



# TABLA DE CONTENIDOS

<b>1 INTRODUCCIÓN</b> .....	<b>4</b>
1.1 Presentación de las soluciones .....	4
1.2 Información sobre el copyright .....	4
1.3 Aviso de confidencialidad.....	4
<b>2 INSTALACIÓN FÍSICA</b> .....	<b>5</b>
2.1 Instalación física .....	5
2.1.1 Alimentación .....	5
2.1.2 Red .....	5
2.1.3 Cámaras analógicas .....	5
2.1.4 Cámaras IP .....	6
2.1.5 Entradas digitales o particiones .....	6
2.1.6 Salidas o relés .....	6
<b>3 CONFIGURACIÓN BÁSICA</b> .....	<b>7</b>
3.1 Sistema.....	7
3.1.1 Configuración de nueva contraseña.....	8
3.2 Configuración.....	8
3.2.1 Instalación.....	8
3.2.2 Vista lógica .....	10
3.3 Acceso.....	12
3.3.1 Acceso al sistema .....	12
3.3.2 Visor .....	14
3.4 Cámaras .....	15
3.4.1 Gestión de cámaras.....	15
3.4.2 Cámara.....	16
3.4.3 Herramienta de calibración de zoom.....	21
3.4.4 Perspectiva de la cámara.....	22
3.4.5 Creación de reglas.....	25
3.4.6 Tipos de detección.....	26
3.4.7 Zona de exclusión de regla .....	28
3.4.8 Respuestas de regla .....	30
3.5 Dispositivos.....	32
3.5.1 Creación de dispositivos .....	32
3.5.2 Testeo de dispositivos.....	33
<b>4 CONFIGURACIÓN AVANZADA</b> .....	<b>34</b>
4.1 Configuración.....	34
4.1.1 Central Receptora de Alarmas (CRA) .....	34
4.1.2 Particiones .....	35
4.1.3 Relés .....	36
4.1.4 Correo.....	37
4.1.5 Entorno .....	39
4.1.6 HTTP .....	40
4.2 Cámaras .....	41
4.2.1 Menú de opciones.....	41
4.2.2 Configuración general.....	45
4.2.3 Gestión de cámaras.....	49
4.2.4 Horarios de regla .....	49
4.2.5 Regla Entrar / Salir.....	50
4.2.6 Regla Movimiento .....	51
4.2.7 Regla Objeto abandonado/robado .....	52
4.2.8 Regla Sabotaje .....	53
4.2.9 Regla Aglomeración.....	54
4.2.10 Regla Entrada externa .....	55
4.2.11 Región de exclusión.....	56

4.2.12	Parámetros .....	58
4.2.13	Máscara de privacidad .....	66
4.2.14	Virtual IR .....	66
4.2.15	Posicionamientos PTZ .....	67
4.2.16	Calibración del Zoom .....	70
4.2.17	Vista conceptual .....	71
4.3	Asistencia .....	77
4.4	Apagar .....	77
<b>5</b>	<b>ALARMAS .....</b>	<b>78</b>
5.1	Buscador de alarmas .....	78
5.1.1	Buscador de alarmas .....	78
5.1.2	Acciones de alarmas .....	79
<b>6</b>	<b>ACCESO REMOTO WEB .....</b>	<b>82</b>
6.1	Alarmas .....	83
6.2	Cámaras .....	84
6.3	Instalación .....	85
<b>7</b>	<b>GAMA DE SOLUCIONES Y CARACTERÍSTICAS .....</b>	<b>86</b>
7.1	DAVIEW MINI .....	86
7.2	DAVIEW S .....	86
7.3	DAVIEW LR .....	86
7.4	DFUSION .....	86
7.5	DFUSIONPRO .....	87
7.6	DAVIEW SMART CITIES .....	87

# 1 INTRODUCCIÓN

## 1.1 PRESENTACIÓN DE LAS SOLUCIONES

Este manual describe la instalación y configuración inicial de la serie de soluciones DAVANTIS, compuesta por Daview S (Standard), Daview LR (Long Range), Daview MINI, DFUSION y DFUSIONPRO.

Daview LR y DFUSIONPRO incluyen todas las funcionalidades de la solución Daview S, así como funcionalidades adicionales aplicables tanto a cámaras visibles como a cámaras térmicas, para la detección en largas distancias.

