas a los que están sometidos los sistemas.
- **Superar el Diagnóstico de Cumplimiento** del ENS (validación por semáforo)
- Cuyos **riesgos identificados** son **mitigados** con la implementación de un Perfil de Cumplimiento Específico (validación mediante el Módulo de Verificación de Perfiles de Cumplimiento en cuanto al Riesgo – **MVPCR**)

3. ¿Cómo se aplica µCeENS? (fases)

Implantación de la Metodología µCeENS mediante seis (6) fases

Planificación aproximada de cuatro (4) a seis (6) meses.



Alcance determinado para cada fase:

1. Formación en el ENS, de manera asíncrona, a través de la plataforma ÁNGELES

1.1 Diagnóstico de Cumplimiento para determinar la situación y posibilidad de abordar un proceso de adecuación al ENS.

2. Gobierno y Adecuación. Política de seguridad, establecer una estructura, determinar roles asignando responsabilidades y flujos de relación, inventario de activos, categorización, declaración de aplicabilidad e informe de riesgos.

3. Implementación de medidas, marco normativo, desarrollo procedimental, adopción de soluciones técnicas, recogida de evidencias y registros.

4. Auditoría de Certificación

5. Obtención de la certificación.

6. Mejora continua, progreso y avance del nivel de implantación, tareas de mantenimiento y acciones puntuales del sistema.

3. ¿Cómo se aplica µCeENS? (entregables)

Durante las fases de µCeENS se generan diferentes entregables:

1

Perfil de Cumplimiento Específico (PCE)

- Conjunto de medidas de seguridad como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad

2

Informe de Resultados del Diagnóstico de cumplimiento

- Análisis de desviaciones indicando las medidas que requieren de una acción compleja para su subsanación o bien son subsanables con una implementación procedimental y/o servicios ABS de seguridad.

3

Modelo para la designación de Roles y Política de Seguridad

- Designación de los Responsables de Gobierno, Supervisión y Operación. Asignación de responsabilidades y establecimiento de flujos de interrelación.
- Aprobación de la Política de Seguridad de la Información.

4

Plan de Adecuación (Categorización del Sistema y Declaración de Aplicabilidad)

- **Categorización del Sistema**: propuesta de inventario de servicios-información y su valoración.
- **Declaración de Aplicabilidad**.
- **Informe de riesgo residual**.

5

Normativa de uso de medios electrónicos

- Regulación del uso de los recursos puestos a disposición del personal.

6

Marco Normativo de Seguridad

- Procedimientos que soportan el cumplimiento de las medidas.

7

Registro de Seguridad

- Modelo de registro de seguridad para el inventario de activos y de entrada y salida de soportes.

8

Lista de mantenimiento del sistema y acciones puntuales

- Medidas y acciones puntuales que propicien el mantenimiento y mejora continua de la seguridad.

4. Actividades de implantación

4.1. Cómo acceder µCeENS – Portal de Gobernanza

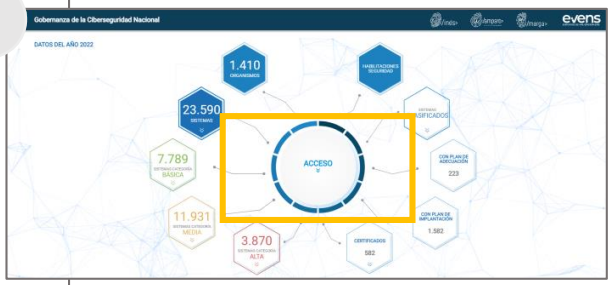
Para acceder a µCeENS, se debe acceder al Portal de Gobernanza desde los **Portales del CCN (www.ccn.cni.es)**, **CCN-CERT (www.ccn-cert.cni.es)**, **EVENS (www.ccn-cert.cni.es/evens/)**

1 Desde el portal del CCN (www.ccn.cni.es):

2

3

4



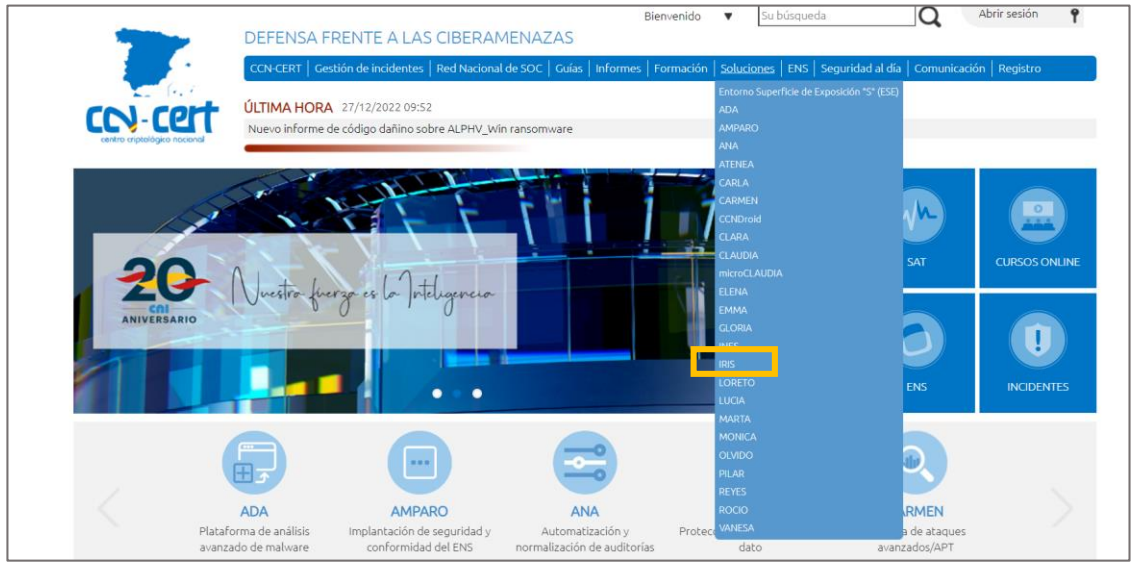
Instrucciones:

1. Debe ingresar al portal del CCN y pulsar en la sección de soluciones.
2. Buscar la imagen correspondiente a la Solución INES.
3. Buscar en la parte inferior de la página el "Acceso a INES".
4. Debe pulsar la figura central, denominada "Acceso".

4. Actividades de implantación

4.1. Cómo acceder µCeENS – Portal de Gobernanza

1 Desde el portal del CCN-CERT (www.ccn-cert.cni.es)



2

3

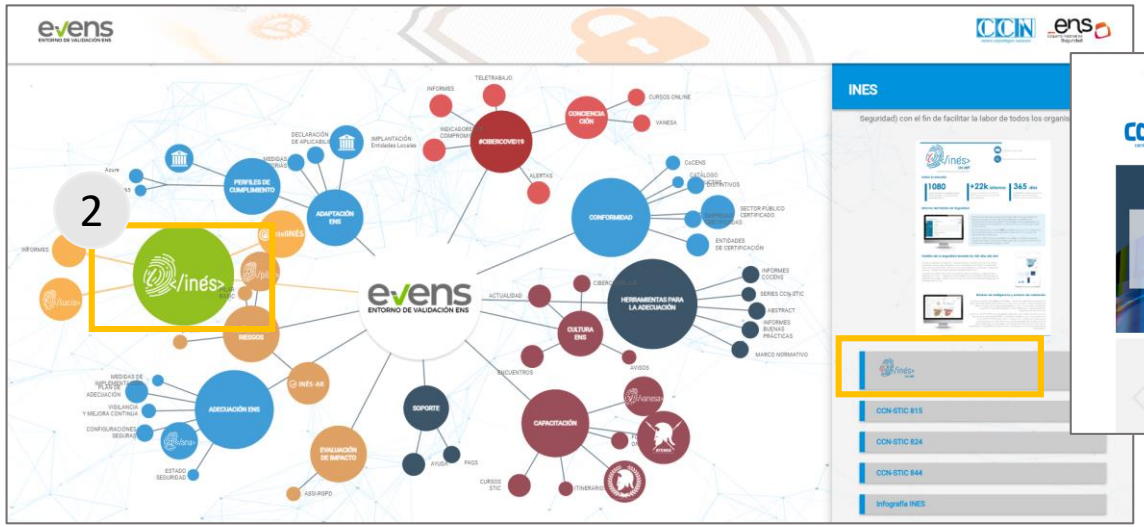
Instrucciones:

1. Debe ingresar al portal del CCN y pulsar en la sección de soluciones y buscar en la lista la Solución INES.
2. Buscar en la parte inferior de la página el "Acceso a INES".
3. Debe pulsar la figura central, denominada "Acceso".

4. Actividades de implantación

4.1. Cómo acceder µCeENS – Portal de Gobernanza

1 Desde el portal EVENS (www.ccn-cert.cni.es/evens/)



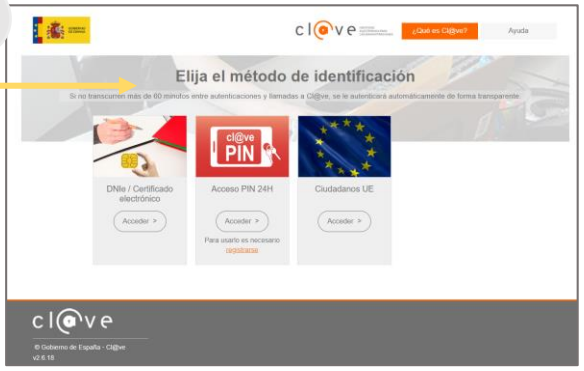
Instrucciones:

1. Debe ingresar al portal del EVENS.
2. Buscar en la Solución INES y pulsar el botón de la lista desplegable.
3. Buscar en la parte inferior de la página el “Acceso a INES”.
4. Debe pulsar la figura central, denominada “Acceso”.

4.1. Cómo acceder al asistente - Portal de Gobernanza

1

2



Instrucciones:

1. Una vez que ingrese al Portal de Gobernanza, debe acceder a la **parte privada de su organismo**, a través de **cl@ve.**
2. Elija el método de autenticación de su organismo.

