

INSTRUCCIONES PARA CUMPLIMENTAR EL FORMULARIO DE ACREDITACIÓN DE SEGURIDAD (FASE)



1. OBJETO	4
2. ALCANCE.....	4
3. CONSIDERACIONES PREVIAS	4
4. CONFIGURACIÓN DE ADOBE ACROBAT	5
4.1. ACTIVAR JAVAScript	5
4.2. SEGURIDAD MEJORADA.....	6
4.3. OPCIONES DE VISUALIZACIÓN DE LOS CAMPOS DEL FORMULARIO	7
5. CUMPLIMENTACIÓN DEL FORMULARIO	7
5.1. CÓMO INTERACTUAR	8
5.2. ESTRUCTURA.....	8
5.3. VALIDACIÓN	9
5.4. FIRMA	10
6. TRAMITACIÓN	10
7. CASO PRÁCTICO: CENTRO DE INVESTIGACIÓN.....	11
7.1. RENOVACIÓN ACREDITACIÓN ZAR ÓRGANO DE CONTROL	13
7.1.1. Datos básicos.....	13
7.1.2. Entorno global	15
7.1.3. Entorno local	26
7.1.4. Entorno próximo	37
7.1.5. Plan de emergencia.....	46
7.1.6. Declaración	48
7.2. APERTURA ZAR SALA DE REUNIONES.....	50

7.2.1. Datos básicos	50
7.2.2. Entorno global.	51
7.2.3. Entorno local	52
7.2.4. Entorno próximo	56
7.2.5. Plan de emergencia.....	58
7.2.6. Declaración	58
7.3. APERTURA ZAR CENTRO DE PROCESO DE DATOS	60
7.3.1. Datos básicos.....	60
7.3.2. Entorno global	61
7.3.3. Entorno local	62
7.3.4. Entorno próximo	66
7.3.5. Plan de emergencia.....	68
7.3.6. Declaración	68

1. OBJETO

La presente guía tiene por objeto proporcionar las instrucciones para cumplimentar el formulario de acreditación de seguridad (FASE) donde se declaran las medidas de seguridad en el entorno físico de las zonas de acceso restringido (ZAR) donde se maneja información clasificada.

2. ALCANCE

Esta guía es de aplicación para los órganos de control (OC) que precisen constituir una ZAR.

FASE estará disponible en la página web del CNI dentro de la pestaña de la [Oficina Nacional de Seguridad](#), siendo recomendable descargar dicho formulario cada vez que se solicite una acreditación para asegurar que se utiliza la versión en vigor.

3. CONSIDERACIONES PREVIAS

FASE es un documento PDF interactivo donde se declaran las medidas y procedimientos de seguridad implantados en un local para solicitar su acreditación (apertura o renovación) como ZAR.

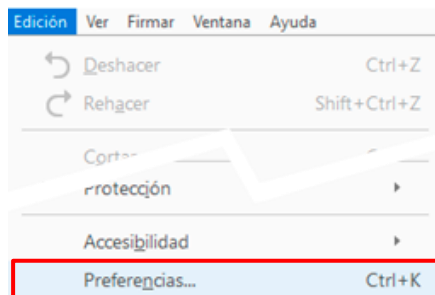
Para abrirlo y rellenarlo, se recomienda tener instalado en el ordenador la última versión del software *Adobe Acrobat Reader*. También puede completarse desde los principales navegadores web siempre y cuando dispongan del *plugin* de *Acrobat* actualizado. No se recomienda el empleo de aplicaciones ni *plugins* de terceros ya que pueden no admitir todas las opciones de PDF y presentar problemas de compatibilidad con este tipo de formularios.

Adobe Acrobat Reader puede descargarse de forma gratuita desde [aquí](#).

Como último paso antes de su envío, el formulario requiere ser firmado, por lo que es necesario disponer de firma digital. No es objeto de esta guía explicar cómo obtener o instalar el certificado digital sino simplemente el procedimiento para incorporar la firma en el PDF.

4. CONFIGURACIÓN DE ADOBE ACROBAT

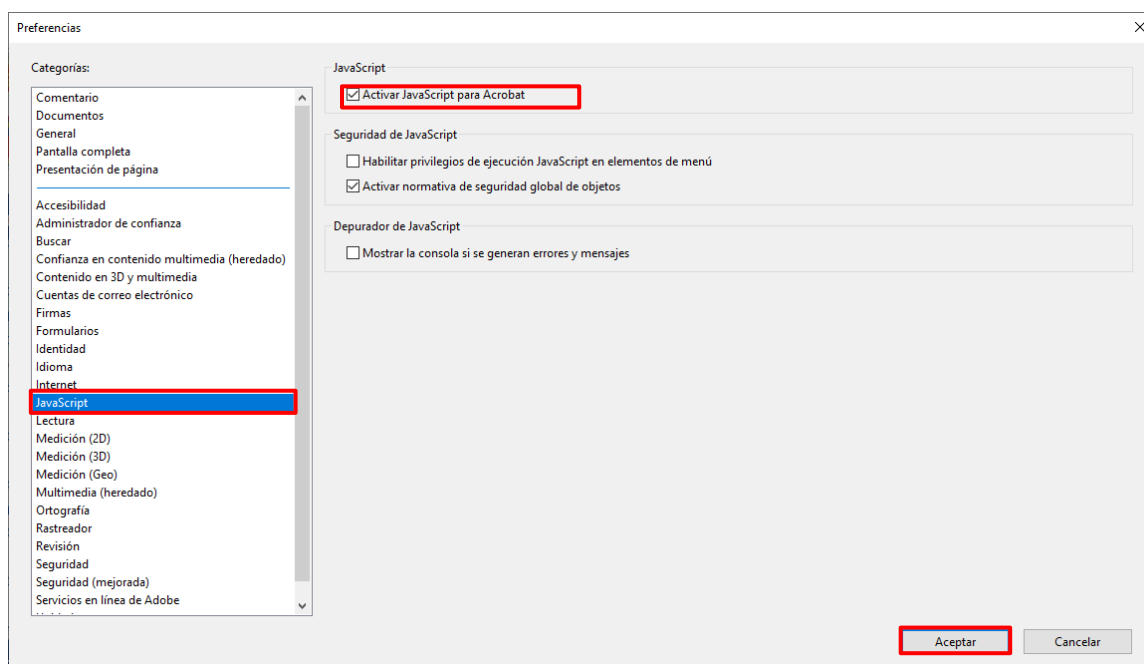
Cuando se instala el software *Adobe Reader*, la configuración por defecto permite trabajar desde el primer momento con el formulario. Ahora bien, para una adecuada visualización y funcionamiento del mismo es necesario activar las siguientes características que se encuentran en el menú “Edición > Preferencias”:



4.1. Activar JavaScript

Esta opción es imprescindible para rellenar los formularios:

- En la ventana “Preferencias”, clicar en la sección categorías la opción “JavaScript”.
- Marcar la opción “Activar JavaScript para Acrobat”.
- Pulsar “Aceptar”.



4.2. Seguridad mejorada

“Seguridad mejorada” permite proteger el equipo frente a amenazas, al bloquear o permitir de manera selectiva acciones para ubicaciones y archivos de confianza. Si la seguridad mejorada está activa, sólo los archivos, carpetas y ubicaciones en los que se ha confiado están exentos de restricciones. Por tanto, resulta muy importante que FASE sea considerado como un archivo de confianza:

- En la ventana “Preferencias”, clicar en la sección “Categorías” la opción “Seguridad (mejorada)”.
- Revisar que si está marcada la opción "Activar seguridad mejorada".
- Gestionar los archivos, carpetas o ubicaciones a través de las opciones que aparecen en la sección “Ubicaciones privilegiadas” (“Agregar archivo”, “Agregar ruta de carpeta” y “Agregar host” respectivamente).
- Presionar el botón “Aceptar”. Cuando se cierre el formulario y se vuelva abrir se aplicarán los cambios efectuados.

Preferencias

Categorías:

- Comentario
- Documentos
- General
- Pantalla completa
- Presentación de página
- Accesibilidad
- Administrador de confianza
- Buscar
- Confianza en contenido multimedia (heredado)
- Contenido en 3D y multimedia
- Cuentas de correo electrónico
- Firmas
- Formularios
- Identidad
- Idioma
- Internet
- JavaScript
- Lectura
- Medición (2D)
- Medición (3D)
- Medición (Geo)
- Multimedia (heredado)
- Ortografía
- Rastreador
- Revisión
- Seguridad
- Seguridad (mejorada)**
- Servicios en línea de Adobe
- Unidades

Protecciones de la zona de pruebas

☒ Habilitar modo protegido al iniciar ☐ Ejecutar en AppContainer ☐ Crear un archivo de registro en modo protegido [Visualizar registro](#)

Vista protegida: ☒ Desactivado

☐ Archivos de ubicaciones potencialmente no seguras

☐ Todos los archivos

Seguridad mejorada

☒ Activar seguridad mejorada ☐ Archivo de registro entre dominios [Ver](#)

Ubicaciones privilegiadas

Si tiene flujos de trabajo que se vean afectados de forma negativa por la configuración de seguridad, utilice Ubicaciones privilegiadas para confiar en archivos, carpetas y hosts de forma selectiva para excluirlos de las restricciones establecidas en la configuración de seguridad. Las ubicaciones privilegiadas le permiten trabajar de forma segura mientras otorga confianza a los elementos de su flujo de trabajo.

☐ Confiar automáticamente en los documentos con una certificación válida

☒ Confiar automáticamente en sitios de las zonas de seguridad de mi Win OS [Ver sitios de confianza de Windows](#)

[Agregar archivo](#) [Agregar ruta de carpeta](#) [Agregar host](#) [Quitar](#)

[¿Qué es el modo protegido?](#) [¿Qué es la seguridad mejorada?](#) [¿Qué son las ubicaciones privilegiadas?](#)

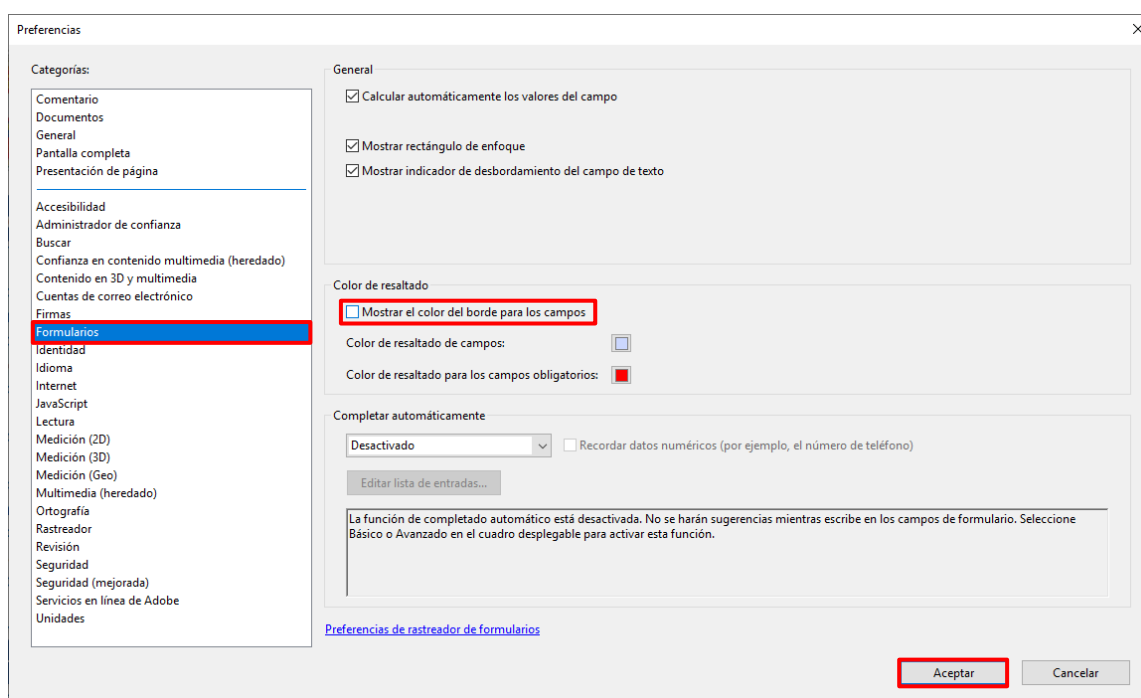
[Aceptar](#) [Cancelar](#)

Nota: Si no puede efectuar cambios en esta opción póngase en contacto con el administrador del sistema.

4.3. Opciones de visualización de los campos del formulario

Mediante esta opción se controla que la visualización del formulario sea la idónea para el correcto funcionamiento del mismo:

- En la ventana “Preferencias”, clicar en la sección “Categorías” la opción “Formularios”.
- Desmarcar la opción “Mostrar el color del borde para los campos” si estuviera señalada.
- Pulsar “Aceptar”.



5. CUMPLIMENTACIÓN DEL FORMULARIO

FASE está compuesto por múltiples campos, fundamentalmente cajas de texto, donde se describen procedimientos, y listas desplegables para seleccionar una opción de entre un conjunto de valores posibles. Estos campos a su vez pueden presentar dos estados distintos:

- Campo activo. Puede ser rellenado. El proceso de validación (que se describe abajo) no permitirá enviar el formulario si el campo es obligatorio y no se ha cumplimentado.
- Campo bloqueado. No se puede introducir ningún dato en ellos. Se distinguen por estar sombreados en color gris.

Existen algunos campos cuya selección condiciona el estado de otros así, por ejemplo, en el apartado “2.3 Puerta de emergencia” si en el campo “Tipo” seleccionamos “No dispone” automáticamente el resto de los campos de ese apartado pasan a estar bloqueados. La selección en ciertos campos provoca cambios en el color de algunas opciones. Estos colores proporcionan al usuario información de si cumplen con la normativa vigente. Por estas razones se recomienda rellenar el formulario siguiendo el orden de sus páginas.

Todos los campos disponen de pequeñas etiquetas emergentes color amarillo que se muestran cuando el cursor del ratón queda parado durante unos instantes encima del mismo, donde se muestra información adicional a la función del campo o botón.

2.2 PUERTA DE ENTRADA.

Tipo:	- Seleccionar -
Muelle:	Seleccionar el tipo de puerta considerando su construcción: "Blindada", cuando la estructura de hoja y cerco es de madera con refuerzos de acero; "Acorazada", cuando la estructura de hoja y cerco es de acero; y "Otro", para
Cerradura:	puertas convencionales o de otro tipo
Sensor apertura:	- Seleccionar -

La cumplimentación del formulario se realiza sin conexión, es decir, no necesita estar conectado a internet. El formulario parcialmente cumplimentado puede guardarse en cualquier momento y volver a él más tarde; si guarda el formulario regularmente evitará la pérdida de datos.



5.1. Cómo interactuar

Para desplazarse y seleccionar los distintos campos del formulario utilizaremos el ratón. Ahora bien, si lo desea puede emplear únicamente el teclado:

- Presione la tecla *Tab* para desplazarse por los campos hacia adelante o *Mayús+Tab* para desplazarse hacia atrás.
- Si el campo con el foco es una casilla de verificación o un botón, presionando *Intro* o la barra espaciadora se podrá seleccionar (o anular la selección si ya lo estaba).
- Si el campo con el foco es una lista desplegable, las flechas del teclado nos permitirán desplazarnos por los distintos elementos de la lista.

5.2. Estructura

El formulario consta de seis páginas que deben de cumplimentarse para la acreditación de cada local. En la primera de ellas se consignarán los datos básicos de la ZAR

relativos a su ubicación (dirección, provincia, país, edificio, etc.), y a la solicitud de acreditación para el manejo y/o custodia de información clasificada (ámbito, grado máximo, clase, especialidad, etc.). También se debe añadir el plano en planta del local a acreditar, sin incorporar simbología de ningún tipo (sistemas de seguridad, incendios, etc.) ni ceñirse exclusivamente al límite de la ZAR, sino mostrar una visión más amplia del entorno como por ejemplo un ala o planta del edificio.

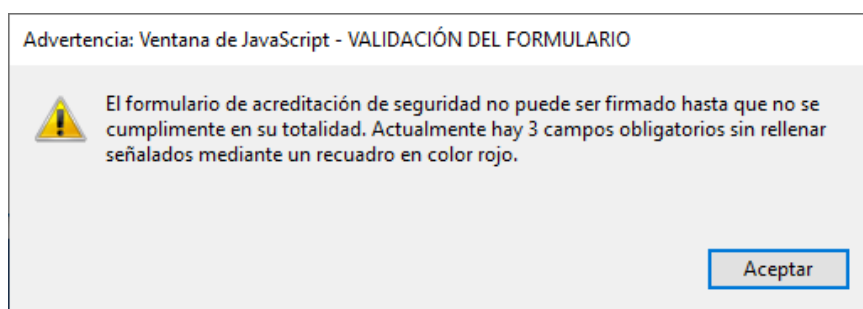
En las tres páginas siguientes (pág. 2, 3 y 4) y siguiendo el esquema de defensa en profundidad, se describe la seguridad existente en cada uno de los entornos (global, local y próximo) y perímetros en los que se divide la instalación. Cada página se estructura en diferentes apartados que agrupan las distintas medidas de seguridad adoptadas, y cada apartado en distintos campos formados por listas desplegables o cuadros de texto. En estos cuadros de texto generalmente se recogen los procedimientos de seguridad donde se explicarán las medidas organizativas adoptadas para reducir el riesgo existente.

La página 5 del formulario está dedicada a describir las medidas organizativas de seguridad a adoptar para mantener la protección de la información clasificada ante contingencias de tipo extraordinario. Al igual que el resto del formulario se divide en apartados donde se detallan los distintos procedimientos y actuaciones, tanto comunes como particulares ante distintos tipos de emergencias.

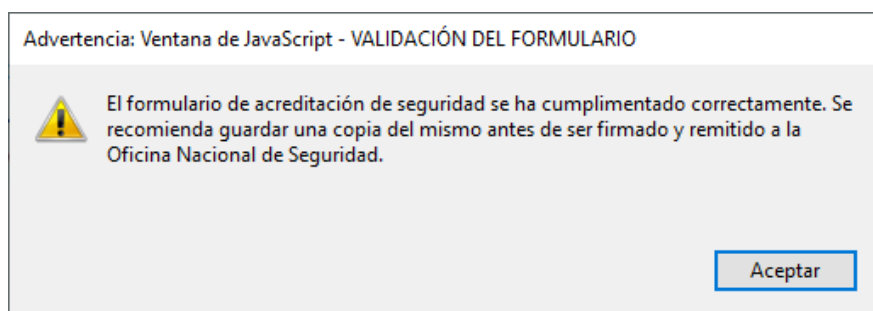
En la última página del formulario se dispone de un espacio para efectuar cualquier aclaración u observación a lo declarado en el mismo, indicando el número del apartado al que hace referencia. También en esta página se encuentra el botón para “VALIDAR FORMULARIO” y los campos para ser firmado digitalmente.

5.3. Validación

Tras cumplimentar totalmente el formulario, debe validarse antes de poder ser firmado. Para ello pulsar sobre el botón “VALIDAR FORMULARIO” que efectuará una serie de comprobaciones en el mismo y mostrará mediante un recuadro rojo los campos obligatorios que no han sido rellenados.



Cumplimentados todos los campos se debe volver a validar el formulario y una vez indique que se ha completado correctamente se recomienda archivar en su ordenador una copia del mismo.



5.4. Firma

El formulario de acreditación de seguridad requiere de dos firmas. La primera de ellas corresponde al responsable de seguridad de la ZAR y encargado de la elaboración del documento. Mediante esta firma declara que son ciertos los datos consignados en él y, una vez incluida, los datos del formulario no podrán ser modificados.

La segunda de las firmas corresponde al jefe del órgano de control del que depende la ZAR y con ella declara que ha verificado que las medidas de seguridad recogidas en el formulario son correctas y se encuentran adecuadamente implantadas. Cuando el propio jefe del órgano de control sea a su vez responsable de seguridad de la ZAR, la responsabilidad será del jefe del órgano de control superior.

6. TRAMITACIÓN

El proceso de solicitud de acreditación (renovación o apertura) de una ZAR lo iniciará el órgano de control del que depende enviando el formulario cumplimentado junto con un oficio a la ONS a través de su estructura jerárquica para la protección de la información clasificada.

