

Manual μ CeENS Y Requisitos Esenciales



μ Ce
ens

Certificación
esencial en el ENS

Área de Normativa y Servicios de Ciberseguridad



1. ¿Qué es μ CeENS?

- Definición
- Actuaciones principales derivadas de la Metodología.
- Desarrollo de la Metodología: Herramientas de Gobernanza y Soluciones ABS.

2. ¿Quién puede beneficiarse de μ CeENS?

3. ¿Cómo se aplica μ CeENS?

- Fases de la metodología.
- Entregables.

4. Actividades de adopción de μ CeENS

4.1. Cómo acceder a μ CeENS – Portal de Gobernanza

4.2. Cómo crear un sistema

4.3. Cómo acceder al sistema

4.4. Secciones de μ CeENS

- Diagnóstico de Cumplimiento
- Gobierno
- Plan de adecuación
- Implantación
- Conformidad



1. ¿Qué es μ CeENS?

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.

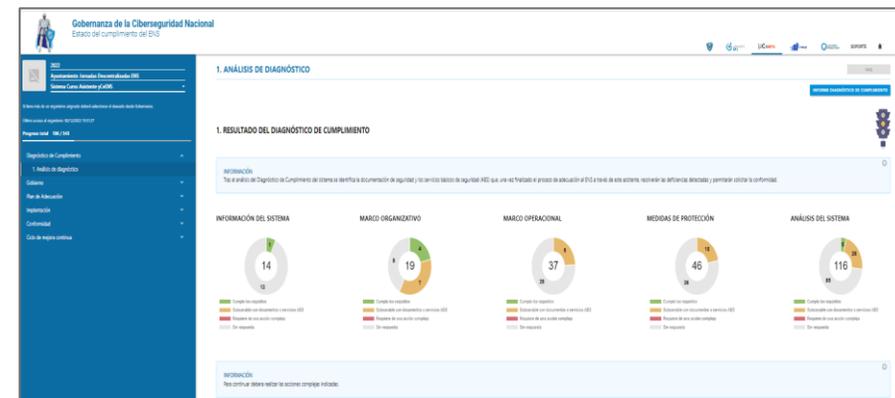
Acompañamiento en base a fases y actuaciones durante el proceso de la Certificación de Conformidad:

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. ¿Quiénes puede beneficiarse de μ CeENS?

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**)



Gobernanza de la Ciberseguridad Nacional
Estado del cumplimiento del ENS

DIAGNÓSTICO DE CUMPLIMIENTO

INFORMACIÓN
Cuestionario previo para conocer las características del sistema y el grado de cumplimiento de las medidas del Esquema Nacional de Seguridad según un Perfil de Cumplimiento Específico en base a unos requisitos esenciales de seguridad.

Una vez completado, el semáforo indicará si es posible abordar la adecuación según el modelo μ CeENS siguiendo el siguiente criterio:

- Cumple los requisitos
- Subsanable con documentos o servicios ABS
- Requiere de una acción compleja

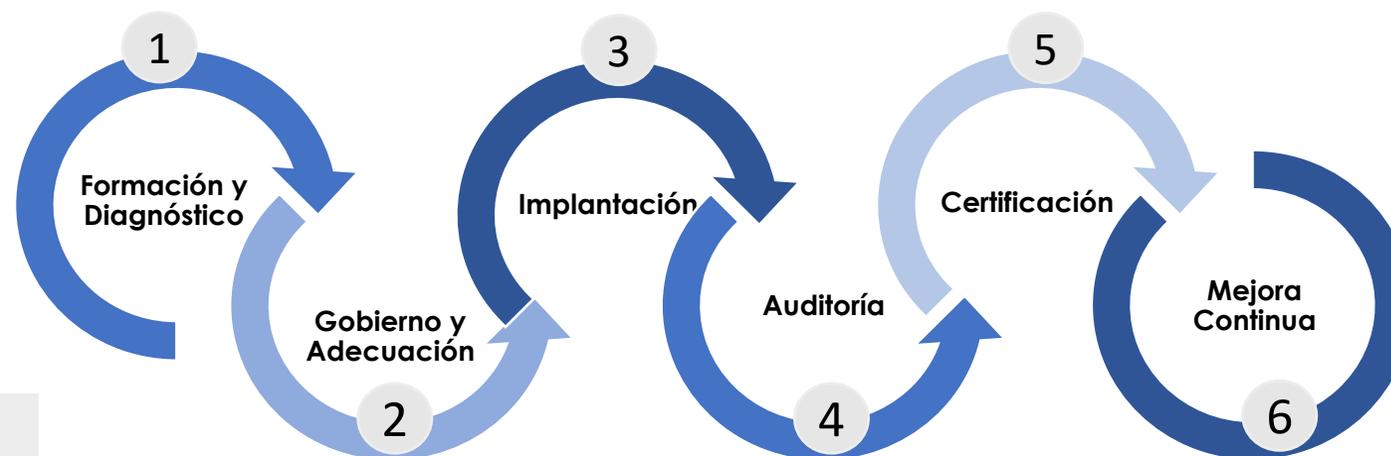
En el apartado de Análisis del Diagnóstico se indican las acciones que será necesario llevar a cabo para afrontar la certificación en el ENS conforme al modelo μ CeENS.

Información del organismo | Marco organizativo | Marco operacional | Medidas de protección

3. ¿Cómo se aplica μ CeENS? (fases)

Implantación de la Metodología μ CeENS 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 μ CeENS? (entregables)

Durante las fases de μ CeENS 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

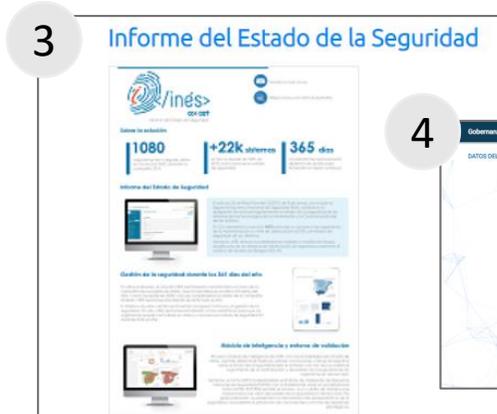
- Medidas y acciones puntuales que propicien el mantenimiento y mejora continua de la seguridad.

4. Actividades de implantación

4.1. Cómo acceder μ CeENS – Portal de Gobernanza

Para acceder a μ CeENS, 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):



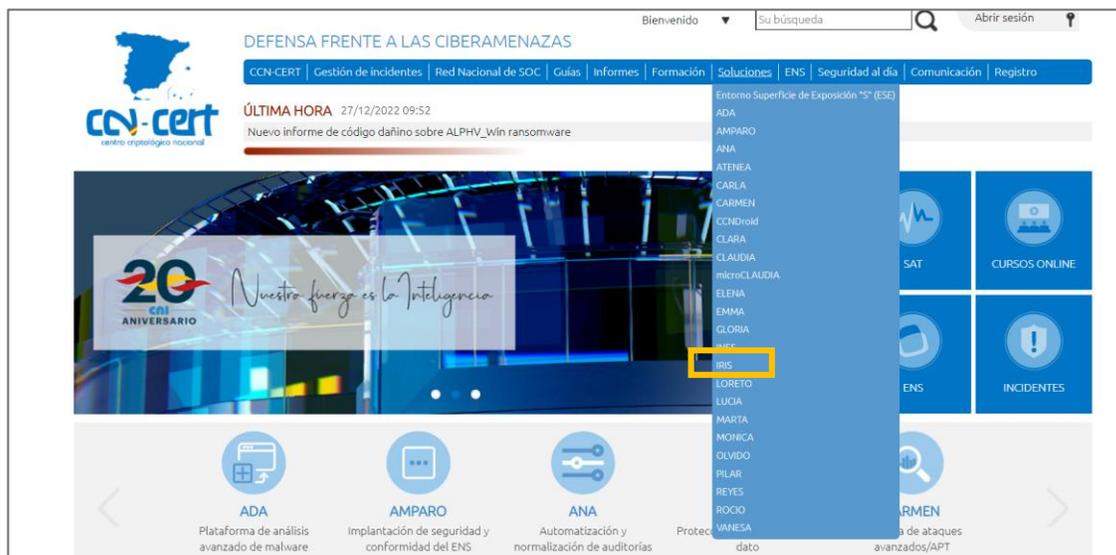
Instrucciones:

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)



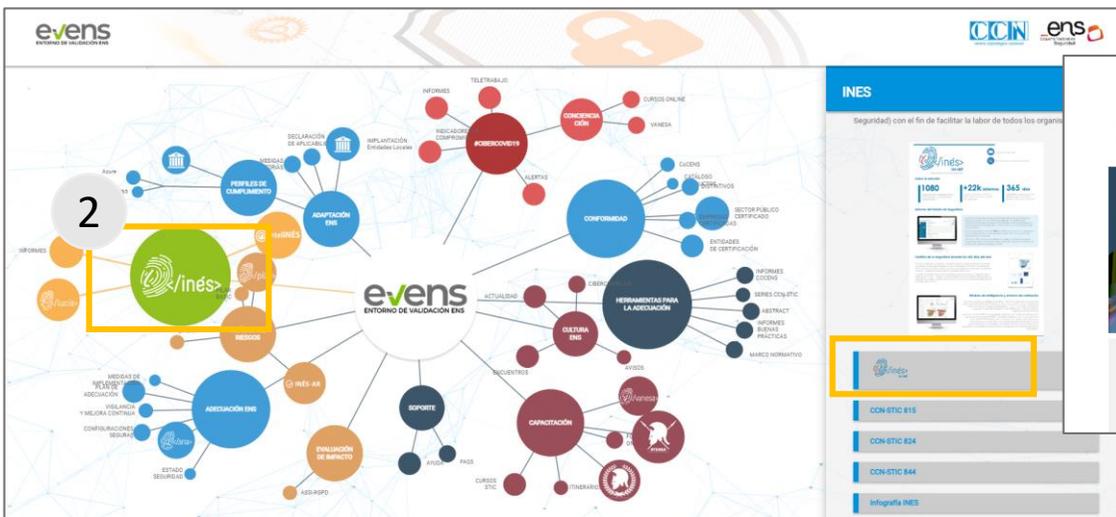
Instrucciones:

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 μ CeENS – 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



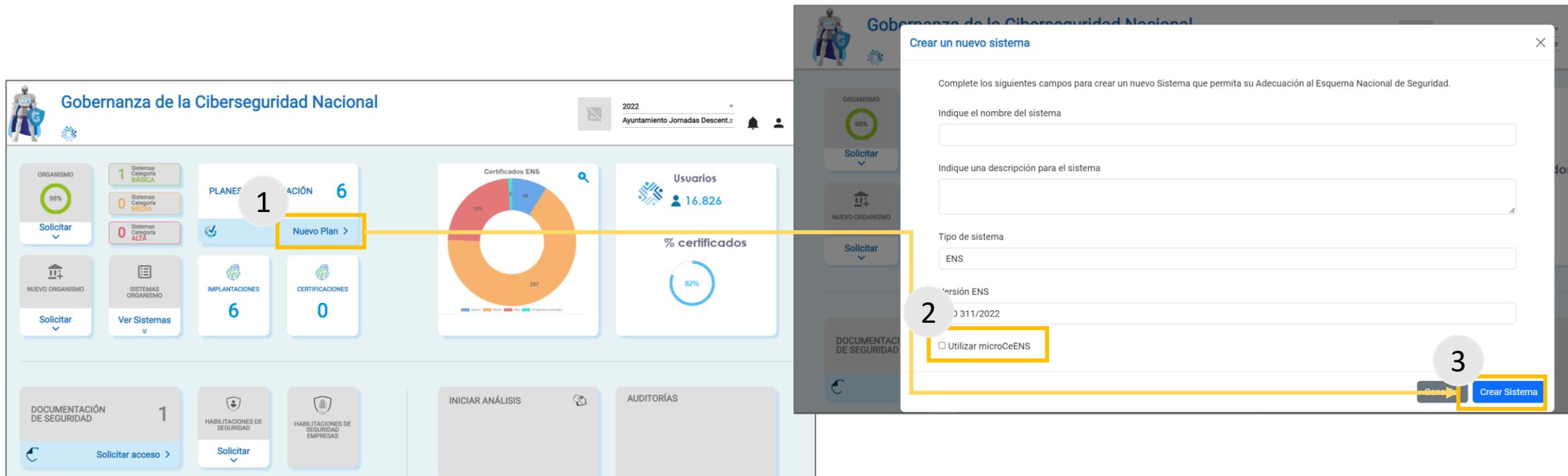
Funcionalidades:

- 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

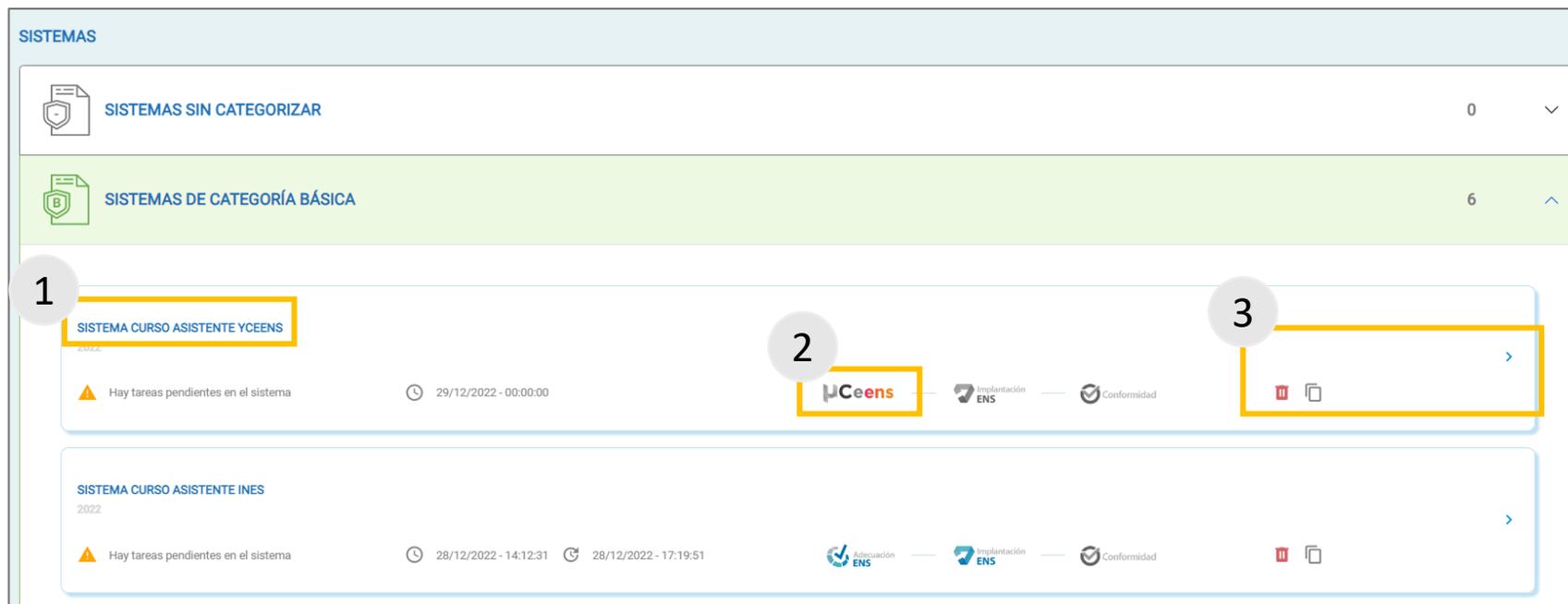


The image shows the μCeENS dashboard with a focus on creating a new system. The main dashboard includes sections for 'ORGANISMO' (98%), 'Sistemas Categoría BÁSICA' (1), 'Sistemas Categoría MEDIA' (0), 'Sistemas Categoría ALTA' (0), 'PLANES DE ADECUACIÓN' (6), 'Certificados ENS' (donut chart), 'Usuarios' (16.826), '% certificados' (82%), 'NUEVO ORGANISMO', 'SISTEMAS ORGANISMO', 'IMPLANTACIONES' (6), 'CERTIFICACIONES' (0), 'DOCUMENTACIÓN DE SEGURIDAD' (1), 'HABILITACIONES DE SEGURIDAD', and 'HABILITACIONES DE SEGURIDAD EMPRESAS'. A 'Nuevo Plan' button is highlighted with a yellow box and a callout '1'. An inset window titled 'Crear un nuevo sistema' is shown, with fields for 'Indique el nombre del sistema', 'Indique una descripción para el sistema', 'Tipo de sistema' (ENS), and 'Versión ENS' (311/2022). A checkbox 'Utilizar microCeENS' is highlighted with a yellow box and a callout '2'. A 'Crear Sistema' button is highlighted with a yellow box and a callout '3'.

Instrucciones:

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

4.3. Cómo acceder al sistema



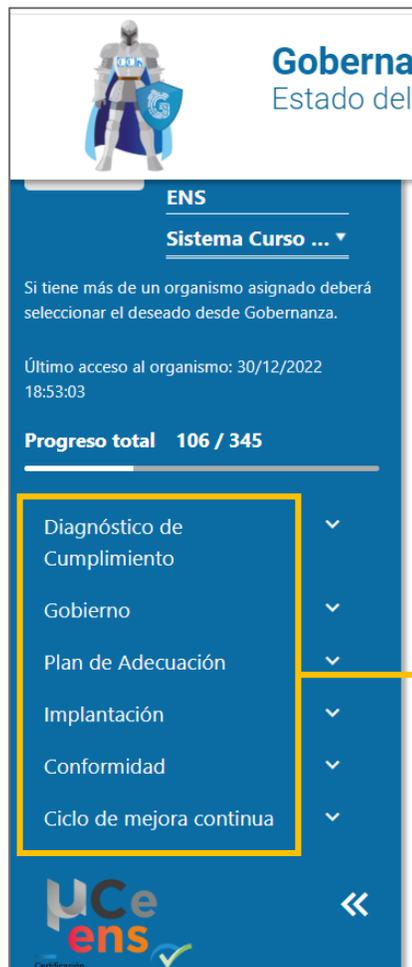
The screenshot displays the 'SISTEMAS' section of the μCeENS interface. It is divided into two main categories: 'SISTEMAS SIN CATEGORIZAR' (0 items) and 'SISTEMAS DE CATEGORÍA BÁSICA' (6 items). The 'SISTEMAS DE CATEGORÍA BÁSICA' section is highlighted in green. Below this, two system cards are shown. The first card, 'SISTEMA CURSO ASISTENTE YCEENS', is highlighted with a yellow box and labeled '1'. It includes a warning icon, the text 'Hay tareas pendientes en el sistema', a clock icon, the date '29/12/2022 - 00:00:00', and a row of icons: μCeens, Implantación ENS, Conformidad, and a red trash can. A blue arrow icon is on the right, labeled '3'. The second card, 'SISTEMA CURSO ASISTENTE INES', is also highlighted with a yellow box and labeled '2'. It includes a warning icon, the text 'Hay tareas pendientes en el sistema', a clock icon, the date '28/12/2022 - 14:12:31', a refresh icon, the date '28/12/2022 - 17:19:51', and a row of icons: Admisión ENS, Implantación ENS, Conformidad, and a red trash can. A blue arrow icon is on the right.

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 μ CeENS



μ CeENS 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)

1

DIAGNÓSTICO DE CUMPLIMIENTO

FAQ

INFORMACIÓN

Cuestionario previo para conocer las características del sistema y el grado de cumplimiento de las medidas del Esquema Nacional de Seguridad según un Perfil de Cumplimiento Específico en base a unos requisitos esenciales de seguridad.

Una vez completado, el semáforo indicará si es posible abordar la adecuación según el modelo μCeENS siguiendo el siguiente criterio:

■ Cumple los requisitos
 ■ Subsanable con documentos o servicios ABS
 ■ Requiere de una acción compleja

En el apartado de Análisis del Diagnóstico se indican las acciones que será necesario llevar a cabo para afrontar la certificación en el ENS conforme al modelo μCeENS.

Información del organismo

Marco organizativo

Marco operacional

2



- **Rojo:** no apto y requiere acción compleja.
- **Ámbar:** apto y tiene deficiencia subsanable.
- **Verde:** apto: sin desviaciones.

INFORMACIÓN

Para continuar deberá realizar las acciones complejas indicadas.

¿Se compromete a realizar las **acciones complejas** pertinentes identificadas tras el diagnóstico?

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 μ CeENS - Diagnóstico de cumplimiento (II)

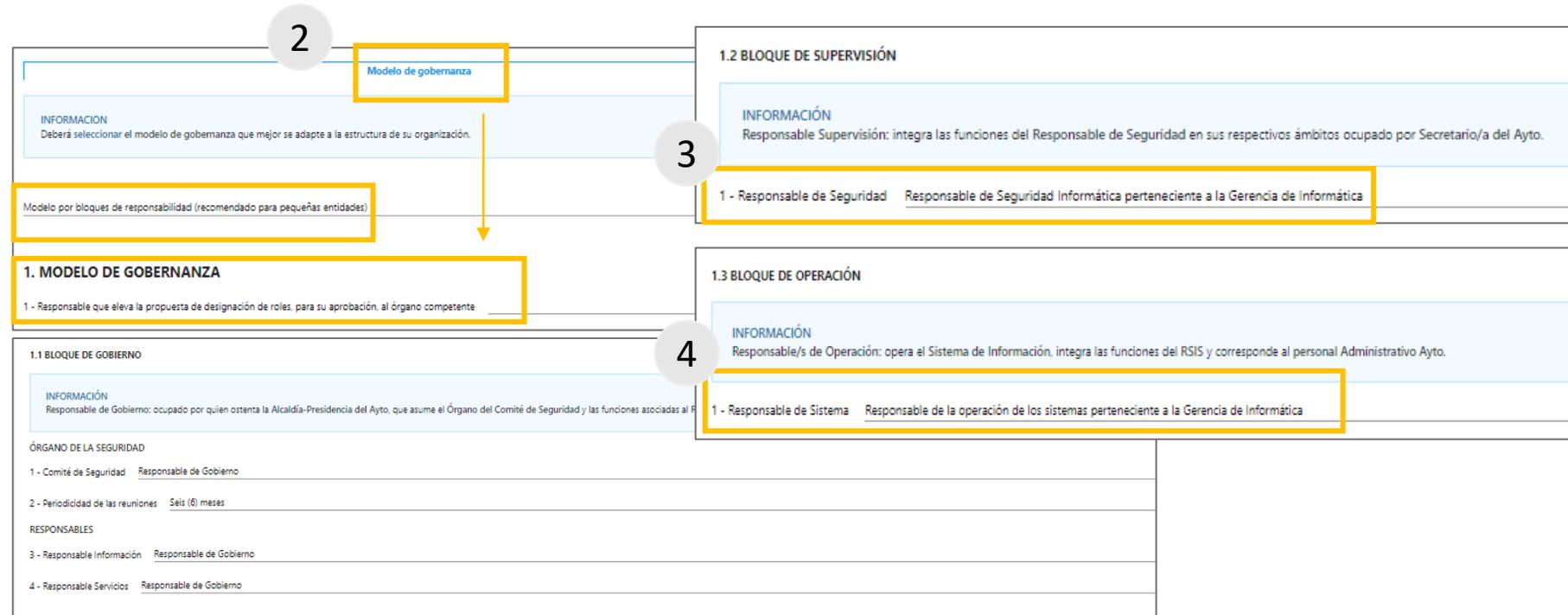
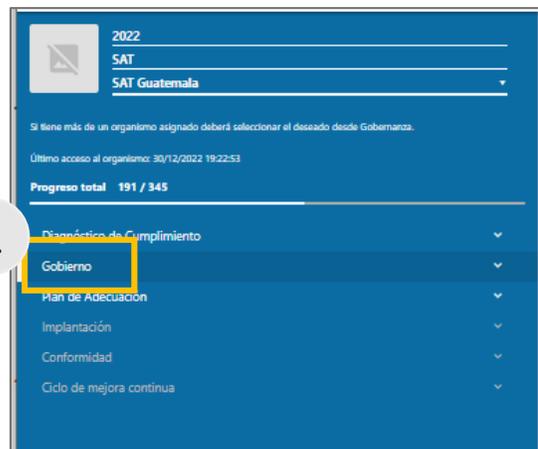