4.1. Cómo acceder al asistente - Portal de Gobernanza

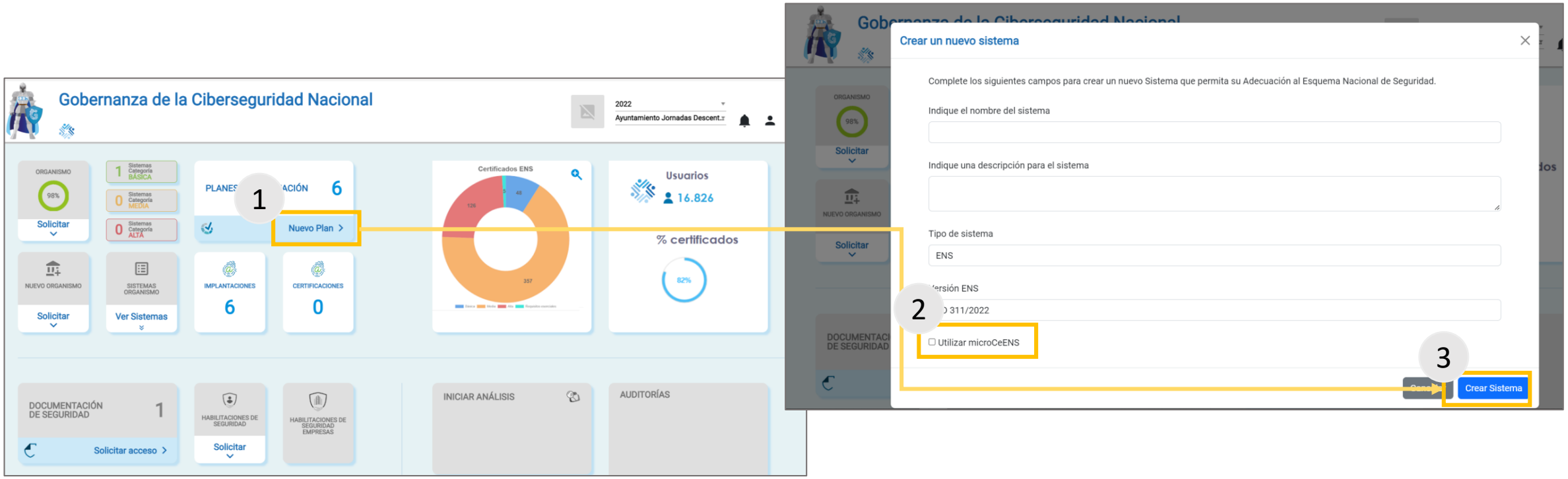
Funcionalidades:

- Desde **INES,** dentro del Portal de Gobernanza, se facilita la **obtención** de la **conformidad** de **los sistemas TIC de categoría BÁSICA** de un organismo, con la ayuda de **µCeENS.**
- A través de µCeENS, el organismo puede **crear** los sistemas que tiene que adecuar al ENS, y **acometer** todas **las fases para obtener la conformidad de los sistemas,** entre otras**:**
  - Obtener una Política de Seguridad;
  - Revisar el plan de adecuación, previamente completado;
  - Realizar la implantación de las medidas con las evidencias necesarias;
  - Solicitar la Certificación de Conformidad.

Generalidades:

- En la parte **privada del Portal de Gobernanza** del organismo, el usuario puede ver sistemas creados desde µCeENS, editarlos y consultar el estado de su conformidad.
- También puede solicitar acceso a otros asistentes como a otros organismos.

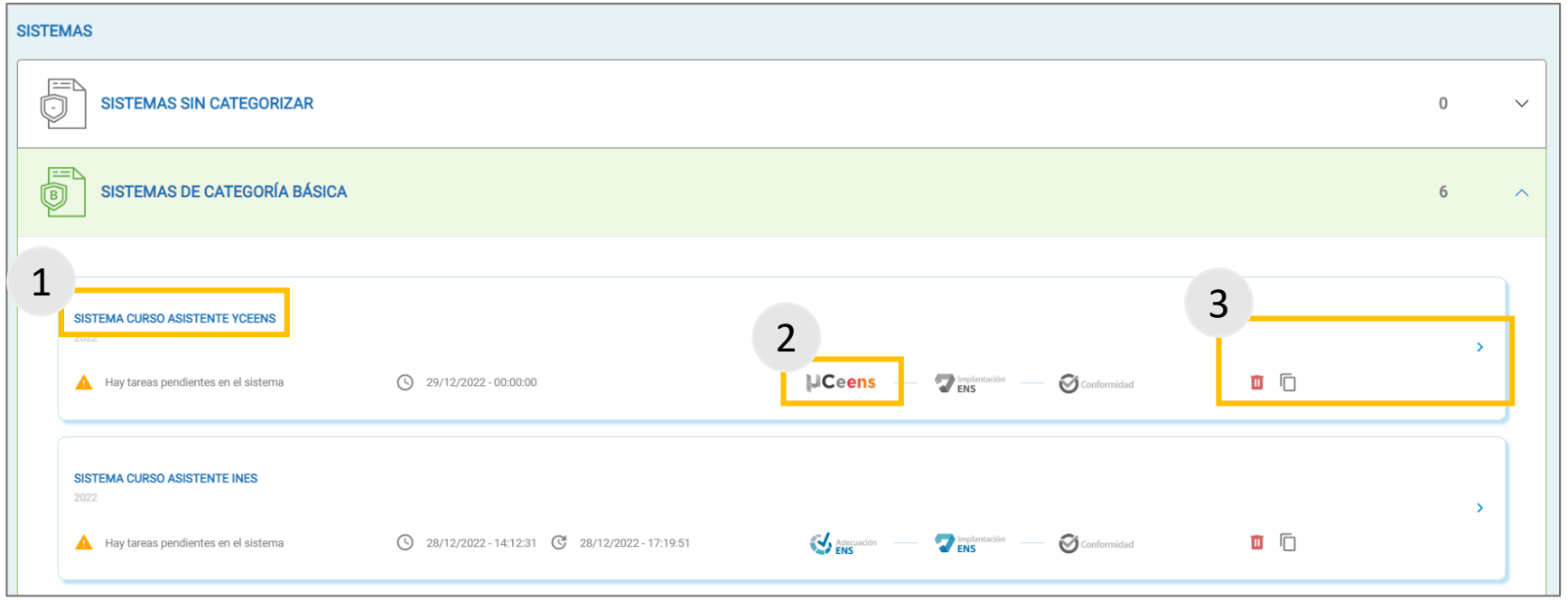
4.2. Cómo crear un sistema



Instrucciones:

1. Para crear un nuevo sistema en µCeENS, debe pulsar en **"Nuevo plan"** dentro de "Planes de adecuación".
2. Debe completar los datos que se solicitan, indicando que se va a utilizar µCeENS,
3. Para finalizar la creación del sistema debe y pulsar "Crear Sistema"

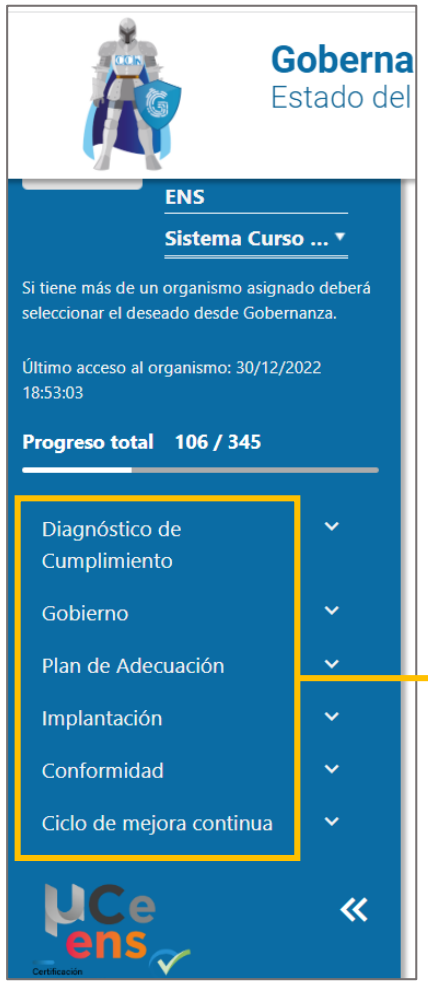
4.3. Cómo acceder al sistema



Instrucciones:

1. Una vez creado el sistema, en la parte inferior aparece una agrupación de los sistemas por tipo y/o categoría; donde se encuentran todos los sistemas que se han ido creando.
2. Si se ha seleccionado "Utilizar µCeENS" aparecerá indicado en el Sistema.
3. Para acceder al Asistente, debe pulsar la flecha que se encuentra a la derecha del sistema. Si desea borrar el sistema y todo lo relacionado con él, debe pulsar la papelera roja.

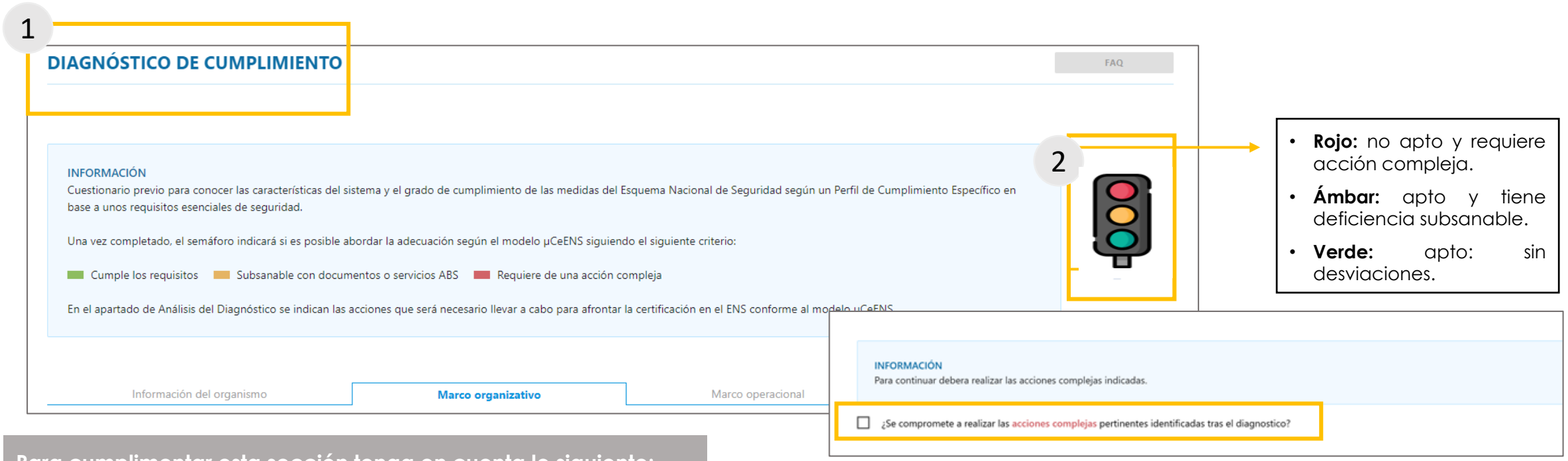
4.4. Secciones µCeENS



µCeENS se divide en **seis (6) secciones**, que son navegables a través del menú lateral izquierdo y que **se habilitan según se vayan completando secciones anteriores**:

1. **Diagnóstico de cumplimiento**
   - Se verifica la situación de cumplimiento del ENS a través del semáforo.
2. **Gobierno:**
   - Se define el modelo de gobernanza y se genera la política de seguridad
3. **Plan de Adecuación:**
   - Se revisa y/o adapta el plan de adecuación del sistema
4. **Implantación:**
   - Se revisa y suben las evidencias para la implantación del sistema
5. **Conformidad:**
   - Se solicita y consulta la conformidad del sistema
6. **Ciclo de mejora continua:**
   - Se realizan las tareas de mantenimiento y acciones puntuales.