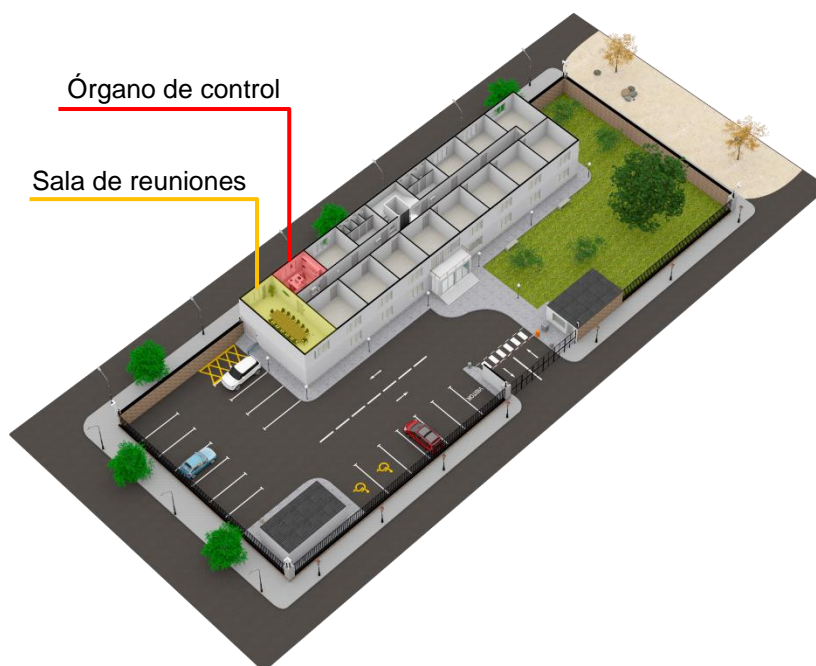
Una vez revisado y analizado el formulario por parte de la ONS se remitirá una "Hoja de resultados" donde se muestran los resultados en cada uno de los apartados declarados en FASE. Estos resultados pueden ir acompañados de observaciones y/o recomendaciones que se deberán tener en cuenta en futuros procesos de acreditación de la ZAR. Si no se detectarán deficiencias graves se emitirá el correspondiente certificado de acreditación de locales (CAL) que indica que el local objeto de estudio dispone de las medidas y procedimientos de seguridad suficientes para una adecuada protección de la información clasificada.

7. CASO PRÁCTICO: CENTRO DE INVESTIGACIÓN

Para ilustrar mejor cómo rellenar el formulario consideremos la siguiente instalación ficticia como ejemplo.



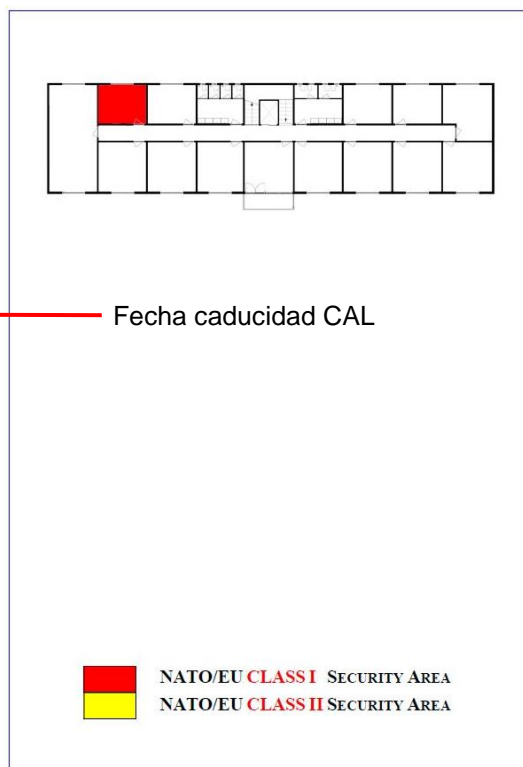
Se trata de un centro de investigación que dispone en la actualidad de estructura para la protección de información clasificada, en concreto, un órgano de control OTAN/UE situado en la primera planta. Puesto que la acreditación del local está próxima a caducar se debe solicitar su renovación.



Centro de investigación. Planta primera del edificio principal

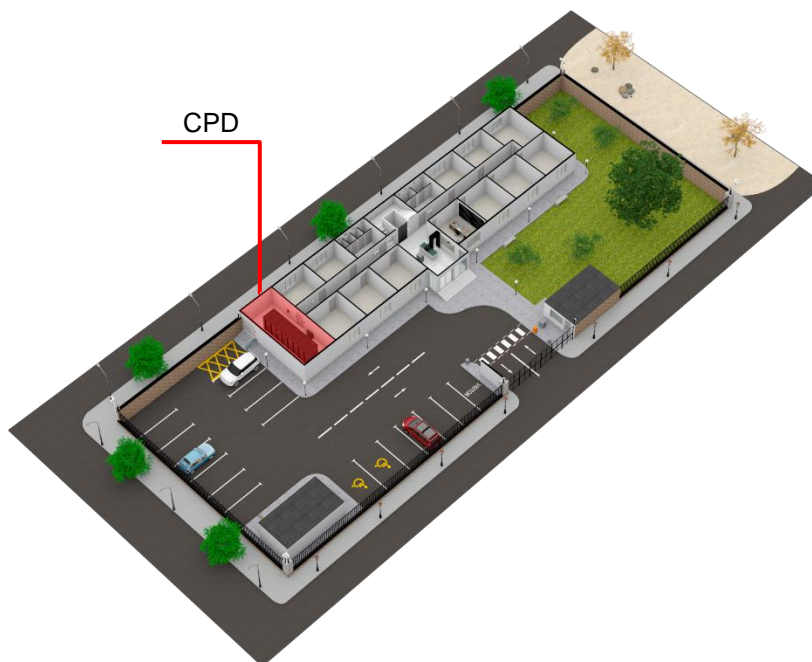
CERTIFICADO DE ACREDITACIÓN DE LOCALES	
NÚMERO DE CERTIFICADO: CAL-1000 / FECHA DE EXPIRACIÓN: 15/12/2023	
OFICINA NACIONAL DE SEGURIDAD	
SUBREGISTRO PRINCIPAL	OTAN/UE MINISTERIO DE INVESTIGACIÓN Y DESARROLLO
ORGANISMO / EMPRESA	CENTRO DE INVESTIGACIÓN
DIRECCIÓN COMPLETA	C/ REAL, 7 28000 - MADRID
DEPENDENCIA ACREDITADA	ÓRGANO DE CONTROL EDIFICIO: PRINCIPAL, PLANTA: 1, ALA IZDA., LOCAL: P1A3
RESPONSABLE	JEFE DE SEGURIDAD PUNTO DE CONTROL CENTRO DE INVESTIGACIÓN
JUSTIFICACIÓN	MANEJO Y CUSTODIA DE INFORMACIÓN CLASIFICADA
DOCUMENTACIÓN	D-OC-CI-10000001-S-18-02187 DE FECHA 15 DE DICIEMBRE DE 2018
CLASIFICACIÓN: ZONA DE ACCESO RESTRINGIDO CLASE I GRADO Y TIPOS: NATO SECRET / EU SECRET	
CUALQUIER MODIFICACIÓN DEL LOCAL ACREDITADO DEBERÁ SER APROBADA POR LA OFICINA NACIONAL DE SEGURIDAD. EN CASO CONTRARIO ESTE CERTIFICADO NO SERÁ VÁLIDO. Madrid, 15 de diciembre de 2018	
 ONS SECTOR PÚBLICO <small>Oficina Nacional de Seguridad Sector Público de Investigación</small>	

Formulario FPO-ASIP-01-06.02



Certificado Acreditación de Locales (CAL) de la ZAR Órgano de control.

Además, se necesitan acreditar otros dos nuevos locales: una sala de reuniones adyacente al órgano de control en la planta primera y un CPD situado en la planta baja que aloja sistemas OTAN/UE.



Centro de investigación. Planta baja del edificio principal

7.1. RENOVACIÓN ACREDITACIÓN ZAR ÓRGANO DE CONTROL**7.1.1. Datos básicos**

- a) **Datos de la zona de acceso restringido (ZAR).** En primer lugar, en la cabecera del apartado seleccionar que el formulario se rellena con motivo de una renovación (opción por defecto). Aquí también se encuentra el botón “LIMPIAR FORMULARIO”, que restaura los controles del formulario a sus valores por defecto.

DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)	<input checked="" type="checkbox"/> Renovación	<input type="checkbox"/> Apertura	LIMPIAR FORMULARIO
---	--	-----------------------------------	---------------------------

A continuación, se consignarán los datos identificativos de la ZAR y los relativos a la solicitud de manejo/custodia de información clasificada.

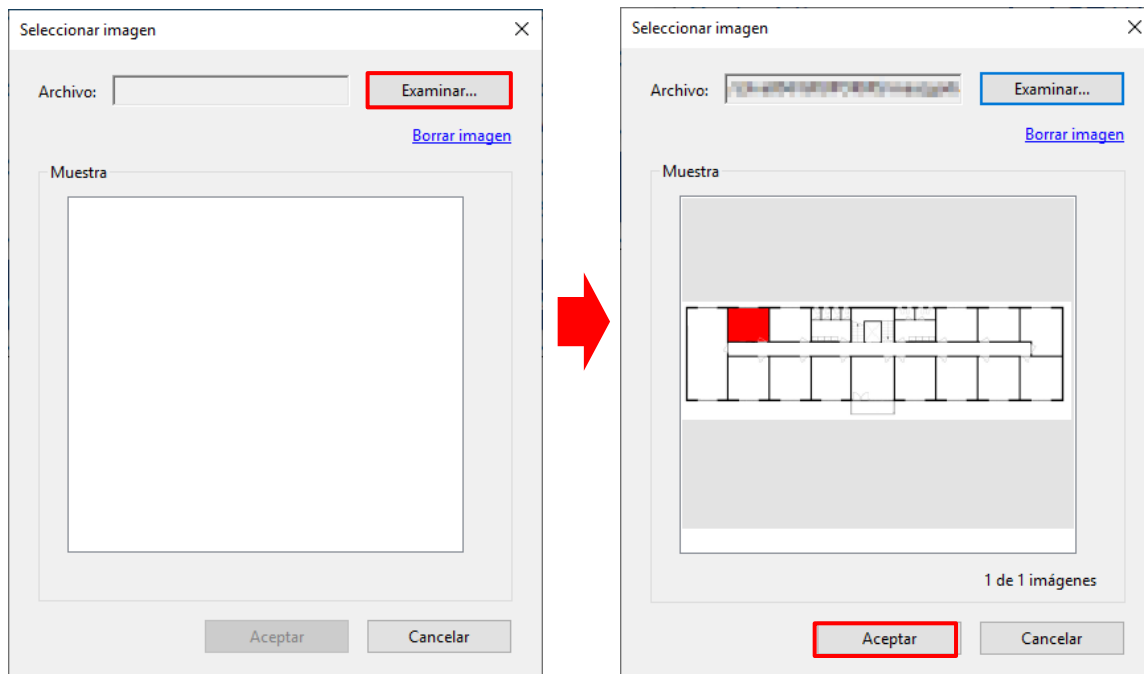
DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)		<input checked="" type="checkbox"/> Renovación	<input type="checkbox"/> Apertura	LIMPIAR FORMULARIO
ZAR Nº: 1000 ①	Órgano de control del que depende: PC CENTRO DE INVESTIGACIÓN ②			
Dirección: CALLE REAL, 7		Código postal: 28000		
Localidad:	Provincia: MADRID ③	País: ESPAÑA		
Edificio: PRINCIPAL	Planta: 1, ALA IZDA			
Local: P1A3				
Denominación: ÓRGANO DE CONTROL ④				
Grado máximo información clasificada (I.C.): RESERVADO o equivalente ⑤	Ámbito: ⑥	<input checked="" type="checkbox"/> OTAN	<input checked="" type="checkbox"/> UE	<input type="checkbox"/> ESA <input type="checkbox"/> NACIONAL
Clase: I ⑦	Uso: Manejo y custodia ⑧	Especialidad: Ninguna ⑨		

Fig. 1

- ZAR N°. Teclear el número del certificado de acreditación de locales (CAL) de la ZAR que se pretende renovar. En el caso del ejemplo 1000. (Fig. 1 ①)
- Órgano de control del que depende. Nombre del órgano de control del que depende la ZAR. En este caso la ZAR es el propio local donde se encuentra ubicado el Punto de Control OTAN/UE del Centro de investigación. (Fig. 1 ②)
- Dirección. Completar con la dirección postal de la ZAR (Calle Real, 7).
- Código postal. Introducir el código postal de la ZAR (28000).
- Localidad. Si la localidad es la misma que la provincia, este campo puede dejarse en blanco.
- Provincia. Si la ZAR se encuentra en España seleccionar la provincia de la lista desplegable (Madrid en este caso); si no es así, seleccionar previamente el país en el campo “País” y posteriormente introducir el nombre de la provincia, departamento, estado...(Fig. 1 ③)

- País. Seleccionar un país de la lista desplegable. (España)
 - Edificio. Identificación del edificio: nombre o número... (Edificio Principal)
 - Planta. Número de planta. En el caso de existir diferenciación por ala o zona, incorporar esta información separándola con una coma del número de planta. (1, Ala Izda.)
 - Local. Numeración, si existiese, del local o puerta dentro de la planta (P1A3). Si la ZAR estuviese formada por varios locales, indicar sus números separados por comas, "P1A3, P1A4, P1A5, P1A6". Si se tratara de una numeración consecutiva se puede indicar como "P1A3 a P1A6".
 - Denominación. Nombre que se da a la ZAR. Se debe evitar utilizar el número del local y/o el término ZAR, ya que sería redundante. En el ejemplo, al corresponder la ZAR con el Punto de Control OTAN/UE se denomina "Órgano de Control". (Fig. 1 ④)
 - Grado máximo información clasificada (I.C.). Indica la mayor calificación de seguridad relativa a la información clasificada con la que se puede trabajar en la ZAR. En el ejemplo "RESERVADO" (Fig. 1 ⑤)
 - Ámbito. Distingue el origen de la información clasificada que se va a manejar y/o custodiar. Para ello marcar los organismos u organizaciones internacionales mediante el ratón. En el ejemplo la información con la que se trabaja proviene de OTAN y UE. (Fig. 1 ⑥)
 - Clase. La diferencia entre ambas (clase I y clase II) radica en las condiciones de accesibilidad a la información clasificada dentro de cada zona. En el ejemplo, como no es posible ocultar toda la información clasificada o puede producirse con cierta probabilidad un acceso fortuito a la misma, se solicita que la ZAR sea Clase I. (Fig. 1 ⑦)
 - Uso. Indica si en la ZAR se va a almacenar o no información clasificada. En el caso del ejemplo la información clasificada se almacena en una caja fuerte por lo que se seleccionará "Manejo y custodia" en la lista. (Fig. 1 ⑧)
 - Especialidad. Indicar si se maneja información perteneciente a ámbitos más concretos que exigen una especial preparación y control más exhaustivo, como por ejemplo Atómico, Cripto, Sigint... En esta ZAR no se maneja este tipo de información por lo que se selecciona "Ninguna". (Fig. 1 ⑨)
- b) Plano de planta de la ZAR.** Se debe añadir el plano en planta del local a acreditar sin incorporar simbología de ningún tipo (sistemas de seguridad, incendios, etc.) ni ceñirse exclusivamente al límite de la ZAR, sino mostrar una visión más amplia

del entorno como por ejemplo un ala o planta del edificio. Para ello pulsar sobre el área destinada al plano con el botón izquierdo del ratón y en la ventana emergente seleccionar la imagen con el plano (fichero *jpg*, *png*, *bmp*, ...) a través del botón “Examinar”:



Finalmente pulsar el botón “Aceptar” para incorporar el plano al formulario.

7.1.2. Entorno global

- a) **Sistema de identificación personal.** Seleccionar las características del medio de identificación empleado en la organización:

1.1 SISTEMAS DE IDENTIFICACIÓN PERSONAL		
Tipo: Tarjeta de seguridad ①	Diferenciación personal/visitas (colores): Sí ②	Existe registro tarjetas expedidas: Sí ③
Descripción del procedimiento de gestión: altas, bajas, actuación en caso de pérdida, etc. ④		
La elaboración y codificación de las tarjetas corresponde a la división de seguridad del Centro, siendo de su responsabilidad la gestión de terminales y accesos. Estas tarjetas tienen impresa la foto del titular, número del DNI, Nombre y Apellidos, así como código de categoría (Oficial, Suboficial o Tropa).		

Fig. 2

- **Tipo.** Se debe seleccionar en la lista desplegable entre tarjeta de seguridad si integra algún sistema de acceso (banda magnética, RFID, etc.) u otro tipo de tarjeta o medio. En la instalación del ejemplo se utiliza una tarjeta de proximidad MIFARE (chip RFID), por lo que se selecciona “Tarjeta de seguridad”. (Fig.2 ①)

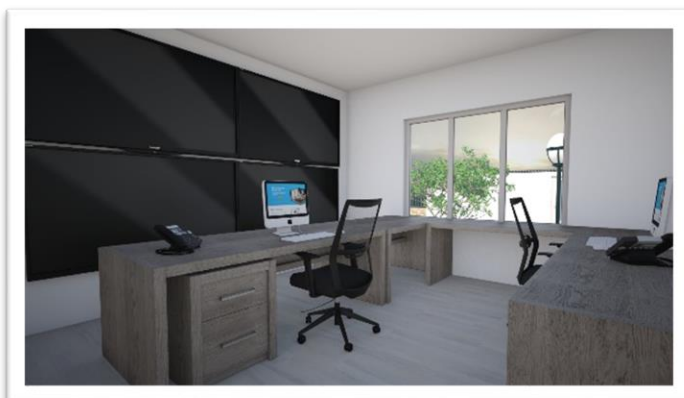
- Diferenciación personal/visitas (colores). Con el fin de practicar una identificación suplementaria entre visitantes y trabajadores que han accedido a los distintos entornos de seguridad se deben utilizar códigos de colores o símbolos diferentes que permita distinguirlos. En el Centro de Investigación se utilizan tarjetas de dos colores distintos: blanca para los trabajadores y naranja para las visitas por lo que en este campo se selecciona “Si”. (Fig. 2 ②)
- Existe registro tarjetas expedidas. Indicar si existe un registro de las tarjetas expedidas. En el caso del ejemplo, el sistema informático de seguridad del Centro mantiene una base de datos con las tarjetas emitidas, por lo que en este campo se selecciona “Si”. (Fig. 2 ③)
- Descripción del procedimiento de gestión. En este campo se detallan los procedimientos relativos al sistema de control de accesos disponible: alta y baja de usuarios, asignación de permisos, control de usuarios, elaboración de tarjetas de acceso, etc. (Fig. 2 ④)

b) Servicio de seguridad y centro de control de alarmas

1.2 SERVICIO DE SEGURIDAD Y CENTRO DE CONTROL DE ALARMAS			
Monitorización de alarmas (7x24): Monitorización interna (in-situ)	①	Alerta a servicio de seguridad: Sí	②
Tipo servicio de seguridad: Personal propio o FCSE	③	Habilitación seguridad de empresas: - Selecciona	④
Realiza patrullas u otros apoyos complementarios: Sí	⑤	Tiempo de respuesta a alarma: Adecuado	⑥
Descripción del procedimiento en caso de alarma:		⑦	
En caso de producirse una alarma ya sea por intrusión o sabotaje, la transmisión de la misma es automática al Centro de Control de Alarmas, activándose las actuaciones previstas en el Plan de Emergencia de la ZAR.			

