

Manual de uso solución DOCSEG



Mayo 2025



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022

Fecha de Edición: mayo de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
2. OBJETIVO.....	4
3. SOLUCIÓN DOCSEG	4
3.1 ACCESO.....	4
3.2 FORMULARIO DE ALTA.....	7
4. CREACION DE SISTEMAS.....	8
4.1 ELIMINACIÓN DE SISTEMAS	11
5. RELLENADO DE LA DOCUMENTACIÓN	12
6. SECCIONES.....	12
6.1 SECCIÓN INFORMACIÓN DEL SISTEMA	13
6.2 SECCIÓN DOCUMENTACIÓN	13
6.3 DATOS DE SISTEMA	14
6.3.1 DESCRIPCIÓN	14
6.4 ANÁLISIS DE RIESGOS Y AMENAZAS.....	21
6.4.1 ANÁLISIS DE RIESGOS Y AMENAZAS.....	21
6.4.2 OTROS FICHEROS.....	21
6.5 ORGANIZACIÓN DE LA SEGURIDAD	22
6.5.1 SEGURIDAD DOCUMENTAL	22
6.5.2 RESPONSABILIDADES, ROLES Y USUARIOS.....	22
6.5.3 ESTRUCTURA ORGÁNICA.....	24
6.6 CONFIGURACIÓN DEL SISTEMA	25
6.6.1 EQUIPOS	25
6.6.2 PERIFÉRICOS	27
6.6.3 SERVIDORES.....	28
6.6.4 ELECTRÓNICA DE RED.....	29
6.6.5 SERVICIOS TIC	30
6.6.6 PROTOCOLOS Y PUERTOS.....	31
6.6.7 HERRAMIENTAS DE SEGURIDAD	32
6.6.8 APLICACIONES	33
6.7 SEGURIDAD DEL SISTEMA	33
6.8 GESTIÓN DE LA SEGURIDAD TIC.....	36
6.8.1 ENTRADA Y SALIDA DE DOCUMENTACIÓN	36
6.8.2 DISPOSITIVOS REMOVIBLES	38
6.8.3 COPIAS DE SEGURIDAD	39
6.8.4 GESTIÓN DE INCIDENTES.....	39
6.8.5 INFORME ANUAL DE ACREDITACIÓN	41
6.8.6 GESTIÓN DE USUARIOS	41
6.8.7 MANTENIMIENTO DEL SISTEMA	41
6.8.8 GESTIÓN DE ETIQUETAS	41
6.9 REPOSITORIO DOCUMENTAL	42
6.10 SOLICITUD DE ACREDITACIÓN.....	42
6.10.1 TRAMITACIÓN	42
6.10.2 HISTÓRICO	43

1. INTRODUCCIÓN

De conformidad con la Ley 9/1968, de 5 de abril, sobre secretos oficiales, la información clasificada que es manejada por un sistema de información debe protegerse contra la pérdida de confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad, ya sea de forma accidental o intencionada.

Como garantía de protección, dichos sistemas deben acreditarse según lo establecido en la Política de Seguridad de las TIC, señalada en la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI) y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN).

Dicho proceso de acreditación consta de varias acciones a realizar, siendo una de ellas la recopilación y envío por parte de la entidad solicitante de la documentación de seguridad del sistema que propone acreditar.

La solución DOCSEG es únicamente válida para sistemas aislados, con un grado máximo de clasificación de **DIFUSIÓN LIMITADA**.

Para normalizar, facilitar y agilizar el proceso de envío de documentación, El Centro Criptológico Nacional ha desarrollado la solución DOCSEG, que permite a los usuarios cargar la documentación del sistema a acreditar de manera segura.

2. OBJETIVO

El objetivo de la presente guía es mostrar al usuario el uso de la solución DOCSEG y el producto final obtenido una vez se completa el proceso de carga de documentación.

3. SOLUCIÓN DOCSEG

3.1 ACCESO

El acceso a DOCSEG se realiza exclusivamente a través de cl@ve.

Se deberá acceder a la siguiente url:

- <https://gobernanza.ccn-cert.cni.es>

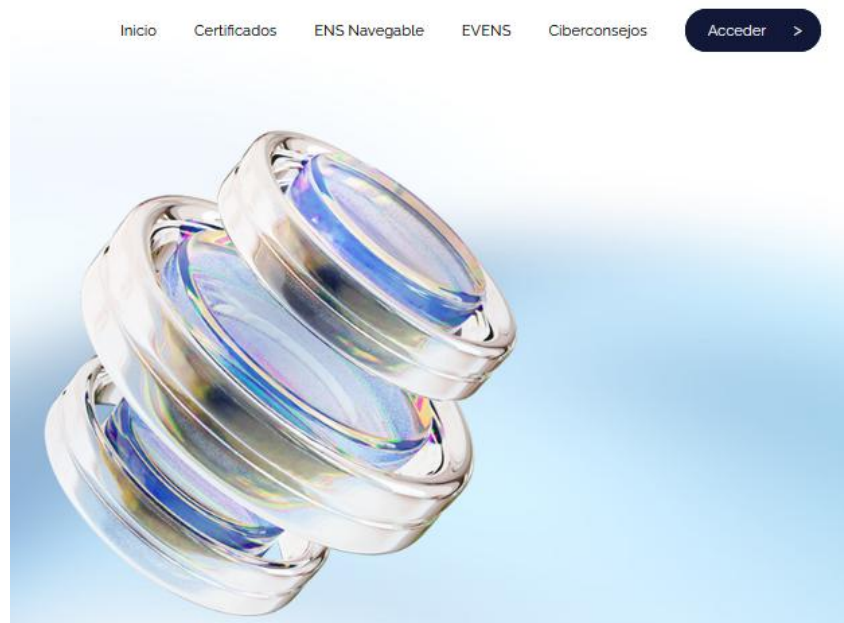


Ilustración 1. Detalle del botón acceder dentro del inicio de GOBERNANZA.

Una vez se haya accedido, para iniciar el proceso de autenticación, se deberá pulsar sobre el texto “Acceder”, situado en la esquina superior derecha.

Al pulsar sobre él, se redirigirá a la siguiente pantalla de autenticación:



Iniciar Sesión

Bienvenido al portal de Gobernanza



Acceder >

Volver

Acceso restringido >

Ilustración 2. Pantalla de acceso con cl@ve.

Al pulsar sobre el botón “Acceder”, el usuario será redirigido a la pasarela de cl@ve, donde completará el proceso de autenticación:

Plataforma de identificación para las Administraciones

Seleccione el método de identificación de Cl@ve

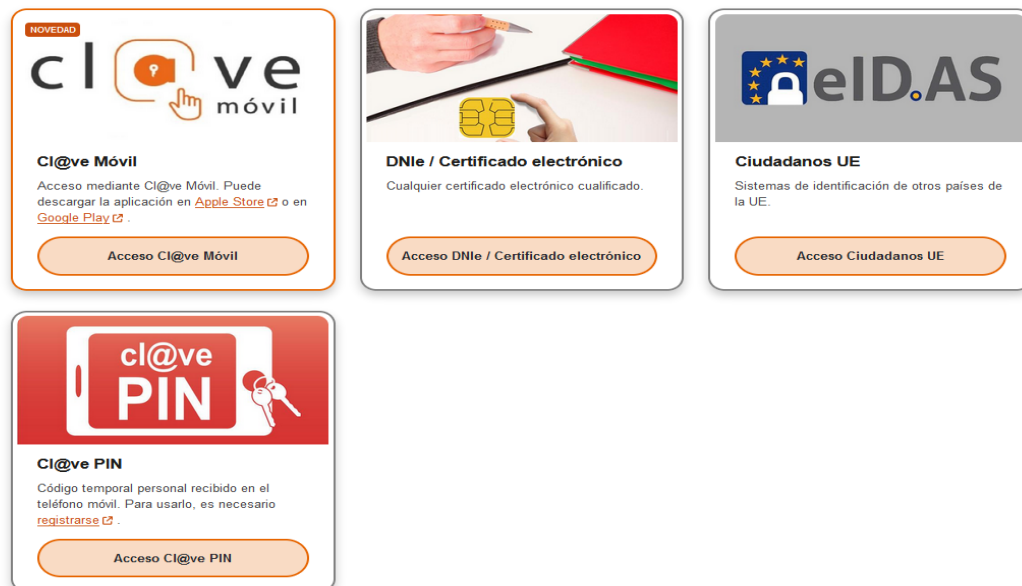


Ilustración 3. Pasarela cl@ve.

Una vez completado el proceso de autenticación, existen dos posibilidades:

- El usuario ya poseía acceso, por lo que será redirigido a la pantalla principal de Gobernanza para usuarios autenticados.

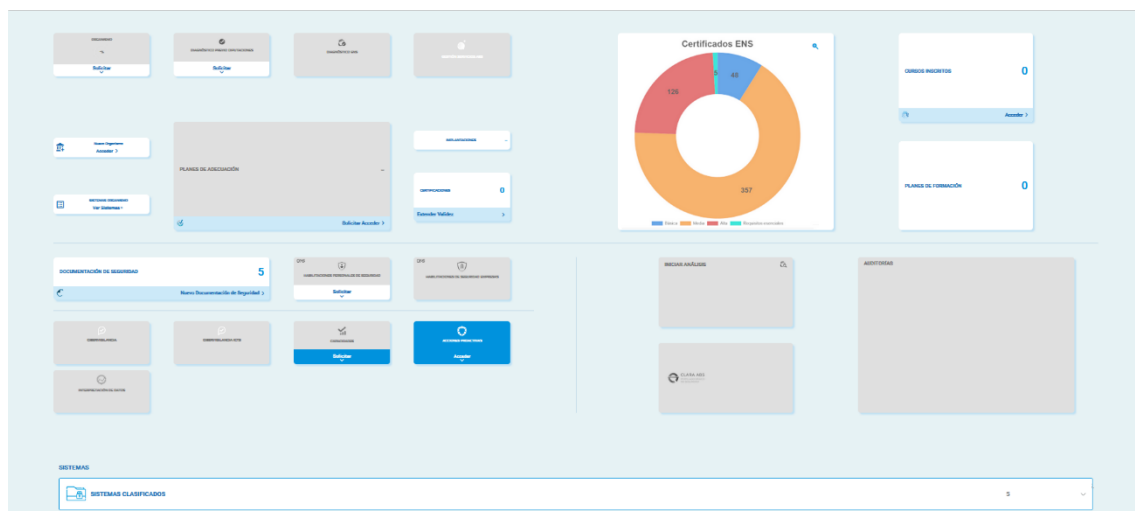


Ilustración 4. Acceso a la pantalla principal de usuario autenticado.