4.4. Secciones µCeENS - Diagnóstico de cumplimiento (I)



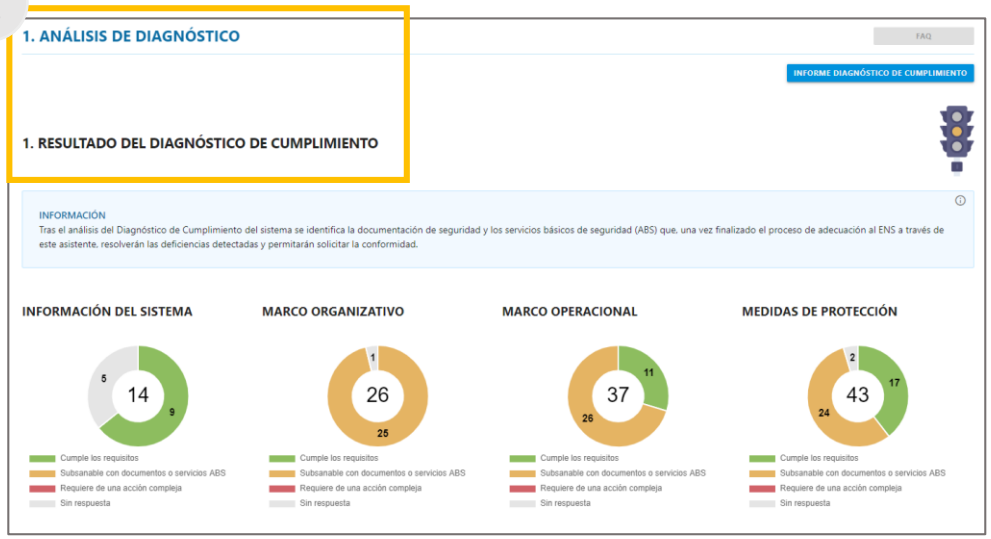
Para cumplimentar esta sección tenga en cuenta lo siguiente:

1. En la sección de **Diagnóstico de cumplimiento** debe cumplimentar el cuestionario para verificar la situación de cumplimiento en el ENS del Organismo para obtener la Certificación de Conformidad según el Perfil de Cumplimiento Específico.
   - Indicar compromiso en adopción de acciones complejas.

2. Este cuestionario está validado a través de un **semáforo** que:
   - **Habilita o no los siguientes pasos** para la obtención de la certificación de conformidad, en función del resultado.
   - **Indica qué medidas requieren de una acción compleja para su subsanación.**
   - **Indica qué medidas se pueden subsanar con actuaciones procedimentales y/o servicios ABS de seguridad**

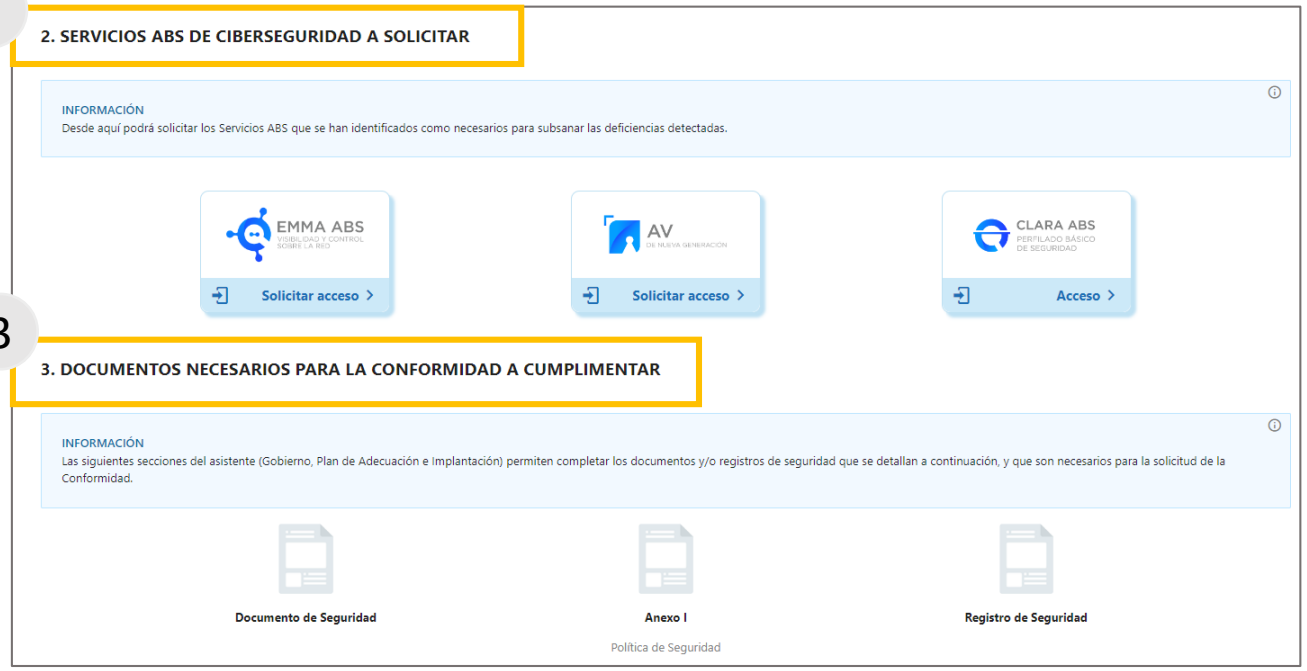
4.4. Secciones µCeENS - Diagnóstico de cumplimiento (II)

1



2

3

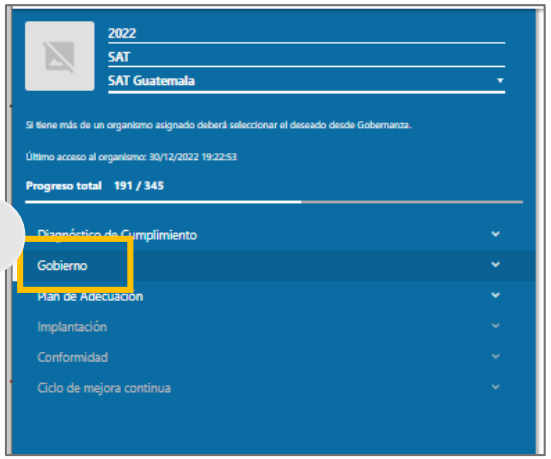


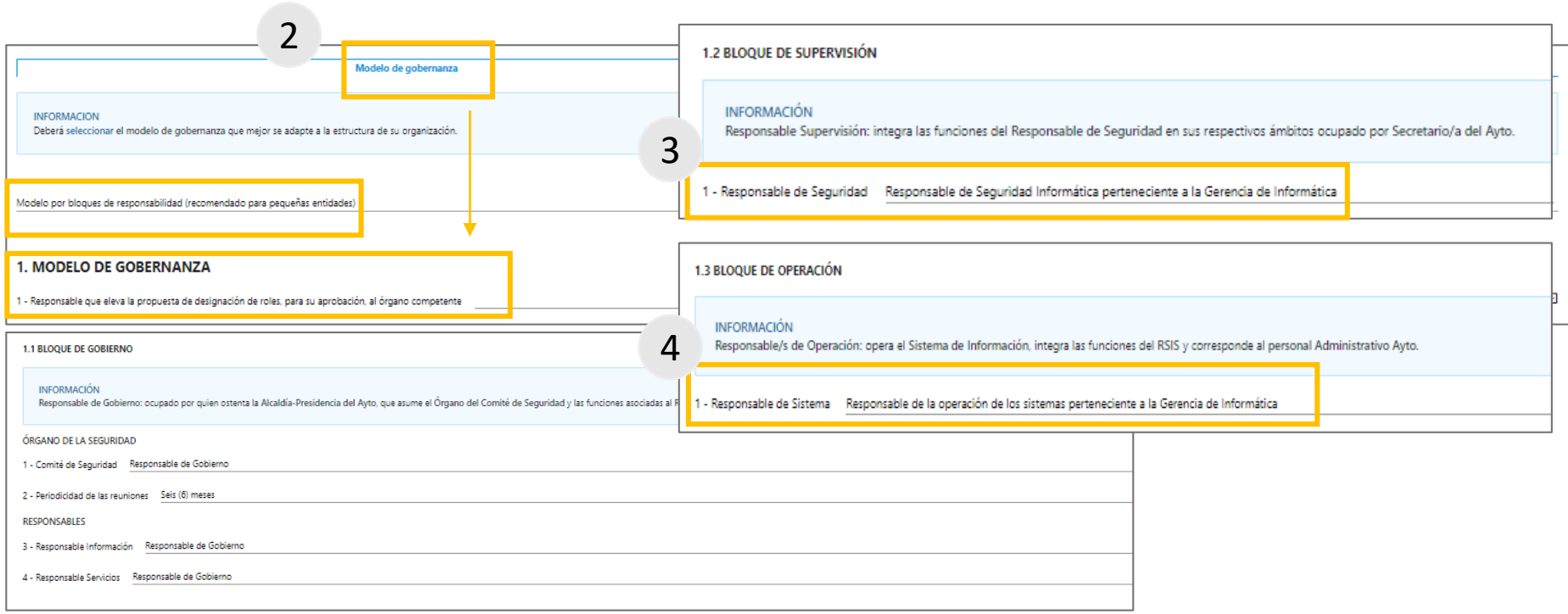
Instrucciones:

1. En el apartado de **Análisis de diagnóstico "Resultados del diagnóstico de cumplimento"** tras el análisis del Diagnóstico de Cumplimiento del sistema, se identifican las desviaciones en el ámbito procedimental y los servicios básicos de seguridad (ABS) necesarios que resolverán las deficiencias detectadas y permitirán solicitar la Conformidad.
2. En esta sección se podrán **solicitar los Servicios ABS que se han identificados como necesarios** para subsanar las deficiencias detectadas en la sección anterior.
3. Las secciones del asistente (Gobierno, Plan de Adecuación e Implantación) permiten completar el marco normativo y/o registros de seguridad que son necesarios para la solicitud de la Conformidad.

4.4. Secciones µCeENS - Modelo de Gobernanza (I)

Modelo de Gobernanza por Bloques de Responsabilidad





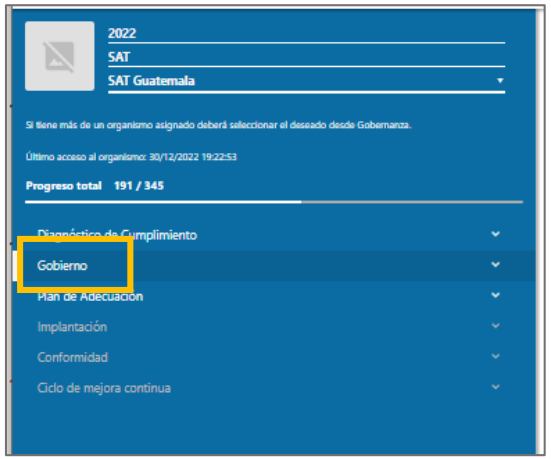
Instrucciones:

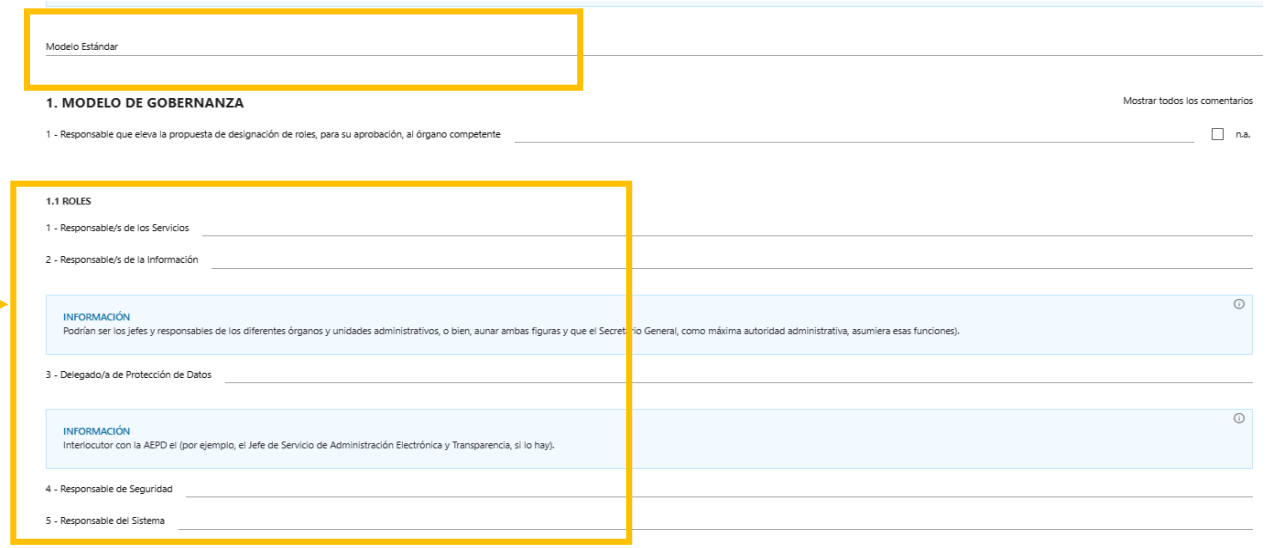
1. Debe pulsar la sección de Gobierno y seleccionar la pestaña de "**Modelo de Gobernanza**" donde **se identificarán los Responsables del ENS, indicando** las **personas** del organismo que tienen asignadas **las responsabilidades asociadas a los tres (3) responsables que se describen a continuación**:

2. **Responsable de Gobierno**: ocupado por quien ostenta la Alcaldía-Presidencia de la entidad, que asume el **Órgano del Comité de Seguridad** y las funciones asociadas al **Responsable/s Información** y **Responsable/s Servicio**, pudiendo delegar en un Concejal o Concejales
3. **Responsable de Supervisión**: integra las funciones del **Responsable de Seguridad** en sus respectivos ámbitos ocupado por Secretario/a de la entidad.
4. **Responsable de Operación**: opera el Sistema de Información, integra las funciones del **Responsable del Sistema** y corresponde al personal de la organización (incluso personal administrativo).

4.4. Secciones µCeENS - Modelo de Gobernanza (II)

Modelo de Gobernanza estándar





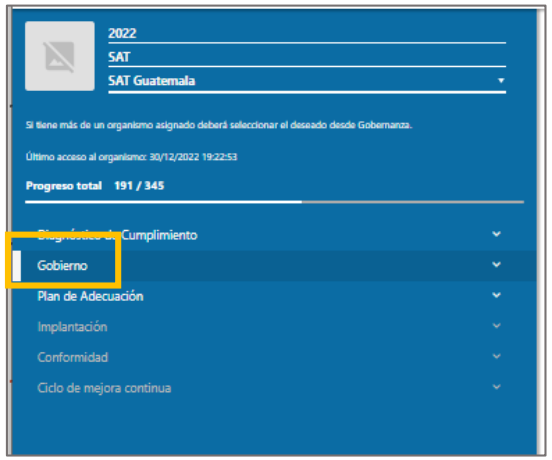
Para cumplimentar esta sección tenga en cuenta los siguientes aspectos:

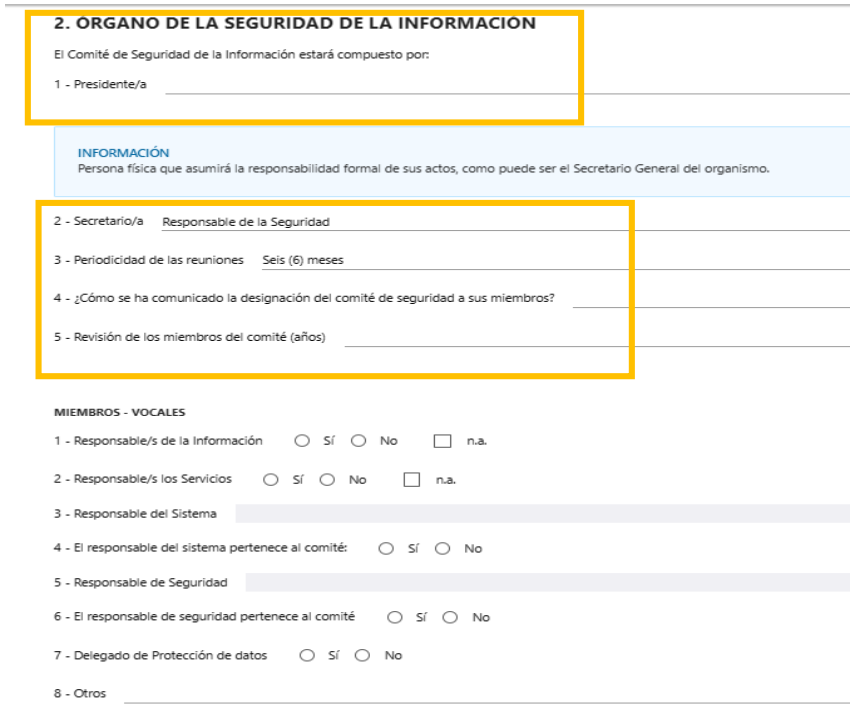
Modelo estándar:

- Responsable de los servicios.
- Responsable de la información: podrán ser los jefes y responsables de los diferentes órganos y unidades administrativos, o bien, aunar ambas figuras y que el Secretario General, como máxima autoridad administrativa, asumiera esas funciones.
- Delegado de protección de datos: es el interlocutor con la AEPD (por ejemplo, el Jefe de Servicio de Administración Electrónica y Transparencia, si lo hay).
- Responsable de la seguridad de la información.
- Responsable del sistema: habitualmente, es el Jefe del Servicio de Informática.

4.4. Secciones µCeENS - Modelo de Gobernanza (III)

Modelo de Gobernanza estándar - Comité de Seguridad

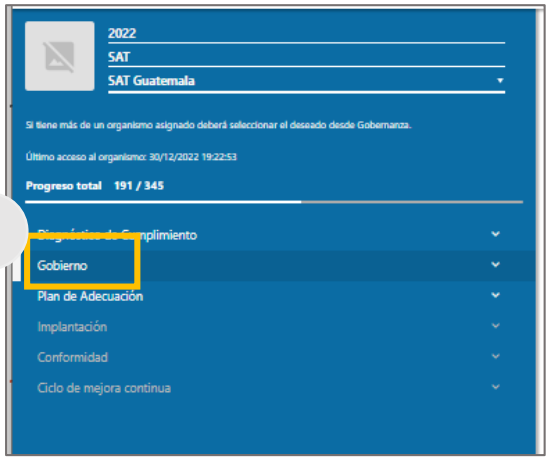


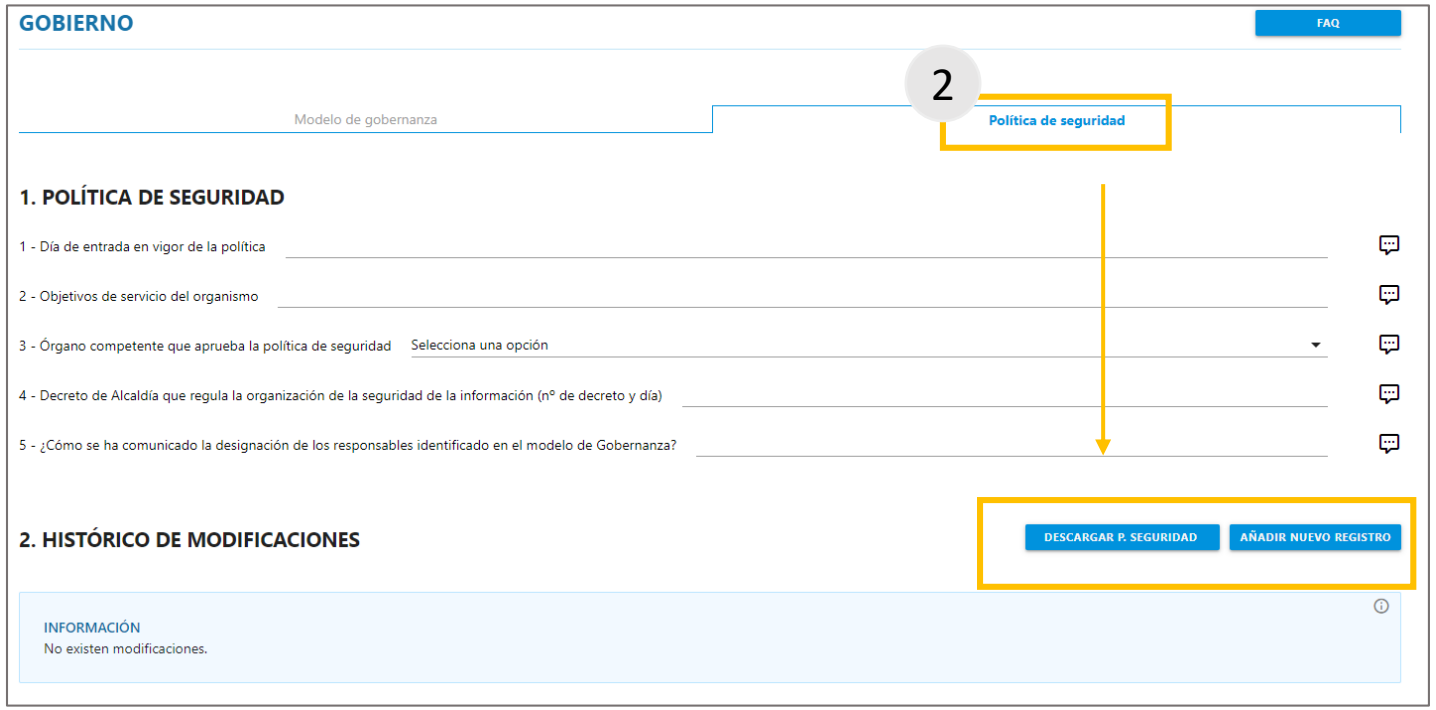


Definir el Comité de Seguridad del Organismo, indicando:

- El presidente: es la persona física que asumirá la responsabilidad formal de sus actos, como puede ser el Secretario General del Organismo.
- El secretario: generalmente es el Responsable de la Seguridad de la Información.
- La periodicidad de las reuniones: generalmente son cada seis (6) meses