Instrucciones:

- En el apartado de **Análisis de diagnóstico “Resultados del diagnóstico de cumplimiento”** 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.
- En esta sección se podrán **solicitar los Servicios ABS que se han identificados como necesarios** para subsanar las deficiencias detectadas en la sección anterior.
- 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 μ CeENS - Modelo de Gobernanza (I)

Modelo de Gobernanza por Bloques de Responsabilidad



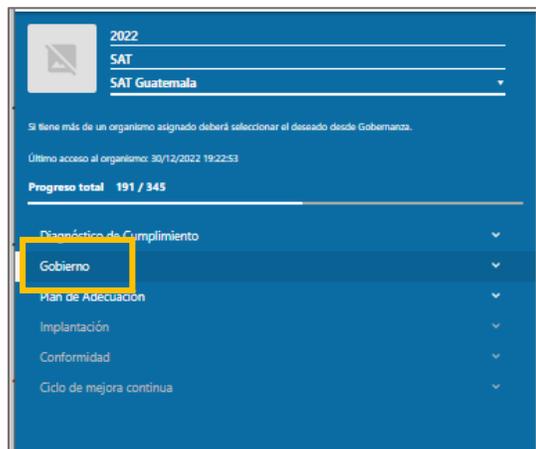
Instrucciones:

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



Modelo Estándar

1. MODELO DE GOBERNANZA Mostrar todos los comentarios

1 - Responsable que eleva la propuesta de designación de roles, para su aprobación, al órgano competente n.a.

1.1 ROLES

1 - Responsable/s de los Servicios _____

2 - Responsable/s de la Información _____

INFORMACIÓN
Podrían 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.

3 - Delegado/a de Protección de Datos _____

INFORMACIÓN
Interlocutor con la AEPD (por ejemplo, el Jefe de Servicio de Administración Electrónica y Transparencia, si lo hay).

4 - Responsable de Seguridad _____

5 - Responsable del Sistema _____

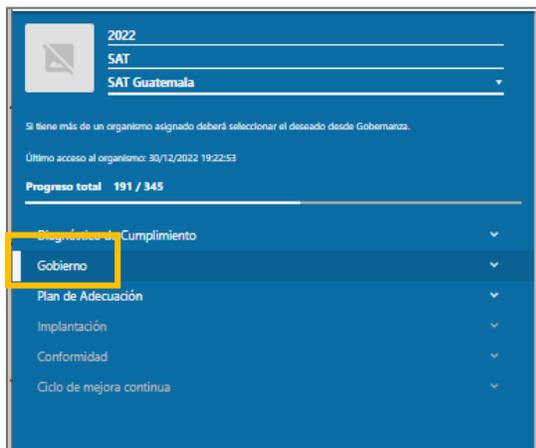
Para cumplimentar esta sección tenga en cuenta los siguientes aspectos:

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



2. ORGANO DE LA SEGURIDAD DE LA INFORMACION

El Comité de Seguridad de la Información estará compuesto por:

1 - Presidente/a _____

INFORMACIÓN
Persona física que asumirá la responsabilidad formal de sus actos, como puede ser el Secretario General del organismo.

2 - Secretario/a Responsable de la Seguridad

3 - Periodicidad de las reuniones Seis (6) meses

4 - ¿Cómo se ha comunicado la designación del comité de seguridad a sus miembros? _____

5 - Revisión de los miembros del comité (años) _____

MIEMBROS - VOCALES

1 - Responsable/s de la Información Sí No n.a.

2 - Responsable/s los Servicios Sí No n.a.

3 - Responsable del Sistema _____

4 - El responsable del sistema pertenece al comité: Sí No

5 - Responsable de Seguridad _____

6 - El responsable de seguridad pertenece al comité Sí No

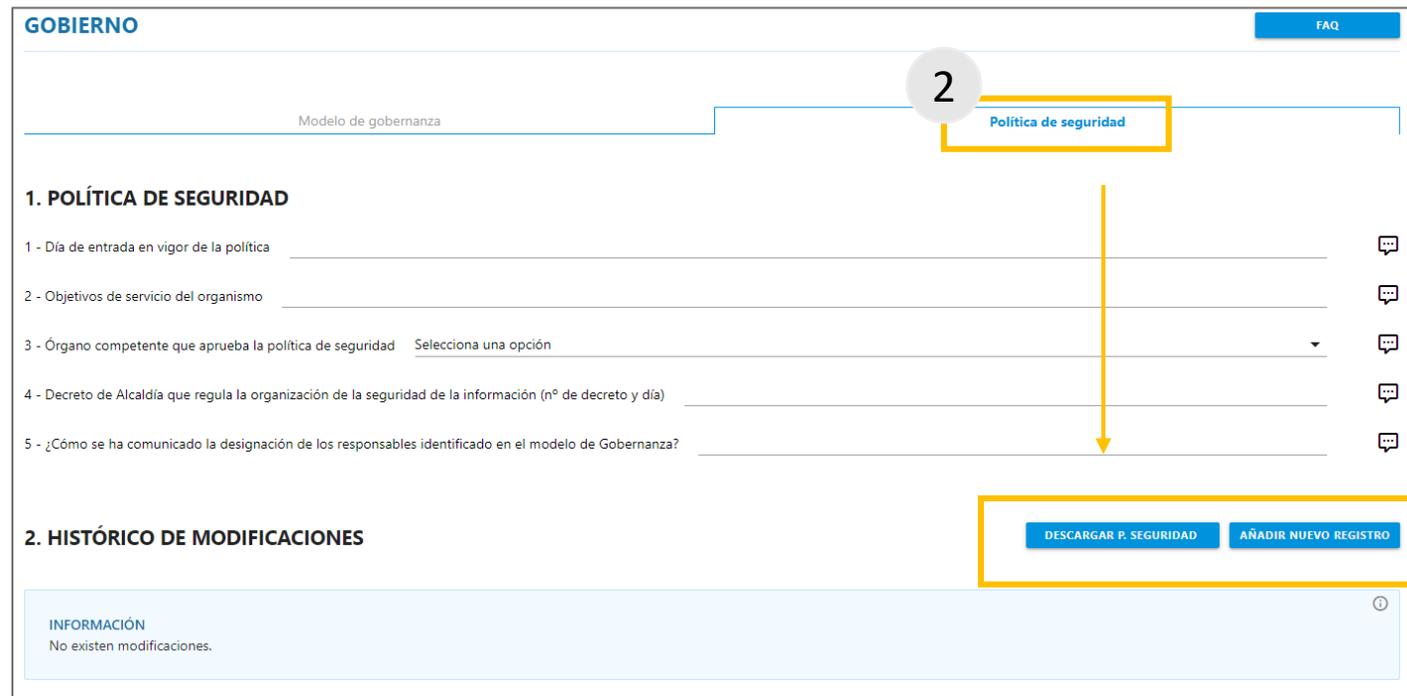
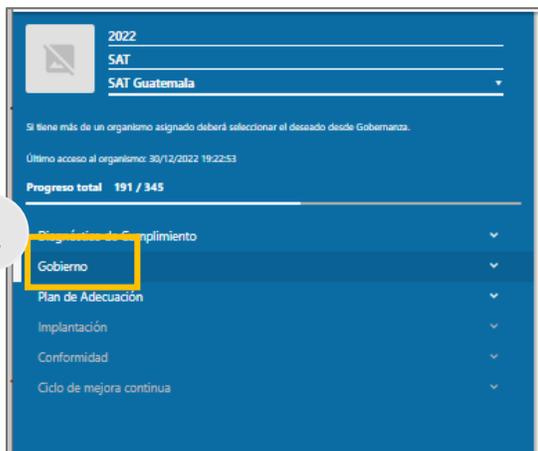
7 - Delegado de Protección de datos Sí No