- El usuario es nuevo y todavía no posee acceso, por lo que será redirigido al formulario de alta en la solución:

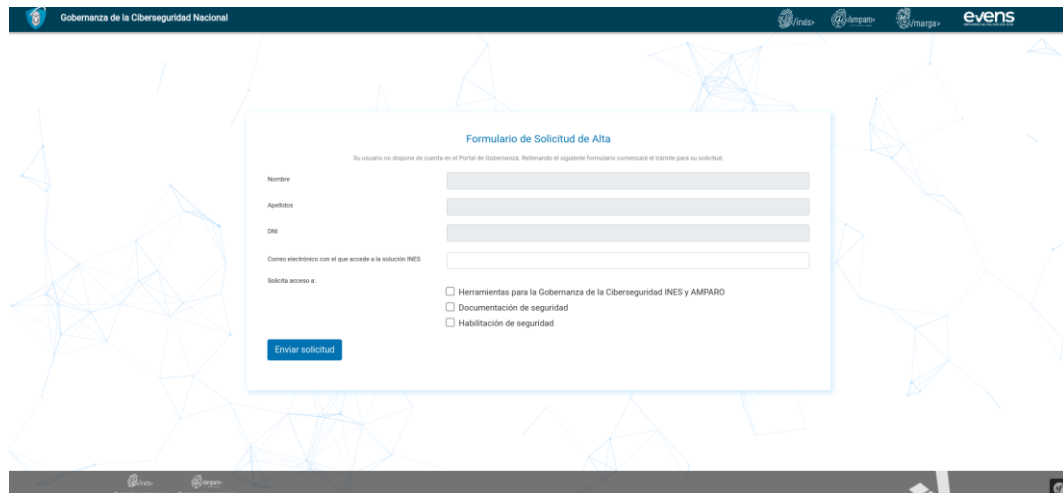


Ilustración 5. Formulario de alta.

3.2 FORMULARIO DE ALTA

Si no se posee un usuario para poder usar la aplicación habrá que solicitar la creación de uno.

Para ello, una vez autenticado en cl@ve, se habrá de rellenar el formulario al que se redirigirá, tal y como muestra la ilustración 5.

Se procederá a rellenar los campos obligatorios, marcados en gris.

Para poder utilizar DOCSEG se marcará la opción “Documentación de seguridad”.

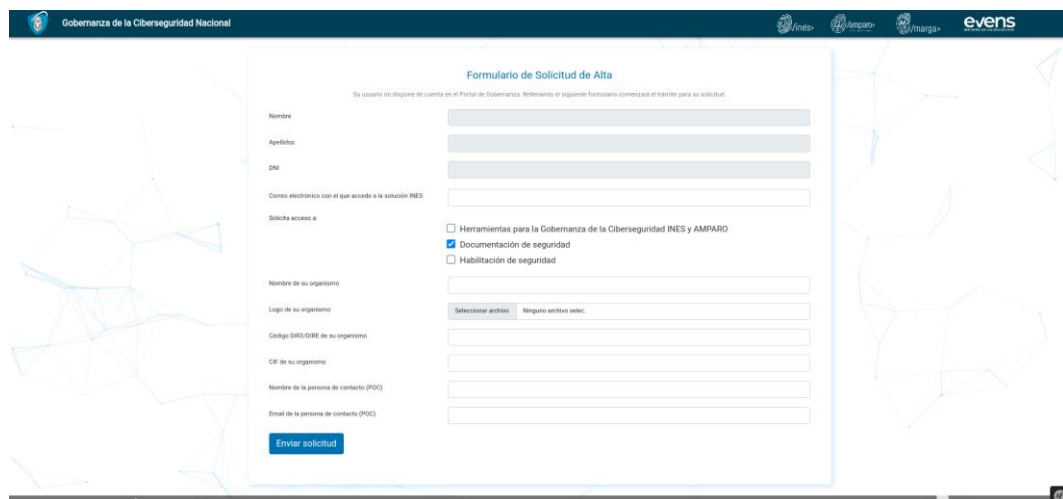


Ilustración 6. Formulario de alta.

Al seleccionar la opción, se desplegarán nuevos campos que se deberán cumplimentar, tal y como aparece en la ilustración 6.

Una vez rellenados los campos, se pulsará el botón “Enviar solicitud”.

Cuando la petición de alta de usuario, sea revisada y aprobada, se notificará al usuario vía correo electrónico de que ya tiene disponible su cuenta.

Una vez el usuario tiene acceso a DOCSEG, en la barra superior podrá observar lo siguiente:

- Desplegable organismo: Permite seleccionar el organismo sobre el que se desea ver o modificar los datos. Normalmente sólo existirá uno.
- Botón campana: Muestra las alertas que han sido generadas para el usuario.
- Botón usuario: Permite ver el usuario actualmente autenticado y desconectarse de DOCSEG.

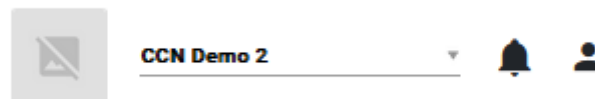


Ilustración 7. Detalle acciones barra superior.

4. CREACION DE SISTEMAS

Una vez el usuario se ha autenticado y accedido a la pantalla principal de usuario, se podrán crear sistemas para iniciar la carga de documentación de seguridad.

Para ello se deberá pulsar sobre el texto “Nueva documentación de seguridad”.

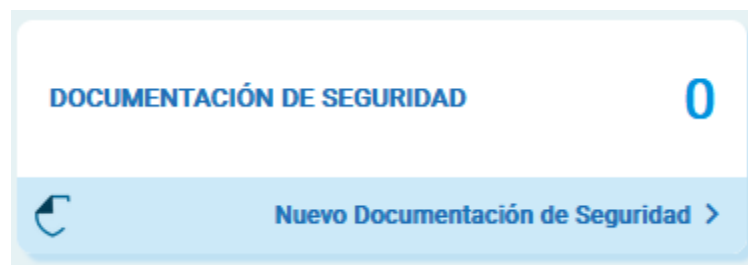


Ilustración 8. Detalle del botón para añadir nueva documentación de seguridad.

Se abrirá una nueva ventana en la que se ingresará el nombre del sistema y la descripción, ambos campos obligatorios. El tipo de sistema será CLASIFICADO.

DOCSEG se ha desarrollado con el fin de que sea una solución fácil e intuitiva, muchos de los campos a rellenar o pasos a seguir no necesitan explicación, pueden ser resueltos por el usuario fácilmente leyendo el título del campo, por ejemplo, por lo que todos los pasos a realizar en el alta, rellenado de documentación o subida de archivos no se detallan.

Información del sistema

Declaración de cumplimiento

Documentación

Datos del sistema

Tramitación

Complete los siguientes campos para crear un nuevo Sistema que permita su Adecuación al Esquema Nacional de Seguridad.

Indique el nombre del sistema *

SISTEMA TIC DIFUSIÓN LIMITADA SALA ZAR MADRID II - DL-ZAR-MADRID-II

Indique una descripción para el sistema *

Equipo aislado para el manejo de información clasificada de grado DIFUSIÓN LIMITADA NACIONAL / NATO RESTRICTED / EU RESTRICTED / ESA RESTRICTED, situado en la sala ZAR de las instalaciones situadas en Madrid "MADRID II". Modo seguro de operación DEDICADO.

255/2048 Caracteres

Tipo de sistema *

CLASIFICADO

Categoría *

1-EMPRESAS

Dispone código NEASTIC * ☒ Sí * ☐ No *

Introduzca el código

XXXX-XXXX-XXXX

Subir fichero de solicitud

Examinar... NEASTIC_FIRMADO_POR_LA_ONS.pdf

Responsable de seguridad del sistema / Persona de contacto *

Nombre y apellidos completos

Correo electrónico de contacto *

acreditacion.ccn@cni.es

Órgano de control (OC) *

Nombre del órgano de control

Jefe de seguridad del OC *

Nombre y apellidos completos

Correo del jefe de seguridad del OC *

jefe_seguridad@ccn.es

Siguiente

Ilustración 9. Formulario de creación de nuevo sistema.

Se pulsará el botón “Siguiente” y será redirigido a la pantalla de “Declaración de cumplimiento”. En esta pantalla no se deberá rellenar ningún dato y se pulsará en el botón “Siguiente”. Al hacerlo se mostrará un cuadro de diálogo, en el que se pulsará sobre la opción “Aceptar”.