4.4. Secciones µCeENS - Política de Seguridad

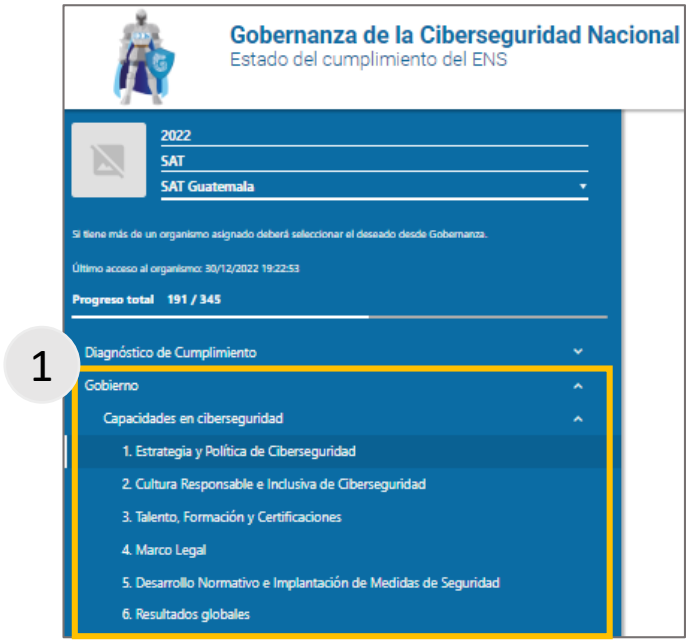


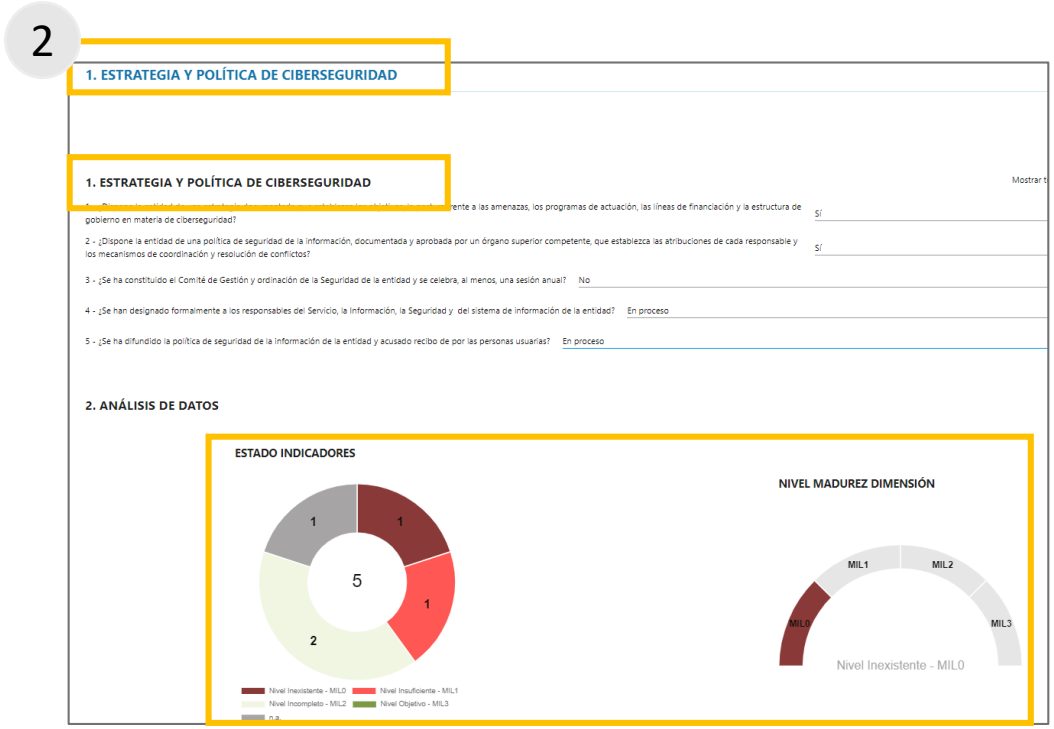


Instrucciones:

1. Debe pulsar la sección de Gobierno y seleccionar la pestaña de **"Modelo de Gobernanza"**.
2. En la pestaña **"Política de Seguridad"** puede elaborar y descargar la política de seguridad, desde el botón **"Descargar P. Seguridad"**, así como registrar las modificaciones que se han realizado en la política de seguridad.

4.4. Secciones µCeENS - Gobierno / Capacidades en Ciberseguridad



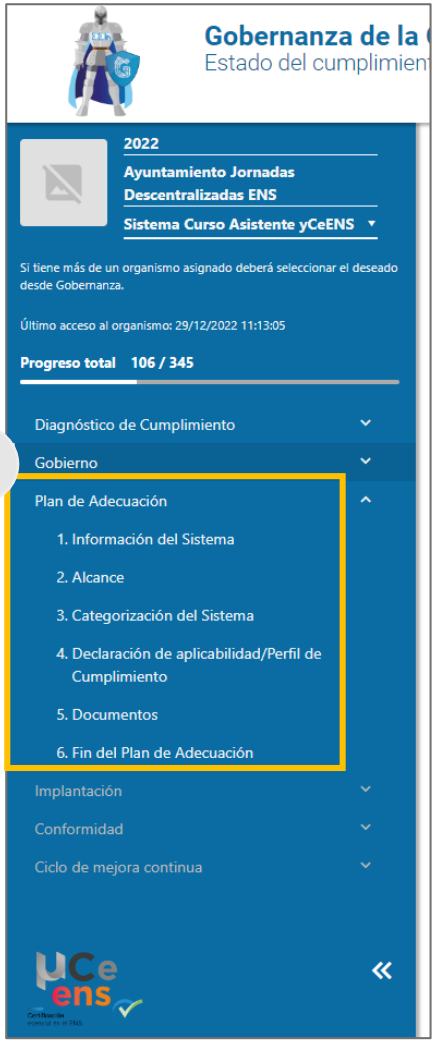


Instrucciones:

1. Debe pulsar en la sección de **Gobierno** y seleccionar la opción de **"Capacidades en Ciberseguridad"**. Allí puede realizar el **modelo de Gobernanza que más se adapte a su organización y generar la política de seguridad**.

2. Además puede ver el estado de los **indicadores y el nivel de madurez** que tiene su organismo en materia de ciberseguridad, a **través de un cuestionario.**

4.4. Secciones µCeENS - Plan de Adecuación (I)



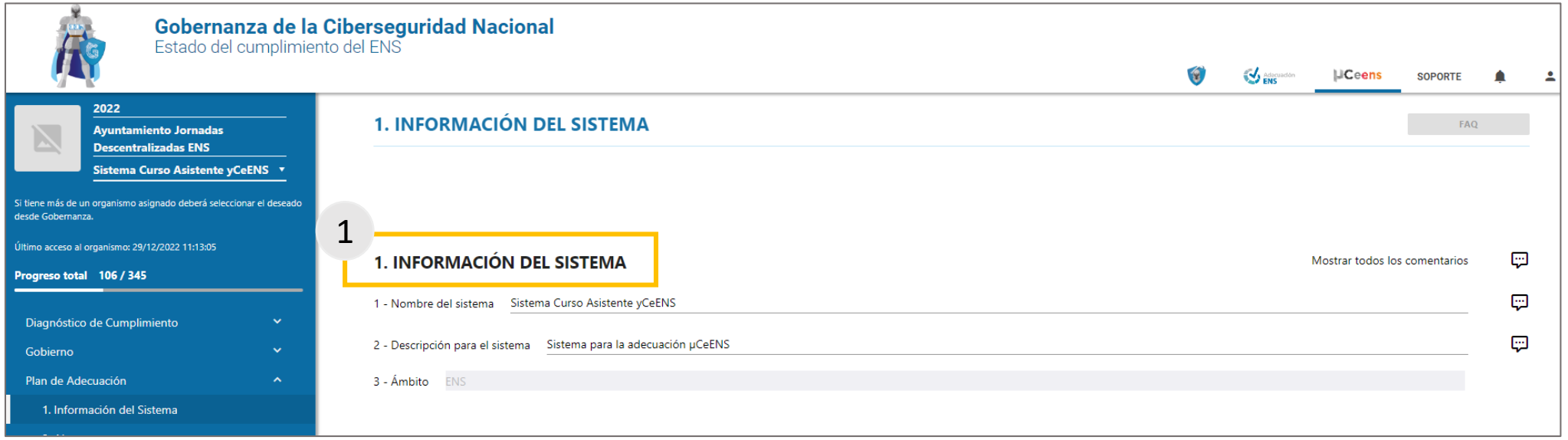
Para cumplimentar esta sección tenga en cuenta los siguientes aspectos:

1. La sección de **Plan de Adecuación** se encuentra previamente completada con un modelo de catálogo de servicios de un sistema TIC de **categoría BÁSICA.**

La sección se compone de **seis (6) apartados**:

1. **Información del sistema**
2. **Alcance**
3. **Categorización del Sistema**
4. **Declaración de Aplicabilidad / Perfil de cumplimiento**
5. **Documentos**
6. **Fin del Plan de Adecuación**

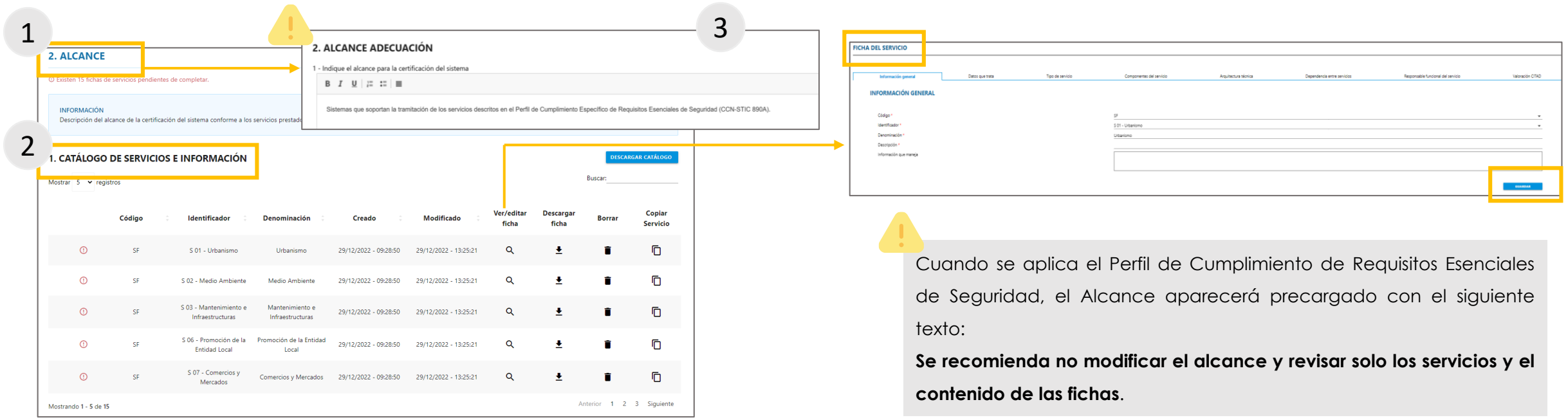
4.4. Secciones µCeENS - Plan de Adecuación (II)



Para cumplimentar el apartado de "Información del sistema" en cuenta los siguientes aspectos:

1. En este apartado se puede ver y modificar la información del sistema.
    1. **Nombre del sistema.**
    2. **Descripción del sistema.**
    3. **Ámbito: en ese caso siempre va a ser ENS.**