Fig.3

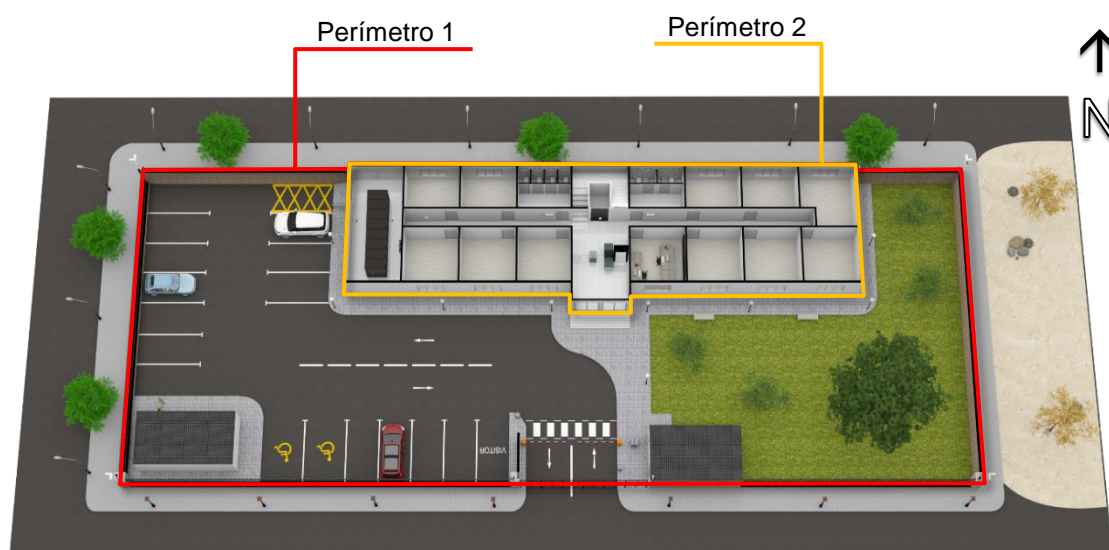
- Monitorización de alarmas (7x24). Indicar dónde se realiza la monitorización de las señales o alarmas: “Monitorización interna (in situ)” si se realiza en la misma instalación, “Monitorización externa” si se lleva a cabo en una empresa de seguridad o “Monitorización mixta” si por ejemplo en la jornada laboral se efectúa en la instalación, pero fuera se realiza desde una empresa de seguridad.



La instalación del ejemplo dispone de un Centro permanente de seguridad desde el que se controlan los sistemas de seguridad y alarmas (“Monitorización interna (in-situ)”). (Fig. 3 ①)

- Alerta a servicio de seguridad. Indicar si ante una alarma, el centro de control de alarmas tiene la capacidad de avisar al servicio de seguridad. En el Centro de investigación las alertas son gestionadas por el mismo servicio de seguridad, por lo que se selecciona “Sí”. (Fig. 3 ②)
 - Tipo de servicio de seguridad. Seleccionar el tipo de personal que lleva a cabo el servicio de seguridad. En el caso práctico lo efectúa personal militar, por lo que se selecciona “Personal propio o FCSE”. (Fig. 3 ③)
 - Habilitación de seguridad de empresas. En el caso que las labores de seguridad las desempeñe personal de una empresa privada, se debe indicar si dicha empresa dispone de la correspondiente habilitación de seguridad de empresas (HSEM). Como en el ejemplo la seguridad la proporciona personal militar, este campo aparece bloqueado. (Fig. 3 ④)
 - Realiza patrullas u otros apoyos complementarios. Indicar si el personal del servicio de vigilancia efectúa patrullas, guardias, inspecciones u otros apoyos complementarios al sistema de seguridad. En el caso que nos ocupa se realizan patrullas durante la noche e inspecciones de los despachos al finalizar la jornada laboral, por lo que se selecciona “Sí”. (Fig. 3 ⑤)
 - Tiempo respuesta a alarma. Se debe indicar si se considera adecuado o no el tiempo de reacción ante un caso de alarma. En el ejemplo se selecciona “Adecuado”, ya que en menos de dos minutos se cuenta con la presencia de las fuerzas de respuesta en cualquier punto de la instalación. (Fig. 3 ⑥)
 - Descripción procedimiento en caso de alarma. Describir la actuación del centro de recepción de alarmas. Procedimiento para la comunicación y actuación del personal implicado en la respuesta: guardia, fuerzas de reacción, responsables de seguridad, etc. (Fig. 3 ⑦)
- c) **Perímetros de seguridad**. Aplicando al caso del ejemplo el esquema de defensa en profundidad, en el que se divide la instalación en sucesivos perímetros de seguridad, se distinguen:
- Perímetro 1. Perímetro de seguridad más externo a la ZAR a proteger. En el caso del ejemplo lo delimitan los muros, vallas y la fachada norte del edificio principal.
 - Perímetro 2. Es el segundo perímetro de seguridad que nos encontramos al intentar acceder a la información clasificada. En el ejemplo consistiría en el propio edificio principal del Centro de investigación.
Los perímetros 1 y 2 constituyen el entorno global de seguridad de esta instalación.

- Perímetro 3. Lo forma la ZAR donde se encuentra la información a proteger y constituye el entorno local de seguridad de la misma.



Centro de Investigación. Entorno global, perímetros de seguridad.

En el apartado 1.3 del formulario, y en columnas separadas, se rellenan las características de los distintos elementos de seguridad pasiva y sistemas activos de protección que componen cada perímetro de seguridad del entorno global. En el ejemplo se cumplimentaría solo con los datos de los perímetros 1 y 2 ya que el perímetro 3 constituye el entorno local de seguridad y se describe en la página 3.

PERÍMETRO 1

- Cerramiento. Describe las características de los elementos estructurales de protección, indicando su tipo (muro, verja, valla, alambrada), resistencia y altura.

CERRAMIENTO	PERÍMETRO 1
Tipo:	Combinación de tipos ①
Resistencia:	Media ②
Altura:	Igual o mayor de 2,15 m ③

Fig. 4

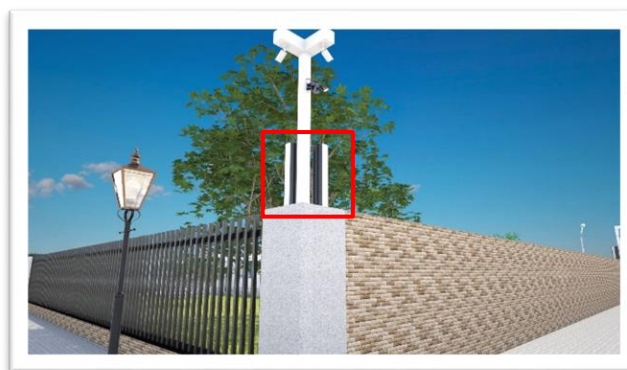
- *Tipo*. En el Centro de investigación, el cerramiento del primer perímetro de seguridad está formado por elementos de distinto tipo. Así la zona sur y este presenta murete con valla, mientras que el resto dispone de muro y la propia fachada norte del edificio principal. Se selecciona por tanto “Combinación de tipos” en el desplegable. (Fig. 4 ①)

- *Resistencia.* La resistencia del cerramiento será la menor de las partes que lo componen, en el ejemplo: muro con valla cuya resistencia se considera “Media”. (Fig. 4 ②)
- *Altura.* La altura del cerramiento es mayor de 2.15 m en todas sus zonas por lo que se selecciona “Igual o mayor a 2,15 m”. (Fig. 4 ③)
- Sistema perimetral de detección de intrusos. Los sistemas de seguridad pasivos descritos anteriormente se complementarán con sistemas activos de protección perimetral (barreras de infrarrojos, barreras de microondas, volumétricos exteriores, cables sensores, etc.) de los que se deberán detallar sus características.

SISTEMA PERIMETRAL DE DETECCIÓN DE INTRUSOS		
Tipo:	Barrera infrarrojos	①
Cobertura:	Todo el recinto	②
Antisabotaje:	Sí	③
Conectado a alarma:	Sí, al centro de control de alarmas	④
Conectado a sistema alternativo de energía:	Sí	⑤

Fig. 5

- *Tipo.* En el Centro de investigación dispone de barreras de infrarrojos que cubren la totalidad del primer perímetro de seguridad. Por tanto, seleccionar “Barrera infrarrojos” en el desplegable. (Fig. 5 ①)
- *Cobertura.* En el ejemplo el sistema perimetral de detección de intrusos cubre la totalidad del primer perímetro de seguridad. (Fig. 5 ②)
- *Antisabotaje.* Indicar si el dispositivo o sistema dispone de detección de intento de sabotaje (interruptor *tamper*, anti-inhibidores de frecuencia, *anti-masking*). El dispositivo instalado en el Centro de investigación dispone de antisabotaje. (Fig. 5 ③)
- *Conectado a alarma.* Indicar si el sistema o dispositivo está conectado con un centro de monitorización y control permanente de alarmas, o está conectado a un sistema autónomo que activa únicamente una alerta sonora al dispararse la alarma. En el ejemplo, todas las alarmas se reciben en el Centro permanente de seguridad. (Fig. 5 ④)

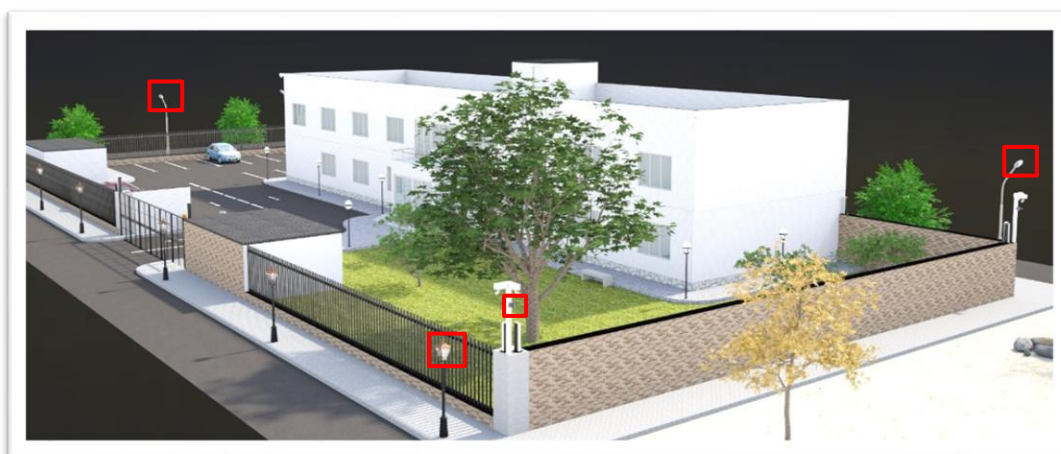


- *Conectado a sistema alternativo de energía.* Indicar si el sistema o dispositivo está conectado a algún sistema alternativo de energía (SAI, grupo electrógeno, batería, etc.) que permita su funcionamiento ante un corte de suministro eléctrico. (Fig. 5 ⑤)
- Sistema de iluminación del perímetro. Completar con las características de los sistemas de iluminación.

SISTEMA DE ILUMINACIÓN DEL PERÍMETRO	
Tipo:	Combinación de tipos ①
Visibilidad las 24h:	Sí ②
Antisabotaje:	No
Conectado a alarma:	No
Conectado a sistema alternativo de energía:	No

Fig. 6

- *Tipo.* Indicar si la iluminación es continua, como es el caso del alumbrado público; sorpresiva, cuyo funcionamiento está asociado a alguna alarma o evento, o móvil, cuando las luces se pueden desplazar a otras ubicaciones. El perímetro del Centro de investigación dispone de dos sistemas de iluminación: alumbrado público con farolas y báculos que cubre prácticamente la totalidad de la instalación e iluminación sorpresiva en la zona oeste. Al emplearse ambos sistemas, seleccionar “Combinación de tipos” en el desplegable del campo. (Fig. 6 ①)



- *Visibilidad las 24h.* Seleccionar si la totalidad del perímetro dispone de suficiente iluminación, ya sea natural o, artificial, a lo largo de todo el día. En el caso del ejemplo, seleccionar “Sí” ya que el perímetro se encuentra suficientemente iluminado. (Fig. 6 ②)
- *Antisabotaje, Conectado a alarma y Conectado a sistema alternativo de energía.* Los conceptos de los tres campos son análogos a los explicados en el caso de los PIDS. En el caso del ejemplo, el alumbrado público no

dispone de sistema antisabotaje, ni está conectado a ninguna alarma ni sistema alternativo de energía, por lo que se debe seleccionar “No” en los tres campos.

- Circuito cerrado de televisión (CCTV). Completar con las características de los sistemas de video vigilancia.

CIRCUITO CERRADO DE TELEVISIÓN (CCTV)	
Tipo:	Visión diurna/nocturna ①
Tiempo conservación grabaciones:	Mayor o igual a un mes ②
Antisabotaje:	Sí
Conectado a alarma:	Sí, al centro de control de alarmas
Conectado a sistema alternativo de energía:	Sí

Fig. 7

- *Tipo.* Atendiendo a su modo de funcionamiento, seleccionar el tipo de las cámaras de seguridad que controlan el perímetro. Seleccionar "Combinación de tipos" si se emplean conjuntamente cámaras solo de visión diurna y cámaras de visión diurna/nocturna. El perímetro del Centro de investigación dispone de cámaras de seguridad capaces de trabajar en condiciones de poca luz (infrarrojos), por lo que se debe seleccionar “Visión diurna/nocturna”. (Fig. 7 ①)
 - *Tiempo conservación grabaciones.* Indicar si se almacenan las grabaciones de seguridad y el tiempo de conservación de las mismas. Seleccionar “Mayor o igual a un mes” ya que en el Centro de investigación las videograbaciones se conservan durante 30 días. (Fig. 7 ②)
 - *Antisabotaje, Conectado a alarma y Conectado a sistema alternativo de energía.* Los conceptos de los tres campos son análogos a los explicados en apartados anteriores. En el caso del ejemplo, el sistema de vídeo vigilancia es monitorizado 7x24h en el Centro permanente de seguridad de la instalación (que a su vez es el centro de control de alarmas) y todas sus cámaras, dotadas de sistemas antisabotaje, están conectadas a un sistema alternativo de energía. Se debe seleccionar “Sí” en los tres campos.
- Sistema de control de acceso del perímetro.

SISTEMA DE CONTROL DE ACCESO DEL PERÍMETRO	
Tipo:	Personal de seguridad y electrónico ①
Identificación de vehículos:	Sí ②
Antisabotaje:	Sí
Conectado a alarma:	Sí, al centro de control de alarmas
Conectado a sistema alternativo de energía:	Sí

Fig. 8

- *Tipo.* El control podrá ser electrónico o mediante guardia de seguridad o recepcionista. Los sistemas de control de acceso automatizado pueden ser a su vez de un factor (electrónico simple) o de dos (electrónico doble factor). El perímetro del Centro de investigación dispone tanto de tornos con un sistema de credencial material (tarjeta) como de guardias de seguridad en la caseta adyacente para gestionar las visitas e incidencias que pudieran surgir. Por tanto, se debe seleccionar “Personal de seguridad y electrónico” en la lista desplegable del campo. (Fig. 8 ①)



- *Identificación de vehículos.* Indicar si existe algún sistema de identificación de vehículos, ya sea automático o mediante otro procedimiento (tarjetas). Seleccionar “Sí”, ya que en el Centro de investigación se permite el paso de vehículos previa identificación y entrega de la correspondiente tarjeta. (Fig. 8 ②)
- *Antisabotaje, Conectado a alarma y Conectado a sistema alternativo de energía.* Los conceptos de los tres campos son análogos a los explicados en apartados anteriores. En el caso del ejemplo, el sistema electrónico de control de acceso (los tornos) dispone de sistema antisabotaje y está conectado a un sistema alternativo de energía, además de monitorizar las alarmas que se generan en el Centro permanente de seguridad de la instalación. Se debe seleccionar “Sí” en los tres campos.

PERÍMETRO 2

Se procede de igual forma con el segundo perímetro de seguridad, en este caso el edificio propiamente dicho, completando la columna dedicada al perímetro 2.

- Cerramiento.

CERRAMIENTO	PERÍMETRO 2
Tipo:	Muro ①
Resistencia:	Muy alta ②
Altura:	Igual o mayor de 2,15 m ③

Fig. 9

- *Tipo.* En el Centro de investigación el segundo perímetro de seguridad está formado por las fachadas del propio edificio principal. Se trata pues de un cerramiento tipo “Muro”. (Fig. 9 ①)
 - *Resistencia.* Al tratarse del propio edificio, la resistencia de sus muros exteriores es “Muy alta”. (Fig. 9 ②)
 - *Altura.* Por último, la altura del mismo es mayor de 2.15 m en todas sus zonas, por lo que se selecciona “Igual o mayor a 2,15 m”. (Fig. 9 ③)
- Sistema perimetral de detección de intrusos.

SISTEMA PERIMETRAL DE DETECCIÓN DE INTRUSOS	
Tipo:	No dispone ①
Cobertura:	- Seleccionar -
Antisabotaje:	- Seleccionar -
Conectado a alarma:	- Seleccionar -
Conectado a sistema alternativo de energía:	- Seleccionar -

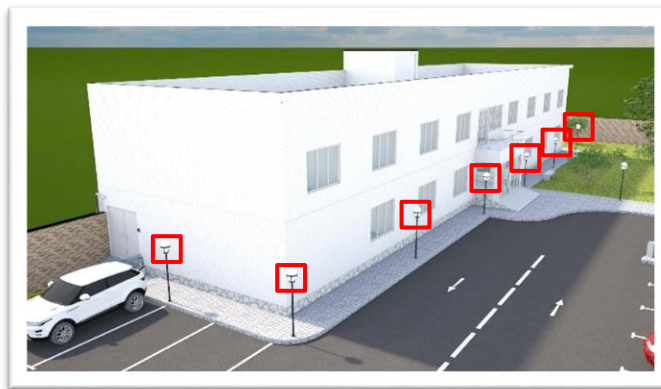
Fig. 10

- *Tipo.* El segundo perímetro de seguridad del ejemplo no dispone de otros sistemas activos de protección perimetral (barreras de infrarrojos, barreras de microondas, volumétricos exteriores, cables sensores, etc.), por lo que habrá que seleccionar “No dispone” en el desplegable. (Fig. 10 ①)
 - *Cobertura, Antisabotaje, Conectado a alarma y Conectado a sistema alternativo de energía.* Al no disponer de ningún sistema activo de detección de intrusos perimetral, estos campos se bloquean.
- Sistema de iluminación del perímetro. Completar con las características de los sistemas de iluminación.

SISTEMA DE ILUMINACIÓN DEL PERÍMETRO	
Tipo:	Continua ①
Visibilidad las 24h:	Sí ②
Antisabotaje:	Sí ③
Conectado a alarma:	Sí, al centro de control de alarmas ④
Conectado a sistema alternativo de energía:	Sí ⑤

Fig. 11

- *Tipo.* El edificio del Centro de investigación está rodeado de farolas cuyo alumbrado es gestionado internamente, por lo que en el desplegable del campo se debe seleccionar “Continua”. (Fig. 11 ①)
- *Visibilidad las 24h.* El segundo perímetro también se encuentra suficientemente iluminado a lo largo de todo el día, por lo que se debe seleccionar “Sí” en la lista desplegable. (Fig. 11 ②)
- *Antisabotaje.* Todos los dispositivos de alumbrado del edificio disponen de *tamper* para detectar si son manipulados. Por tanto, seleccionar “Sí” en la lista (Fig. 11 ③)
- *Conectado a alarma.* La iluminación del edificio, tanto interna como externa, es controlada mediante un BMS (*Building Management System*) que proporciona alarmas cuando se produce algún fallo, por ello seleccionar “Sí, al centro de control de alarmas” en la lista desplegable. (Fig. 11 ④)
- *Conectado a sistema alternativo de energía.* La iluminación del edificio está conectado a un sistema alternativo de energía, por lo que se debe seleccionar “Sí” en la lista desplegable. (Fig. 11 ⑤)
- Circuito cerrado de televisión (CCTV). El edificio comparte con el primer perímetro de seguridad las cámaras que controlan la fachada norte, además dispone en su azotea de otras dos cámaras que permiten vigilar el resto de fachadas. Las características del sistema de video vigilancia del segundo perímetro son idénticas a las del primero.



CIRCUITO CERRADO DE TELEVISIÓN (CCTV)	
Tipo:	Visión diurna/nocturna
Tiempo conservación grabaciones:	Mayor o igual a un mes
Antisabotaje:	Sí
Conectado a alarma:	Sí, al centro de control de alarmas
Conectado a sistema alternativo de energía:	Sí

- Sistema de control de acceso del perímetro.

SISTEMA DE CONTROL DE ACCESO DEL PERÍMETRO	
Tipo:	Personal de seguridad y electrónico ①
Identificación de vehículos:	No permite entrada de vehículos ②
Antisabotaje:	Sí
Conectado a alarma:	Sí, al centro de control de alarmas
Conectado a sistema alternativo de energía:	Sí

Fig. 12

- *Tipo.* El acceso al edificio principal del Centro de Investigación dispone de tornos, arco detector de metales y escáner. También tiene guardias de seguridad en el centro permanente de seguridad (CPS) ubicado en la sala contigua al hall de entrada.