Sigue las indicaciones de las secciones “Instalación física” y “Configuración básica” para configurar un nuevo sistema. Para conocer todas las funcionalidades adicionales, sigue las instrucciones indicadas en “Configuración avanzada”.

Si necesitas ayuda durante el proceso de instalación, consulta a tu proveedor o contacta con [support@davantis.com](mailto:support@davantis.com).

## 1.2 INFORMACIÓN SOBRE EL COPYRIGHT

El contenido de este Manual de Administrador es propiedad de DAVANTIS TECHNOLOGIES, SL y está sujeto a las leyes sobre propiedad intelectual del Estado español. No está permitido realizar copias totales o parciales de su contenido sin la autorización escrita de la empresa DAVANTIS TECHNOLOGIES, SL.

## 1.3 AVISO DE CONFIDENCIALIDAD

Este documento tiene derechos de autor y contiene información comercialmente sensible y confidencial. El lector se responsabiliza de su utilización, única y exclusivamente, para los fines por los cuales ha sido elaborado. El lector acepta que no está permitido difundir este documento a terceros, total o parcialmente, sin el consentimiento expreso de los autores.

Solamente se permite el uso del presente documento si se ha adquirido una o varias licencias de la serie de soluciones DAVANTIS.

## 2 INSTALACIÓN FÍSICA

Instala el servidor en una ubicación adecuada y conecta las conexiones correspondientes.

### 2.1 INSTALACIÓN FÍSICA

#### 2.1.1 Alimentación

Conecta el cable de alimentación suministrado con el equipo.

#### 2.1.2 Red

El sistema puede funcionar en modo autónomo o conectado a una red local de tipo Ethernet, con protocolo TCP/IP. Será necesario conectar el equipo a una red en los casos siguientes:

- Si en tu instalación hay más de un equipo.
- Si quieres acceder a las alarmas desde otro equipo que no sea el servidor.
- Si quieres que el sistema envíe las alarmas a una central receptora de alarmas (CRA).

Si no se cumple ninguna de las condiciones anteriores, no será necesario conectar el equipo a la red local.

Para conectar el sistema a la red local, usa el conector RJ-45 situado en la parte posterior del equipo.

#### 2.1.3 Cámaras analógicas

El sistema de videoanálisis es compatible con la mayoría de cámaras analógicas del mercado que funcionen con cable coaxial y conexión BNC. En caso de que tus cámaras dispongan de otro tipo de conexión (como cable de par trenzado), será necesaria la instalación de un adaptador (par trenzado - BNC coaxial).

En el caso de tener instalado un grabador analógico de vídeo o digital (DVR), será necesario insertar bifurcadores de señal para enviar la señal de cada cámara a monitorizar al servidor. En caso de no utilizar ningún grabador, las cámaras se conectarán directamente a las entradas de vídeo BNC en la parte posterior del sistema.

Pasos a seguir:

- 1) Con el aparato apagado, conecta las cámaras analógicas a la parte posterior del sistema.
- 2) Conecta un monitor común de ordenador, un ratón y un teclado al sistema.
- 3) Enciende el aparato y espera hasta que el sistema se inicie automáticamente.

### 2.1.4 Cámaras IP

El sistema es compatible con la mayoría de las cámaras IP del mercado, y permite una adaptación rápida a cualquier dispositivo IP que se comunique por protocolo ONVIF o RTSP.

En caso de utilizar cámaras IP, únicamente es necesario asegurarse de que el sistema esté conectado a la misma red de área local a la que están conectadas las cámaras.

Pasos a seguir:

- Conecta el sistema a la red de área local.
- Conecta las cámaras a la red de área local.
- Conecta un monitor de ordenador, un ratón y un teclado al sistema.
- Enciende el servidor y espera hasta que el sistema se inicie automáticamente.

### 2.1.5 Entradas digitales o particiones

Se pueden usar las entradas externas para activar o desactivar las particiones del sistema. Las entradas son optoacopladas para proteger la unidad. Son **normalmente cerradas** por defecto, pero se pueden cambiar a normalmente abiertas desde la ventana de configuración del software.

El pinout depende del modelo adquirido y está completamente detallado en la guía de instalación incluida en la caja de la unidad.