4.4. Secciones µCeENS - Plan de Adecuación (III)



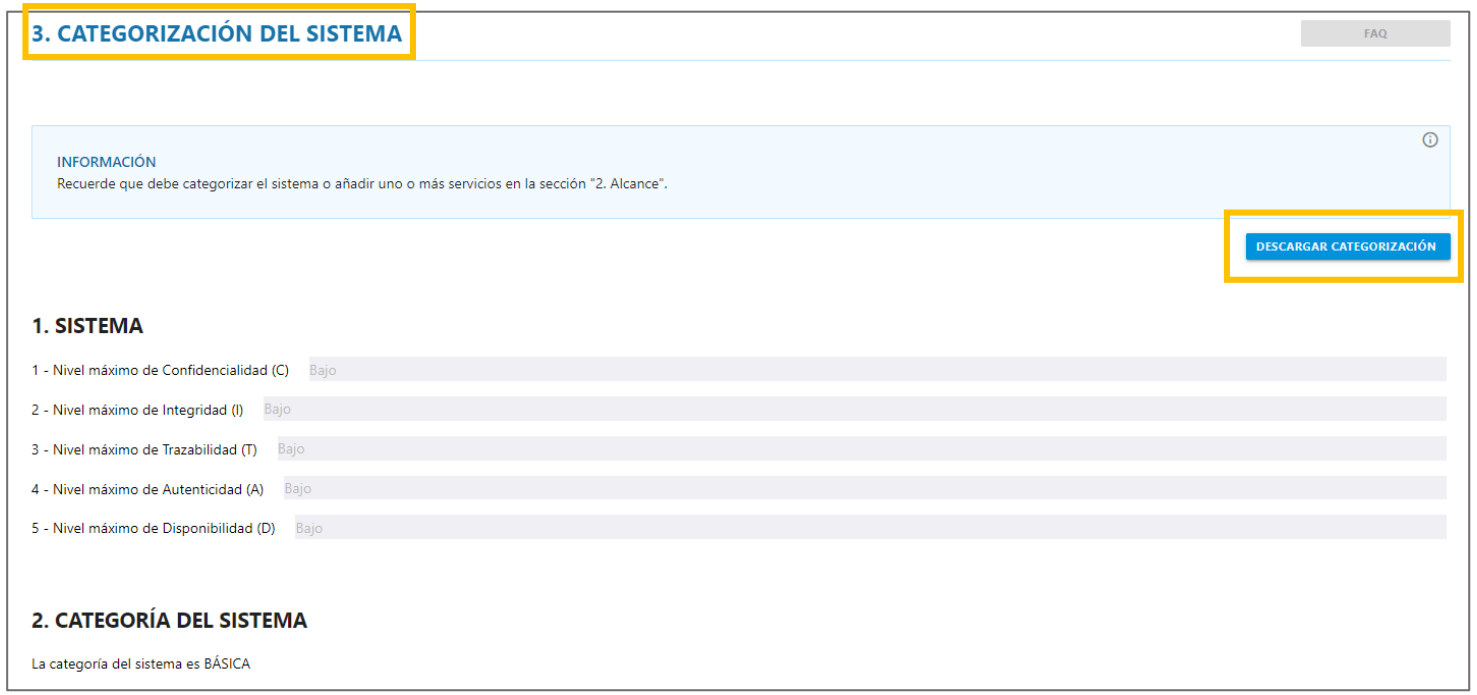
Cuando se aplica el Perfil de Cumplimiento de Requisitos Esenciales de Seguridad, el Alcance aparecerá precargado con el siguiente texto:

Se recomienda no modificar el alcance y revisar solo los servicios y el contenido de las fichas.

Para cumplimentar esta sección se tienen en cuenta los siguientes aspectos:

1. El **Alcance del sistema a certificar viene determinado por dónde se alojan los activos esenciales de la organización**: los servicios que se prestan y la información que manejan.
2. En función del tipo de organismo (EELL, Universidad, otros…) aparecerá precargada una lista de servicios para su revisión. **Para el Perfil de Cumplimiento de Requisitos Esenciales el nivel de las dimensiones de seguridad (CITAD) es BAJO**.
3. Se podrá **ver y editar cada ficha para lo cual deberá:**
   - **Rellenar** las **fichas de los servicios** desde el **botón "Ver/editar ficha"**
   - Borrar los servicios.
   - Copiar los servicios.
   - **Descargar** el catálogo de servicios, en Excel, desde el **botón "Descargar catálogo"**.
   - **Revisar** el **alcance de la certificación** del sistema conforme a los **servicios que se prestan** y la **información manejada.**

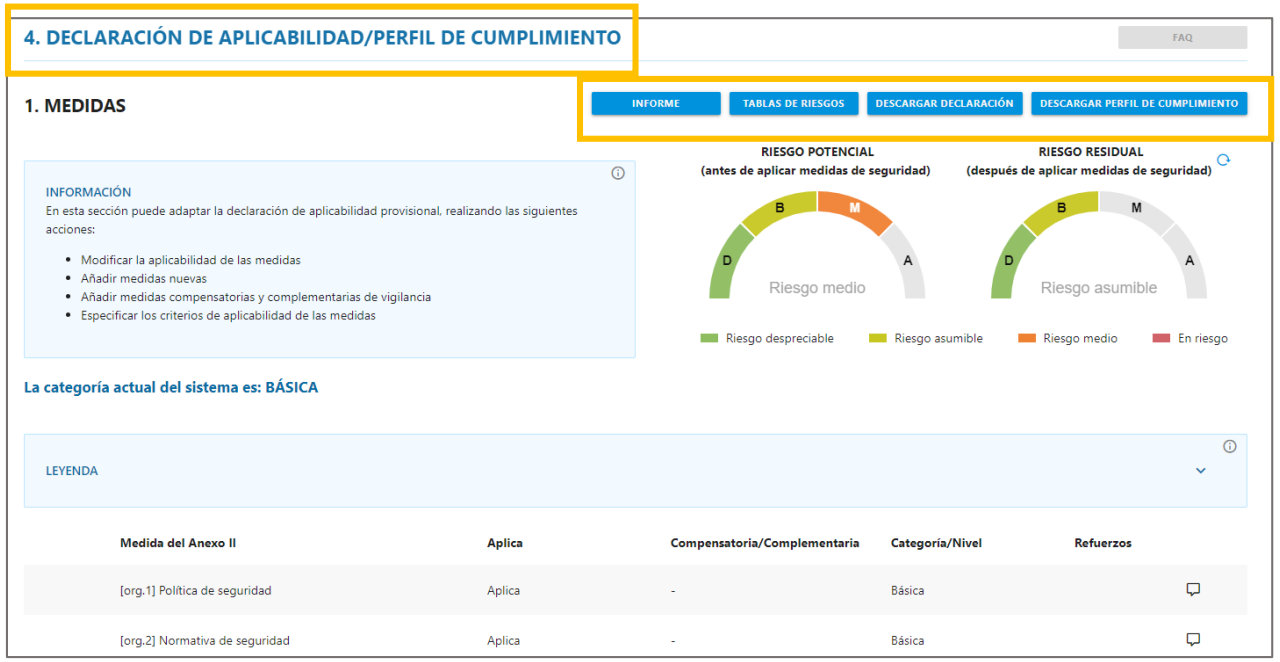
4.4. Secciones µCeENS - Plan de Adecuación (IV)



"Categorización del sistema": en este apartado tenga en cuenta los siguientes aspectos:

- Se muestra la categorización del sistema a **categoría BÁSICA**, como se corresponde con el **Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.** Se puede descargar el documento de categorización del sistema para su firma, necesaria para la implantación.

4.4. Secciones µCeENS - Plan de Adecuación (V)



Tenga en cuenta los siguientes aspectos el apartado de "Declaración de aplicabilidad de cumplimiento" :

En este apartado se podrá:

- **Revisar** la Declaración de Aplicabilidad.
- **Especificar** los criterios de aplicabilidad de las medidas.
- **Descargar** la Declaración de Aplicabilidad para firma del Responsable de Seguridad.
- **Verificar** el riesgo de las medidas antes (Riesgo Potencial) y después de aplicarlas (Riesgo Residual).
- **Descargar** el informe de análisis de riesgos.

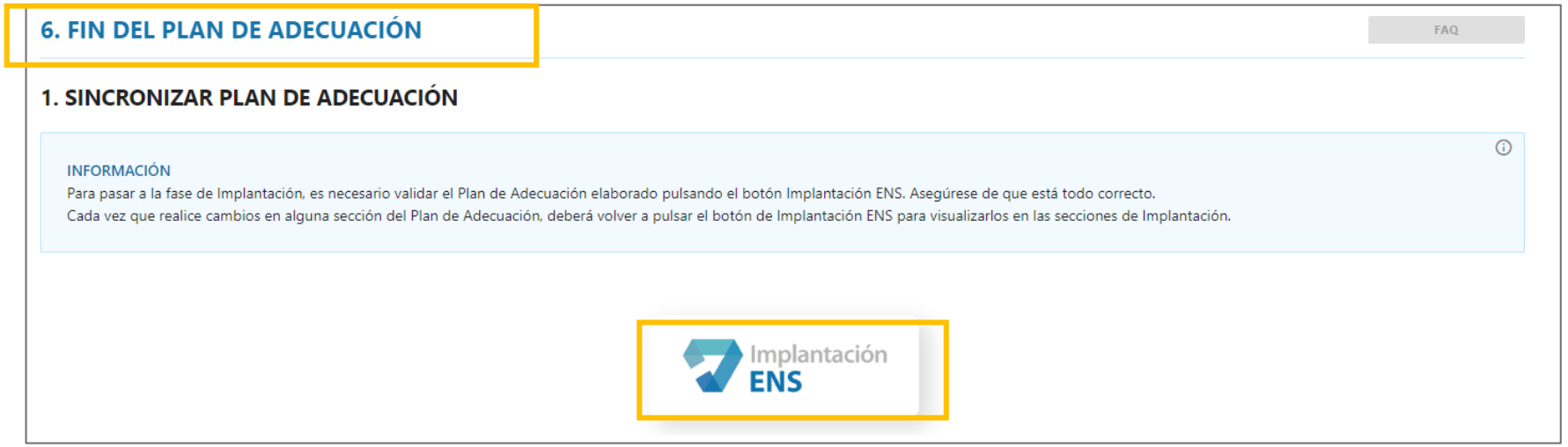
4.4. Secciones µCeENS - Plan de Adecuación (VI)

Tenga en cuenta los siguientes aspectos el apartado de "Documentos":

En este apartado se encuentra agrupados todos los documentos que se pueden **descargar desde sus propias secciones para facilitar su localización**. Estos documentos son:

- Política de Seguridad.
- Declaración de aplicabilidad – Perfil de cumplimiento.
- Categorización del Sistema.
- Informe simplificado de riesgos.
- Catálogo de servicios.
- Fichas de servicios.

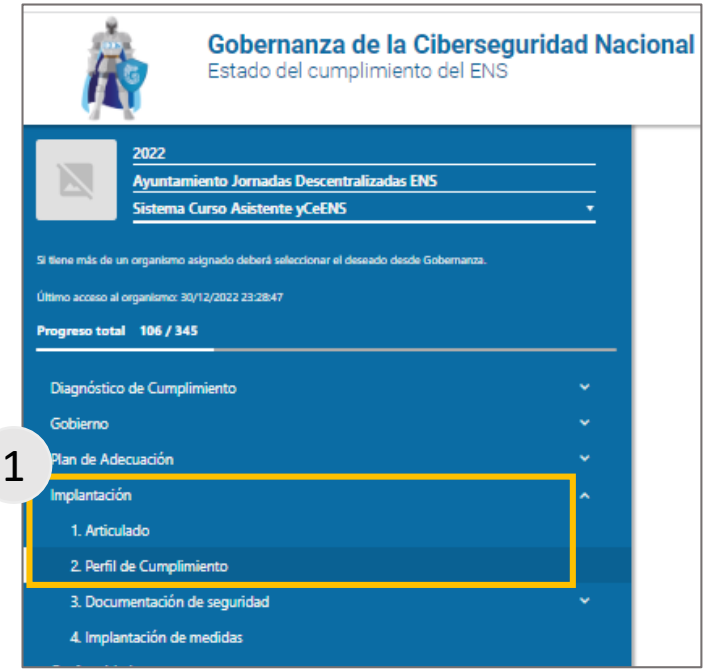
4.4. Secciones µCeENS - Plan de Adecuación (VII)