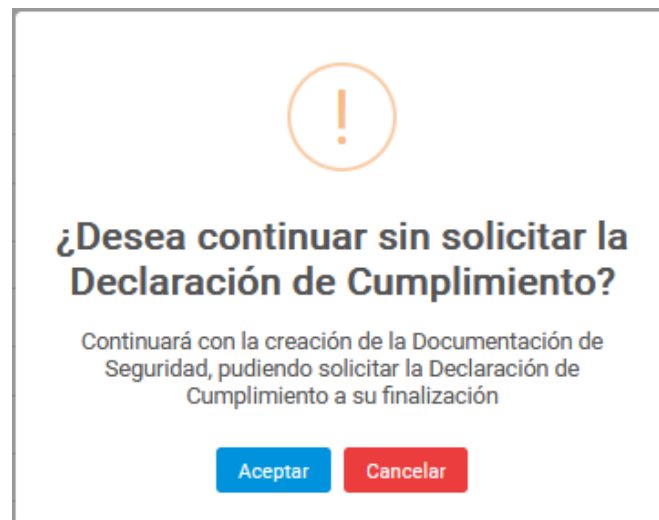


Ilustración 10. Aceptar para continuar sin solicitar declaración de cumplimiento.

En la siguiente pantalla, se pulsará en el botón “OMITIR”.

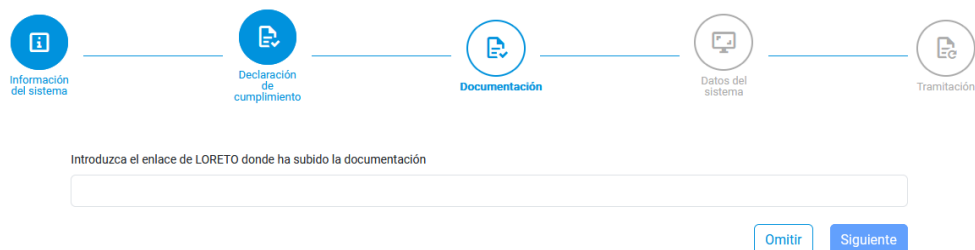


Ilustración 11. Omitir enlace de LORETO.

Posteriormente, aparecerá el escudo de DOCSEG, sobre el que se deberá pulsar para finalizar con la creación del sistema.



Ilustración 12. Omitir enlace de LORETO.

Una vez DOCSEG finalice todo el proceso, será redirigido a la pantalla de documentación de seguridad. Aparecerá un cuadro de diálogo sobre el que pulsaremos “Sí”.

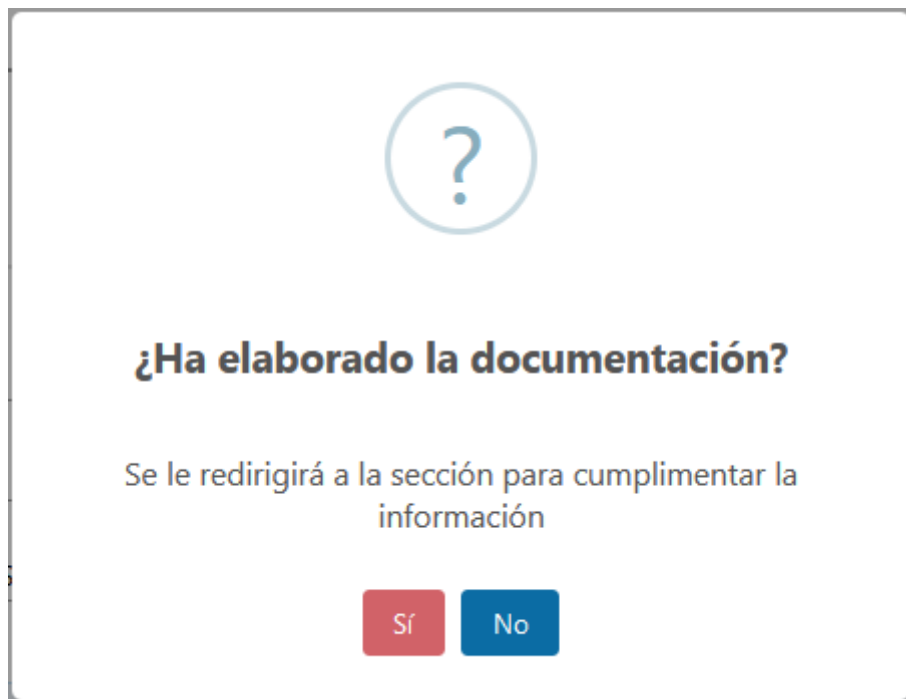


Ilustración 13. Omitir enlace de LORETO.

Tras un breve proceso de carga el sistema se habrá creado y estará situado en la siguiente pantalla, donde ahora sí se podrá especificar el espacio de LORETO, en caso de disponer de uno.

Ilustración 14. Nuevo sistema creado.

Una vez creado el sistema, si se pulsa sobre el logotipo de GOBERNANZA, será redirigido a la pantalla principal.



Ilustración 15. Logo de GOBERNANZA.

4.1 ELIMINACIÓN DE SISTEMAS

Si se desea eliminar un sistema, desde la pantalla principal de DOCSEG, se pulsará en el icono de la papelera y se aceptará el cuadro de dialogo.

Si el desplegable de sistema no se encuentra desplegado, se pulsará sobre la flecha del recuadro azul.

Ilustración 16. Desplegar listado.

Una vez desplegado, se pulsará sobre el icono de la papelera del sistema que se quiera eliminar.



¿Desea borrar este sistema?

SISTEMA TIC DIFUSION LIMITADA SALA ZAR MADRID II
_ DL_ZAR_MADRID_II 2024

Se eliminará toda la información relacionada con la
Declaración de Cumplimiento.

Esta acción no podrá ser revertida.

Aceptar

Cancelar

Ilustración 17. Borrar sistema.

5. RELLENADO DE LA DOCUMENTACIÓN

Con la creación de un sistema, ya se podrá iniciar un proceso de subida de documentación a la solución DOCSEG.

La información que se aportará en los diferentes apartados puede ser desde texto a archivos que se deberán subir.

En las diferentes secciones se podrá observar de manera intuitiva qué tipo de información se nos solicita.

Para iniciar el proceso, se pulsará sobre el icono de flecha, situado en el extremo derecho de la casilla del sistema.

El usuario será redirigido directamente a la sección 3 de DOCSEG, donde se podrá insertar la documentación.

6. SECCIONES

El proceso de carga de la documentación de seguridad se encuentra íntegramente en la sección 3, la cual consta de siete secciones.

Se puede saltar de una a otra pulsando sobre el menú lateral izquierdo, aunque se recomienda ir en orden, ya que hay secciones que se retroalimentan de lo introducido en secciones anteriores.

La información que se introduce en los campos de texto, normalmente queda grabada automáticamente, por lo que no es necesario pulsar ningún botón para ello.

En algunos puntos de la solución, será necesario pulsar un botón para guardar la información.

El proceso se puede posponer en cualquier momento y continuar más adelante.

Durante el proceso, existirán campos que sea obligatorio completarlos y otros no. En la medida de lo posible es preferible rellenar el máximo de campos, ya que de esa manera la documentación final quedará más completa. Asimismo, existen campos con validación de la información introducida, y se tendrá que pasar esa validación para poder escribir en ellos, como es por ejemplo el campo de introducción de teléfono, en el que no podremos introducir letras.

A medida que se avanza en el proceso, la solución mostrará el estado del progreso.

Progreso total 33 / 78

Ilustración 18. Progreso de la sección completado.

6.1 SECCIÓN INFORMACIÓN DEL SISTEMA

En esta sección se insertará la información básica del sistema y la persona de contacto.

En cada campo de texto, pulsando sobre el botón de diálogo, se pueden añadir comentarios adicionales.

En este apartado se ha de rellenar también la información sobre el órgano de control propio.

Ilustración 19. Información del sistema.

6.2 SECCIÓN DOCUMENTACIÓN

En esta sección se han de indicar los enlaces del espacio reservado de LORETO que se posean.

En caso de no disponer de espacio de LORETO pueden solicitarlo en la dirección de correo acreditación@ccn.cni.es.

6.3 DATOS DE SISTEMA

Esta es la sección, como se indicaba anteriormente, donde se rellenan todos los datos del sistema, sobre todo los de aspecto técnico y de seguridad.

Las secciones, campos y apartados son muy intuitivos, por lo que no se explicarán todos en profundidad, ya que por ejemplo el propio nombre del campo indicará qué hay que poner en él.

Esta sección se divide en siete secciones.

6.3.1 DESCRIPCIÓN

6.3.1.1 TIPOLOGÍA DEL SISTEMA

Misión: Indicar a qué uso va a estar destinado el sistema.

Tipo de sistema: Indicar si se trata de un sistema o un equipo aislado.

Ámbito de clasificación: NACIONAL, OTAN, UE, ESA o todos.

Grado de clasificación: Grado máximo de clasificación para el que se pedirá la acreditación del sistema. El valor de este campo se formará automáticamente atendiendo al valor seleccionado en el desplegable anterior.

Se podrán añadir comentarios adicionales en los campos 1, 2, 3 y 4.

3.1. DESCRIPCIÓN

1- Misión
El SISTEMA TIC DIFUSIÓN LIMITADA SALA ZAR MADRID II tiene como misión manejar información clasificada hasta grado difusión limitada, cubriendo de esta forma las necesidades de la empresa con los contratos nacionales e internacionales que exigen este requisito.

2- Tipo de sistema Equipos aislados

3- Ámbito de clasificación Nacional, OTAN, UE, ESA

4- Grado de clasificación de la información Difusión limitada/Restricta/Restricta/Restricta

INFORMACIÓN
El modo de seguro de operación será UNIFICADO A NIVEL SUPERIOR

Ilustración 20. Tipología del sistema.