Por tanto, se debe seleccionar “Personal de seguridad y electrónico” en la lista desplegable del campo. (Fig. 12 ①)



- *Identificación de vehículos.* Seleccionar “No permite entrada de vehículos”, ya que al edificio principal no se puede pasar con coche. (Fig. 12 ②)
- *Antisabotaje, Conectado a alarma y Conectado a sistema alternativo de energía.* En el caso del ejemplo, el sistema electrónico de control de acceso (los tornos) dispone de sistema antisabotaje y está conectado a un sistema alternativo de energía además de monitorizar las alarmas que se generan en el CPS de la instalación. Se debe seleccionar “Sí” en los tres campos.

7.1.3. Entorno local

- a) **Medidas estructurales.** Continuando con el esquema de defensa en profundidad pasaríamos a describir el llamado entorno local de seguridad constituido por la sala donde se encuentra la información a proteger. En concreto en este apartado se recoge toda la información relativa a los elementos estructurales de protección como son los paramentos tanto verticales (paredes) como horizontales (suelo y techo).

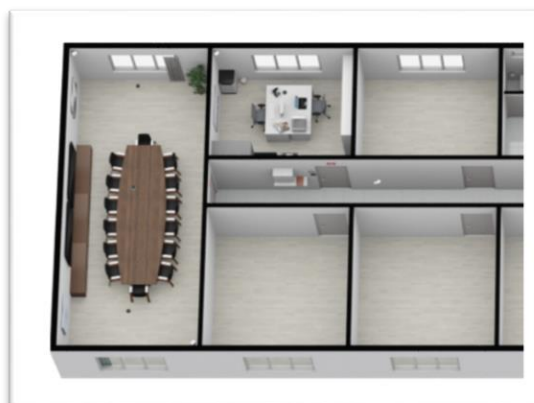
2.1 MEDIDAS ESTRUCTURALES

Resistencia paredes: Alta. Piedra, hormigón o ladrillo macizo de más de 15 cm de espesor, acero de buques o sheeps	①	Limitófes con el exterior: Sí	②
Construcción paredes: De verdadero suelo a verdadero techo	③	Huecos excluyendo ventanas: Sí, protegidos (rejās, sensores, concertina,...)	④
Suelo: Verdadero suelo	⑤	Techo: Verdadero techo	⑥

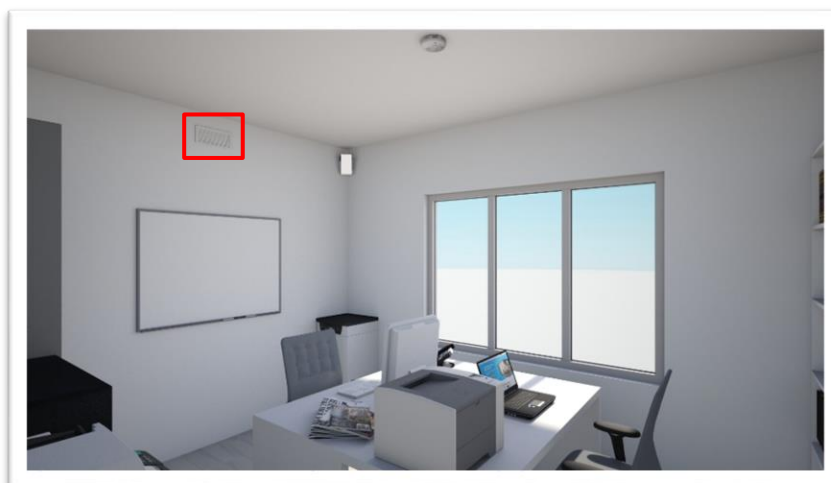
Fig. 13

- Resistencia paredes. Se debe seleccionar el nivel de resistencia de las paredes de la ZAR. Si las paredes no son todas iguales indicar las características de la que presente menor resistencia. Se establecen tres grados de resistencia: alta, media o baja, según los materiales con los que se han alzado las paredes.

El paramento exterior del edificio principal está construido con muro, capa aislante y material de revestimiento mientras que la tabiquería interior se levanta con ladrillo hueco. Por tanto, la resistencia de las paredes de la ZAR del órgano de control es “Media. Ladrillo hueco o macizo menor de 15 cm de espesor”. (Fig. 13 ①)



- Limitófes con el exterior. Indicar si alguna de las paredes de la ZAR da al exterior de la instalación. En el Centro de investigación, la pared norte de la ZAR del Órgano de Control limita con un vial público por lo que se debe seleccionar “Sí” en el campo. (Fig. 13 ②)
- Construcción paredes. Indicar si los paramentos verticales discurren desde el verdadero suelo hasta el verdadero techo, como es el caso del ejemplo. (Fig. 13 ③)
- Huecos excluyendo ventanas. Indicar si en los paramentos de la ZAR existen huecos y si están protegidos. En la ZAR del órgano de control existe un hueco destinado a la ventilación que se encuentra protegido mediante una reja. “Sí, protegidos (rejās, sensores, concertina, ...)”. (Fig. 13 ④)



- **Suelo.** Indicar si el pavimento de la ZAR es el original o dispone de suelo técnico elevado. En la ZAR del órgano de control el suelo es el original que se ha revestido de tarima, es decir “Verdadero suelo”. (Fig. 13 ⑤)
 - **Techo.** Indicar si la ZAR dispone de falso techo. El local del ejemplo tiene techo de escayola separado 30 cm del techo real, por lo que se debe seleccionar “Falso techo” en la lista desplegable. (Fig. 13 ⑥)
- b) **Puerta de entrada.** Se recogen las características de la puerta de acceso. Si la ZAR dispusiera de varias puertas de acceso (excluyendo la de emergencia) se debe cumplimentar con las del tipo de menor grado de resistencia.

2.2 PUERTA DE ENTRADA. Si existen varias puertas de acceso (excluir la de emergencia) rellenar con las características del tipo con menor grado de resistencia

Tipo: Acorazada ①	Grado según UNE-EN-1627: Grado 4 ②
Muelle/cierra puertas: Sí ③	Otros elementos de seguridad: No dispone ④
Cerradura mecánica: Alta seguridad (5 puntos de cierre al frente) ⑤	Cerradura electrónica: Sí, en modo FailSecure (normalmente cerrada) ⑥
Sensor apertura: Sí ⑦	Antisabotaje: Sí ⑧
	Conexión alarma: Sí, al centro de control de alarmas ⑨

Fig. 14

- **Tipo.** Se debe seleccionar el tipo de puerta. Se distingue entre puerta blindada, cuando su estructura (marco y hoja) está fabricada en madera con refuerzos de hierro; acorazada, si su estructura es de acero con placas de madera, u otro, si se trata de otra clase de puerta (cristal, metálica o madera sin refuerzos). La ZAR del ejemplo dispone de una puerta acorazada. (Fig. 14 ①)



- Grado UNE-EN-1627. La norma UNE-EN-1627 es una norma europea que especifica los requisitos y sistemas de clasificación para la resistencia a la efracción¹ de puertas y otros productos de construcción. Existen seis grados o clases de resistencia (del 1 al 6) según los métodos de ataque utilizados. La ZAR del ejemplo dispone de una puerta acorazada que cumple con la clasificación UNE-EN-1627 de grado 4. (Fig. 14 ②)
- Muelle-cierra puertas. Indicar si la puerta de acceso dispone de algún dispositivo automático que asegure el cierre de la misma cuando no esté en uso. La puerta de la ZAR del órgano de control dispone de muelle-cierra puertas. (Fig. 14 ③)



Muelle cierra puertas



Cerradura de seguridad

¹ Resistencia a la efracción: capacidad de un producto para resistir intentos de entrada forzada utilizando la fuerza física y con la ayuda de herramientas predefinidas en una sala o área protegida.

- Otros elementos de seguridad. Indicar si la puerta de acceso dispone de otros elementos de seguridad como mirilla, videoportero, interfono u otro. La puerta del ejemplo no tiene ninguno, por lo que se debe seleccionar “No dispone” en la lista desplegable. (Fig. 14 ④)
- Cerradura mecánica. Los dispositivos de cierre de las puertas que dan acceso a las ZAR serán accionados por cerraduras de seguridad. Seleccionar una opción en la lista desplegable entre los tipos de cerradura: Básica, Seguridad (3 puntos de cierre al frente) y Alta Seguridad (5 puntos de cierre al frente). La puerta de acceso de la ZAR del órgano de control tiene instalada una cerradura con cinco puntos de cierre al frente: “Alta seguridad (5 puntos de cierre al frente)”. (Fig. 14 ⑤)
- Cerradura electrónica. Las cerraduras electrónicas son utilizadas asociadas a los sistemas de control de acceso. Los términos “*Fail Safe*” (normalmente abierto) y “*Fail Secure*” (normalmente cerrado) son utilizados para definir la manera en la que las cerraduras y los dispositivos de señal trabajan cuando se asocian con sistemas de control de acceso. Una cerradura “*Fail Safe*” es aquella que se abre cuando no existe corriente, y, requiere electricidad para mantenerse cerrada. Por el contrario, una del tipo “*Fail Secure*” permanece bloqueada hasta que se aplica corriente, aunque permiten la salida sin restricción al empujar o accionar el mecanismo del picaporte. Es decir, si la electricidad falla, la cerradura no limitará la salida, aunque sí impedirá el acceso en entrada.
El sistema de control de acceso instalado en el local está configurado en modo “*Fail Secure*”. (Fig. 14 ⑥)
- Sensor apertura. Indicar si la puerta de acceso dispone de un dispositivo de seguridad que alerte de su apertura. La puerta de la ZAR lo tiene instalado, por lo que se selecciona “Sí” en la lista. (Fig.14 ⑦)
- Antisabotaje. Indicar si el sensor de apertura tiene algún mecanismo de detección de intento de sabotaje o manipulación. En el ejemplo el sensor instalado dispone de él, por lo que se debe seleccionar “Sí”. (Fig.14 ⑧)
- Conexión alarma. Indicar si el sensor de apertura está conectado con un centro de monitorización y control permanente de alarmas, una Central receptora de alarmas (CRA), o está conectado a un sistema autónomo que activa únicamente una alerta sonora al dispararse la alarma. Todas las alarmas que se producen en el Centro de investigación llegan al centro permanente de



seguridad, así que se selecciona “Sí, al centro de control de alarmas” en la lista desplegable. (Fig.14 ⑨)

- c) **Puerta de emergencia.** Si la ZAR dispusiera de puerta de emergencia en este apartado se recogen sus características.

2.3 PUERTA DE EMERGENCIA		
Tipo: No dispone ①	Uso controlado: - Seleccionar - ②	
Sensor apertura: - Seleccionar -	Antisabotaje: - Seleccionar -	Conexión alarma: - Seleccionar -

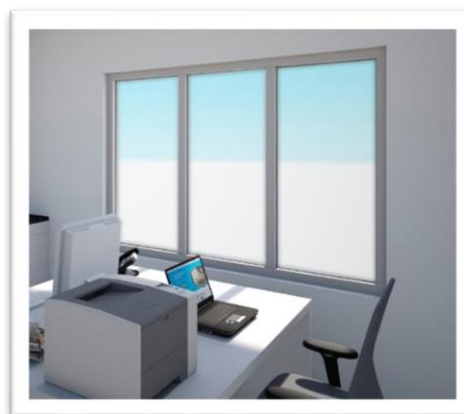
Fig. 15

- **Tipo.** Se debe seleccionar el tipo de puerta. En el caso de la ZAR del ejemplo se selecciona “No dispone” ya que no existe puerta de emergencia. (Fig. 15 ①)
 - **Uso controlado.** Indicar como se controla la puerta de emergencia limitando su uso a casos de emergencia o ensayo. Al no disponer de puerta de emergencia este campo aparece bloqueado en el ejemplo. (Fig. 15 ②)
 - **Sensor apertura, Antisabotaje, Conexión alarma.** Los conceptos de los tres campos son análogos a los explicados en apartado de la puerta de acceso. En el caso del ejemplo, los campos están bloqueados al no existir puerta de emergencia.
- d) **Ventanas exteriores.** Este apartado recoge las características de las ventanas de la ZAR que se encuentran en los muros del edificio. En el caso de que la ZAR dispusiera de varias ventanas que den al exterior (o a patios interiores), se debe completar con las características del tipo de menor grado de resistencia.

2.4 VENTANAS EXTERIORES. Si existen varias ventanas que den al exterior rellenar con las características del tipo con menor grado de resistencia		
Tipo: Sí, protegida con sensores ①	Distancia al suelo/tejado: Igual o superior a 5,5 ②	Cristales: Transparentes con vinilo/persiana/cortina ③
Sensor apertura: No ④	Antisabotaje: - Seleccionar -	Conexión alarma: - Seleccionar -
Sensor rotura: Sí ⑤	Antisabotaje: Sí	Conexión alarma: Sí, al centro de control de alarmas

Fig. 16

- **Tipo.** Indicar si la ventana dispone de algún medio o sistema de protección, ya sea reja de seguridad, barreras de infrarrojos o microondas, o sensores de apertura o de rotura de cristales. En el caso de la ZAR del ejemplo existe una única ventana ubicada en la fachada norte del edificio principal, cuyos cristales disponen de sensor de rotura. Por tanto, se debe seleccionar “Sí, protegida con sensores” en la lista desplegable. (Fig. 16 ①)



- Distancia al suelo/tejado. Indicar si la ventana está situada a menos de 5,5 m por encima del nivel del suelo, o del tejado/cornisa. La distancia de la ventana de la ZAR a la azotea es “Inferior a 5,5 m”. (Fig. 16 ②)
- Cristales. Indicar si los cristales de las ventanas que dan al exterior son transparentes u opacos/translúcidos. Si son transparentes se debe indicar si disponen de vinilo, persiana o cortina que impida cualquier visión nítida desde el exterior. La ventana de la ZAR del órgano de control tiene los cristales transparentes cubiertos con vinilo. Seleccionar “Transparentes con vinilo/persiana/cortina”. (Fig. 16 ③)
- Sensor apertura, Antisabotaje, Conexión alarma. Los conceptos de los tres campos son análogos a los explicados en el apartado de la puerta de acceso. En el caso del ejemplo, la ventana es fija y no tiene sensor de apertura por lo que al seleccionar “No” (Fig. 16 ④) sus campos asociados “Antisabotaje” y “Conexión alarma” se bloquean. También cambia a rojo el color del texto “No”, lo que indica que la ventana debería disponer de esta medida de seguridad. Por tanto, es necesario reseñar en la última página del formulario dentro del apartado “Observaciones” que la ventana no tiene instalado un sensor de apertura porque es fija.

OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.
1.3 El Perímetro 1 constituye el cerramiento exterior de la instalación y el Perímetro 2 el propio edificio principal del Centro de Investigación.
2.4 La ventana no dispone de sensor de apertura ya que se trata de un ventanal cuyas hojas son fijas (no se pueden abrir).
2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.
3.1 Se desconoce la clase de la cerradura del armario de seguridad según la norma UNE-EN-1300. Se trata de una cerradura de gorjas con llave de doble paleta. Dispone de certificación VdS Clase 2.

- Sensor rotura, Antisabotaje, Conexión alarma. Indicar si los cristales de la ventana tienen instalado un dispositivo que detecta su rotura. En el caso del ejemplo, la ventana cuenta con dicho sistema y está conectado al centro de control de alarmas de la instalación. (Fig.16 ⑤)

- e) **Sistema de control de acceso.** En este apartado se definen las características del sistema de control de accesos de la ZAR.

2.5 SISTEMA DE CONTROL DE ACCESO

Tipo: Electrónico doble factor ①	Tiempo de conservación de los registros: Igual o superior a un ②	Antipassback: No ③
Antisabotaje: Sí	Conexión alarma: Sí, al centro de control de alarmas	Conexión a sistema alternativo de energía: Sí

Fig. 17

- Tipo. Indicar si el control de acceso a la ZAR es llevado a cabo de forma manual por personal de seguridad o a través de un sistema electrónico, ya sea simple (por ejemplo, solo tarjeta) o de doble factor (tarjeta y PIN). En el caso de la ZAR

del ejemplo se selecciona “Electrónico doble factor” porque para entrar es necesario la tarjeta de seguridad y una clave personal. (Fig. 17 ①)

- Tiempo de conservación del registro. Los sistemas de control de acceso deben incluir también dispositivos en los que se mantengan registros de las entradas y salidas del personal, en horario de trabajo y, especialmente, fuera de dicho horario. Indicar el tiempo que se conservan estos registros. En el caso del ejemplo este tiempo es “Igual o superior a un año”. (Fig. 17 ②)
- Antipassback. Señalar si el sistema instalado obliga a los usuarios a salir antes de poder entrar y viceversa, evitando de esta forma el abuso en la utilización de los sistemas de credencial para entrar más de un individuo con un mismo dispositivo de acceso. En la ZAR del ejemplo no está implementada esta tecnología por lo que se selecciona “No” en la lista desplegable. (Fig. 17 ③)
- Antisabotaje, Conexión alarma y Conexión a sistema alternativo de energía. En el caso del ejemplo, el sistema electrónico de control de acceso (el lector de tarjetas con código) dispone de sistema antisabotaje y de baterías que garantizan su funcionamiento en caso de un corte de energía. También está conectado al CPS de la instalación para monitorizar las alarmas que se generan. Se debe seleccionar “Sí” en los tres campos.

f) **Personal que accede a la ZAR.** En este apartado se definen algunos aspectos relativos al personal que accede a la ZAR.

2.6 PERSONAL QUE ACCEDE A LA ZAR			
Formación en protección de la I.C.: Sí, con frecuencia igual o menor a un año	①	Registro formación: Sí	②
Registros aleatorios a la entrada/salida: Sí			③
Servicio de limpieza: Personal empresa externa	④	Escoltado: Sí	⑤
		Habilitación personal de seguridad: No	⑥
Servicio de mantenimiento: Personal empresa externa		Escoltado: Sí	
		Habilitación personal de seguridad: No	

Fig.18

- Formación en protección de la información clasificada. Se debe indicar si el personal destinado en la ZAR recibe formación periódica en materia de protección de información clasificada. En el Centro de investigación se imparte formación anual al personal que tiene acceso a información clasificada. (Fig.18 ①)
- Registro formación. Indicar si se ha guardado evidencia objetiva de impartir formación en materia de protección de información clasificada. En el caso del ejemplo, se selecciona “Sí” ya que se archivan las hojas con las firmas de los asistentes a las jornadas formativas. (Fig.18 ②)
- Registros aleatorios a la entrada/salida. Señalar si se realizan controles aleatorios esporádicos para detectar posibles fallos en los sistemas de

seguridad establecidos. En el Centro de investigación se efectúan registros aleatorios al salir de la instalación. (Fig.18 ③)

- Servicio de limpieza. Se debe indicar quien efectúa las labores de limpieza: personal de empresa externa, personal de la organización o el personal propio de la ZAR. En el Centro de investigación mantiene un contrato con una empresa privada de limpieza, por lo que hay que seleccionar “Personal empresa externa” en la lista. (Fig.18 ④)
- Escortado. Indicar si las labores de limpieza se realizan en presencia de personal de la organización con la correspondiente HPS. En la ZAR del ejemplo siempre se acompaña al personal de limpieza. (Fig.18 ⑤)
- Habilitación personal de seguridad. Se debe indicar si las personas que realizan las labores de limpieza disponen de habilitación personal de seguridad (HPS). El personal de limpieza que presta servicio en la ZAR no dispone de HPS (“No” en la lista desplegable), por lo que cuando se efectúan dichas labores se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma. Este hecho se debe reflejar en el apartado correspondiente a las “Observaciones” tal y como indica que la palabra “No” se muestre en color rojo. (Fig.18 ⑥)

OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.

1.3 El Perímetro lo constituye el cerramiento exterior de la instalación y el Perímetro 2 el propio edificio principal del Centro de Investigación.

2.4 La ventana no dispone de sensor de apertura ya que se trata de un ventanal cuyas hojas son fijas (no se pueden abrir).

2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.

- Servicio de mantenimiento, Escortado, Habilitación personal de seguridad. Los conceptos de los tres campos son análogos a los explicados para el servicio de limpieza. En el caso del ejemplo, la situación para el servicio de mantenimiento es igual que para el de limpieza, se tiene contratada a una empresa externa cuyo personal no dispone de HPS.

- g) **Circuito cerrado de televisión (CCTV).** Completar con las características del sistema de vídeo vigilancia que controla los movimientos en las inmediaciones de la puerta que da acceso a la ZAR.