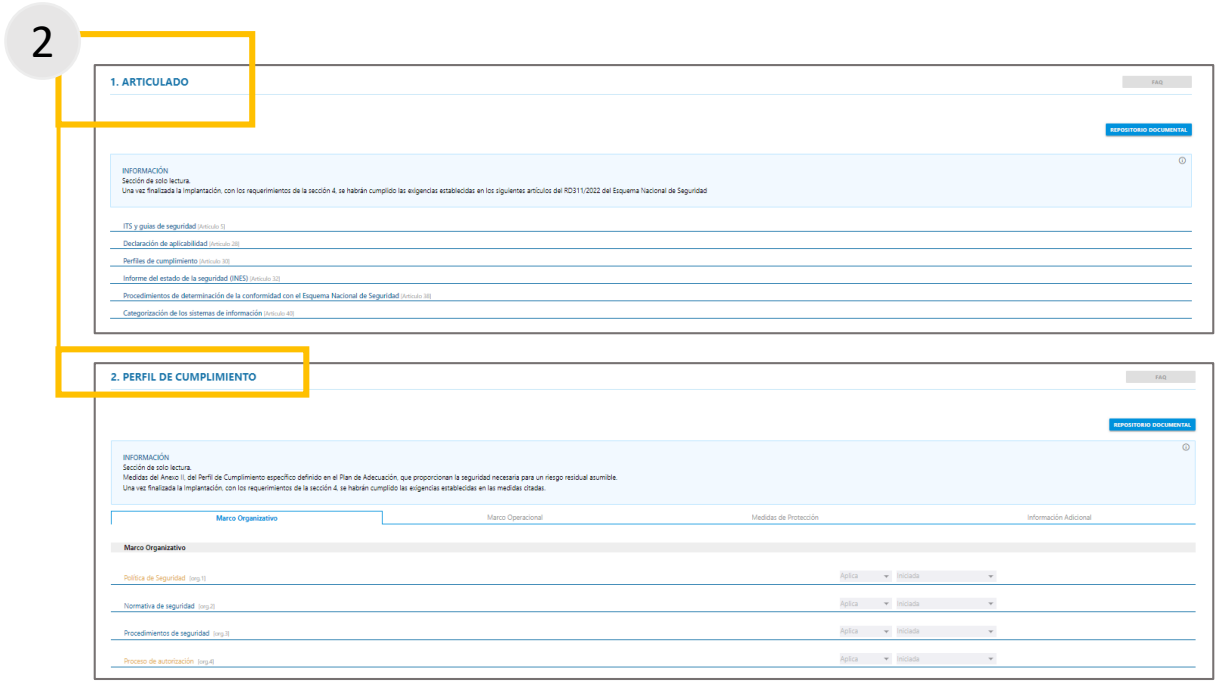


Tenga en cuenta los siguientes aspectos el apartado de "Fin del Plan de Adecuación":

- En el apartado de **Fin del Plan de Adecuación** se finaliza el plan de adecuación pasando a la **fase de implantación**. Para ello es necesario validar el Plan de Adecuación elaborado pulsando el botón "**Implantación ENS**".
- Cada vez que se realicen cambios en alguna sección del Plan de Adecuación, se deberá volver a pulsar el botón de Implantación ENS para visualizarlos en las secciones de Implantación.

4.4. Secciones µCeENS - Implantación (I)



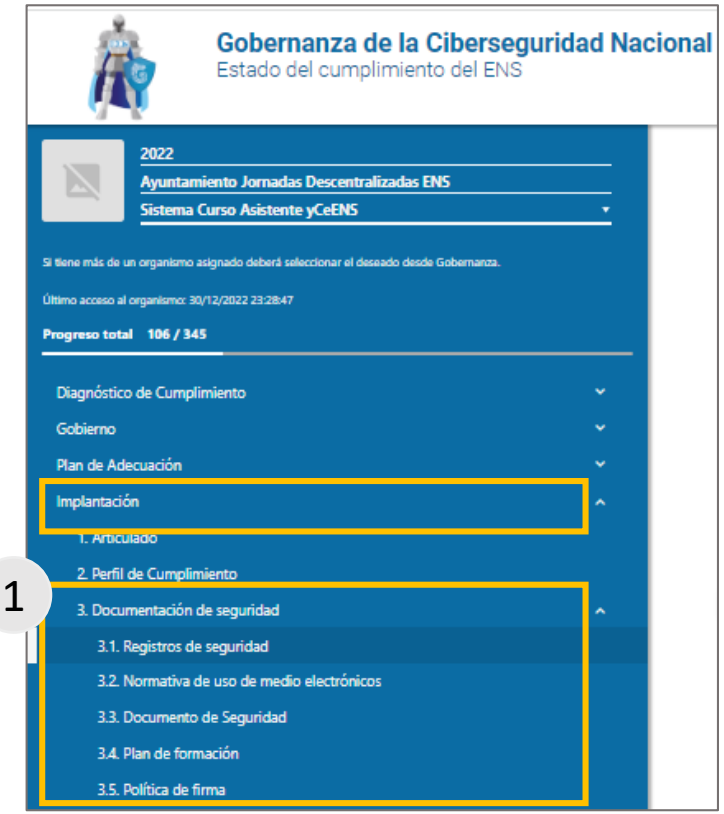


Tenga en cuenta los siguientes aspectos el apartado de "Implantación" así como de "Articulado" y "Perfil de Cumplimiento":

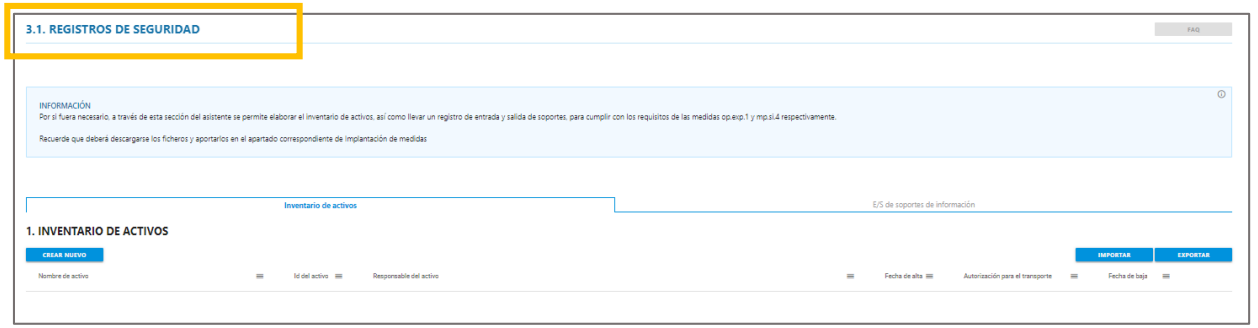
1. En este apartado puede revisar la **implantación de las medidas en el sistema TIC que se quiere adecuar**, así como la generación de documentos necesarios en la implantación.
    - En todos los apartados se dispone de un repositorio documental, pulsando el botón "Repositorio documental".

2. Los apartados **Articulado** y **Perfil de Cumplimiento, cuando se aplica el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad**, son de solo lectura, ya que su aplicabilidad y grado de implantación proporcionan la seguridad necesaria para un riesgo residual asumible.
    - Las tareas de implantación se realizan en la sección 4. Implantación de medidas.

4.4. Secciones µCeENS - Implantación (II)



1

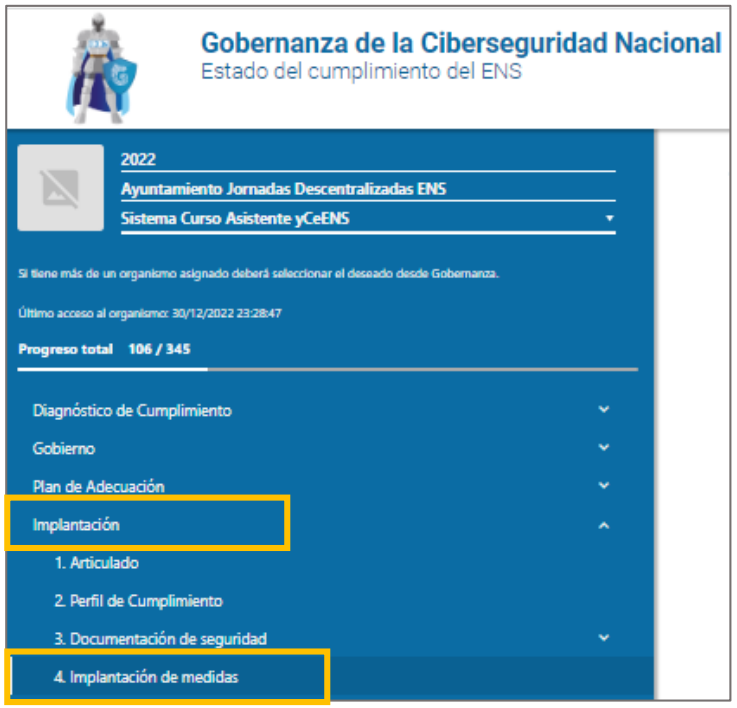


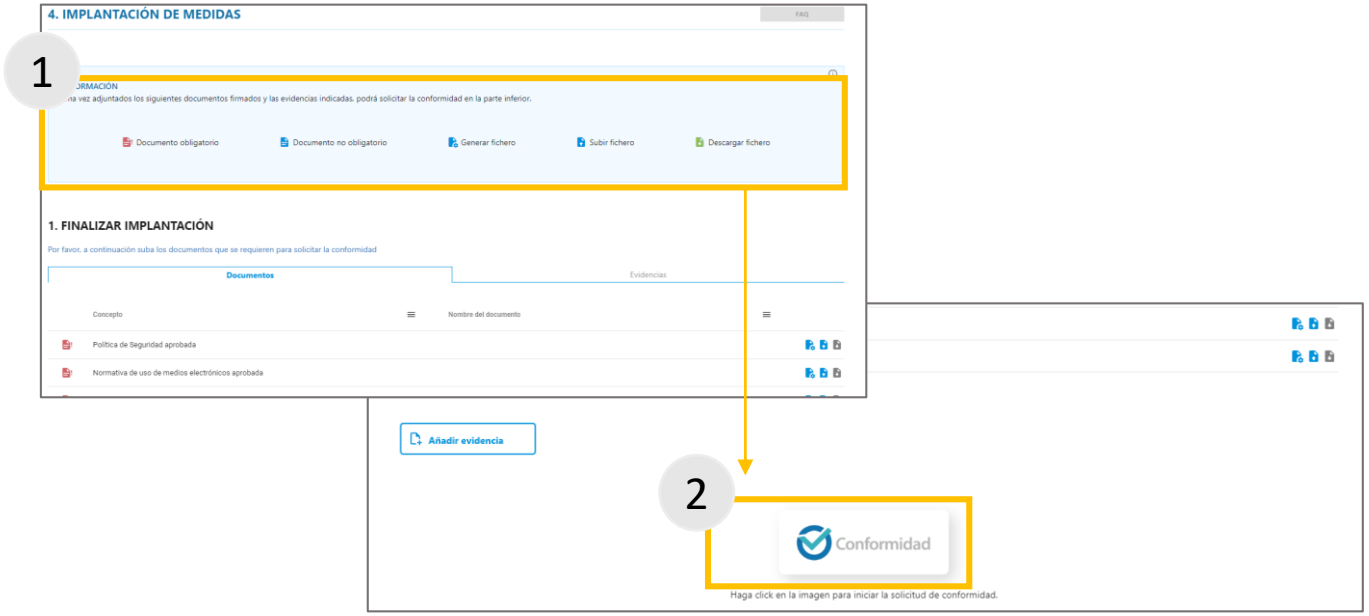
Tenga en cuenta los siguientes aspectos el apartado de "Documentos de Seguridad":

1. En este apartado se pueden **generar los registros necesarios para la implantación**. Además de crear de manera individual, se puede importar desde un fichero Excel, descargable desde la sección. También se puede exportar el listado en formato Excel.