6.3.1.2 COMPOSICIÓN GLOBAL DEL SISTEMA

Aquí se especificarán los locales, servidores, equipos, dispositivos periféricos, dispositivos de comunicación y dispositivos de criptografía de los que consta el sistema. También existe un campo “Otros”, para incluir aquellos elementos que no se encuentren dentro de alguno de los grupos anteriores.

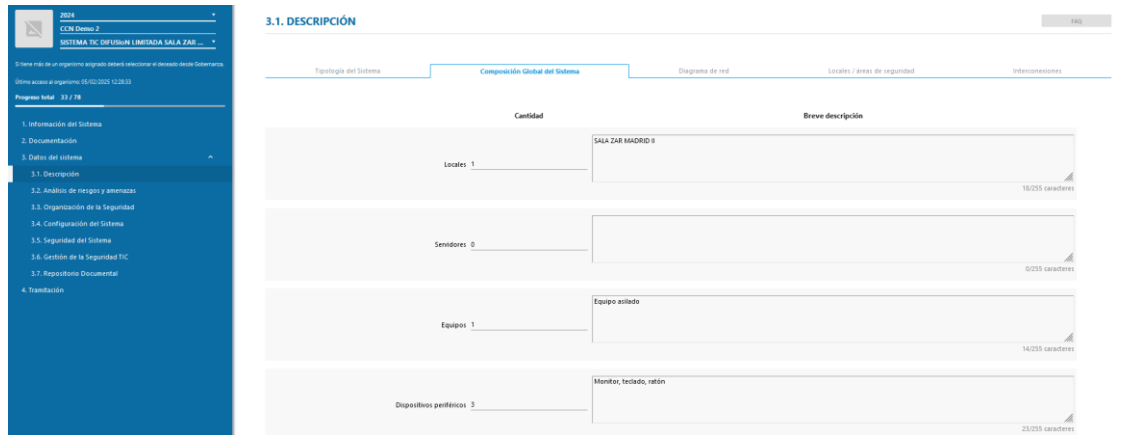


Ilustración 21. Composición global del sistema.

6.3.1.3 DIAGRAMA DE RED

En esta sección existen tres apartados, cuya operativa y método de incluir la información es la misma:

- Diagrama lógico.
- Diagrama físico-lógico.
- Diagrama físico.

6.3.1.3.1 Subir diagrama

En este apartado de la sección, se podrá especificar el diagrama de red actual del sistema. Para ello se puede subir una imagen del diagrama que el usuario tenga almacenada.

1. SUBIR DIAGRAMA



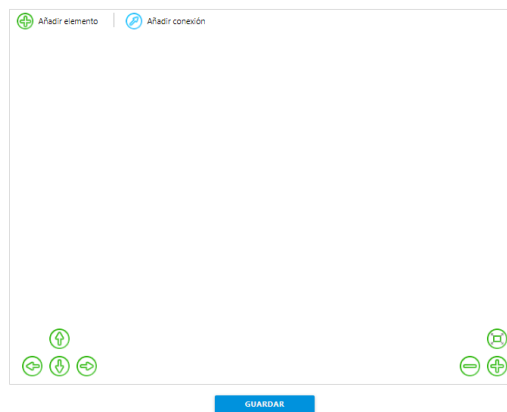
Ilustración 22. Cargar diagrama de red.

Al pulsar el botón “GUARDAR”, se podrá visualizar la imagen resultante en el apartado “3. FICHERO ACTUAL”.

6.3.1.3.2 Editor de diagrama

La solución DOCSEG, en caso de que no tengamos una imagen con el diagrama de red del sistema, nos permite crear uno de forma fácil. Al inicio, el editor se mostrará vacío.

2. EDITOR DE DIAGRAMA

*Ilustración 23. Elaborar diagrama de red.*

Para añadir un elemento, será necesario pulsar sobre el botón añadir elemento. Seguidamente el editor nos mostrará el siguiente mensaje “Haga click en un lugar vacío para colocar un nuevo elemento”. Una vez hecho, se mostrará una ventana modal para introducir el nombre del elemento y un icono, ambos campos obligatorios. El campo ID es autogenerado.

Para guardar y añadir el elemento pulsar en el botón “AÑADIR”.

AÑADIR ELEMENTO

EXISTEN CAMPOS OBLIGATORIOS *

ID *	caaf4916-68a8-4369-89bb-01a1d0b01283
Texto	Servidor información clasificada
Icono *	Servidor ▼

AÑADIRCANCELAR

Ilustración 24. Creación de elemento.

Posteriormente se pueden crear más elementos, y establecer conexiones entre ellos. Esta acción se puede realizar, habiendo más de un elemento en el diagrama, puesto sobre el botón “Añadir conexión”.

Las conexiones tienen sentido, por lo que se deberá primero seleccionar el elemento desde donde comienza la selección y soltar el puntero del ratón en el elemento en el que termine.

Pueden establecerse conexiones bidireccionales.



Ilustración 25. Conexión de elementos.

Para editar o borrar un elemento, se deberá pulsar sobre el elemento que se desee. Para realizar la acción y pulsar el botón de acción correspondiente.

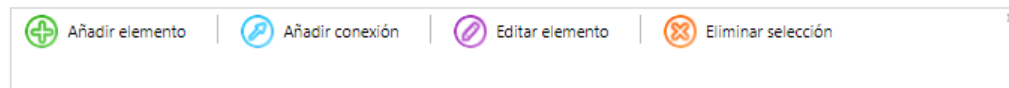


Ilustración 26. Botonera completa.

Una vez terminado el diagrama de red, se deberá pulsar el botón “GUARDAR” para que quede reflejado en DOCSEG.

6.3.1.3.3 Fichero actual

En este apartado quedará reflejado el diagrama que se ha cargado en DOCSEG, tanto si ha realizado mediante la subida de un archivo como utilizando el editor de diagrama.

3. FICHERO ACTUAL
1658300404.png

BORRAR FICHERO



Ilustración 27. Diagrama de red subido y botón borrar.

Si se pulsa el botón “**BORRAR ARCHIVO**”, dejará de constar un diagrama de red y se podrá añadir otro con los procedimientos descritos anteriormente.

No es necesario borrar el actual archivo de imagen para sustituirlo, si se añade uno nuevo, por cualquiera de los procedimientos disponibles, este sustituirá al existente.

6.3.1.4 LOCALES / ÁREAS DE SEGURIDAD

6.3.1.4.1 Locales / Áreas de seguridad

En este apartado, se podrá subir información de los locales y áreas de seguridad que forman parte del proceso de acreditación del sistema.

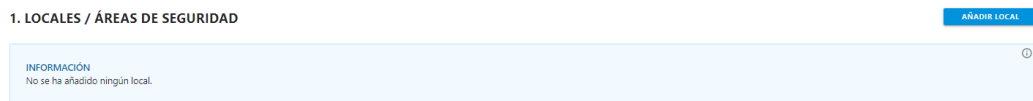


Ilustración 28. Locales y áreas de seguridad.

Para añadir un nuevo local o área, se deberá pulsar en el botón “**AÑADIR LOCAL**”.

NUEVO LOCAL

Complete los campos para añadir un nuevo local.

EXISTEN CAMPOS OBLIGATORIOS *

UBICACIÓN

Nombre *	
Edificio *	
Planta *	
Local *	
Descripción	

CAL

Nombre del Certificado de Acreditación *	
Tipo *	Selecciona una opción
Fecha de caducidad *	dd/mm/aaaa

Ilustración 29. Formulario nuevo local o área de seguridad.

En el formulario que aparece, se tendrán que rellenar obligatoriamente todos los campos de los apartados “**UBICACIÓN**” y “**CAL**”, salvo el apartado descripción.

EQUIPAMIENTO

	Cantidad	Breve descripción
Servidores		
Equipos		
Dispositivos periféricos		
Dispositivos de comunicación		
Dispositivos cripto		
Otros		

[CREAR LOCAL](#)

Ilustración 30. Formulario nuevo local o área de seguridad.

En el apartado “EQUIPAMIENTO”, se podrán indicar los elementos que están dentro del local o área de seguridad.

Una vez añadido el local, figurará en el listado de locales o áreas de seguridad.

1. LOCALES / ÁREAS DE SEGURIDAD [DESCARGAR LISTADO](#) [AÑADIR LOCAL](#)

Mostrar: registros Buscar:

Nombre	Edificio	Planta	Local	CAL	Ver/editar	Borrar	Copiar
Local tipo ZAR I	Edificio de seguridad	1ª planta	LC-001				

Mostrando 1 - 1 de 1 Anterior 1 Siguiente

Ilustración 31. Local añadido.

Tal y como se puede apreciar en la imagen anterior, una vez añadido al menos un local, se pueden realizar las siguientes acciones:

1. Acciones generales:

- **Descargar listado:** Al pulsar este botón se descargará un archivo en formato Excel, que contendrá el listado de todos los locales introducidos.

2. Acciones individuales:

- **Añadir certificado CAL:** Si se pulsa el botón rojo con el símbolo del certificado, se podrá incluir el archivo de certificado de acreditación local.

CERTIFICADO DE ACREDITACIÓN LOCAL (CAL)

Complete los campos indicados.

Crear y añadir versión

Versiones

INFORMACIÓN

Recuerde que para un sistema de difusión limitada sólo es necesaria la declaración de zona ZAP.

CREAR Y AÑADIR VERSIÓN

Nombre del Certificado de Acreditación: CAL 20/07/2022

Tipo: ZAR - Área Clase I

Fecha de caducidad: 20/07/2024

Fichero: CAL LC-001.pdf

CREAR Y AÑADIR VERSIÓN

Ilustración 32. Añadir certificado de acreditación local.