2.7 CIRCUITO CERRADO DE TELEVISIÓN. Si existen varios accesos controlados por CCTV, rellenar con las características del tipo menos favorable

Tipo: Visión diurna/nocturna ①	Tiempo conservación grabaciones seguridad: Igual o superior a un mes ②	Iluminación del acceso las 24 h: No ③
Antisabotaje: Sí	Conexión alarma: Sí, al centro de control de alarmas	Conexión a sistema alternativo de energía: Sí

Fig. 19

- Tipo. Atendiendo a su modo de funcionamiento, seleccionar el tipo de las cámaras de seguridad que controlan las puertas de acceso. El acceso a la ZAR es monitorizado a través de una cámara con la función día/noche, que activa el modo nocturno cuando las condiciones de iluminación son escasas. Por tanto, se debe seleccionar “Visión diurna/nocturna” en la lista desplegable. (Fig. 19 ①)
- Tiempo conservación grabaciones seguridad. Indicar si se almacenan las grabaciones de seguridad y el tiempo de retención de las mismas. Seleccionar “Igual o superior a un mes”, ya que en el Centro de investigación las vídeograbaciones se conservan durante 30 días. (Fig. 19 ②)
- Iluminación del acceso las 24h. Se debe indicar si el acceso dispone de suficiente iluminación, ya sea natural o artificial, a lo largo de todo el día. Seleccionar “No”, ya que fuera de la jornada laboral se apagan todas las luces del edificio principal del Centro de investigación. (Fig. 19 ③)
- Antisabotaje, Conexión alarma y Conexión a sistema alternativo de energía. Los conceptos de los tres campos son análogos a los explicados en apartados anteriores. En el caso del ejemplo, el sistema de vídeo vigilancia es monitorizado 7x24h en el CPS de la instalación (que a su vez es el centro de control de alarmas) y todas sus cámaras, dotadas de sistemas antisabotaje, están conectadas a un sistema alternativo de energía. Se debe seleccionar “Sí” en los tres campos.



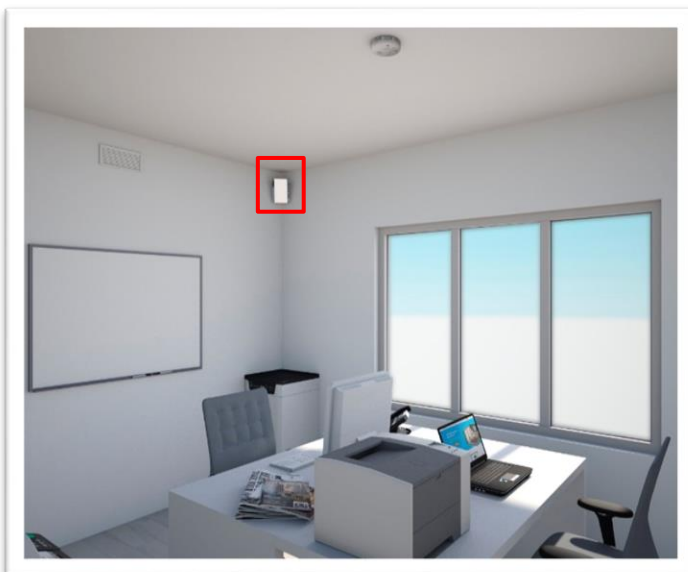
h) **Sistema detección de intrusos (SDI).** Indicar con las características del sistema.

2.8 SISTEMA DE DETECCIÓN DE INTRUSOS (SDI)

Tipo: Detector de movimiento de doble tecnología ①		
Antisabotaje: Sí	Conexión alarma: Sí, al centro de control de alarmas	Conexión a sistema alternativo de energía: Sí

Fig. 20

- **Tipo.** Atendiendo a su modo de funcionamiento, seleccionar el tipo de los detectores volumétricos instalados en el entorno local. Se distinguen: detectores de movimiento simples, dotados de infrarrojos o microondas, y mixtos o de doble tecnología. En el caso DE que la ZAR estuviera ocupada las 24 h del día no es necesario la instalación de estos sistemas, aunque se debe reflejar este hecho seleccionando la opción “No necesario, ocupado 24x7”. La ZAR dispone de un volumétrico de doble tecnología (infrarrojo y microondas) que cubre la totalidad del local. Por tanto, se debe seleccionar “Detector de movimiento de doble tecnología” en la lista desplegable. (Fig. 20 ①)



- **Antisabotaje, Conexión alarma y Conexión a sistema alternativo de energía.** Los conceptos de los tres campos son análogos a los explicados en apartados anteriores. En el caso del ejemplo, los detectores de intrusión están conectados con el CPS de la instalación (que a su vez es el centro de control de alarmas) y dotados de sistema antisabotaje. El sistema está conectado a un SAI ante posibles cortes de electricidad. Se debe seleccionar “Sí” en los tres campos.

- i) **Otros elementos y medidas de seguridad.** En este apartado se recoge si existen otros elementos y sistemas de seguridad.

2.9 OTROS ELEMENTOS Y MEDIDAS DE SEGURIDAD

Detector sísmico: No ①	Detector agua: No ②	Detector incendios: Sí ③	Elementos extinción: Extintores ④
Sistemas TIC acreditados: Sí ⑤	Etiquetas de seguridad: Sí ⑥	Casilleros de seguridad externos: Sí ⑦	
Zona TEMPEST: Zona 3 ⑧	Medición válida hasta: 26-06-2028 ⑨	Medidas TEMPEST adicionales: No ⑩	

Fig. 21

- **Detector sísmico.** Indicar si los paramentos de la ZAR disponen de sensores que detectan las vibraciones que se producen por las herramientas e instrumentos que se utilizan en un intento de intrusión. Seleccionar “No”, ya que la ZAR no tiene este tipo de sensores. (Fig. 21 ①)
- **Detector agua.** Se debe indicar si la ZAR dispone de sensores que detecten fugas de agua u otros líquidos. Seleccionar “No” ya que la ZAR no tiene este tipo de sensores. (Fig. 21 ②)

- Detector incendios. Seleccionar si la dependencia dispone de sensores que detecten la presencia de humos, calor o fuego. En el techo de la ZAR existe un detector, por lo que se debe seleccionar “Sí” en la lista desplegable. (Fig. 21 ③)



- Elementos extinción. Indicar el tipo de elemento de extinción de incendios con los que cuenta la ZAR. En el caso de la ZAR del ejemplo en el pasillo existen extintores. (Fig. 21 ④)

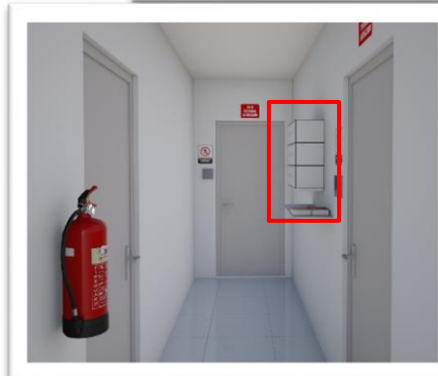
- Sistemas TIC acreditados. Se debe indicar si la ZAR dispone de sistemas TIC acreditados que permitan visualizar, almacenar, procesar o transmitir información clasificada internacional. El órgano de control del Centro de investigación dispone de un portátil aislado acreditado para poder visualizar información clasificada OTAN/UE, por lo que hay que seleccionar “Sí” en el desplegable. (Fig. 21 ⑤)



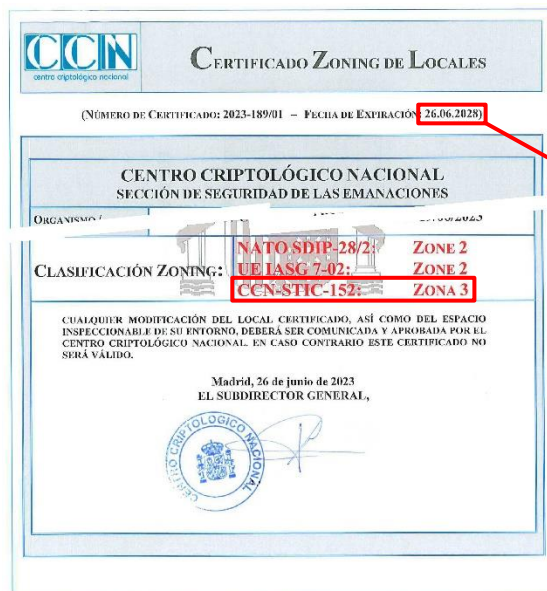
- Etiquetas de seguridad. Se debe indicar si los sistemas TIC acreditados disponen de etiquetas de seguridad que eviten la manipulación de los mismos. Seleccionar “Sí”, ya que la estación aislada que existe en la ZAR tiene dichas etiquetas. (Fig. 21 ⑥)
- Casilleros de seguridad externos. Indicar si en el exterior de la ZAR existen casilleros para depositar dispositivos electrónicos (teléfonos, portátil, etc.).



En el caso del ejemplo, junto a la entrada a la ZAR se han instalado casilleros de seguridad. Por tanto, seleccionar “Sí”. (Fig. 21 ⑦)



- Zona TEMPEST. Seleccionar la clasificación de la ZAR atendiendo a una medición TEMPEST certificada, preferentemente según la guía CCN-STIC-152.



Fecha expiración Certificado

Seleccionar “Zona 3”, ya que según certificado del Centro Criptológico Nacional todos los locales de la primera planta del edificio tienen esa clasificación. (Fig. 21 ⑧)

- Medición válida hasta. Seleccionar la fecha de expiración del certificado zoning de locales. (Fig. 21 ⑨)
- Medidas TEMPEST adicionales. Seleccionar si los sistemas TIC que manejan información clasificada internacional están dotados de alguna medida adicional para evitar las emanaciones electromagnéticas no deseadas. La estación aislada existente en la ZAR no dispone de ninguna medida TEMPEST adicional, por lo que se selecciona “No” en la lista. (Fig. 21 ⑩)

7.1.4. Entorno próximo

- Mobiliario de seguridad.** Continuando con el esquema de defensa en profundidad pasaríamos a describir el llamado entorno próximo de seguridad, constituido por los elementos últimos de protección de la información clasificada. Dentro de estos elementos se encuentra el mobiliario de seguridad, donde se custodian documentos y soportes con información clasificada que no están cifrados por un medio aprobado. Si se dispone de distintos modelos de contenedores de seguridad que almacenan información clasificada, se debe rellenar las características de cada uno en una columna distinta. Así, por ejemplo, en la ZAR existe tanto una caja fuerte y un armario metálico de seguridad cuyas

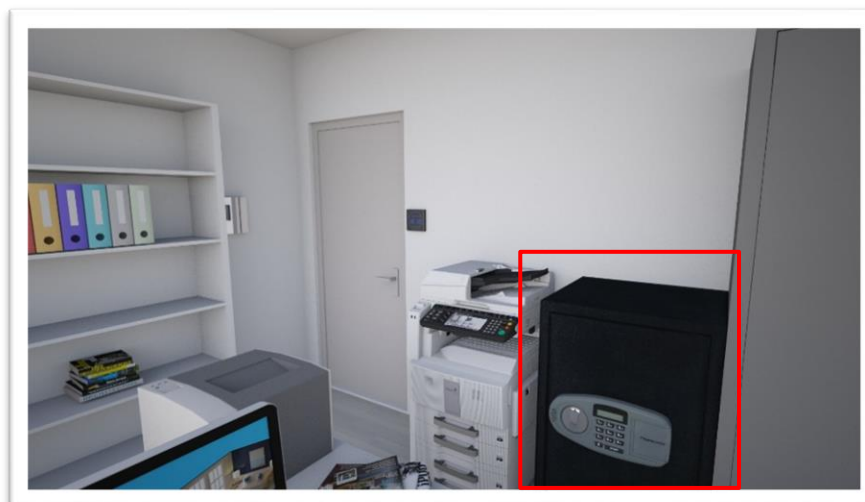
características indicaremos en la columna “Mobiliario de seguridad tipo 1” y “Mobiliario de seguridad tipo 2” respectivamente.

MOBILIARIO DE SEGURIDAD TIPO 1		
Tipo:	Caja fuerte	①
Nivel (UNE-EN-1143-1):	Nivel IV	②
Tipo cerradura 1:	Llave	③
Clase cerradura 1 (UNE-EN-1300):	Clase B	④
Tipo cerradura 2:	Combinación electrónica	⑤
Clase cerradura 2 (UNE-EN-1300):	Clase B	⑥
Grado máximo de la I.C. que custodia:	RESERVADO o equivalente	⑦
Compartimentación de la I.C.:	Sí	⑧

Fig. 22

MOBILIARIO DE SEGURIDAD TIPO 1

- Tipo. Indicar el tipo de contenedor de seguridad entre las siguientes opciones: armario metálico de seguridad, caja fuerte, cámara acorazada o no dispone. En el caso de la ZAR del ejemplo se selecciona “Caja fuerte”. (Fig. 22 ①)



- Nivel (UNE-EN-1143-1). La norma UNE-EN-1143-1 es una norma europea que especifica los requisitos y nivel de clasificación de las unidades de almacenamiento de seguridad según su resistencia al robo. Existen diez niveles de resistencia (del I al X) según los métodos de ataque utilizados. En el caso del ejemplo la caja fuerte es “Nivel IV”. (Fig. 22 ②).

CAJA FUERTE / SAFE	
N.º Placa / Plate Number	0002187
Modelo / Model	CORVUS
Tipo de producto / Product Type	C.F.D.
N.º Serie / Serial Number	S941/21
Grado / Resistance Grade	IV
Peso / Weight	800 Kgs
Año / Year	2015

055/000014 UNE-EN 1143-1

- Tipo Cerradura 1. Indicar el tipo cerradura de la caja fuerte: llave, combinación mecánica o combinación electrónica. La apertura de la caja fuerte de la ZAR se efectúa mediante llave y combinación electrónica. Por lo tanto, dispone de dos cerraduras. Seleccionar “Llave” en la lista desplegable de la cerradura 1. (Fig. 22 ③)
- Clase Cerradura 1 (UNE-EN-1300). Indicar el tipo de clasificación de las cerraduras de alta seguridad de acuerdo con su resistencia a la apertura no autorizada. La llave de la caja fuerte del ejemplo es una “Clase B” según la norma UNE-EN-1300. (Fig. 22 ④)
- Tipo Cerradura 2. La segunda cerradura de la caja fuerte de la ZAR es del tipo combinación electrónica. Por lo tanto, seleccionar “Combinación electrónica” en la lista desplegable. (Fig. 22 ⑤)
- Clase Cerradura 2 (UNE-EN-1300). La combinación electrónica de la caja fuerte del ejemplo es también “Clase B” según la norma UNE-EN-1300. (Fig. 22 ⑥)
- Grado máximo de la información clasificada que custodia. Se debe indicar el grado máximo de clasificación de la documentación o material que se almacena en el contenedor de seguridad. En el órgano de control del Centro de investigación la caja fuerte se utiliza para custodiar documentación hasta “RESERVADO”. (Fig. 22 ⑦)
- Compartimentación de la I.C.. Indicar si en el caso de existir información clasificada de diferentes tipos (orígenes y/o grados) se custodia en contenedores o estantes separados sin acceso visual posible a los contenidos. En la caja fuerte del ejemplo se separa la documentación OTAN y UE en diferentes baldas y, dentro de cada balda, en carpetas según su clasificación (SECRETO y CONFIDENCIAL), por lo que hay que seleccionar “Sí”. (Fig. 22 ⑧)

MOBILIARIO DE SEGURIDAD TIPO 2

Se procede de igual forma con el segundo tipo de mobiliario de seguridad de la ZAR, en este caso el armario metálico de seguridad, completando la columna dedicada al tipo 2.

MOBILIARIO DE SEGURIDAD TIPO 2	
Tipo:	Armario metálico de seguridad ①
Nivel (UNE-EN-1143-1):	Nivel III ②
Tipo cerradura 1:	Llave ③
Clase cerradura 1 (UNE-EN-1300):	Desconocida ④
Tipo cerradura 2:	No dispone ⑤
Clase cerradura 2 (UNE-EN-1300):	- Seleccionar - ⑥
Grado máximo de la I.C. que custodia:	DIFUSIÓN LIMITADA o equivalente ⑦
Compartimentación de la I.C.:	Sí ⑧

Fig. 23

- Tipo. Indicar que el tipo de contenedor de seguridad es “Armario metálico de seguridad”. (Fig. 23 ①)
- Nivel (UNE-EN-1143-1). En el caso del ejemplo el armario cumple con las características de la clasificación “Nivel III” según la norma UNE-EN-1143-1. (Fig. 23 ②).
- Tipo Cerradura 1. La apertura del armario se efectúa mediante llave. Por lo tanto, seleccionar “Llave” en la lista desplegable de la primera cerradura. (Fig. 23 ③)
- Clase Cerradura 1 (UNE-EN-1300). En la documentación del fabricante no aparece la clasificación de la llave del armario según la norma UNE-EN-1300, por lo que se debe seleccionar “Desconocido” en la lista desplegable y aportar la información adicional que se disponga en el apartado “Observaciones” en la última página del formulario. (Fig. 23 ④)

OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.

1.3 El Perímetro lo constituye el cerramiento exterior de la instalación y el Perímetro 2 el propio edificio principal del Centro de Investigación.
 2.4 La ventana no dispone de sensor de apertura ya que se trata de un ventanal cuyas hojas son fijas (no se pueden abrir).
 2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.
 3.1 Se desconoce la clase de la cerradura del armario de seguridad según la norma UNE-EN-1300. Se trata de una cerradura de gorjas con llave de doble paleta.
 Dispone de certificación VdS Clase 2.

- Tipo Cerradura 2. El armario no dispone de segunda cerradura. Por tanto, se debe seleccionar “No dispone” en la lista desplegable. (Fig. 23 ⑤)
- Clase Cerradura 2 (UNE-EN-1300). Este campo se muestra bloqueado ya que el contenedor de seguridad solo tiene una cerradura. (Fig. 23 ⑥)
- Grado máximo de la I.C. que custodia. En el armario de seguridad de la ZAR únicamente se guarda información clasificada de grado “DIFUSIÓN LIMITADA”. (Fig. 23 ⑦)

- Compartimentación de la I.C.. En el armario blindado se separa la documentación OTAN y UE en diferentes baldas, por lo que hay que seleccionar “Sí” en la lista desplegable. (Fig. 23 ⑧)
- b) **Control de llaves y combinaciones.** Completar con las características de los medios y las pautas convenientes para obtener y mantener un efectivo control de llaves y combinaciones.
- Llaves puerta acceso y claves sistema de alarma. Completar con los datos de las llaves de la puerta de acceso y las claves del sistema de alarma.

LLAVES PUERTA ACCESO Y CLAVES SISTEMA ALARMA		
Custodia juego de llaves de uso diario:	Sí, armario portallaves electrónico	① -
Custodia juego de llaves de emergencia:	Sí, caja fuerte	② -
Custodia resto de juegos de llaves:	No existen más llaves	③ -
Registro / inventario:	Sí	④ -
Control en la copia de llaves:	Sí	⑤ -
Separación llaves / claves:	Sí	⑥ -
Registro cambio de combinaciones:	Sí	⑦ -
Periodo de cambio de combinaciones:	Cada 6 meses o menos	⑧ -

Fig. 24

- *Custodia juego de llaves de uso diario.* Seleccionar el tipo de contenedor donde se custodian las llaves de uso diario para la apertura de las puertas de acceso a la ZAR. En el ejemplo, las llaves de todas las puertas del edificio se custodian en armarios electrónicos ubicados en cada planta y ala, que permiten asegurar cada llave individualmente y entregar las mismas solo a usuarios autorizados. Por tanto, seleccionar “Sí, armario portallaves electrónico” en la lista. (Fig. 24 ①)




- *Custodia juego de llaves de emergencia.* Se debe seleccionar el tipo de contenedor donde se custodia el juego de llaves de emergencia, si existiese. En el ejemplo, para posibilitar el acceso a las ZAR en caso de emergencia los guardias de seguridad disponen de una copia de la llave que custodian en la caja fuerte del CPS del edificio. Por tanto, seleccionar “Sí, caja fuerte”. (Fig. 24 ②)
- *Custodia resto de juegos de llaves.* Indicar si existen más juegos de llaves de la puerta de acceso a la ZAR y donde se custodian. No existen más llaves de la puerta de acceso a la ZAR. (Fig. 24 ③)

- *Registro / inventario.* Se debe indicar si existe un registro administrativo de las llaves (número de serie, marca de cada llave, así como la cerradura a la que pertenece). Seleccionar “Sí”, ya que en el Centro de investigación del ejemplo se realiza dicho control. (Fig. 24 ④)
- *Control en la copia de llaves.* Indicar si se realiza control de los procedimientos para la copia de las llaves de acceso a la ZAR, para asegurar que ningún empleado pueda generar duplicados. Seleccionar “Sí”, ya que en el Centro de investigación las llaves no abandonan el entorno global de seguridad y para la generación de réplicas es necesario efectuar petición justificada a través de los canales oficiales. (Fig. 24 ⑤)
- *Separación llaves / claves.* Indicar si las llaves de la puerta de acceso al local se guardan en distinto lugar de donde se custodian las claves de combinación del sistema de alarma. Seleccionar “Sí”, ya que en el ejemplo las llaves se custodian en un armario portallaves electrónico y el sistema de alarma es gestionado directamente desde la aplicación de seguridad. (Fig. 24 ⑥)
- *Registro de cambio de combinaciones.* Indicar si existe un registro de los cambios de combinaciones en el sistema de alarma. Seleccionar “Sí” ya que el software que gestiona el sistema de seguridad guarda auditoria de todos los cambios en las claves. (Fig. 24 ⑦)
- *Periodo de cambio de combinaciones.* Indicar cada cuanto tiempo se efectúa el cambio en las combinaciones del sistema de alarma. Seleccionar “Cada 6 meses o menos” ya que en el Centro de investigación las claves del sistema de alarma son cambiadas una vez al semestre. (Fig. 24 ⑧)
- Llaves / claves mobiliario de seguridad.