- Los registros que se pueden generar son:
  - **Registros de seguridad:**
    - Inventario de activos
    - Entrada/salida de soportes
  - **Normativa de uso de medios electrónicos**
  - **Documento de Seguridad**
  - **Plan de formación**
  - **Política de firma**

4.4. Secciones µCeENS - Implantación (III)



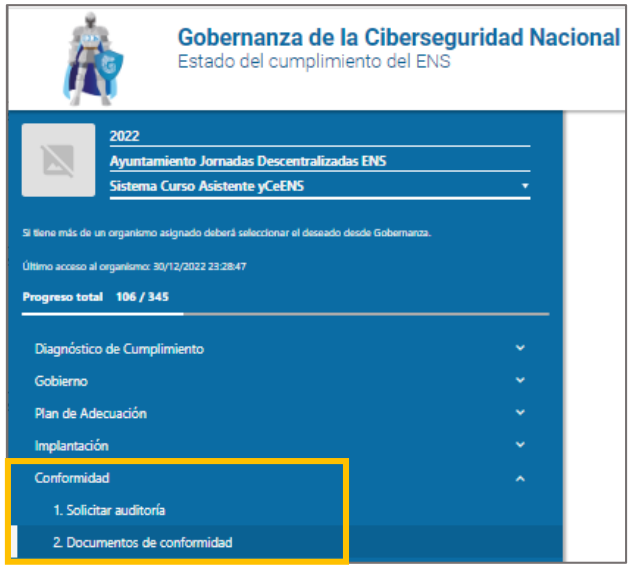


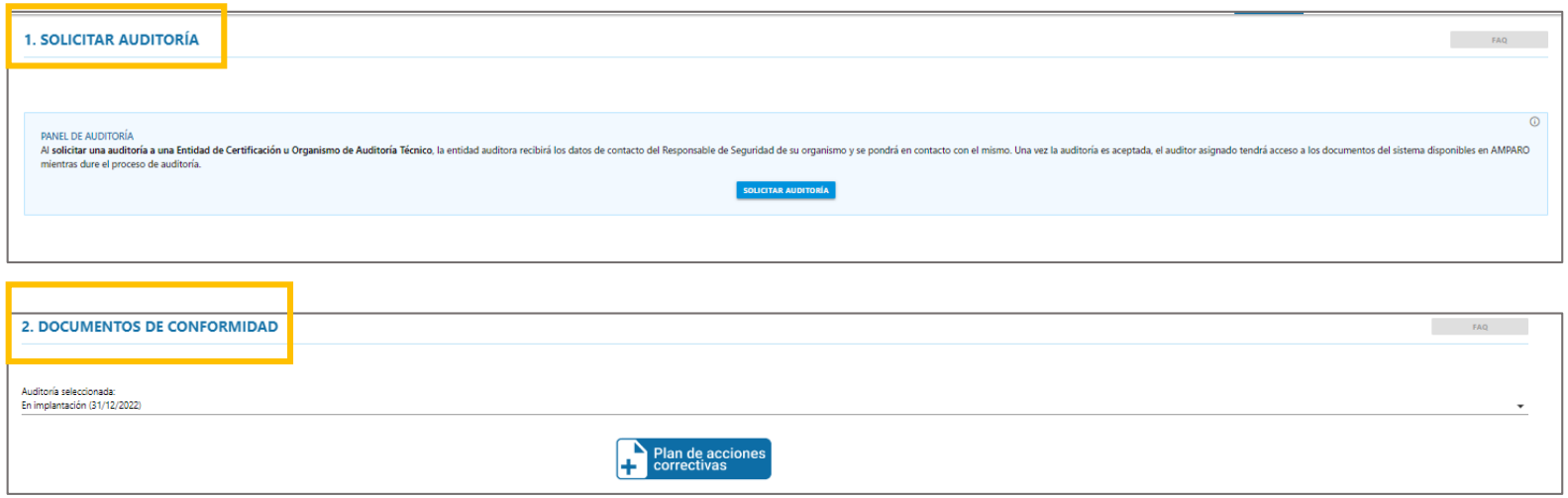
Tenga en cuenta los siguientes aspectos el apartado de "Implantación de medidas":

- En este apartado se **deben incluir los documentos firmados y las evidencias indicadas para poder solicitar la conformidad**.

1. En el caso del **Perfil de Cumplimiento Específico de Requisitos Esenciales** se simplifican las tareas de implantación reduciéndose a lo indicado en la sección 4 de Implantación.
2. Una vez incluidos los documentos y evidencias necesarios, se podrá solicitar la conformidad **pulsando el botón "Conformidad".**

4.4. Secciones µCeENS - Conformidad



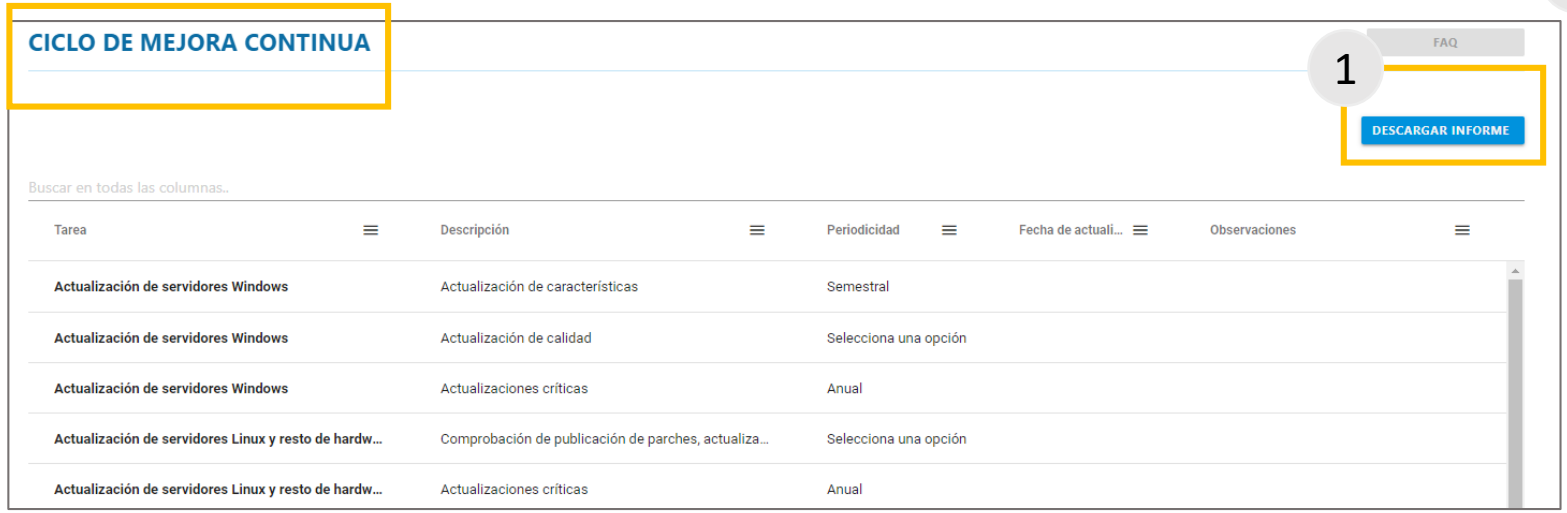


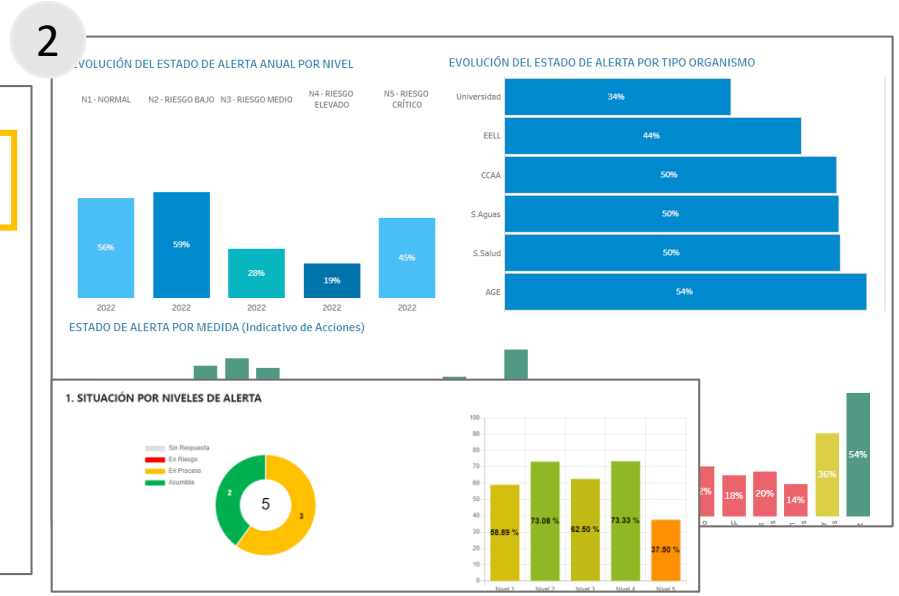
Tenga en cuenta los siguientes aspectos el apartado de "Conformidad":

En este apartado se podrá:

- **Solicitar la auditoría de conformidad** con el ENS en base al Perfil de Cumplimiento Específico para categoría BÁSICA.
- **Ver el estado de la auditoría**: la Entidad de Certificación (EC) o el Órgano de Auditoría Técnica del Sector Público (OAT), tras recibir la solicitud de auditoría, procederá a la realización de la evaluación de las evidencias y la documentación aportada.
- **Comunicarse** con el auditor a través del foro.
- **Realizar** las acciones pertinentes después de la auditoría, como puede ser realizar el **Plan de Acciones Correctivas.**

4.4. Secciones µCeENS - Ciclo de mejora continua





Tenga en cuenta los siguientes aspectos el apartado de "Ciclo de Mejora Continua":

1. Puede descargar el documento "**Lista Mantenimiento del Sistema y Acciones Puntuales"** donde encontrará la realización de tareas de mantenimiento del sistema (actualización de servidores, equipos, revisión de accesos, etc.) que incluye también tareas que garantizan el ciclo de mejora.

    - La reevaluación y actualización periódica de las medidas de seguridad del sistema se consigue mediante acciones puntuales que se presentan cuando haya cambios en el sistema **(nuevo componente en el sistema, nuevo personal, etc.)**

2. En la sección de **Ciclo de mejora continua** se puede **evaluar las capacidades en ciberseguridad y las medidas proactivas de resiliencia** para prevenir ciberataques y resistir ante la amenaza, consiguiendo el triple objetivo:
    - Mantener la **Certificación de Conformidad.**
    - Fomentar la **Mejora Continua.**
    - Alcanzar la **madurez** exigida.

Muchas Gracias

Contacto

normativa@ccn.cni.es

ccn@ccn.cni.es

Páginas Web

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.01.13 11:18:08 +01'00'

ángeles
Formación y Talento en Ciberseguridad

e-ens
ENTORNO DE VALIDACIÓN ENS

μCe ens
Certificación esencial en el ENS

centro criptológico nacional