8 - Otros _____

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

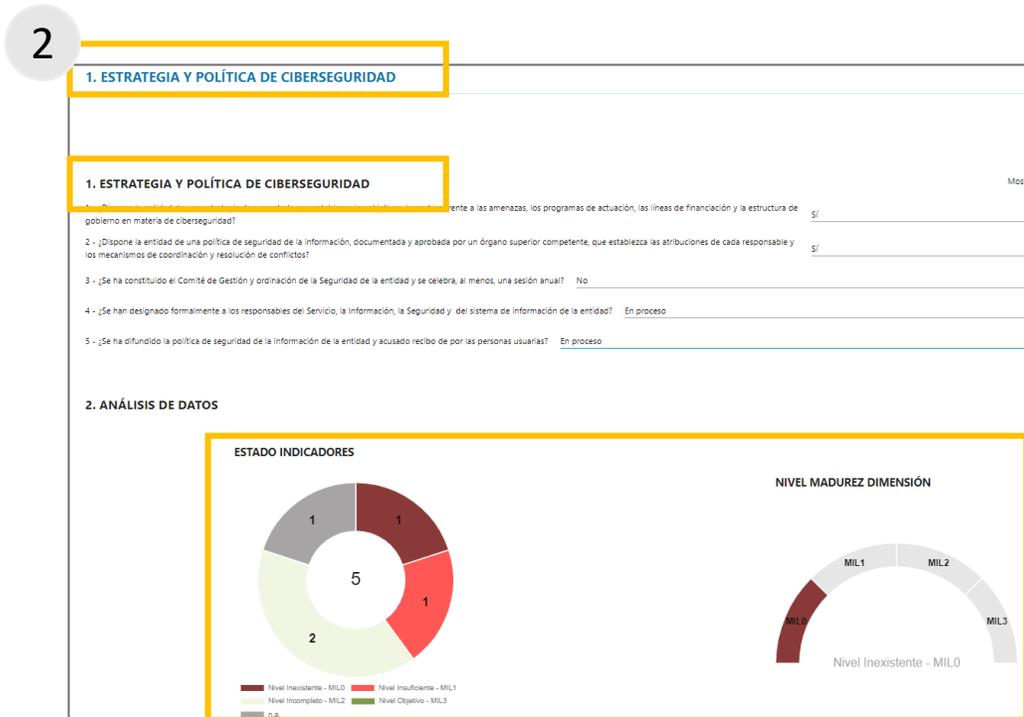
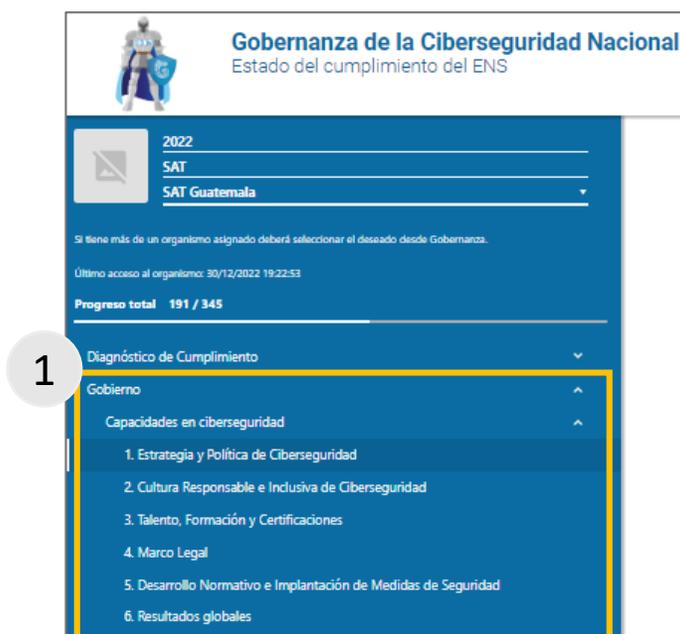


Instrucciones:

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 μ CeENS - 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 μ CeENS - Plan de Adecuación (I)

The screenshot shows the user interface of the μ CeENS system. At the top, it displays 'Gobernanza de la' and 'Estado del cumplimiento'. Below this, there is a navigation menu with several items: '2022', 'Ayuntamiento Jornadas Descentralizadas ENS', and 'Sistema Curso Asistente yCeENS'. A progress bar indicates 'Progreso total 106 / 345'. The main menu items are: 'Diagnóstico de Cumplimiento', 'Gobierno', 'Plan de Adecuación', 'Implantación', 'Conformidad', and 'Ciclo de mejora continua'. The 'Plan de Adecuación' item is expanded, showing a list of six sub-items: '1. Información del Sistema', '2. Alcance', '3. Categorización del Sistema', '4. Declaración de aplicabilidad/Perfil de Cumplimiento', '5. Documentos', and '6. Fin del Plan de Adecuación'. A yellow box highlights this entire list, and a circled '1' is placed to the left of it. The μ CeENS logo is visible in the bottom left corner.