LLAVES / CLAVES MOBILIARIO DE SEGURIDAD		
Custodia juego de llaves de uso diario:	Sí, armario portallaves electrónico	①
Custodia juego de llaves de emergencia:	Sí, caja fuerte	②
Custodia resto de juegos de llaves:	No existen más llaves	③
Registro / inventario:	Sí	④
Control en la copia de llaves:	Sí	⑤
Separación llaves / claves:	Sí	⑥
Registro cambio de combinaciones:	Sí	⑦
Periodo de cambio de combinaciones:	Cada 6 meses o menos	⑧

Fig. 25

- *Custodia juego de llaves de uso diario.* Seleccionar el tipo de contenedor donde se custodian las llaves de uso diario para la apertura del mobiliario de seguridad. En el ejemplo, las llaves de la caja fuerte y del armario blindado se custodian en un pequeño armario electrónico ubicados dentro de la ZAR. Por tanto, seleccionar “Sí, armario portallaves electrónico” en la lista. (Fig. 25 ①)
- 
- *Custodia juego de llaves de emergencia.* En el ejemplo, el juego de llaves de emergencia se guarda en la caja fuerte del despacho del jefe del órgano de control. Por tanto, seleccionar “Sí, caja fuerte”. (Fig. 25 ②)
 - *Custodia resto de juegos de llaves.* No existen más juegos de llaves del mobiliario de seguridad de la ZAR. (Fig. 25 ③)
 - *Registro / inventario.* Seleccionar “Sí”, ya que el personal del órgano de control lleva un registro y control de todas las llaves del mobiliario de seguridad de la ZAR. (Fig. 25 ④)
 - *Control en la copia de llaves.* Seleccionar “Sí”, ya que las llaves del mobiliario de seguridad son llaves protegidas y para copiarlas es necesario presentar la tarjeta de propiedad que custodia el jefe del órgano de control en la caja fuerte de su despacho. (Fig. 25 ⑤)
 - *Separación llaves / claves.* Seleccionar “Sí” ya que las llaves se custodian en un armario portallaves electrónico y las claves son memorizadas por el personal del órgano de control. (Fig. 25 ⑥)
 - *Registro de cambio de combinaciones.* Seleccionar “Sí” ya que se lleva un libro de registro con las fechas en las que se efectúan y los motivos del cambio de clave de todo el mobiliario de seguridad de la ZAR. (Fig. 25 ⑦)
 - *Periodo de cambio de combinaciones.* Seleccionar “Cada 6 meses o menos”, ya que las claves del mobiliario de seguridad son cambiadas al menos una vez al semestre. (Fig. 25 ⑧)
 - Descripción del procedimiento de gestión de llaves y combinaciones. Descripción detallada del procedimiento para el manejo, control, sustitución, registro de cambios, actuación ante pérdidas (o comprometimientos), custodia de las llaves y combinaciones durante y después del trabajo. Si existen diferencias, se indicará el procedimiento para cada llave/clave que tenga un

tratamiento diferente (normalmente no tendrá el mismo trato la llave de la puerta que la llave de la caja fuerte).

Descripción del procedimiento de gestión de llaves y combinaciones: LLAVES a) Puerta de acceso - La llave de uso diario se deposita en un armario de llaves electrónico situado en el pasillo. Sólo el personal encuadrado en el órgano de control está autorizado a la retirada de la misma. Durante la jornada de trabajo estará bajo el control del personal del órgano de control. - El juego de emergencia está depositado en la caja fuerte del Centro Permanente de Seguridad dentro de un sobre sellado y lacrado. La clave de desactivación de la alarma del local no se deposita junto a la llave de emergencia. b) Mobiliario de seguridad - La llave de uso diario se deposita en un armario de llaves electrónico situado tras la puerta de entrada.
--

- c) **Sistemas de destrucción.** Completar con las características de los sistemas de destrucción que existen en la ZAR. Si existen varias destructoras se deben indicar las propiedades de las que genere el residuo de menor tamaño.

3.3 SISTEMAS DE DESTRUCCIÓN. Si existen varias destructoras en la ZAR indicar las características del tipo que genere un residuo de menor tamaño

Tipo: Trituradora de corte en partículas ①	Corte según norma DIN-66399: P-5 RESERVADO. Área <= 30mm2 (restricción ancho a 1,5 mm) ②
Descripción del procedimiento alternativo o complementario: ③	
Los residuos generados por la trituradora de la ZAR son reducidos a pasta mediante una trituradora industrial situada en el mismo complejo.	

Fig. 26

- Tipo. Seleccionar el tipo de sistema de destrucción entre las siguientes opciones: trituradora de corte en partículas, trituradora compacta (reducción a pulpa) o no dispone. En el caso de la ZAR del ejemplo se selecciona "Trituradora de corte en partículas". (Fig. 26 ①)
- Corte según norma DIN-66399. La norma DIN 66399 establece 7 niveles de corte en función del tamaño de las tiras o partículas del residuo generado. En la trituradora del ejemplo, las tiras de residuo son de 1,5mm x 15mm, por lo que se debe seleccionar "P-5 RESERVADO. Área <=30mm2 (restricción de anchura a 1,5 mm)". (Fig. 26 ②)
- Descripción del procedimiento alternativo o complementario. Descripción detallada de las acciones a realizar en caso de emergencia, métodos empleados para la destrucción de soportes informáticos y medidas complementarias cuando el tamaño de corte es superior al permitido. (Fig. 26 ③)



- d) **Sistemas de reproducción.** Completar con las características de los sistemas de reproducción que existen en la ZAR y no están conectados a un sistema TIC acreditado.

3.4 SISTEMAS DE REPRODUCCIÓN. Indicar en cada columna los equipos de reproducción existentes en la ZAR y no conectados a sistemas TIC acreditados			
	SISTEMA DE REPRODUCCIÓN 1	SISTEMA DE REPRODUCCIÓN 2	SISTEMA DE REPRODUCCIÓN 3
Tipo:	Fotocopiadora ①	- Seleccionar -	- Seleccionar -
Identificación de usuario:	Sí ②	- Seleccionar -	- Seleccionar -
Memoria:	No ③	- Seleccionar -	- Seleccionar -
Descripción del procedimiento de uso: ④ La fotocopiadora funciona mediante la tarjeta de empleado y el PIN de acceso por lo que queda auditado su empleo. Para la reproducción de la documentación clasificada se seguirá el procedimiento establecido en las Normas de la ANPIC.			

Fig. 27

- Tipo. Seleccionar si la ZAR dispone de fotocopiadora o equipo multifunción no conectado a ningún sistema TIC acreditado. En la ZAR existe una fotocopiadora. (Fig. 27 ①)
- Identificación de usuario. Se debe indicar si el dispositivo dispone de algún mecanismo que permita tener constancia de quien efectúa cada reproducción. La fotocopiadora del ejemplo funciona mediante la tarjeta de empleado y el PIN de acceso, por lo que queda auditado su empleo en todo momento. (Fig. 27 ②)
- Memoria. Indicar si el medio de reproducción dispone de memoria interna. En el caso de que el sistema la tenga, pero se efectúe un procedimiento de borrado tras la reproducción, seleccionar “No”. Esto último es lo que ocurre en el caso del ejemplo, por lo que se debe seleccionar “No” en la lista desplegable. (Fig. 27 ③)
- Descripción del procedimiento de uso. Descripción detallada de los procedimientos de fotocopiado de documentos clasificados (personal autorizado y registro de copias). (Fig. 27 ④)



7.1.5. Plan de emergencia

Describe las medidas organizativas de seguridad a adoptar o seguir para mantener la protección de la información clasificada ante contingencias de tipo extraordinario.

a) **Procedimientos generales de emergencia.** En cada uno de los supuestos que se contemplan; destrucción, traslado o evacuación, se deben indicar las diferentes actuaciones posibles, en función de las circunstancias (dentro de la jornada laboral, fuera de la jornada laboral, etc).

- Destrucción.

4.1 PROCEDIMIENTOS GENERALES DE EMERGENCIA. Procedimientos comunes a todo tipo de emergencias	
DESTRUCCIÓN	
Prioridad: De mayor a menor grado de clasificación y de más moderno a más antiguo	①
Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.	②
La destrucción de la documentación clasificada es una solución excepcional, especialmente en caso de emergencia producida por acciones hostiles. El responsable de la destrucción cuando se encuentre presente en la Instalación, será el Jefe del Órgano de Control y por el Jefe del Servicio de Seguridad cuando no esté presente.	

Fig. 28

- *Prioridad.* En este desplegable, seleccionar el orden a seguir en la destrucción de información clasificada en caso de emergencia. En el caso del ejemplo, si hubiera una emergencia que exigiera la destrucción de la información clasificada que allí se almacena, se realizaría de mayor a menor grado de clasificación y de más moderno a más antiguo. (Fig. 28 ①)
- *Descripción procedimiento.* Indicar los procedimientos generales a seguir en caso de que se decida esta actuación: responsabilidades, criterios, medios, avisos, y lugares alternativos previstos para la destrucción masiva. (Fig. 28 ②)

- Traslado.

TRASLADO	
Prioridad: De mayor a menor grado de clasificación y de más moderno a más antiguo	①
Local/es alternativos: ZAR CENTRO DE PRUEBAS 2 (CAL-1500)	②
Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.	③
La dirección del traslado, cuando esté presente, (normalmente será durante la jornada de trabajo o cuando se incorpore tras ser avisado) será del Jefe del Órgano de Control y, cuando no esté presente, del Jefe del Servicio de Seguridad.	

Fig. 29

- *Prioridad.* Seleccionar el orden de prioridad en el traslado de información clasificada. En el caso del ejemplo el orden sería el mismo que si se tratara de una destrucción, es decir “De mayor a menor grado de clasificación y de más moderno a más antiguo”. (Fig. 29 ①)

- *Local/es alternativos.* Indicar los lugares donde se trasladaría la información clasificada en caso de emergencia. Deben listarse los números de los certificados de acreditación de locales (CAL). Si el local alternativo no dispone de CAL se indicará. (Fig. 29 ②)
- *Descripción del procedimiento.* Se deben indicar los criterios para adoptar la decisión del traslado y los procedimientos generales a seguir en caso de que se decida esta actuación (itinerarios, medios, avisos, etc). (Fig. 29 ③)
- Evacuación.

EVACUACIÓN	
Prioridad: De mayor a menor grado de clasificación y de más moderno a más antiguo	①
Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.	②
Recoger toda la información clasificada y guardarla en las cajas fuertes. Apagar los equipos informáticos.	

Fig. 30

- *Prioridad.* Seleccionar el orden de prioridad en caso de evacuación. En el caso del ejemplo el orden sería “De mayor a menor grado de clasificación y de más moderno a más antiguo”. (Fig. 30 ①)
 - *Descripción del procedimiento.* Se deben indicar los procedimientos a seguir en caso de que se decida esta actuación: guardado de la información, cierre de contenedores o evacuación del personal. (Fig. 30 ②)
- b) **Actuaciones generales al producirse la emergencia.** Seleccionar las características del medio de identificación empleado en la organización:

4.2 ACTUACIONES GENERALES AL PRODUCIRSE LA EMERGENCIA

EN HORARIO LABORAL	
Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.	①
Se deberá evaluar la emergencia para determinar el tipo de actuación posterior, no obstante en determinadas situaciones, como es el caso de incendio, se deberá reaccionar de manera inmediata, la respuesta y acciones iniciales serán decisivas, por lo que deberá primar el principio de inmediatez, para atajar el fuego en su fase inicial, especialmente en los primeros momentos de producirse el fuego.	
FUERA DEL HORARIO LABORAL	
Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.	②
Se seguirá el siguiente procedimiento: a) En caso de que se detecte una incidencia por parte del sistema de alarma, o de alguna persona, se avisará al jefe del Servicio de Seguridad (teléfono 802187), cuya primera actuación será dirigida por la patrulla, quien ordenará que se dirijan a la ZAR	

Fig. 31

- En horario laboral. Indicar los procedimientos generales a seguir, incluyendo el personal responsable de inicio de las actuaciones, avisos, teléfonos de emergencias, etc. (Fig. 31 ①)
- Fuera del horario laboral. Procedimientos generales a seguir: avisos necesarios, actuación primera de los servicios de vigilancia, responsabilidades,

criterios de acceso a la zona clasificada y teléfonos de emergencias. (Fig. 31 ②)

- c) **Actuaciones generales posteriores a la emergencia.** Indicar los procedimientos generales a seguir y requisitos a cumplir (condiciones de seguridad mínimas necesarias) una vez finalizada la situación de emergencia, para la vuelta a la situación inicial. Procedimiento para el recuento de la información clasificada, análisis de pérdidas, certificados de destrucción, informes de comprometimientos y pérdidas.

4.3 ACTUACIONES GENERALES POSTERIORES A LA EMERGENCIA

Descripción del procedimiento: incluir aquellas tareas que se efectúan después de la emergencia, como la evaluación de los daños y la vuelta a la situación inicial.

EVALUACION DE DAÑOS.

Con la finalidad de comprobar todos los documentos, no se destruirá el último inventario.

- d) **Procedimientos particulares de actuación en caso de emergencia.** Descripción, para cada tipo de emergencia considerado, de las actuaciones complementarias a las generales indicadas anteriormente, y que sería preciso ejecutar para asegurar la protección de la información clasificada. Es conveniente utilizar cada ítem del apartado para un tipo de emergencia distinto y describir cada emergencia en el campo descripción. Así, en el ejemplo se ha utilizado el primer ítem para las emergencias de “Tipo II”, detallando las actuaciones particulares para “INCENDIO”, “INUNDACIÓN”, etc.

4.4 PROCEDIMIENTOS PARTICULARES DE ACTUACIÓN EN CASO DE EMERGENCIA

Tipo de emergencia: Tipo I: emergencias que puedan afectar a la seguridad de la documentación (disturbios, cortes totales de energía,...)

Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.

En caso de producirse acciones hostiles disturbios, acto terrorista, amenaza de bomba, etc, el Jefe del Servicio de Seguridad valorará el alcance de las mismas, proponiendo, en su caso, al personal establecido en el punto de actuaciones generales alguna de las acciones indicadas en el apartado, u otras que considere

Tipo de emergencia: Tipo II: Emergencias que puedan afectar a la integridad de la documentación (incendios, desastres naturales...)

Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.

INCENDIO

a) Activar la alarma de fuego, a través del jefe del servicio de seguridad (megafonía del centro), e informar al resto del personal.

Tipo de emergencia: - Seleccionar -

Descripción del procedimiento: incluir como se produce la comunicación y el responsable de iniciar su ejecución.

7.1.6. Declaración

- a) **Observaciones.** En este apartado se refleja cualquier aclaración u observación a lo declarado en las páginas anteriores del formulario, indicando el número del apartado al que hace referencia. A lo largo de este ejemplo se ha mostrado su utilidad para indicar que la ventana de la ZAR no dispone de sensor de apertura por ser fija, que se oculta la información clasificada cuando se efectúan las labores

de limpieza y para ampliar las características de la cerradura del armario de seguridad. También se ha utilizado para indicar la constitución de los perímetros de seguridad.

OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.

- 1.3 El Perímetro 1 lo constituye el cerramiento exterior de la instalación y el Perímetro 2 el propio edificio principal del Centro de Investigación.
 2.4 La ventana no dispone de sensor de apertura ya que se trata de un ventanal cuyas hojas son fijas (no se pueden abrir).
 2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.
 3.1 Se desconoce la clase de la cerradura del armario de seguridad según la norma UNE-EN-1300. Se trata de una cerradura de gorjas con llave de doble paleta. Dispone de certificación VdS Clase 2.

- b) Declaración y validación.** El proceso de validación se realiza tal y como se indica en el apartado 5.3 de este documento. El formulario no puede ser firmado hasta que no se haya validado, por lo que las casillas de firma permanecerán bloqueadas (color gris) mientras no se compruebe que FASE se ha cumplimentado correctamente.

DECLARACIÓN

El jefe del órgano de control del que dependa la ZAR, será responsable de verificar y declarar que el formulario de acreditación de seguridad es completo, correcto y está adecuadamente implantado. Cuando el propio jefe del órgano de control sea a su vez responsable de seguridad de la ZAR, la responsabilidad será del jefe del órgano de control superior.

VALIDAR FORMULARIO

Los abajo firmantes manifiestan que:

- Lo expuesto en este documento corresponde con las medidas de seguridad implantadas y procedimientos organizativos seguidos para la protección de información clasificada en la instalación.
- Los datos reflejados en el documento indican la situación real de la seguridad del local y el entorno a fecha de la firma.

- c) Firmas.** Mediante las firmas del formulario los firmantes manifiestan que lo expuesto en el mismo se corresponde con las medidas de seguridad implantadas y con los procedimientos organizativos seguidos para la protección de la información clasificada en la instalación. Para firmar pulsar sobre el recuadro de color naranja.

FIRMAS

RESPONSABLE SEGURIDAD DE LA ZAR	JEFE DEL ÓRGANO DE CONTROL

7.2. APERTURA ZAR SALA DE REUNIONES

7.2.1. Datos básicos

- a) **Datos de la zona de acceso restringido (ZAR).** En primer lugar, en la cabecera del apartado seleccionar que el formulario se rellena con motivo de una apertura.

DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)		<input type="checkbox"/> Renovación	<input checked="" type="checkbox"/> Apertura	LIMPIAR FORMULARIO
--	--	-------------------------------------	--	--------------------

A continuación, se consignarán los datos identificativos de la ZAR y los relativos a la solicitud de manejo/custodia de información clasificada. Seguidamente solo se comentarán aquellos apartados que varían respecto a los ya explicados en el apartado 7.1.1.

DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)		<input type="checkbox"/> Renovación	<input checked="" type="checkbox"/> Apertura	LIMPIAR FORMULARIO
ZAR Nº: ①	Órgano de control del que depende: PC CENTRO DE INVESTIGACIÓN			
Dirección: CALLE REAL, 7		Código postal: 28000		
Localidad:	Provincia: MADRID	País: ESPAÑA		
Edificio: PRINCIPAL	Planta: 1, ALA IZDA			
Local: P1A1	②			
Denominación: SALA DE REUNIONES		③		
Grado máximo información clasificada (I.C.): RESERVADO o equivalente ④	Ámbito: <input checked="" type="checkbox"/> OTAN <input checked="" type="checkbox"/> UE <input type="checkbox"/> ESA <input type="checkbox"/> NACIONAL			
Clase: II ⑤	Uso: Manejo ⑥	Especialidad: Ninguna		

Fig. 32

- ZAR Nº. Al tratarse de la apertura de una nueva ZAR este campo aparece bloqueado, ya que su número identificativo lo asigna la ONS una vez aprobada la solicitud. (Fig. 32 ①)
- Local. La sala esta etiquetada como P1A1 en el edificio. (Fig. 32 ②)
- Denominación. La ZAR se denomina “Sala de reuniones”. (Fig. 32 ③)
- Grado máximo información clasificada (I.C.). En esta sala se van a mantener reuniones en las que la información clasificada que se va a manejar será, como máximo, de grado “RESERVADO”. (Fig. 32 ④)
- Clase. Como el acceso al local no lleva consigo el acceso a la información clasificada, se solicita que la ZAR sea Clase II. (Fig. 32 ⑤)
- Uso. En la sala de reuniones no se almacena información clasificada, por lo que se seleccionará “Manejo” en la lista. (Fig. 32 ⑥)

- b) **Plano de planta de la ZAR.** Se debe añadir el plano en planta de la sala de reuniones sin incorporar simbología de ningún tipo (sistemas de seguridad, incendios, etc.) ni ceñirse exclusivamente al límite de la ZAR, sino mostrar una visión más amplia del entorno como por ejemplo un ala o planta del edificio.