Una vez subido el fichero, se podrá observar que el botón de certificado figura en negro. Se pueden añadir más versiones del certificado, que figurarán en la pestaña de versiones. Se pueden descargar las versiones de los CAL subidos.

CERTIFICADO DE ACREDITACIÓN LOCAL (CAL)

Fecha de modificación: 20/07/2022 09:34:44

Añadir versión

Versiones

VERSIONES

Versión 2.0	20/07/2022
Nombre: CAL 20/07/2022	
Tipo: ZAR - Área Clase I	
Fecha de Caducidad: 20/07/2024	
Fichero disponible:	
Versión 1.0	20/07/2022

Ilustración 33. Versiones de certificados de local subidos.

- **Ver / Editar:** Aquí se puede ver o editar la información del local o el área de seguridad introducido anteriormente. Aquí se puede introducir un diagrama de red de este local específico, algo que no se puede hacer en el momento de la creación del local. La carga del diagrama de red se realiza de la misma manera que la explicada anteriormente.
- **Borrar:** Borra el local después de haber aceptado el diálogo emergente.
- **Copiar:** Esta acción permite copiar un local, por si existen varios con las mismas características no tener que crearlo nuevo y, posterior al copiado, editar los campos necesarios. No se copiarán los CAL ni los diagramas de red asociados al local original.

6.3.1.5 INTERCONEXIONES

6.3.1.5.1 Interconexiones

En este apartado se podrá documentar las interconexiones que tiene el sistema.

Por defecto los campos están deshabilitados, hasta que no se seleccione la opción “S” en el desplegable.

Si el sistema no posee interconexiones seleccionaremos la opción “No”.

The screenshot shows the DOCSEG system interface. On the left, a sidebar lists the system components: 1. Información del Sistema, 2. Descripción, 3. Análisis de riesgos y amenazas, 4. Organización de la Seguridad, 5. Configuración del Sistema, 6. Servicios TIC, protocolos y puertos, 7. Seguridad del Sistema, 8. Gestión de la Seguridad TIC, 9. Repositorio Documental, and 10. Solicitud de Acreditación. The main area is titled '1. INTERCONEXIONES' and contains four sub-sections: 1.1 INTERCONEXIÓN DEL SISTEMA, 1.2 MECANISMOS DE INTERCONEXIÓN, 1.3 SISTEMAS CON LOS QUE CONECTA, and 1.4 OTRA INFORMACIÓN ADICIONAL. Each sub-section has a text input field and a dropdown menu for selection.

Ilustración 34. Interconexiones.

6.4 ANÁLISIS DE RIESGOS Y AMENAZAS

6.4.1 ANÁLISIS DE RIESGOS Y AMENAZAS

En este apartado actualmente no se encuentra disponible. Se implementará próximamente.

6.4.2 OTROS FICHEROS

En este apartado se podrán subir otros ficheros que se consideren oportunos, referidos a análisis de riesgos y amenazas.

Al no encontrarse disponible la subida de un análisis de riesgos en el apartado anterior, se deberá subir en este apartado.

Se seleccionará el tipo de archivos a subir en el desplegable “Tipo de archivo” y se seleccionará el fichero.

Al guardar se podrá observar que figurará en el listado inferior. Se podrá descargar para su consulta o borrarlo.

3. OTROS FICHEROS

Tipo de archivo Selecciona una opción FICHERO DE PILAR Fichero de PILAR GUARDAR

Nombre	Tipo	Fecha	Descargar	Borrar
1658305370_Captura.png	Otros	20/07/2022 10:22:50		

Ilustración 35. Subida de otros ficheros.

6.5 ORGANIZACIÓN DE LA SEGURIDAD

En esta sección se incluirá la información relativa a responsabilidades, roles y personas.

6.5.1 SEGURIDAD DOCUMENTAL

En esta sección se incluirá la información del órgano responsable de seguridad, el jefe del órgano superior y el responsable de tramitación de la ONS.

Este apartado es la única parte obligatoria de rellenar en esta sección.

1. SEGURIDAD DOCUMENTAL

1 - Órgano de control responsable

2 - Jefe del órgano superior

3 - Responsable de la tramitación con la ONS

Ilustración 36. Seguridad documental.

6.5.2 RESPONSABILIDADES, ROLES Y USUARIOS

6.5.2.1 Usuarios

En esta sección se podrán introducir los usuarios que operarán en el sistema.

Se pueden añadir manualmente, pulsando el botón “AÑADIR USUARIO” o importar un listado rellenado previamente.

NUEVO USUARIO

Complete los campos para añadir un nuevo usuario.

EXISTEN CAMPOS OBLIGATORIOS *

Nombre *

Tipo * Selecciona una opción

¿Requiere HPS? * Sí

Grado requerido *

HPS VIGENTE

Grado

Fecha de Caducidad dd/mm/aaaa

CREAR USUARIO

Ilustración 37. Creación de nuevo usuario.

IMPORTACIÓN DE REGISTROS DEL SISTEMA

INSTRUCCIONES

Para importar registros de Usuarios del sistema desde un fichero Excel debe descargar esta [plantilla](#) y rellenarla con los nuevos registros a importar.

IMPORTACIÓN

Selecciona la plantilla rellena con los Usuarios del sistema a importar.

CARGAR LISTADO

Ilustración 38. Importación de listado de usuarios.

Una vez añadidos los usuarios, estos figurarán en el listado de usuarios.

DESCARGAR LISTADO IMPORTAR LISTADO AÑADIR USUARIO

Mostrar 5 registros

Buscar:

Nombre	Tipo	POS	Ver/editar	Borrar	Copiar
Usuario del sistema	Usuario				

Mostrando 1 - 1 de 1

Anterior 1 Siguiente

Ilustración 39. Usuario creado.

Al igual que en el listado de roles, si existe al menos un usuario creado, se podrá descargar un archivo que contiene todos los usuarios que figuran.

Cada usuario posee tres botones de acción, de los cuales se detallan sus acciones:

- Botón de descarga de una plantilla ejemplo para que el usuario firme haber leído y comprendido los procedimientos de operativos del sistema (POS).
- Botón de visualización del archivo de aceptación de POS subido. Figurará deshabilitado hasta que no haya un archivo subido.
- Botón de selección de archivo POS a subir.

6.5.2.2 Responsabilidades y roles

En esta sección se podrán añadir responsabilidades y roles. La nomenclatura de los roles es la correspondiente a la definida en la Guía CCN-STIC 201.

Para añadir un rol se deberá pulsar el botón “AÑADIR ROL”.

Usuarios	Responsabilidades y roles
INFORMACIÓN El resumen de responsabilidades del personal indicado, viene reflejado en la Guía CCN-STIC-201.	
DESCARGAR LISTADO AÑADIR ROL	

Ilustración 40. Responsabilidades y roles.

Al pulsarlo, aparecerá un formulario, que consta de algunos campos obligatorios.

NUEVO ROL

✕

Complete los campos para añadir un nuevo rol.

EXISTEN CAMPOS OBLIGATORIOS *

Tipo * Responsable del sistema RSIS

Nombre *

DNI *

Teléfono

E-mail *

¿Requiere HPS? * Sí

Grado requerido *

HPS VIGENTE

Grado

Fecha de Caducidad dd/mm/aaaa

CREAR ROL

Ilustración 41. Formulario creación nuevo rol.

En caso de que se seleccione “Sí” en el desplegable de la HPS, se desplegarán nuevos campos obligatorios para rellenar.

Al guardar el formulario, aparecerá el nuevo rol creado en el listado.

DESCARGAR LISTADO AÑADIR ROL

Mostrar 5 registros

Buscar:

Tipo	Nombre	DNI	Teléfono	E-mail	Ver/editar	Borrar	Copiar
Administrador del sistema AS	Admin AS			correo@mail.es			

Mostrando 1 - 1 de 1

Anterior 1 Siguiente

Ilustración 42. Nuevo rol creado.

Si existe al menos un rol insertado, aparecerá un botón que permite la descarga de un fichero con todos los roles introducidos.

Asimismo, por cada rol creado se podrán realizar acciones individuales de ver y editar, borrar y copiar.

6.5.3 ESTRUCTURA ORGÁNICA

En este apartado se puede detallar a modo de diagrama la estructura de roles y usuarios que posee el sistema.

Al crear roles y usuarios, estos se añadirán automáticamente al diagrama. Estos elementos añadidos se pueden editar o borrar.

Asimismo, también se pueden crear elementos nuevos.

3. ESTRUCTURA ORGÁNICA

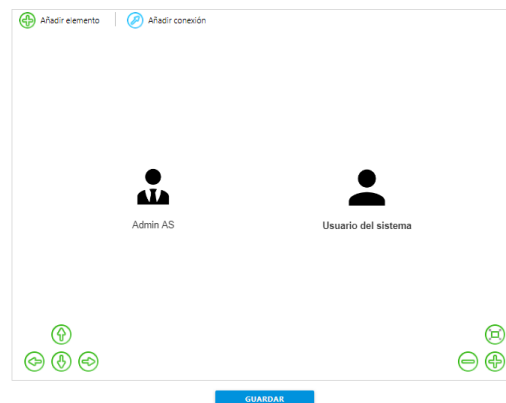


Ilustración 43. Diagrama de usuarios.

6.5.3.1 Fichero actual

Si se guarda el diagrama, este figurará en este apartado y será adjuntado a la documentación final.

3.1 FICHERO ACTUAL
1658313198.png

BORRAR FICHERO



Admin AS



Usuario del sistema

Ilustración 44. Diagrama de usuarios subido.

6.6 CONFIGURACIÓN DEL SISTEMA

En esta sección se podrá rellenar la información relativa a los componentes que forman parte del sistema.

Está dividida en varias secciones, pero no es obligatorio cumplimentarlas para avanzar en el proceso.