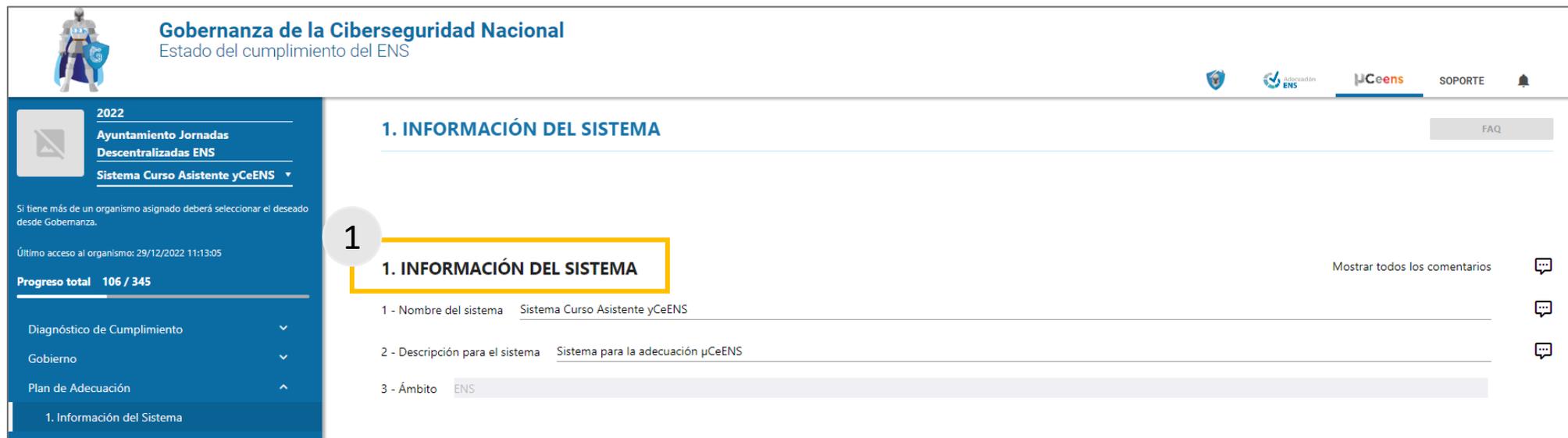
Para cumplimentar esta sección tenga en cuenta los siguientes aspectos:

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)



The screenshot displays the user interface of the μCeENS system. At the top, it reads 'Gobernanza de la Ciberseguridad Nacional' and 'Estado del cumplimiento del ENS'. The left sidebar contains navigation options: '2022', 'Ayuntamiento Jornadas Descentralizadas ENS', 'Sistema Curso Asistente yCeENS', 'Progreso total 106 / 345', and menu items for 'Diagnóstico de Cumplimiento', 'Gobierno', 'Plan de Adecuación', and '1. Información del Sistema'. The main content area is titled '1. INFORMACIÓN DEL SISTEMA' and features a yellow box with the number '1' highlighting the section title. Below this, three fields are visible: '1 - Nombre del sistema' (Sistema Curso Asistente yCeENS), '2 - Descripción para el sistema' (Sistema para la adecuación μCeENS), and '3 - Ámbito' (ENS). A 'FAQ' button is located in the top right corner of the main content area, and a 'Mostrar todos los comentarios' link with a comment icon is on the right side.

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 μ CeENS - Plan de Adecuación (IV)

3. CATEGORIZACIÓN DEL SISTEMA

FAQ

INFORMACIÓN
Recuerde que debe categorizar el sistema o añadir uno o más servicios en la sección "2. Alcance".

[DESCARGAR CATEGORIZACIÓN](#)

1. SISTEMA

1 - Nivel máximo de Confidencialidad (C)

2 - Nivel máximo de Integridad (I)

3 - Nivel máximo de Trazabilidad (T)

4 - Nivel máximo de Autenticidad (A)

5 - Nivel máximo de Disponibilidad (D)

2. CATEGORÍA DEL SISTEMA

La categoría del sistema es **BÁSICA**

“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 μ CeENS - Plan de Adecuación (V)

4. DECLARACIÓN DE APLICABILIDAD/PERFIL DE CUMPLIMIENTO

[FAQ](#)

INFORME
TABLAS DE RIESGOS
DESCARGAR DECLARACIÓN
DESCARGAR PERFIL DE CUMPLIMIENTO

1. MEDIDAS

INFORMACIÓN

En esta sección puede adaptar la declaración de aplicabilidad provisional, realizando las siguientes acciones:

- Modificar la aplicabilidad de las medidas
- Añadir medidas nuevas
- Añadir medidas compensatorias y complementarias de vigilancia
- Especificar los criterios de aplicabilidad de las medidas

La categoría actual del sistema es: BÁSICA

LEYENDA

Medida del Anexo II	Aplica	Compensatoria/Complementaria	Categoría/Nivel	Refuerzos
[org.1] Política de seguridad	Aplica	-	Básica	🗨
[org.2] Normativa de seguridad	Aplica	-	Básica	🗨

RIESGO POTENCIAL
(antes de aplicar medidas de seguridad)



Riesgo medio

RIESGO RESIDUAL
(después de aplicar medidas de seguridad)



Riesgo asumible

■ Riesgo despreciable
■ Riesgo asumible
■ Riesgo medio
■ En riesgo

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

En este apartado se podrá:

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

4.4. Secciones μCeENS - Plan de Adecuación (VI)



5. DOCUMENTOS

1. DOCUMENTOS DISPONIBLES PARA SU DESCARGA

INFORMACIÓN
Estos documentos deberán descargarse y firmarse por la auditoría competente para adjuntarlos en la sección 4. Implantación de medidas.

Documentos para la adecuación | Otros documentos

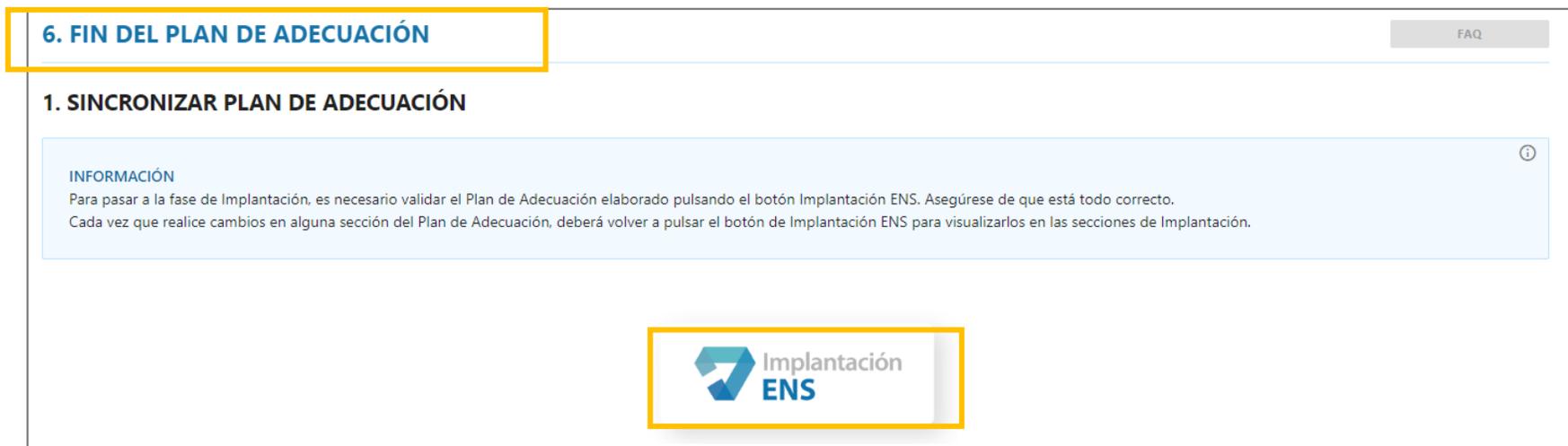
Concepto	Nombre del documento	Extensión	Enlace
Política de seguridad	PS_Ayuntamiento Jornadas Descentralizadas ENS	docx	DESCARGAR
Declaración Aplicabilidad Definitiva – Perfil de Cumplimiento	DADefinitiva – PerfilDeCumplimiento_Sistema Curso Asistente yCeENS	docx	DESCARGAR
Categorización del Sistema	CCN-STIC-890 Anexo II. Categorización_Sistema Curso Asistente yCeENS	docx	DESCARGAR
Informe simplificado de riesgos	Análisis_de_Riesgos_Sistema Curso Asistente yCeENS	docx	DESCARGAR