### 2.1.6 Salidas o relés

Las salidas de los relés son contactos secos y, por tanto, no dan ningún voltaje.

Estas salidas son **normalmente cerradas** por defecto, pero este comportamiento se puede cambiar modificando los interruptores o jumpers situados dentro de la unidad. Esta operación **solo** puede efectuarla un operario calificado.

Dependiendo del número de salidas deseado, hay diferentes modelos disponibles.

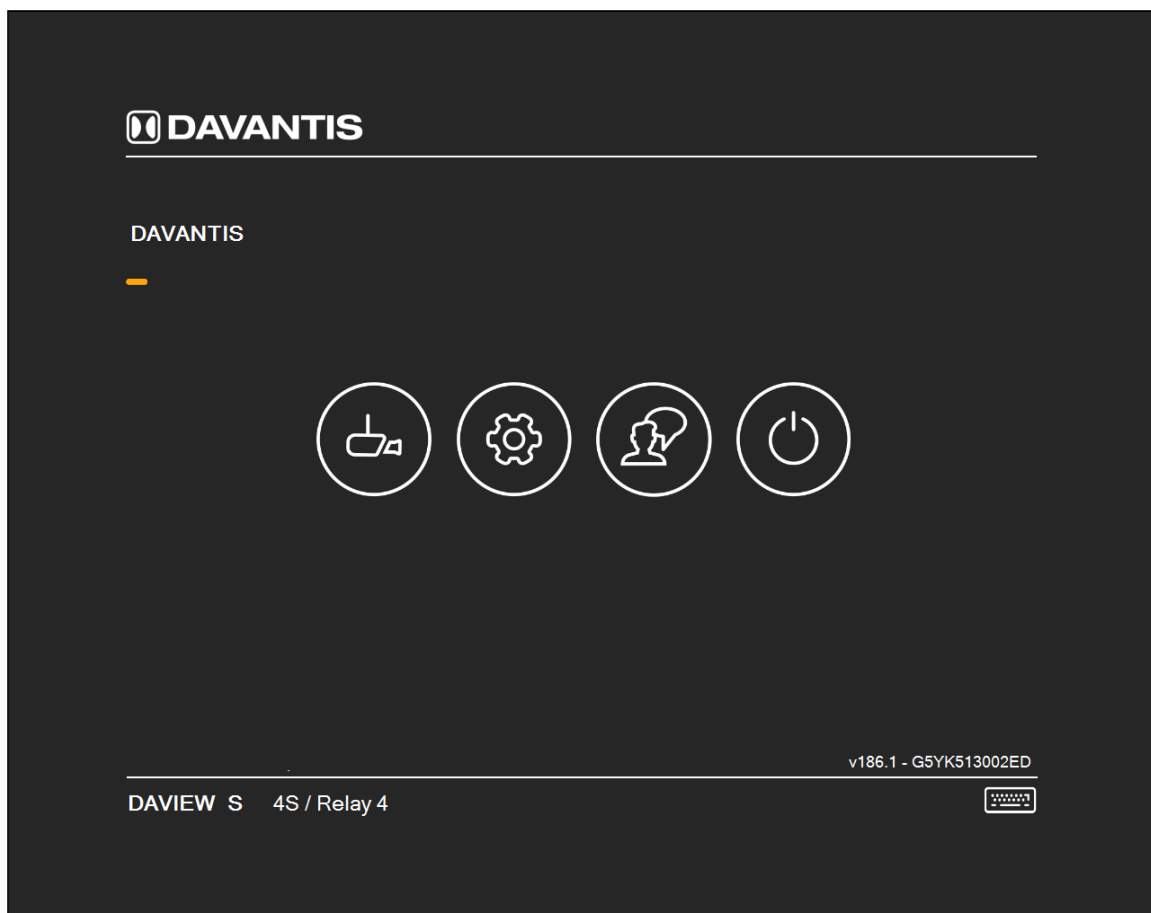
El pinout depende del modelo adquirido y está completamente detallado en la guía de instalación incluida en la caja de la unidad.

## 3 CONFIGURACIÓN BÁSICA

### 3.1 SISTEMA

Una vez se hayan conectado correctamente las cámaras, el monitor y el teclado al sistema, pulsa el botón de encendido del equipo y espera a que se inicie el sistema. Si tu sistema consta de más de un equipo, conecta dichos periféricos al equipo que elijas como equipo máster. Todos los equipos están preparados para ser máster, pero una vez elijas uno, este va a ser el equipo al que se conectarán los periféricos siempre, ya que se accederá a todo el sistema desde este equipo.