Existe un botón denominado “*DIAGRAMA DE RED*”, en el que se podrá consultar el diagrama subido anteriormente.

Para todos los elementos que se pueden dar de alta en esta sección, obligatoriamente habrá que especificar un local donde se encuentran. El listado de locales disponible para asignar, viene determinado por aquellos que se dieron de alta en el apartado 6.3.1.4.

6.6.1 Equipos

Para dar de alta un equipo se deberá pulsar el botón “*AÑADIR EQUIPO*”.

Una vez pulsado, aparecerá un formulario. Parte de los campos son obligatorios.

EXISTEN CAMPOS OBLIGATORIOS *

UBICACIÓN	Tipo *	Selecciona una opción
	Local *	Selecciona una opción
OTROS DATOS	Marca *	
	Modelo *	
	Número de serie	
	Nombre del host	
	Microprocesador *	
	RAM *	
	Disco duro *	
	Monitor *	Selecciona una opción
	Teclado *	Selecciona una opción
	Ratón *	Selecciona una opción
	Otra Información *	
	Sistema Operativo *	Selecciona una opción
	Versión del Sistema Operativo	
	¿Dispone de etiquetas de seguridad (antitámpen)?	Selecciona una opción

Ilustración 45. Formulario nuevo equipo.

A los equipos se les puede incorporar herramientas de seguridad y aplicaciones.

HERRAMIENTAS DE SEGURIDAD		+
	Tipo	Detección de software dañino
1	Nombre	
	Versión	
	Certificación	
APLICACIONES		+
1	Nombre	
	Versión	

CREAR EQUIPO

Ilustración 46. Formulario nuevo equipo, herramientas y aplicaciones.

Una vez guardado, el nuevo equipo aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los equipos dados de alta. Los equipos se pueden ver o editar, borrar y copiar.

1. HARDWARE Y SOFTWARE

Equipos	Periféricos	Servidores	Electrónica de red
---------	-------------	------------	--------------------

DESCARGAR LISTADO AÑADIR EQUIPO

Mostrar: 5 registros

Buscar:

Tipo	Marca	Modelo	Microprocesador	Ver/editar	Borrar	Copiar
Puestos cliente	HP	Desktop	i9			

Mostrando 1 - 1 de 1

Anterior 1 Siguiente

Ilustración 47. Nuevo equipo dado de alta.

6.6.2 Periféricos

Para dar de alta un periférico se deberá pulsar el botón “AÑADIR PERIFÉRICO”.

Una vez pulsado, aparecerá un formulario. Parte de los campos son obligatorios.

NUEVO PERIFÉRICO

Complete los campos para añadir un nuevo periférico.

EXISTEN CAMPOS OBLIGATORIOS *

UBICACIÓN

Tipo *

Local *

OTROS DATOS

Marca *

Modelo *

Número de serie

Versión del software *

Otra Información *

¿Dispone de etiquetas de seguridad (antitamper)?

CREAR PERIFÉRICO

Ilustración 48. Formulario nuevo periférico.

Una vez guardado, el nuevo periférico aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los periféricos dados de alta. Los periféricos se pueden ver o editar, borrar y copiar.

1. HARDWARE Y SOFTWARE

Equipos

Periféricos

Servidores

Electrónica de red

DESCARGAR LISTADO

AÑADIR PERIFÉRICO

Mostrar 5 registros

Buscar:

Tipo	Marca	Modelo	Versión del software	Ver/editar	Borrar	Copiar
Memorias USB	USB genérico	MOD-001	SOFT-001			

Mostrando 1 - 1 de 1

Anterior

1

Siguiente

Ilustración 49. Nuevo periférico dado de alta.

6.6.3 Servidores

Para dar de alta un servidor se deberá pulsar el botón “AÑADIR EQUIPO”.

Una vez pulsado, aparecerá un formulario. Parte de los campos son obligatorios.

EXISTEN CAMPOS OBLIGATORIOS *

UBICACIÓN

Tipo * Selecciona una opción ▼

Local * Selecciona una opción ▼

OTROS DATOS

Marca *

Modelo *

Número de serie

Nombre del host

Microprocesador *

RAM *

Disco duro *

Monitor * Selecciona una opción ▼

Teclado * Selecciona una opción ▼

Ratón * Selecciona una opción ▼

Otra información *

Sistema Operativo * Selecciona una opción ▼

Versión del Sistema Operativo

¿Dispone de etiquetas de seguridad (antitámpen)? Selecciona una opción ▼

Ilustración 50. Formulario nuevo servidor.

A los servidores se les puede incorporar herramientas de seguridad y aplicaciones.

HERRAMIENTAS DE SEGURIDAD

Tipo: Detección de software dañino

Nombre:

Versión:

Certificación:

APLICACIONES

Nombre:

Versión:

CREAR SERVIDOR

Ilustración 51. Formulario nuevo servidor, herramientas y aplicaciones.

Una vez guardado, el nuevo servidor aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los servidores dados de alta. Los servidores se pueden ver o editar, borrar y copiar.

1. HARDWARE Y SOFTWARE

Equipos Periféricos **Servidores** Electrónica de red

DESCARGAR LISTADO **AÑADIR SERVIDOR**

Mostrar: 5 registros Buscar:

Tipo	Marca	Modelo	Microprocesador	Ver/editar
Servidor de aplicaciones	HP	Proliant	Xeon	

Mostrando 1 - 1 de 1 Anterior 1 Siguiente

Ilustración 52. Servidor dado de alta.

6.6.4 ELECTRÓNICA DE RED

Para dar de alta un dispositivo de electrónica de red se deberá pulsar el botón “AÑADIR ELECTRÓNICA”.

Una vez pulsado, aparecerá un formulario. Parte de los campos son obligatorios.

NUEVA ELECTRÓNICA DE RED

Complete los campos para añadir una nueva electrónica de red.

EXISTEN CAMPOS OBLIGATORIOS *

UBICACIÓN

Tipo *

Local *

OTROS DATOS

Marca *

Modelo *

Número de serie

Versión del software *

Otra Información *

¿Dispone de etiquetas de seguridad (antitáper)?

CREAR ELECTRÓNICA

Ilustración 53. Formulario nuevo periférico.

Una vez guardado, el nuevo dispositivo de electrónica de red aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los dispositivos de electrónica de red dados de alta. Los dispositivos de electrónica de red se pueden ver o editar, borrar y copiar.

1. HARDWARE Y SOFTWARE

Equipos

Periféricos

Servidores

Electrónica de red

DESCARGAR LISTADO

AÑADIR ELECTRÓNICA

Mostrar 5 registros

Buscar:

Tipo	Marca	Modelo	Versión del software	Ver/editar	Borrar	Copiar
Router	Cisco	MOD-001	SOFT-001			

Mostrando 1 - 1 de 1

Anterior

1

Siguiente

Mostrando 1 - 1 de 1

Anterior 1 Siguiente

Ilustración 54. Nuevo periférico dado de alta.

6.6.5 SERVICIOS TIC

Para dar de alta un servicio TIC se deberá pulsar el botón “AÑADIR SERVICIO”. Una vez pulsado, aparecerá un formulario, todos los campos son obligatorios.

NUEVO SERVICIO

Complete los campos para añadir un nuevo servicio.

EXISTEN CAMPOS OBLIGATORIOS *

Tipo *

Nombre *

Política de uso *

Permisos establecidos *

Derechos establecidos *

Descripción *

[CREAR SERVICIO](#)

Ilustración 55. Formulario nuevo servicio.

Una vez guardado, el nuevo servicio TIC aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los servicios TIC dados de alta. Los servicios TIC se pueden ver o editar, borrar y copiar.

1. SERVICIOS TIC, PROTOCOLOS Y PUERTOS

Servicios TIC

Protocolos y Puertos

DESCARGAR LISTADO

AÑADIR SERVICIO

Mostrar 5 registros

Buscar:

Tipo	Nombre	Ver/editar	Borrar	Copiar
Servicio de almacenamiento de ficheros	Servicio de almacenamiento de ficheros			

Mostrando 1 - 1 de 1

Anterior

1

Siguiente

Ilustración 56. Nuevo servicio dado de alta.

6.6.6 PROTOCOLOS Y PUERTOS

Al acceder a este apartado, se podrá observar que existen unos protocolos por defecto ya insertados. Estos protocolos se pueden editar, borrar o copiar.

Para dar de alta un nuevo protocolo y puerto se deberá pulsar el botón “AÑADIR PROTOCOLO”.

Una vez pulsado, aparecerá un formulario, todos los campos son obligatorios.

NUEVO PROTOCOLO

Complete los campos para añadir un nuevo protocolo.

EXISTEN CAMPOS OBLIGATORIOS *

Tipo *

Aplicación asociada *

Puerto/s *

Observaciones *

[CREAR PROTOCOLO](#)

Ilustración 57. Formulario protocolos y puertos.

Una vez guardado, el nuevo protocolo y puerto aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los nuevos protocolo y puertos dados de alta. Los nuevos protocolos y puertos se pueden ver o editar, borrar y copiar.

1. SERVICIOS TIC, PROTOCOLOS Y PUERTOS

Servicios TIC

Protocolos y Puertos

DESCARGAR LISTADO

AÑADIR PROTOCOLO

Mostrar

5

 registros

Buscar:

Tipo	Aplicación asociada	Puerto/s	Observaciones	Ver/editar	Borrar	Copiar
FTP	Uso de administración	20-21				
Telnet	Uso de administración	23				
SMTP	Correo	25				
POP 3	Correo	110				
IMAP	Correo	143				

Mostrando 1 - 5 de 11

Anterior

1

2

3

Siguiente

Ilustración 58. Listado de protocolos.