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 μ CeENS - Plan de Adecuación (VII)

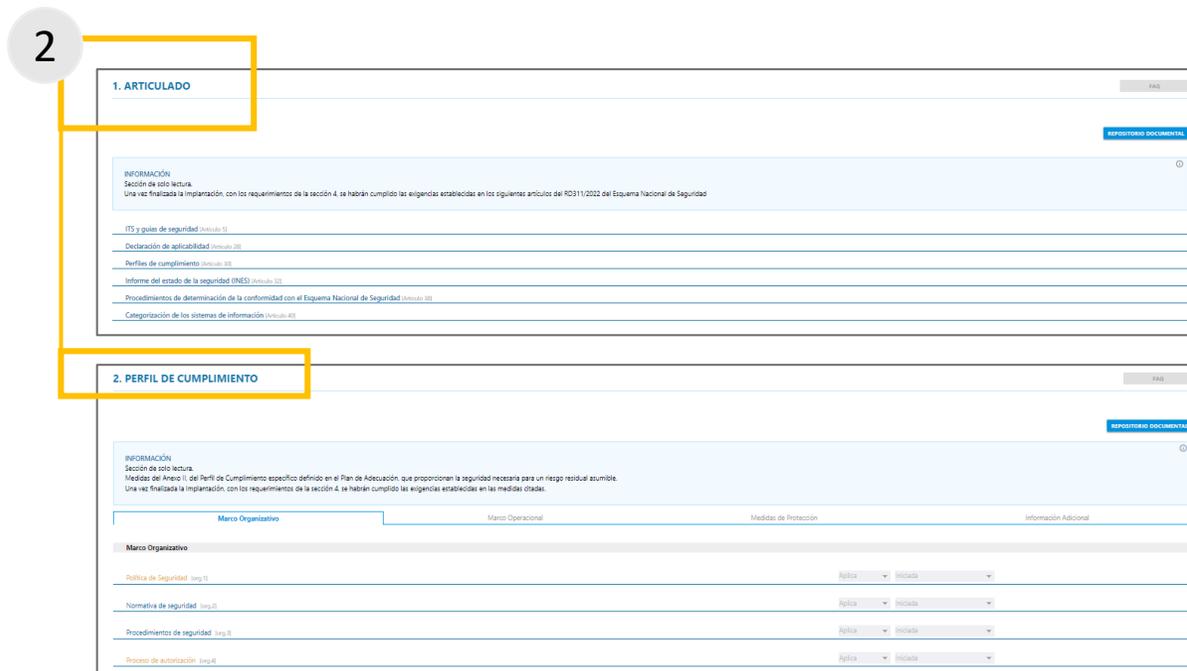
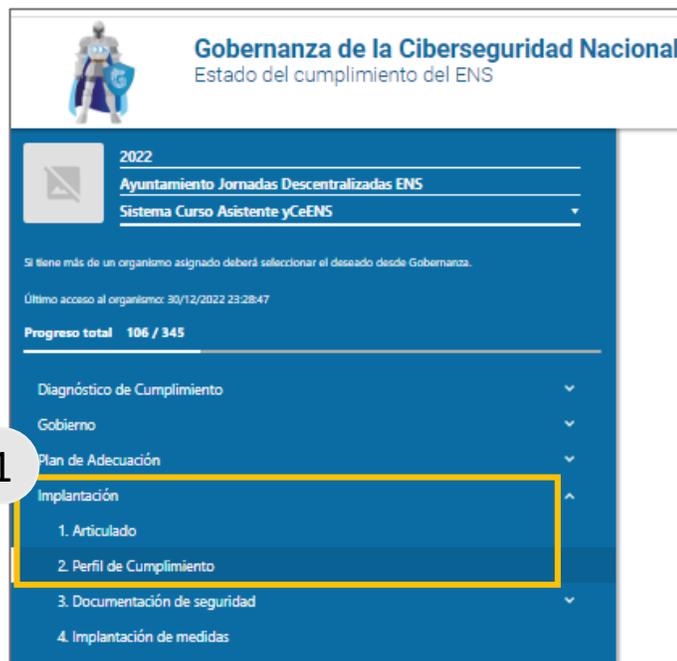


The screenshot shows a software interface with a yellow border. At the top left, a yellow box highlights the text '6. FIN DEL PLAN DE ADECUACIÓN'. To the right of this box is a grey button labeled 'FAQ'. Below the main title, there is a sub-section '1. SINCRONIZAR PLAN DE ADECUACIÓN'. Underneath this, a light blue information box contains the text: 'INFORMACIÓN Para pasar a la fase de Implantación, es necesario validar el Plan de Adecuación elaborado pulsando el botón Implantación ENS. Asegúrese de que está todo correcto. Cada vez que realice cambios en alguna sección del Plan de Adecuación, deberá volver a pulsar el botón de Implantación ENS para visualizarlos en las secciones de Implantación.' At the bottom center of the interface, a button labeled 'Implantación ENS' is highlighted with a yellow border. The button features a blue icon of a right-pointing arrow inside a square.

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 μ CeENS - 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)

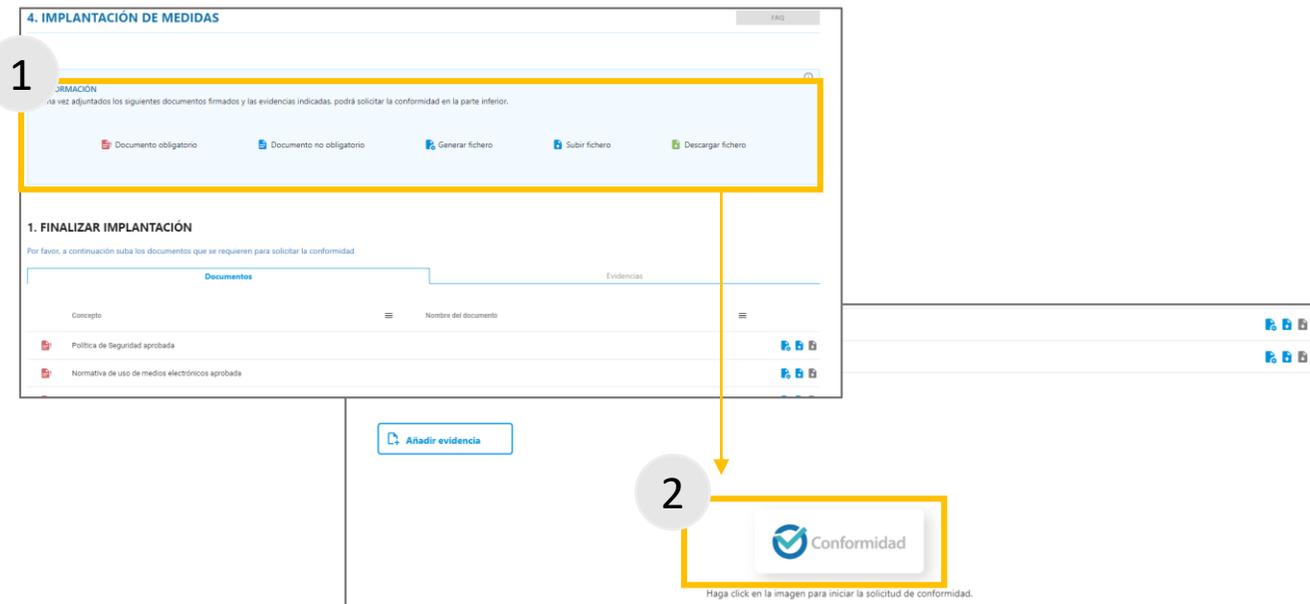
Tenga en cuenta los siguientes aspectos el apartado de “Documentos de Seguridad”:

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
- **Documento de Seguridad**
- **Plan de formación**
- **Política de firma**
- **Normativa de uso de medios electrónicos**

4.4. Secciones μCeENS - Implantación (III)

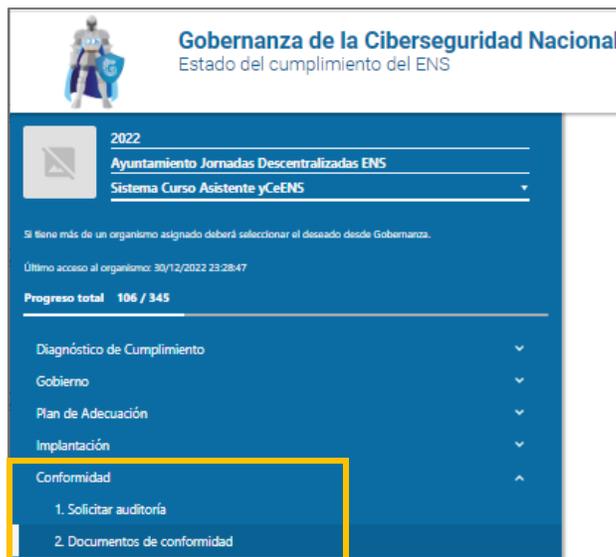


Tenga en cuenta los siguientes aspectos el apartado de “Implantación de medidas”:

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

- 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.
- Una vez incluidos los documentos y evidencias necesarios, se podrá solicitar la conformidad **pulsando el botón “Conformidad”**.

4.4. Secciones μ CeENS - Conformidad



Gobernanza de la Ciberseguridad Nacional
Estado del cumplimiento del ENS

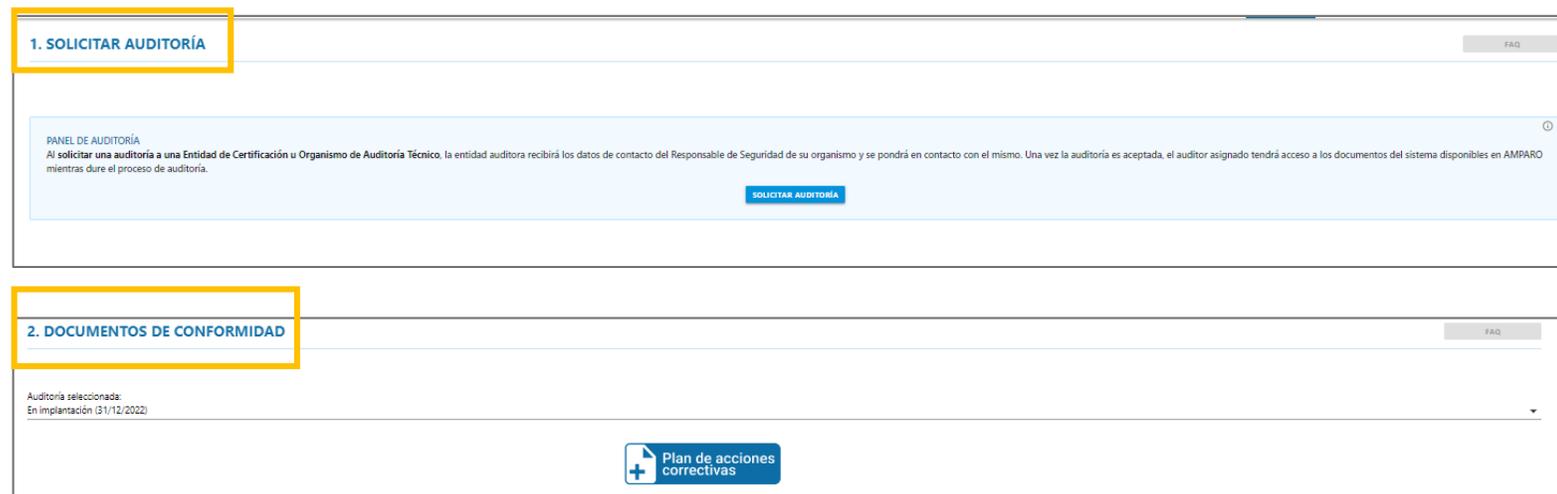
2022
Ayuntamiento Jornadas Descentralizadas ENS
Sistema Curso Asistente yCeENS

Si tiene más de un organismo asignado deberá seleccionar el deseado desde Gobernanza.

Último acceso al organismo: 30/12/2022 23:28:47

Progreso total 106 / 345

- Diagnóstico de Cumplimiento
- Gobierno
- Plan de Adecuación
- Implantación
- Conformidad**
 - 1. Solicitar auditoría
 - 2. Documentos de conformidad



1. SOLICITAR AUDITORÍA

PANEL DE AUDITORÍA
Al solicitar una auditoría a una Entidad de Certificación u Organismo de Auditoría Técnico, la entidad auditora recibirá los datos de contacto del Responsable de Seguridad de su organismo y se pondrá en contacto con el mismo. Una vez la auditoría es aceptada, el auditor asignado tendrá acceso a los documentos del sistema disponibles en AMPARO mientras dure el proceso de auditoría.

SOLICITAR AUDITORÍA

2. DOCUMENTOS DE CONFORMIDAD

Auditoría seleccionada:
En Implantación (31/12/2022)

Plan de acciones correctivas

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

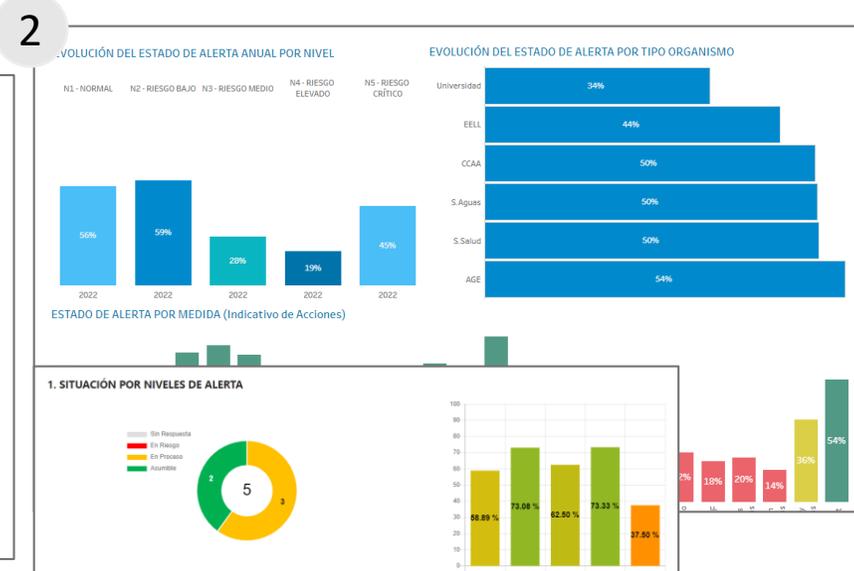
CICLO DE MEJORA CONTINUA

FAQ
DESCARGAR INFORME

1

Buscar en todas las columnas.

Tarea	Descripción	Periodicidad	Fecha de actuali...	Observaciones
Actualización de servidores Windows	Actualización de características	Semestral		
Actualización de servidores Windows	Actualización de calidad	Selecciona una opción		
Actualización de servidores Windows	Actualizaciones críticas	Anual		
Actualización de servidores Linux y resto de hardw...	Comprobación de publicación de parches, actualiza...	Selecciona una opción		
Actualización de servidores Linux y resto de hardw...	Actualizaciones críticas	Anual		



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