Una vez arrancado, se mostrará la pantalla inicial del servidor:

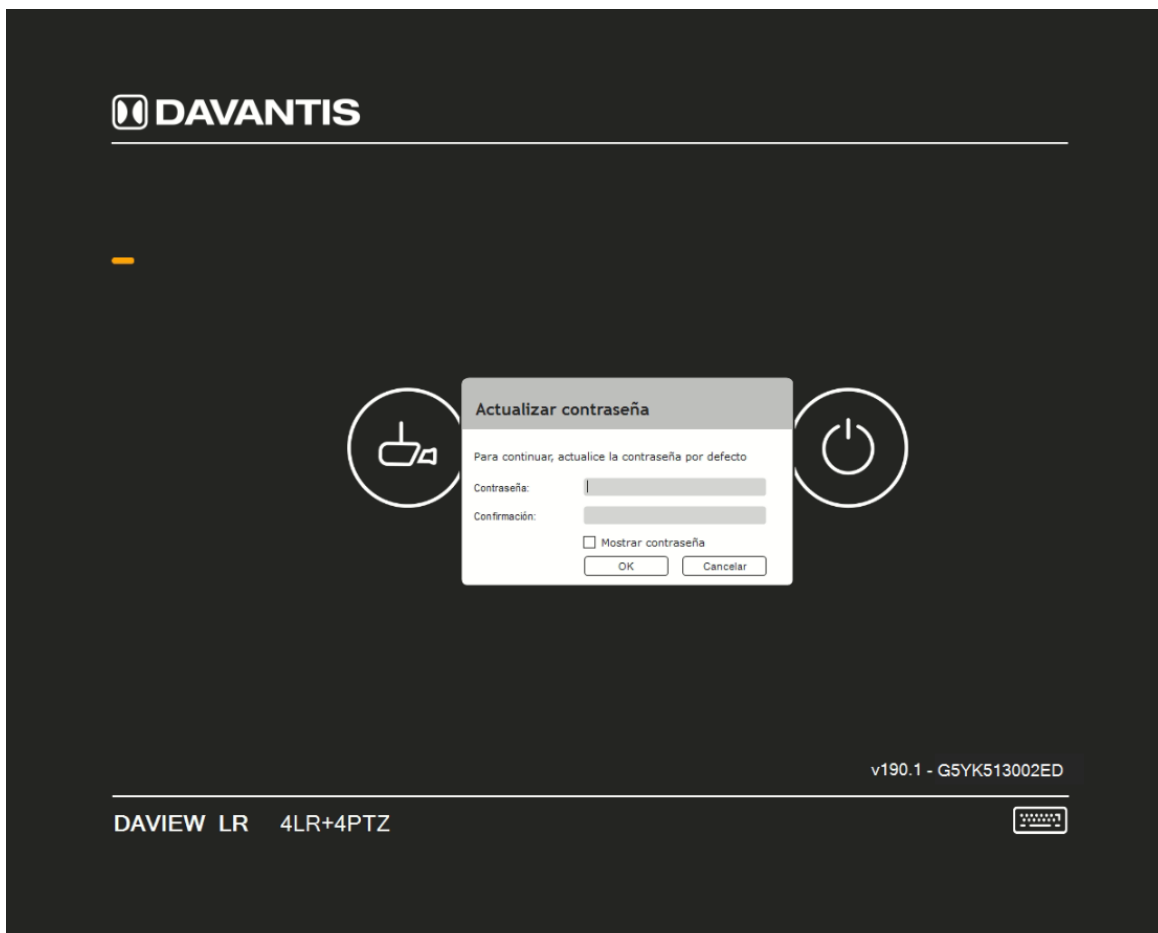


Desde la pantalla principal puedes acceder a 4 opciones:

- Cámaras:** inicia la aplicación de visualización y gestión del sistema.
- Configuración:** muestra los datos de la configuración básica del equipo.
- Asistencia:** en caso de problemas, puedes permitir el acceso a tu equipo al servicio técnico. Para más información, consulta el apartado “Asistencia” más adelante en este manual.
- Apagar:** ofrece reiniciar o apagar. En este último caso, cierra el sistema y apaga el servidor.