6.6.7 HERRAMIENTAS DE SEGURIDAD

En esta sección se darán de alta las herramientas destinadas a la seguridad del sistema, como, por ejemplo:

- Detección de software dañino.
- Borrado seguro.
- Análisis del tráfico.
- Cifrado de archivos.

NUEVA HERRAMIENTA DE SEGURIDAD

Completa los campos para añadir una nueva herramienta de seguridad.

EXISTEN CAMPOS OBLIGATORIOS *

Tipo *

Nombre *

Versión *

Certificación *

[CREAR HERRAMIENTA](#)

Ilustración 59. Formulario de herramientas de seguridad.

Tipo	Nombre	Versión	Ver/editar	Borrar	Copiar
Detección de software dañino	Antivirus	1.0			

Ilustración 60. Listado de herramientas de seguridad.

6.6.8 APLICACIONES

En esta sección se darán de alta las distintas aplicaciones instaladas en el sistema.

NUEVA APLICACIÓN

Completa los campos para añadir una nueva aplicación.

EXISTEN CAMPOS OBLIGATORIOS *

Nombre *

Versión *

[CREAR APLICACIÓN](#)

Ilustración 61. Formulario de alta de aplicaciones.

Nombre	Versión	Ver/editar	Borrar	Copiar
Aplicación para leer PDF	1.0			

Ilustración 62. Listado de aplicaciones.

6.7 SEGURIDAD DEL SISTEMA

6.7.1.1 Declaración de aplicabilidad

En este apartado se podrá contestar al formulario de la declaración de aplicabilidad, indicando si los criterios aplican en el sistema o no. Asimismo, se podrá indicar las medidas compensatorias o complementarias que se desean presentar al criterio, e incluir información sobre ellas.

Se podrá descargar una plantilla Excel (“DESCARGAR EXCEL”) y un documento Word (“DESCARGAR DOC”) para facilitar el proceso.

1. DECLARACIÓN DE APLICABILIDAD

INFORMACIÓN
Los criterios de aplicación de las medidas serán los correspondientes a los requisitos de seguridad del sistema.

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

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

Nº total de medidas **62**

Medidas	Dimensiones	Aplica	Compensatoria/Complementaria
[org-1] Política de seguridad	Todas	Aplica	
[org-2] Normativa de seguridad	Todas	Aplica	

Ilustración 63. Declaración de aplicabilidad.

Para incluir una medida complementaria o compensatoria, primera se deberá seleccionar “Aplica” en el desplegable (seleccionada por defecto) y posteriormente seleccionar en el siguiente desplegable la opción elegida. El icono de dialogo se coloreará azul, indicando que se puede añadir un criterio de aplicabilidad. Al lado de este aparecerá un icono rojo y dependiendo de la opción elegida en el desplegable de tipo de medida, se deberá completar el formulario específico. Una vez rellenado el icono se coloreará azul.

CRITERIO DE APLICABILIDAD

Criterio:

GUARDAR

Ilustración 64. Insertar criterio de aplicabilidad.

MEDIDA COMPLEMENTARIA

Nombre *

Limitaciones o restricciones

Objetivo

GUARDAR

Ilustración 65. Insertar medida complementaria.

MEDIDA COMPENSATORIA



Nombre *	
Limitaciones o restricciones	
Objetivo	
Riesgo identificado	
Definición	
Validación	
Mantenimiento	

GUARDAR

Ilustración 66. Insertar medida compensatoria.

Medidas	Dimensiones	Aplica	Compensatoria/Complementaria
[org.1] Política de seguridad	Todas	Aplica	Compensatoria
⚠ [org.2] Normativa de seguridad	Todas	Aplica	Complementaria
⚠ [org.3] Procedimientos de seguridad	Todas	Aplica	Compensatoria

Ilustración 67. Detalle de iconos con criterio o medidas rellenos.

6.7.1.2 Seguridad de las emisiones

En esta sección se podrán subir los certificados de emisiones con los que cuenta el sistema.

Por defecto existe ya un certificado creado, el *TEMPEST*, en cuya fila se puede subir el archivo que muestra la certificación. Este certificado se puede ver o editar, o borrar.

El certificado se puede subir o sustituir pulsando sobre el icono de la columna “Subir”, se puede consultar una vez subido pulsando sobre el icono de la columna “Descargar”.

Para poder subir un certificado, es necesario haber creado el registro que lo alojará en DOCSEG, para ello se pulsará el botón “AÑADIR CERTIFICADO”.

NUEVO CERTIFICADO

Complete los campos para añadir un nuevo certificado.

EXISTEN CAMPOS OBLIGATORIOS *

Nombre *

CREAR CERTIFICADO

Ilustración 68. Formulario nuevo certificado.

The screenshot shows a web interface with a navigation bar at the top containing four tabs: 'Seguridad de las TIC', 'Seguridad de las emisiones' (which is active), 'Seguridad criptológica', and 'Dispositivos removibles'. Below the tabs, there is a 'Mostrar' dropdown set to '5 registros' and a 'Buscar:' field. A table with five columns is displayed: 'Nombre', 'Subir', 'Descargar', 'Ver/editar', and 'Borrar'. The table contains one row with the text 'Certificado TEMPEST'. Below the table, it says 'Mostrando 1 - 1 de 1'. On the right side of the interface, there is a button labeled 'AÑADIR CERTIFICADO' and a 'Anterior 1 Siguiente' pagination control.

Ilustración 69. Nuevo certificado subido.

6.8 GESTIÓN DE LA SEGURIDAD TIC

En esta sección se detallarán las acciones para el mantenimiento de la configuración de seguridad del sistema y su gestión.

Consta de varias secciones que será necesario completar para avanzar en el proceso.

6.8.1 ENTRADA Y SALIDA DE DOCUMENTACIÓN

6.8.1.1 Descripción general del proceso

En campo de texto designado se dará una explicación de cómo se realiza el proceso de entrada y salida de la información.

1.1 DESCRIPCIÓN GENERAL DEL PROCESO

1 - Indique la descripción general del proceso.

An empty rectangular text input field with a thin border, intended for the user to provide a general description of the process.

Ilustración 70. Descripción general del proceso de entrada y salida de información.

6.8.1.2 Entrada de información

En campo de texto designado se dará una explicación de cómo se realiza el proceso de entrada de información más detallado.

El desplegable “Soportes autorizados”, estará formado por los soportes que se dieron de alta en el apartado 6.6.2 de esta guía. En caso de seleccionar “Otros” se deberá incluir información sobre el soporte en el campo de texto que se habilitará.

1.2 ENTRADA DE INFORMACIÓN

1 - Indique el procedimiento que se sigue para la entrada de información

2 - Soportes autorizados

3 - Otros

4 - Información adicional

Ilustración 71. Entrada de información.

6.8.1.3 Salida de información

En campo de texto designado se dará una explicación de cómo se realiza el proceso de salida de información más detallado.

El desplegable “*Soportes autorizados*”, estará formado por los soportes que se dieron de alta en el apartado 6.6.2 de esta guía. En caso de seleccionar “*Otros*” se deberá incluir información sobre el soporte en el campo de texto que se habilitará.

1.3 SALIDA DE INFORMACIÓN

1 - Indique el procedimiento que se sigue para la salida de información

2 - Soportes autorizados

3 - Otros

4 - Información adicional

Ilustración 72. Salida de información.

6.8.1.4 Otros datos de interés

En este campo de texto se podrán expresar aquellos datos sobre la entrada y salida de la información que no se encuentren contemplados u otro apartado.

1.4 OTROS DATOS DE INTERÉS

1 - Indique otros datos de interés

Ilustración 73. Otros datos de interés.

6.8.1.5 Personal autorizado

En este listado se podrá añadir aquel personal involucrado en el manejo de información.

Para añadir nuevo personal se pulsará sobre el botón “*AÑADIR PERSONAL*”.

Sólo se podrán añadir aquellos roles que previamente se hayan creado en el apartado 6.5.2.1 de esta guía.

NUEVO PERSONAL AUTORIZADO

Complete los campos para añadir un nuevo personal autorizado.

EXISTEN CAMPOS OBLIGATORIOS *

Rol *

Indique la tarea del rol *

[CREAR PERSONAL](#)

Ilustración 74. Formulario alta de personal.

Una vez guardado, el nuevo personal aparecerá en el listado. El personal añadido se puede ver o editar y borrar.

1.5 PERSONAL AUTORIZADO [AÑADIR PERSONAL](#)

Mostrar registros

Buscar:

Rol	Tarea	Ver/editar	Copiar
Administrador del sistema AS	Admin	🔍	🗑️

Mostrando 1 - 1 de 1

[Anterior](#) [Siguiente](#)

Ilustración 75. Nuevo personal dado de alta.

6.8.2 DISPOSITIVOS REMOVIBLES

Para dar de alta un dispositivo removable se deberá pulsar el botón “AÑADIR DISPOSITIVO”.

Una vez pulsado, aparecerá un formulario, todos los campos son obligatorios.

NUEVO DISPOSITIVO REMOVIBLE

Completa los campos para añadir un nuevo dispositivo removable.

EXISTEN CAMPOS OBLIGATORIOS *

Nombre *

Descripción *

Etiquetado *

[CREAR DISPOSITIVO REMOVIBLE](#)

Ilustración 76. Formulario nuevo dispositivo removable.

Una vez guardado, el dispositivo removable aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los dispositivos removibles dados de alta. Los dispositivos removibles se pueden ver o editar, borrar y copiar.