PLANO EN PLANTA DE LA ZAR. Rellenar la zona de seguridad en color rojo (ZAR Clase I) o amarillo (ZAR Clase II)

El diagrama muestra una planta de un edificio con varias salas y pasillos. Una zona rectangular en el extremo izquierdo está resaltada en amarillo, representando la Zona de Acceso Restringido (ZAR) Clase II. El resto del edificio está delineado con líneas negras. En la parte inferior derecha del diagrama, hay una leyenda con dos cuadros: uno rojo etiquetado como 'ZAR Clase I' y uno amarillo etiquetado como 'ZAR Clase II'.

7.2.2. Entorno global.

La ZAR “Sala de reuniones” tiene el mismo entorno global de seguridad que la ZAR “Órgano de control” ya que para llegar a la propia zona de acceso restringido es necesario sobrepasar los mismos perímetros y zonas de seguridad exteriores. Por esta razón, los campos del formulario relativos al entorno global son exactamente iguales a los declarados en el apartado 7.1.2

📄 **Nota:** Para efectuar aperturas de nuevas ZAR dentro de la misma instalación o plasmar actualizaciones en sus medidas de seguridad puede resultar útil guardar una copia del formulario antes de ser firmado y emplearlo de plantilla.

7.2.3. Entorno local

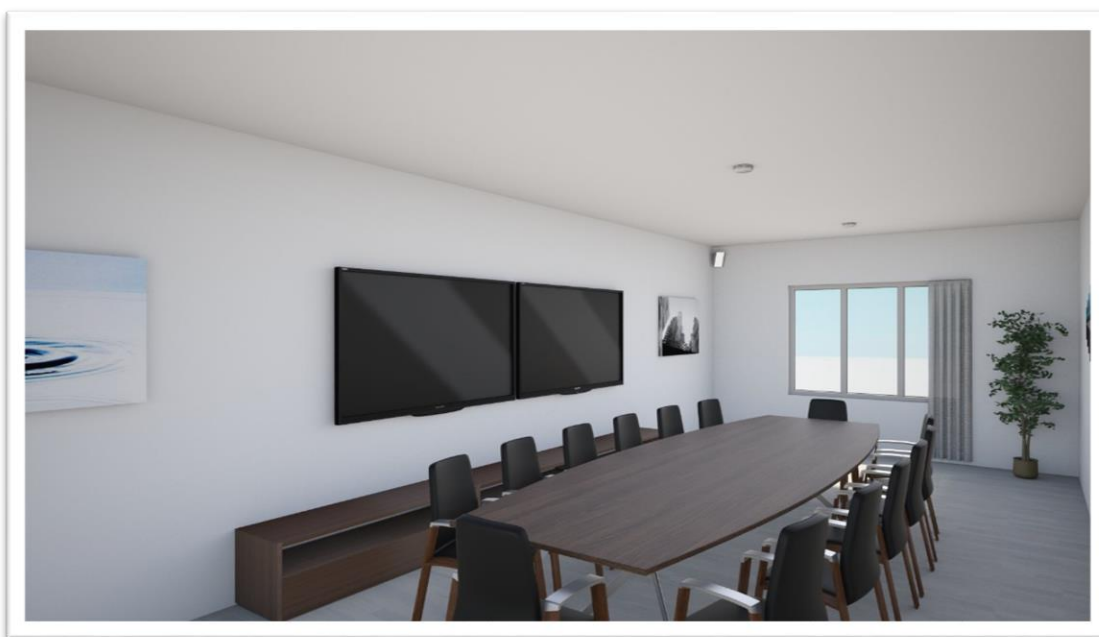
- a) **Medidas estructurales.** La resistencia de los elementos estructurales de protección de esta dependencia son iguales a los de la ZAR “Órgano de control”; por lo que consultar el apartado 7.1.3 si existen dudas.

2.1 MEDIDAS ESTRUCTURALES

Resistencia paredes: Media, Ladrillo hueco o macizo menor de 15 cm de espesor	Limitrofes con el exterior: Sí
Construcción paredes: De verdadero suelo a verdadero techo	Huecos excluyendo ventanas: No dispone ①
Suelo: Verdadero suelo	Techo: Falso techo

Fig. 33

- Huecos excluyendo ventanas. En los paramentos de la ZAR no existen huecos, por lo que se debe seleccionar “No dispone” en la lista desplegable. (Fig.33 ①)



- b) **Puerta de entrada.** Las características de la puerta de acceso son análogas a las recogidas en el apartado 7.1.3 b) de la ZAR “Órgano de control”.
- c) **Puerta de emergencia.** La ZAR Sala de Reuniones no tiene puerta de emergencia.

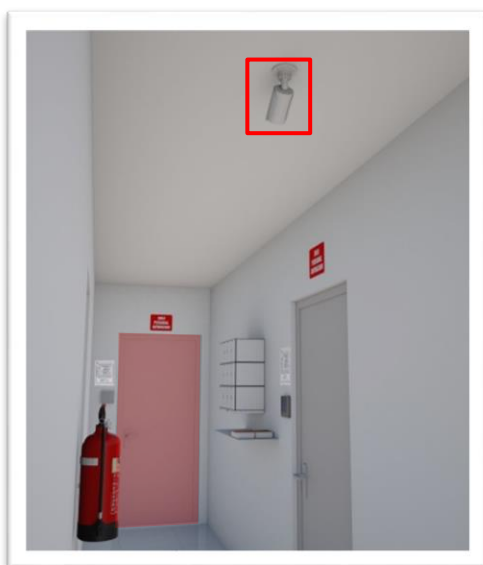
- d) **Ventanas exteriores.** La ZAR “Sala de reuniones” dispone de dos ventanas que dan al exterior (una en la fachada norte y otra en la sur). Ambas tienen las mismas características que la ventana de la ZAR “Órgano de control”, declaradas en el apartado 7.1.3 d), salvo que se impide la visión desde el exterior mediante cortinas.
- e) **Sistema de control de acceso.** Las características del sistema de control de accesos son análogas a las recogidas en el apartado 7.1.3 e) de la ZAR “Órgano de control”.
- f) **Personal que accede a la ZAR.** Los aspectos relativos al personal que accede a la ZAR “Sala de reuniones” no varían respecto a los recogidos en el apartado 7.1.3 f). Observar que, en esta ocasión, a pesar de que el personal externo que realiza las labores de limpieza y mantenimiento no dispone de habilitación personal de seguridad, los campos HPS no se muestran en color rojo. Esto es debido a que la ZAR “Sala de reuniones” es Clase II y, por tanto, no precisa que este personal disponga de HPS.

2.6 PERSONAL QUE ACCEDE A LA ZAR

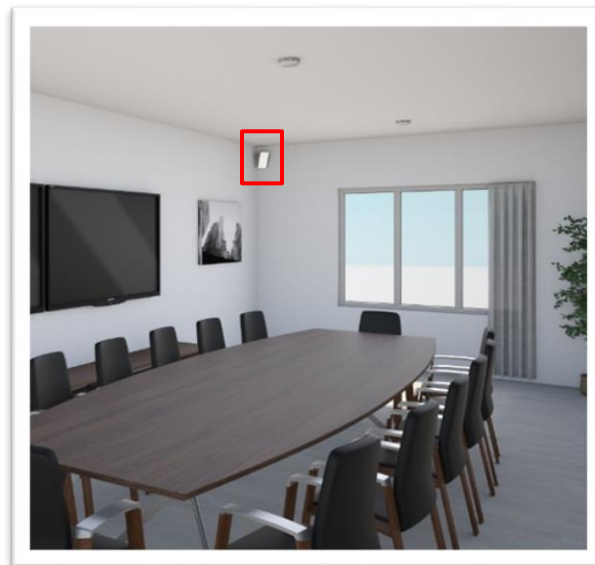
Formación en protección de la I.C.: Sí, con frecuencia igual o menor a un año	Registro formación: Sí
Registros aleatorios a la entrada/salida: Sí	
Servicio de limpieza: Personal empresa externa	Escortado: Sí
Servicio de mantenimiento: Personal empresa externa	Escortado: Sí
	Habilitación personal de seguridad: No
	Habilitación personal de seguridad: No

- g) **Circuito cerrado de televisión (CCTV).** Las puertas de acceso a la ZAR “Órgano de control” y a la ZAR “Sala de reuniones” son continuas y se controlan mediante la misma cámara de seguridad, cuyas características se recogen en el apartado 7.1.3 g) de este documento.

- h) **Sistema detección de intrusos (SDI).** La ZAR “Sala de reuniones” tiene instalado un detector de movimiento de doble tecnología de iguales características que el del apartado 7.1.3 h).



Sistema CCTV



Sistema detección de intrusos

- i) **Otros elementos y medidas de seguridad.** El resto de elementos y medidas de seguridad se recogen en este apartado.

2.9 OTROS ELEMENTOS Y MEDIDAS DE SEGURIDAD			
Detector sísmico: No	Detector agua: No	Detector incendios: Sí	Elementos extinción: Extintores
Sistemas TIC acreditados: No	① Etiquetas de seguridad: - Seleccionar -	② Casilleros de seguridad externos: Sí	
Zona TEMPEST: Zona 3	Medición válida hasta: 26-06-2028	Medidas TEMPEST adicionales: No	

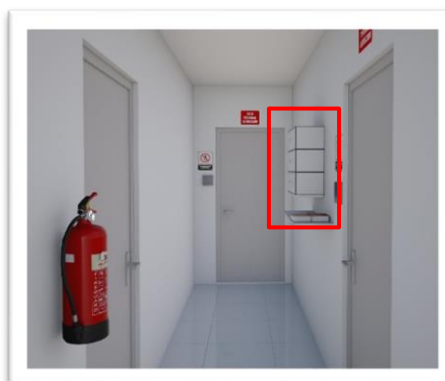
Fig. 34

- Detector sísmico. Seleccionar “No”, ya que la ZAR no tiene este tipo de sensores.
- Detector agua. Seleccionar “No”, ya que la ZAR no tiene sensor de líquidos.

- Detector incendios. En el techo de la ZAR “Sala de reuniones” existen varios detectores, por lo que se debe seleccionar “Sí” en la lista desplegable.



- Elementos extinción. Al igual que la ZAR “Órgano de control”, la ZAR “Sala de reuniones” dispone de extintores en el pasillo.
- Sistemas TIC acreditados. La ZAR no dispone de sistemas TIC acreditados, por lo que se debe seleccionar “No” en el desplegable. (Fig. 34 ①)
- Etiquetas de seguridad. Al no disponer de sistemas TIC acreditados el campo etiquetas de seguridad se muestra bloqueado. (Fig. 34 ②)
- Casilleros de seguridad externos. Al ser despachos contiguos la ZAR “Sala de reuniones” comparte casilleros de seguridad con la ZAR “Órgano de control”. Por tanto, seleccionar “Sí”.
- Zona TEMPEST. Seleccionar “Zona 3”, ya que según certificado del Centro Criptológico Nacional todos los locales de la primera planta del edificio tienen esa clasificación.
- Medición válida hasta. Seleccionar la fecha de expiración del certificado zoning de locales.



- Medidas TEMPEST adicionales. Seleccionar “No” en la lista, ya que la sala no cuenta con ninguna medida extra.

7.2.4. Entorno próximo

- a) **Mobiliario de seguridad.** En la ZAR “Sala de reuniones” no se custodian documentos ni soportes con información clasificada, por lo que se selecciona en el campo “Tipo” de la primera columna (Mobiliario de seguridad tipo 1) “No dispone”. El resto de columnas pueden dejarse con la opción “-Seleccionar-” o rellenar también con “No dispone”.

3.1 MOBILIARIO DE SEGURIDAD. Rellenar cada tipo de mobiliario existente en la ZAR en el que se custodia información clasificada en una columna

	MOBILIARIO DE SEGURIDAD TIPO 1	MOBILIARIO DE SEGURIDAD TIPO 2	MOBILIARIO DE SEGURIDAD TIPO 3
Tipo:	No dispone	- Seleccionar -	- Seleccionar -
Nivel (UNE-EN-1143-1):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Tipo cerradura 1:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Clase cerradura 1 (UNE-EN-1300):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Tipo cerradura 2:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Clase cerradura 2 (UNE-EN-1300):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Grado máximo de la I.C. que custodia:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Compartimentación de la I.C.:	- Seleccionar -	- Seleccionar -	- Seleccionar -

- b) **Control de llaves y combinaciones.** Completar con las características de los medios y las pautas para obtener y mantener un efectivo control de llaves y combinaciones.

- Llaves puerta acceso y claves sistema de alarma. El control y protección de las llaves de la puerta de acceso y las claves del sistema de alarma se produce de igual forma que en la, ZAR “Órgano de control”, por lo que los campos de este apartado se rellenaran de la forma explicada en el apartado 7.1.4 b).

	LLAVES PUERTA ACCESO Y CLAVES SISTEMA ALARMA
Custodia juego de llaves de uso diario:	Sí, armario portallaves electrónico
Custodia juego de llaves de emergencia:	Sí, caja fuerte
Custodia resto de juegos de llaves:	No existen más llaves
Registro / inventario:	Sí
Control en la copia de llaves:	Sí
Separación llaves / claves:	Sí
Registro cambio de combinaciones:	Sí
Periodo de cambio de combinaciones:	Cada 6 meses o menos

- Llaves / claves mobiliario de seguridad. La ZAR “Sala de reuniones” no dispone de mobiliario de seguridad, ya que no custodia ningún tipo de documento clasificado. Por tanto, todos los campos relativos al control de llaves y claves del mobiliario de seguridad aparecen bloqueados.

LLAVES / CLAVES MOBILIARIO DE SEGURIDAD
- Seleccionar -
- Seleccionar -
- Seleccionar -
- Seleccionar -
- Seleccionar -
- Seleccionar -
- Seleccionar -
- Seleccionar -

- Descripción del procedimiento de gestión de llaves y combinaciones. Descripción detallada del procedimiento para el manejo, control, sustitución, registro de cambios, actuación ante pérdidas (o comprometimientos) y custodia, durante y después del trabajo, de las llaves y combinaciones. Si existen diferencias, se indicará el procedimiento para cada llave/clave que tenga un tratamiento. Normalmente no tendrá el mismo trato la llave de la puerta que la de la caja fuerte.

Descripción del procedimiento de gestión de llaves y combinaciones: LLAVES - La llave de uso diario se deposita en un armario de llaves electrónico situado en el pasillo. Sólo el personal encuadrado en el órgano de control está autorizado a la retirada de la misma. Durante la jornada de trabajo estará bajo el control del personal del órgano de control. - El juego de emergencia está depositado en la caja fuerte del Centro Permanente de Seguridad dentro de un sobre sellado y lacrado. La clave de desactivación de la alarma del local no se deposita junto a la llave de emergencia. CLAVES La clave de activación/desactivación de la alarma que da acceso al local se guarda de forma segura en la aplicación que gestiona todo el sistema de seguridad.

- c) **Sistemas de destrucción.** En la ZAR “Sala de reuniones” no existe ninguna trituradora.

3.3 SISTEMAS DE DESTRUCCIÓN. Si existen varias destructoras en la ZAR indicar las características del tipo que genere un residuo de menor tamaño	
Tipo: No dispone ①	Corte según norma DIN-66399: - Seleccionar - ②
Descripción del procedimiento alternativo o complementario: ③ Si es necesario la destrucción de documentación se efectuará con los sistemas de destrucción de la ZAR ÓRGANO DE CONTROL.	

Fig. 35

- Tipo. En el caso de la ZAR “Sala de reuniones” no existe ninguna trituradora, por lo que se debe seleccionar “No dispone”. (Fig. 35 ①)
- Corte según norma DIN-66399. Al no existir ninguna trituradora de corte en partículas este campo aparece bloqueado. (Fig. 35 ②)
- Descripción del procedimiento alternativo o complementario. En este caso se indica que, si es necesario la destrucción de algún documento clasificado, se

utilizará el sistema de destrucción existente en la ZAR “Órgano de control” que está ubicada justamente al lado. (Fig. 35 ③)

- d) **Sistemas de reproducción.** En la ZAR “Sala de reuniones” tampoco existe ningún sistema de reproducción, por tanto, seleccionar “No dispone” en el campo “Tipo” de la primera columna. A continuación, se bloquearán el resto de los campos relativos a los sistemas de reproducción.

3.4 SISTEMAS DE REPRODUCCIÓN. Indicar en cada columna los equipos de reproducción existentes en la ZAR y no conectados a sistemas TIC acreditados			
	SISTEMA DE REPRODUCCIÓN 1	SISTEMA DE REPRODUCCIÓN 2	SISTEMA DE REPRODUCCIÓN 3
Tipo:	No dispone	- Seleccionar -	- Seleccionar -
Identificación de usuario:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Memoria:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Descripción del procedimiento de uso:			

7.2.5. Plan de emergencia

Puesto que en esta sala no se va a almacenar información clasificada todos los campos del plan de emergencia aparecen bloqueados.



7.2.6. Declaración

- a) **Observaciones.** En este apartado se reflejan un par de aclaraciones a algún aspecto del formulario. En concreto, que la ventana de la ZAR no dispone de sensor de apertura por ser fija y que se oculta la información clasificada cuando se efectúan las labores de limpieza/mantenimiento.

OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.
2.4 La ventana no dispone de sensor de apertura ya que se trata de un ventanal cuyas hojas son fijas (no se pueden abrir). 2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.

- b) **Declaración y validación.** El proceso de validación se realiza tal y como se indica en el apartado 5.3 de este documento. El formulario no puede ser firmado hasta que no se haya validado.
- c) **Firma.** Mediante las firmas del formulario los firmantes manifiestan que lo expuesto en el mismo corresponde con las medidas de seguridad implantadas y con los procedimientos organizativos seguidos para la protección de información clasificada en la instalación.

FIRMAS

RESPONSABLE SEGURIDAD DE LA ZAR	JEFE DEL ÓRGANO DE CONTROL
	

7.3. APERTURA ZAR CENTRO DE PROCESO DE DATOS

7.3.1. Datos básicos

- a) **Datos de la zona de acceso restringido (ZAR).** En primer lugar, en la cabecera del apartado seleccionar que el formulario se rellena con motivo de una apertura.

DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)	<input type="checkbox"/> Renovación	<input checked="" type="checkbox"/> Apertura	LIMPIAR FORMULARIO
---	-------------------------------------	--	---------------------------

Se consignarán los datos identificativos de la ZAR y los relativos a la solicitud de manejo/custodia de información clasificada. A continuación, solo se comentarán aquellos apartados que varían respecto a los ya explicados en el apartado 7.1.1.