Seguridad de las TIC	Seguridad de las emisiones	Seguridad criptológica	Dispositivos removibles
			DESCARGAR LISTADO AÑADIR DISPOSITIVO
Mostrar 5 registros			Buscar: _____
Nombre	Descripción	Etiquetado	Ver/editar Borrar Copiar
SSD 2,5"	Disco duro externo	ETI-001	🔍 🗑️ 📄
Mostrando 1 - 1 de 1			Anterior 1 Siguiente

Ilustración 77. Nuevo dispositivo removable dado de alta.

6.8.3 COPIAS DE SEGURIDAD

En este apartado se introducirá toda la información relativa a las copias de seguridad del sistema.

Asimismo, en este apartado se detallará la información relativa a las pruebas de restauración del sistema.

1. COPIAS DE SEGURIDAD

- 1 - Indique de qué partes del sistema realiza las copias de seguridad _____
- 2 - Indique el contenido de sus copias de seguridad _____
- 3 - Indique la periodicidad _____
- 4 - Indique dónde almacena las copias de seguridad _____
- 5 - Indique la ubicación interna _____
- 6 - Indique la ubicación externa _____

1.1 PRUEBAS DE RESTAURACIÓN

- 1 - Indique de qué partes del sistema realiza pruebas de restauración _____
- 2 - Indique la frecuencia de las pruebas de restauración _____

Ilustración 78. Información sobre las copias de seguridad.

6.8.4 GESTIÓN DE INCIDENTES

En este apartado se introducirá la información relativa a la gestión de incidentes.

6.8.4.1 Gestión de incidentes

En este apartado se introducirá la información sobre la generación y notificación de incidentes de seguridad.

1. GESTIÓN DE INCIDENTES

INFORMACIÓN
 Personas responsables en la generación y notificación de incidentes

1 - Indique a quién se le comunican los incidentes de seguridad _____
 2 - Indique el procedimiento que se sigue para comunicar los incidentes de seguridad _____
 3 - Indique cómo se informan los incidentes de seguridad _____

Ilustración 79. Gestión de incidentes.

6.8.4.2 Incidentes

En este apartado se podrá rellenar un formulario con la información relativa a incidentes de seguridad que se hayan producido en el sistema.

Para dar de alta un nuevo incidente se deberá pulsar sobre el botón “**AÑADIR INCIDENTE**”.

NUEVO INCIDENTE

Complete los campos de todas las pestañas para añadir un nuevo incidente.

EXISTEN CAMPOS OBLIGATORIOS *

①	Asunto *	
①	OSE/PSD *	
①	Sector estratégico *	
①	Fecha y hora del incidente *	dd/mm/aaaa --:--
①	Fecha y hora de detección del incidente *	dd/mm/aaaa --:--
①	Descripción *	
①	Recursos tecnológicos afectados *	
①	Origen del incidente *	
①	Taxonomía (clasificación) *	Selecciona una opción
①	Nivel de peligrosidad *	
①	Nivel de impacto *	

Ilustración 80. Formulario de alta de nuevo incidente.

①	Impacto transfronterizo *	
①	Plan de acción y contramedidas *	
①	Afectación *	
①	Medios necesarios para la resolución (J-P) *	
①	Impacto económico estimado (si se conoce)	
①	Extensión geográfica (si se conoce)	
①	Daños reputacionales (si se conocen)	
①	Adjuntos *	
①	Regulación afectada *	Selecciona una opción
①	Se requiere actuación de FCCSE *	Selecciona una opción
①	Notificar a *	

! Podrá notificar el incidente desde el apartado ver/editar de la tabla.

CREAR INCIDENTE

Ilustración 81. Formulario de alta de nuevo incidente.

Una vez guardado, el incidente aparecerá en el listado. Como es habitual, se podrá descargar un fichero Excel con todos los incidentes dados de alta. Los incidentes se pueden ver o editar, borrar y copiar.

2. INCIDENTES

DESCARGAR LISTADO

AGREGAR INCIDENTE

INFORMACIÓN

Asistente para la generación de incidentes a los organismos que no tienen LUCÍA.

Mostrar 5 registros

Buscar:

Asunto	Fecha y hora	Taxonomía	Ver/editar	Borrar	Copiar
Incidente ransomware	21/07/2022 00:00:00	Contenido dañino			

Mostrando 1 - 1 de 1

Anterior 1 Siguiente

Ilustración 82. Nuevo incidente dado de alta.

Una vez dado de alta un incidente, se podrá notificar si se ingresa en él a través del botón de la columna “Ver/editar”.

6.8.5 INFORME ANUAL DE ACREDITACIÓN

En este apartado se indicará la fecha en la que se realizarán los informes anuales de acreditación.

1. INFORME ANUAL DE ACREDITACIÓN

INFORMACIÓN

Recuerde que anualmente deberá notificar el estado de seguridad del sistema: si ha sufrido cambios significativos, si se ha modificado configuraciones de seguridad, si se han añadido o eliminado elementos y el motivo.

1 - Indique la fecha anual para el envío de los informes de seguridad 25/07/2022

Ilustración 83. Informe anual de acreditación.

6.8.6 GESTIÓN DE USUARIOS

En este apartado se introducirá la información relativa a la gestión de usuarios.

1 - Procedimiento

0/2048 caracteres

Ilustración 84. Información relativa a los usuarios.

6.8.7 MANTENIMIENTO DEL SISTEMA

En este apartado se introducirá la información relativa a los procedimientos que se llevan a cabo para actualizar los sistemas operativos, aplicaciones y antivirus, entre otros.

1 - Procedimiento

0/2048 caracteres

Ilustración 85. Información relativa al mantenimiento del sistema.

6.8.8 GESTIÓN DE ETIQUETAS

En este apartado se introducirá la información relativa a los procedimientos que se llevan a cabo cuando se instalan o sustituyen las etiquetas de seguridad.

1 - Procedimiento

0/2048 caracteres

Ilustración 86. Información relativa a la gestión de las etiquetas.

6.9 REPOSITORIO DOCUMENTAL

En esta sección se podrán descargar todos los documentos y listados que se han subido durante el proceso a DOCSEG.

Para descargarlos se deberá pulsar el botón correspondiente “DESCARGAR”.

1. DOCUMENTOS DISPONIBLES PARA SU DESCARGA

Concepto	Nombre del documento	Extensión	Enlace
Documentación de seguridad del sistema	Sistema grado reservado nacional_Documentacion de seguridad.docx	docx	DESCARGAR
Declaración de aplicabilidad (xlsx)	Sistema grado reservado nacional_Declaracion de Aplicabilidad	xlsx	DESCARGAR
Declaración de aplicabilidad	Sistema grado reservado nacional_Declaración de Aplicabilidad	docx	DESCARGAR
Certificados de acreditación	Sistema grado reservado nacional_Certificados de acreditación	zip	DESCARGAR
Certificados TEMPEST	Sistema grado reservado nacional_Certificados_TEMPEST	zip	DESCARGAR
Análisis de riesgos y amenazas	Sistema grado reservado nacional_Análisis de riesgos y amenazas	zip	DESCARGAR
Listados	Sistema grado reservado nacional_Listados	zip	DESCARGAR

Ilustración 87. Repositorio documental.

Toda esta información es la que posteriormente se subirá al espacio reservado de LORETO.

Se incluirán además los informes de la solución CLARA STIC de todos los elementos que conforman el sistema, así como cualquier otro documento que se considere relevante para el proceso de acreditación del sistema.

6.10 SOLICITUD DE ACREDITACIÓN

En esta sección, se podrá enviar la solicitud de acreditación con la información adjuntada hasta este momento en DOCSEG.

6.10.1 TRAMITACIÓN

En este apartado se podrá enviar la solicitud de acreditación.

Algunos campos del formulario estarán rellenos con la información aportada en el apartado 6.1 de esta guía.

1. INFORMACIÓN DEL SISTEMA

Responsable de seguridad del sistema / Persona de contacto	Nombre y apellidos completos
Correo electrónico de contacto	acreditacion.ccn@cni.es
¿Tiene el sistema un código NEASTIC anterior?	Sí
Introduzca el código	XXXX-XXXX-XXXX
Órgano de Control (OG)	Nombre del órgano de control
Jefe de Seguridad del OC	Nombre y apellidos completos
Correo del jefe de seguridad del OC	jefe_seguridad@ccn.es

Ilustración 88. Información del sistema.

2. NOTIFICACIÓN

INFORMACIÓN

Una vez completadas y verificadas todas las secciones, deberá notificar a las autoridades competentes que se encuentra disponible la Documentación de Seguridad de su sistema para su tramitación.

Crear notificación

Histórico

Solicitado por: Acreditación (DOCSEG) CCN

Aprobado por:

☐ ¿Se trata de una reacreditación?

NOTIFICAR

Ilustración 89. Notificación.

Para enviar una nueva solicitud se deberá pulsar el botón “NOTIFICAR”, pero antes se ha de especificar en el desplegable “Aprobado por” quien ha aprobado el proceso de acreditación.

6.10.2 HISTÓRICO

En este apartado figurarán las solicitudes creadas por el usuario.

Crear notificación

Histórico

DOCSEG_20250214_0059

Identificador: DOCSEG_20250214_0059

Órgano de Control (OC): Nombre del órgano de control

Jefe de Seguridad del OC: Nombre y apellidos completos

Correo del jefe de seguridad del OC: jefe_seguridad@ccn.es

Responsable de seguridad del sistema / Persona de contacto: Nombre y apellidos completos

Correo electrónico de contacto: acreditacion.ccn@ccn.es

¿Tiene el sistema un código NEASTIC anterior? Sí

¿Se trata de una reacreditación?

Introduzca el código: XXXX-XXXX-XXXX

Solicitado por: Acreditación (DOCSEG) CCN

Aprobado por: Responsable de Seguridad, Jefe del órgano de control

Estado: Enviado

Ilustración 90. Solicitudes creadas.