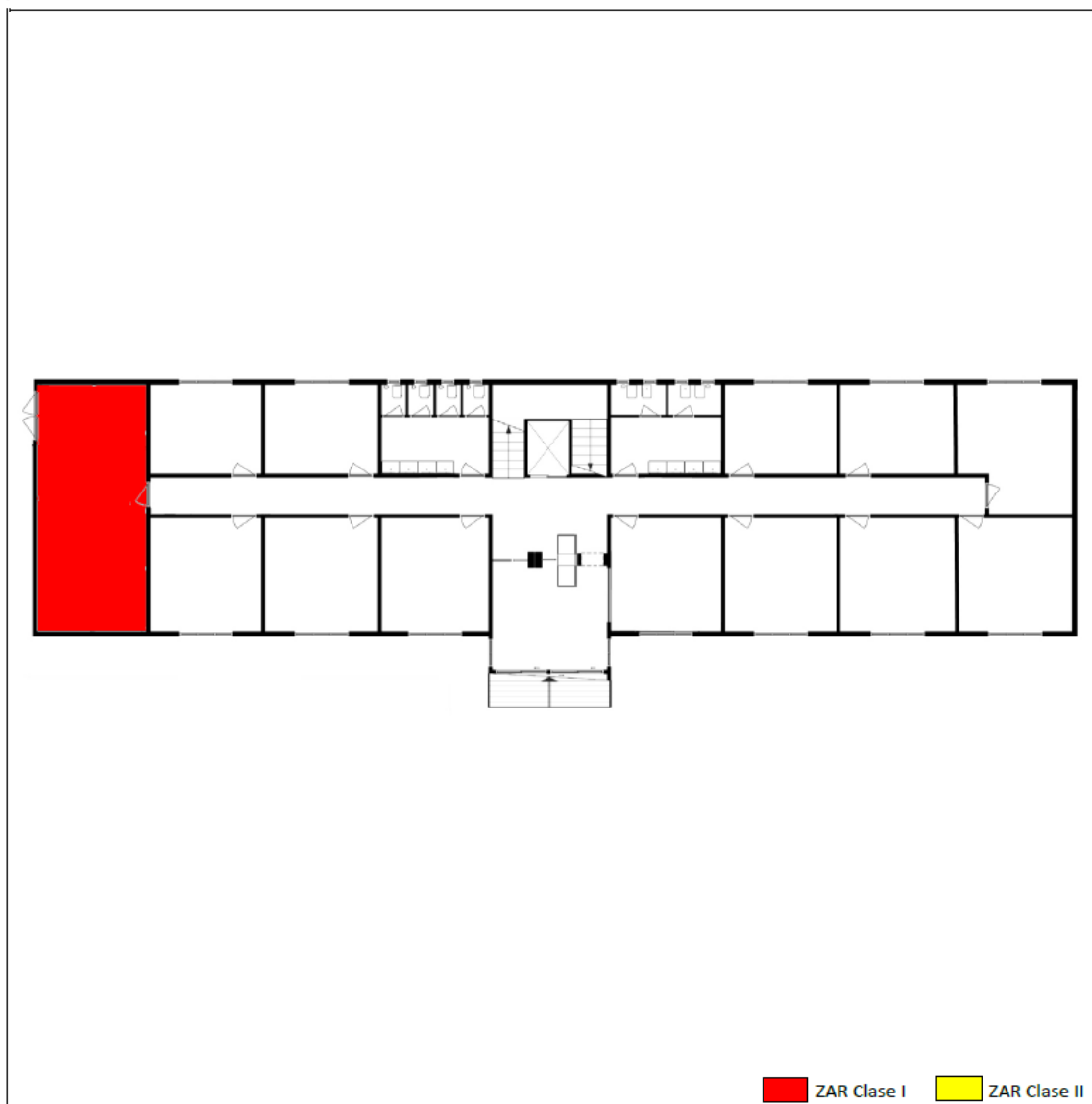
DATOS DE LA ZONA DE ACCESO RESTRINGIDO (ZAR)		<input type="checkbox"/> Renovación	<input checked="" type="checkbox"/> Apertura	LIMPIAR FORMULARIO
ZAR Nº: ①	Órgano de control del que depende: PC CENTRO DE INVESTIGACIÓN			
Dirección: CALLE REAL, 7			Código postal: 28000	
Localidad:	Provincia: MADRID	País: ESPAÑA		
Edificio: PRINCIPAL	Planta: BAJA, ALA IZDA			
Local: PBA1	②			
Denominación: CENTRO DE PROCESO DE DATOS (CPD) ③				
Grado máximo información clasificada (I.C.): RESERVADO o equivalente ④	Ámbito: <input checked="" type="checkbox"/> OTAN <input checked="" type="checkbox"/> UE <input type="checkbox"/> ESA <input type="checkbox"/> NACIONAL			
Clase: I ⑤	Uso: Manejo ⑥	Especialidad: Ninguna		

Fig. 36

- ZAR Nº. Al tratarse de la apertura de una nueva ZAR este campo aparece bloqueado, ya que su número identificativo lo asigna la ONS una vez aprobada la solicitud. (Fig. 36 ①)
 - Local. La sala esta etiquetada como PBA1 en el edificio. (Fig. 36 ②)
 - Denominación. La ZAR se denomina “Centro de proceso de datos (CPD)”. (Fig. 36 ③)
 - Grado máximo información clasificada (I.C.). En esta sala se van a instalar sistemas en los que se va a manejar información clasificada como máximo de grado “RESERVADO”. (Fig. 36 ④)
 - Clase. Como el CPD va a albergar elementos de red y servidores de sistemas clasificados, se solicita que la ZAR sea Clase I. (Fig. 36 ⑤)
 - Uso. La acreditación de un sistema TIC le autoriza para el manejo de información clasificada en las condiciones específicas establecidas, por lo que se seleccionará “Manejo” en la lista. (Fig. 36 ⑥)
- b) **Plano de planta de la ZAR.** Se debe añadir el plano en planta del CPD sin incorporar simbología de ningún tipo (sistemas de seguridad, incendios, etc.) ni

ceñirse exclusivamente al límite de la ZAR, sino mostrar una visión más amplia del entorno como por ejemplo un ala o planta del edificio.

PLANO EN PLANTA DE LA ZAR. Rellenar la zona de seguridad en color rojo (ZAR Clase I) o amarillo (ZAR Clase II)



7.3.2. Entorno global

La ZAR “CPD” tiene el mismo entorno global de seguridad que el resto de las zonas de acceso restringido del edificio ya que para llegar a ella es necesario sobrepasar los mismos perímetros y zonas de seguridad exteriores. Por esta razón los campos del formulario relativos al entorno global son iguales a los declarados en el apartado 7.1.2

Nota: Para efectuar aperturas de nuevas ZAR dentro de la misma instalación o plasmar actualizaciones en sus medidas de seguridad puede resultar útil guardar una copia del formulario antes de ser firmado y emplearlo de plantilla.

7.3.3. Entorno local

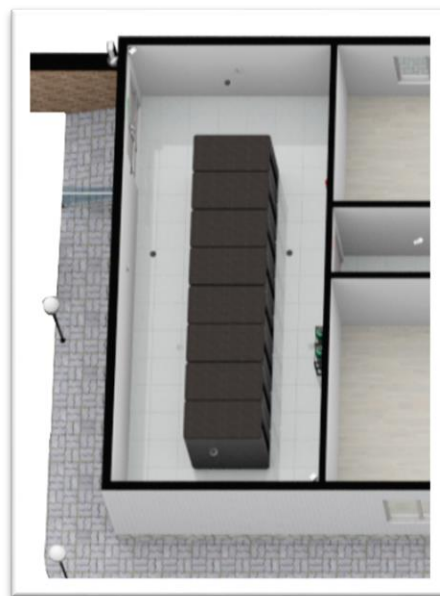
- a) **Medidas estructurales.** En este apartado se recoge toda la información relativa a los elementos estructurales de protección, como son los paramentos verticales (paredes) y horizontales (suelo y techo).

2.1 MEDIDAS ESTRUCTURALES

Resistencia paredes: Alta. Piedra, hormigón o ladrillo macizo de más de 15 cm de espesor, acero de buques o shelters: -	Limitrofes con el exterior: Sí
Construcción paredes: De verdadero suelo a verdadero techo	Huecos excluyendo ventanas: Sí, protegidos (rejas, sensores, concertina,...)
Suelo: Falso suelo	Techo: Falso techo

Fig. 37

- Resistencia paredes. Tres de las cuatro paredes que limitan el CPD forman parte de los muros exteriores del edificio; el cuarto paramento, donde se encuentra la puerta de entrada, está construido con ladrillo macizo de medio pie de espesor. Por tanto, la resistencia de las paredes de la ZAR “CPD” es “Alta. Piedra, hormigón o ladrillo macizo de más de 15 cm de espesor, acero de buques o shelters”. (Fig. 37 ①)
- Limitrofes con el exterior. Tres de las paredes de la ZAR “CPD” dan al exterior. La pared norte limita con un vial público y las sur y oeste con la zona de aparcamientos de la instalación. Seleccionar, por tanto, “Sí” en el campo. (Fig. 37 ②)
- Construcción paredes. Los paramentos verticales discurren desde el verdadero suelo hasta el verdadero techo. (Fig. 37 ③)
- Huecos excluyendo ventanas. En la ZAR “CPD” existen huecos destinados al paso de cableado al interior del local, pero dichos huecos se encuentran protegidos mediante rejillas. Por tanto, seleccionar “Sí, protegidos” (rejillas, sensores, concertina, ...). (Fig. 37 ④)
- Suelo. La ZAR dispone de suelo técnico elevado, por tanto, seleccionar “Falso suelo”. (Fig. 37 ⑤)
- Techo. El CPD del ejemplo dispone de techo practicable por donde se distribuye el cableado y conductos de ventilación, por lo que se debe seleccionar “Falso techo” en la lista desplegable. (Fig. 37 ⑥)



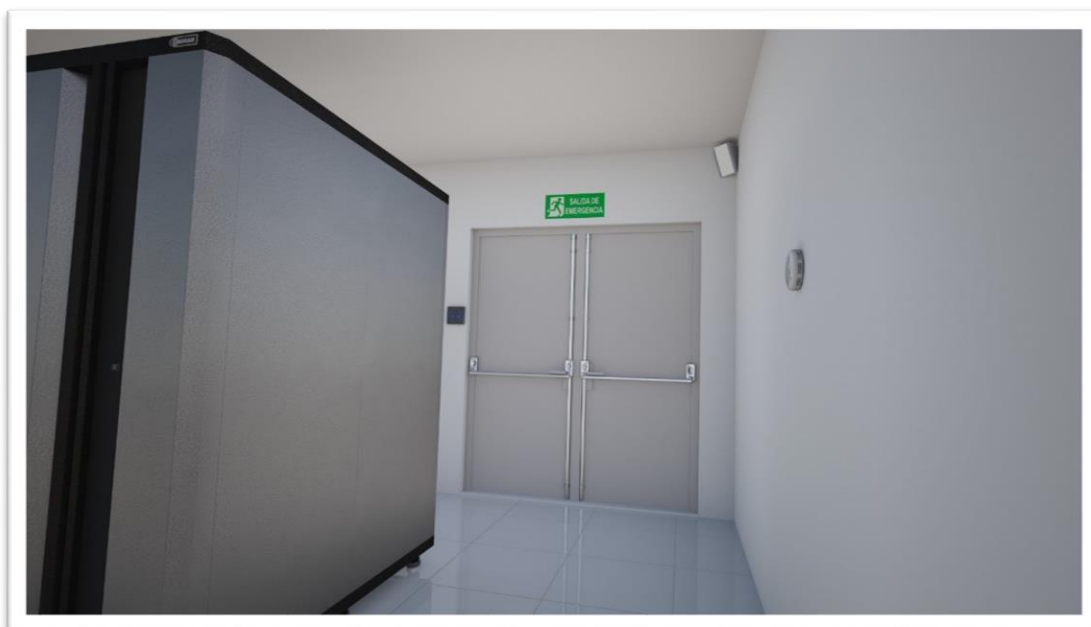
- b) **Puerta de entrada.** Las características de la puerta de acceso son análogas a las recogidas en el apartado 7.1.3 b) de la ZAR “Órgano de control”.
- c) **Puerta de emergencia.** La ZAR “Sala de reuniones” tiene una puerta de emergencia.

2.3 PUERTA DE EMERGENCIA

Tipo: Otro ①	Uso controlado: Sí, mediante sensor de apertura y/o cámara ②
Sensor apertura: Sí	Antisabotaje: Sí Conexión alarma: Sí, al centro de control de alarmas

Fig. 38

- Tipo. En el caso de la ZAR “CPD” se selecciona “Otro” (Fig. 38 ①) y se pasa a añadir las características de la puerta en el apartado “Observaciones” de la última página del formulario.



OBSERVACIONES. Completar con cualquier aclaración que considere importante a lo declarado en las páginas anteriores, indicando el número del apartado al que hace referencia.

2.3 La puerta de emergencia es una puerta metálica de lámina galvanizada dotada de barras anti pánico y certificada para la resistencia al fuego de hasta 180 minutos.

2.6 Cuando se efectúan labores de limpieza y/o mantenimiento se oculta toda la información clasificada si existiese, de tal forma que no pueda producirse acceso a la misma.

- Uso controlado. La puerta de emergencia de la ZAR se controla a través de un sensor de apertura conectado al CPS de la instalación. Además, se completa este control con una cámara de seguridad que permite visualizar las entradas y salidas a través de esa puerta. Por tanto, se debe seleccionar “Sí, mediante sensor de apertura y/o cámara”. (Fig. 38 ②)

- Sensor apertura, antisabotaje, conexión alarma. Los conceptos de los tres campos son análogos a los explicados en apartado de la puerta de acceso. En el caso del ejemplo, se debe seleccionar “Sí”, en todos los campos.
- d) **Ventanas exteriores.** La ZAR “CPD” no dispone de ninguna ventana.
- e) **Sistema de control de acceso.** Las características del sistema de control de accesos son análogas a las recogidas en el apartado 7.1.3 e) de la ZAR “Órgano de control” salvo que en el CPD se tiene configurado el *antipassback*.
- Antipassback. En la ZAR “CPD” está implementada esta tecnología que obliga a los usuarios a salir antes de poder entrar y viceversa, por lo que se selecciona “Sí”, en la lista desplegable.
- f) **Personal que accede a la ZAR.** Los aspectos relativos al personal que accede a la ZAR “CPD” no varían respecto a los recogidos en el apartado 7.1.3 f).
- g) **Circuito cerrado de televisión (CCTV).** Tanto la puerta de acceso a la ZAR “CPD” como la puerta de emergencia son controladas mediante cámaras de seguridad cuyas características se recogen en el apartado 7.1.3 g) de este documento.
- h) **Sistema detección de intrusos (SDI).** La ZAR “CPD” tiene instalado dos detectores de movimiento de doble tecnología de iguales características que el del apartado 7.1.3 h).



- i) **Otros elementos y medidas de seguridad.** El resto de elementos y medidas de seguridad se recogen en este apartado.

2.9 OTROS ELEMENTOS Y MEDIDAS DE SEGURIDAD			
Detector sísmico: Sí ①	Detector agua: Sí ②	Detector incendios: Sí ③	Elementos extinción: Sistema automático ④
Sistemas TIC acreditados: Sí ⑤	Etiquetas de seguridad: Sí ⑥	Casilleros de seguridad externos: Sí ⑦	
Zona TEMPEST: Zona 3	Medición válida hasta: 26-06-2028	Medidas TEMPEST adicionales: Sí ⑧	

Fig. 39

- Detector sísmico. Seleccionar “Sí”, ya que la ZAR “CPD” dispone de detectores sísmicos instalados en las tres paredes que dan al exterior. (Fig. 39 ①)



- Detector agua. Para evitar inundaciones la ZAR “CPD” también dispone de este tipo de sensores. Seleccionar por tanto “Sí”. (Fig. 39 ②)
- Detector incendios. En la ZAR “CPD” existen detectores de incendio tanto en suelo como en techo, por lo que se debe seleccionar “Sí”, en la lista desplegable. (Fig. 39 ③)
- Elementos extinción. La ZAR “CPD” dispone de un sistema automático de extinción consistente en emisión de gas. Además, también dispone de elementos auxiliares como BIE y extintores. (Fig. 39 ④)
- Sistemas TIC acreditados. La ZAR dispone de sistemas de información y comunicaciones acreditados por lo que se debe seleccionar “Sí”, en el desplegable. (Fig. 39 ⑤)

- Etiquetas de seguridad. Todos los elementos de sistemas TIC acreditados disponen de sistemas antimanipulación, por lo que se debe seleccionar “Sí”, en la lista desplegable. (Fig. 39 ⑥)
- Casilleros de seguridad externos. Junto a la puerta de acceso al CPD existe un casillero para dejar los dispositivos electrónicos antes de entrar además del libro de registro de visitas. Por tanto, seleccionar “Sí”. (Fig. 39 ⑦)
- Zona TEMPEST. Seleccionar “Zona 3” ya que según certificado del Centro Criptológico Nacional el CPD tiene esa clasificación.
- Medición válida hasta. Seleccionar la fecha de expiración del certificado zoning de locales.
- Medidas TEMPEST adicionales. Seleccionar “Sí” en la lista, ya que los elementos de los sistemas clasificados se instalan en racks especiales que evitan la emisión de señales. (Fig. 39 ⑧)



7.3.4. Entorno próximo

- a) **Mobiliario de seguridad.** En la ZAR “CPD” no se custodian documentos ni soportes con información clasificada, por lo que se selecciona en el campo “Tipo” de la primera columna (Mobiliario de seguridad tipo 1) “No dispone”. El resto de columnas pueden dejarse con la opción “-Seleccionar-” o rellenar también con “No dispone”.

3.1 MOBILIARIO DE SEGURIDAD. Rellenar cada tipo de mobiliario existente en la ZAR en el que se custodia información clasificada en una columna

	MOBILIARIO DE SEGURIDAD TIPO 1	MOBILIARIO DE SEGURIDAD TIPO 2	MOBILIARIO DE SEGURIDAD TIPO 3
Tipo:	No dispone	- Seleccionar -	- Seleccionar -
Nivel (UNE-EN-1143-1):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Tipo cerradura 1:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Clase cerradura 1 (UNE-EN-1300):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Tipo cerradura 2:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Clase cerradura 2 (UNE-EN-1300):	- Seleccionar -	- Seleccionar -	- Seleccionar -
Grado máximo de la I.C. que custodia:	- Seleccionar -	- Seleccionar -	- Seleccionar -
Compartimentación de la I.C.:	- Seleccionar -	- Seleccionar -	- Seleccionar -

- b) **Control de llaves y combinaciones.** Completar con las características de los medios y las pautas convenientes para obtener y mantener un efectivo control de llaves y combinaciones.

- Llaves puerta acceso y claves sistema de alarma. El control y protección de las llaves de la puerta de acceso y las claves del sistema de alarma se produce de igual forma que en la ZAR “Órgano de control”, por lo que los campos de este apartado se rellenaran de la forma explicada en el apartado 7.1.4 b).

LLAVES PUERTA ACCESO Y CLAVES SISTEMA ALARMA	
Custodia juego de llaves de uso diario:	Sí, armario portallaves electrónico -
Custodia juego de llaves de emergencia:	Sí, caja fuerte -
Custodia resto de juegos de llaves:	No existen más llaves -
Registro / inventario:	Sí -
Control en la copia de llaves:	Sí -
Separación llaves / claves:	Sí -
Registro cambio de combinaciones:	Sí -
Periodo de cambio de combinaciones:	Cada 6 meses o menos -

- Llaves / claves mobiliario de seguridad. La ZAR “CPD” no dispone de mobiliario de seguridad ya que no custodia ningún tipo de documento clasificado. Por tanto, todos los campos relativos al control de llaves y claves del mobiliario de seguridad aparecen bloqueados.
- Descripción del procedimiento de gestión de llaves y combinaciones. Descripción detallada del procedimiento para el manejo, control, sustitución, registro de cambios, actuación ante pérdidas (o comprometimientos), custodia durante y después del trabajo de las llaves y combinaciones. Si existen diferencias, se indicará el procedimiento para cada llave/clave que tenga un tratamiento diferente. Normalmente no tendrá el mismo trato la llave de la puerta que la de la caja fuerte.

Descripción del procedimiento de gestión de llaves y combinaciones: LLAVES a) Puerta de acceso - La llave de uso diario se deposita en un armario de llaves electrónico situado en el pasillo. Sólo el personal encuadrado en el órgano de control está autorizado a la retirada de la misma. Durante la jornada de trabajo estará bajo el control del personal del órgano de control. - El juego de emergencia está depositado en la caja fuerte del Centro Permanente de Seguridad dentro de un sobre sellado y lacrado. La clave de desactivación de la alarma del local no se deposita junto a la llave de emergencia. b) Mobiliario de seguridad - La llave de uso diario se deposita en un armario de llaves electrónico situado tras la puerta de entrada.
--

- c) **Sistemas de destrucción.** En la ZAR “CPD” no existe ninguna trituradora, por lo que los valores serán idénticos a los que aparecen en el apartado 7.2.4 c).
- d) **Sistemas de reproducción.** En el CPD tampoco existe ningún sistema de reproducción. Por tanto, seleccionar “No dispone” en el campo “Tipo” de la primera columna. A continuación, se bloquearán el resto de los campos relativos a los sistemas de reproducción.