### 3.1.1 Configuración de nueva contraseña

Al acceder por primera vez a la plataforma utilizando las credenciales por defecto (*admin / contraseña en blanco*), te aparecerá un cuadro de diálogo para actualizar la contraseña como se muestra a continuación:



Crea una nueva contraseña, y continúa con el proceso de configuración. Podrás cambiar posteriormente las credenciales desde el menú de opciones “Usuarios”

## 3.2 CONFIGURACIÓN

### 3.2.1 Instalación

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Instalación”)



**Configuración**

Nombre de la instalación <b>Davantis</b>	Nombre de la máquina: <b>G5YK513002ED</b>	IP actual <b>198.164.1.109</b>
---	--	-----------------------------------

---

**Instalación**
Vista lógica
CRA
Particiones
Relés
Correo
Entorno
HTTP

**Configuración del master**

Trabajar sin conexión

---

**Configuración de la red**

IP local	198	164	1	109
Máscara	255	255	255	0
Puerta de enlace	198	164	1	1
DNS	198	164	1	1

**Detalles de soporte**

Contraseña

**Configuración del router**

IP / URL Pública	198.164.1.1	🔍
Puerto para cámaras	900	
Puerto para vídeos	21000	Explorador web
Puerto de mantenimiento	5500	
Puertos de audio	5580 & 5581 - 5600	

**Información de la licencia**

Cámaras disponibles	4+0
Final de la licencia	---

29/04/2020 11:22:04

Los parámetros generales de la instalación son los siguientes:

- **Nombre de la instalación:** indica el nombre de la instalación. Este nombre agrupa a los distintos equipos en una misma instalación.
- **Nombre del equipo:** este campo se asigna automáticamente durante la instalación. No es posible modificar su valor desde el sistema.
- **IP actual:** este campo muestra la dirección IP configurada actualmente en el equipo.

Configuración general:


- **Trabajar sin conexión:** para trabajar con un solo equipo no conectado a ninguna red. Si escoges esta opción, no deberás especificar ninguna configuración de red ni de router.
- **Contraseña:** contraseña de conexión remota.

Parámetros de configuración de la red (el administrador de la red local te suministrará esta información):

- **IP local:** especifica la IP del equipo. Para cambiar la IP actualmente asignada, escribe la nueva IP y pulsa “Aceptar” (no es necesario realizar los cambios desde el sistema operativo). Si desconoces la IP que debe tener el sistema, contacta con el administrador de la red local.
- **Máscara:** escribe la máscara de la red local.

- **Puerta de enlace:** escribe la dirección IP de la puerta de enlace de la red local.
- **DNS:** escribe la dirección IP del servidor de DNS de la red.

Parámetros de la configuración del router:

- **IP / URL pública:** escribe la IP pública del router. Si la instalación no se conecta a una central receptora y no dispone de router, escribe la dirección IP local del equipo máster. Si la instalación no dispone de IP estática o dispone de varias instalaciones dentro de la misma red, puedes utilizar una dirección DNS en este campo.
-  **Obtener la IP pública:** pulsa este botón para obtener de forma automática la IP pública del equipo.
- **Puerto para cámaras:** escribe el puerto abierto del router que se utilizará para ver cámaras en directo en la Central Receptora.
- **Puerto para vídeos:** escribe el puerto abierto del router que se utilizará para enviar vídeos a la Central Receptora.
- **Puerto de mantenimiento:** escribe el puerto abierto del router que se utilizará para recibir soporte.
- **Puertos de audio (Simple):** escribe los puertos abiertos del router que se utilizarán para establecer comunicación de audio con Simple. Además del puerto principal, se debe introducir el rango de puertos para la comunicación. No configures el puerto 9036 UDP si vas a usar la comunicación de audio con Speakfreely desde CRA.
- **Explorador Web:** utilízalo para verificar la conexión configurada o bien para acceder al router o a cámaras.

**Importante:** es necesario que los puertos estén abiertos en el router de la instalación por protocolo TCP/UDP y sean redirigidos al equipo. Si desconoces como abrir los puertos, o no tienes autorización para administrar el router de la instalación, ponte en contacto con el administrador de red de la instalación.

Información de licencia.

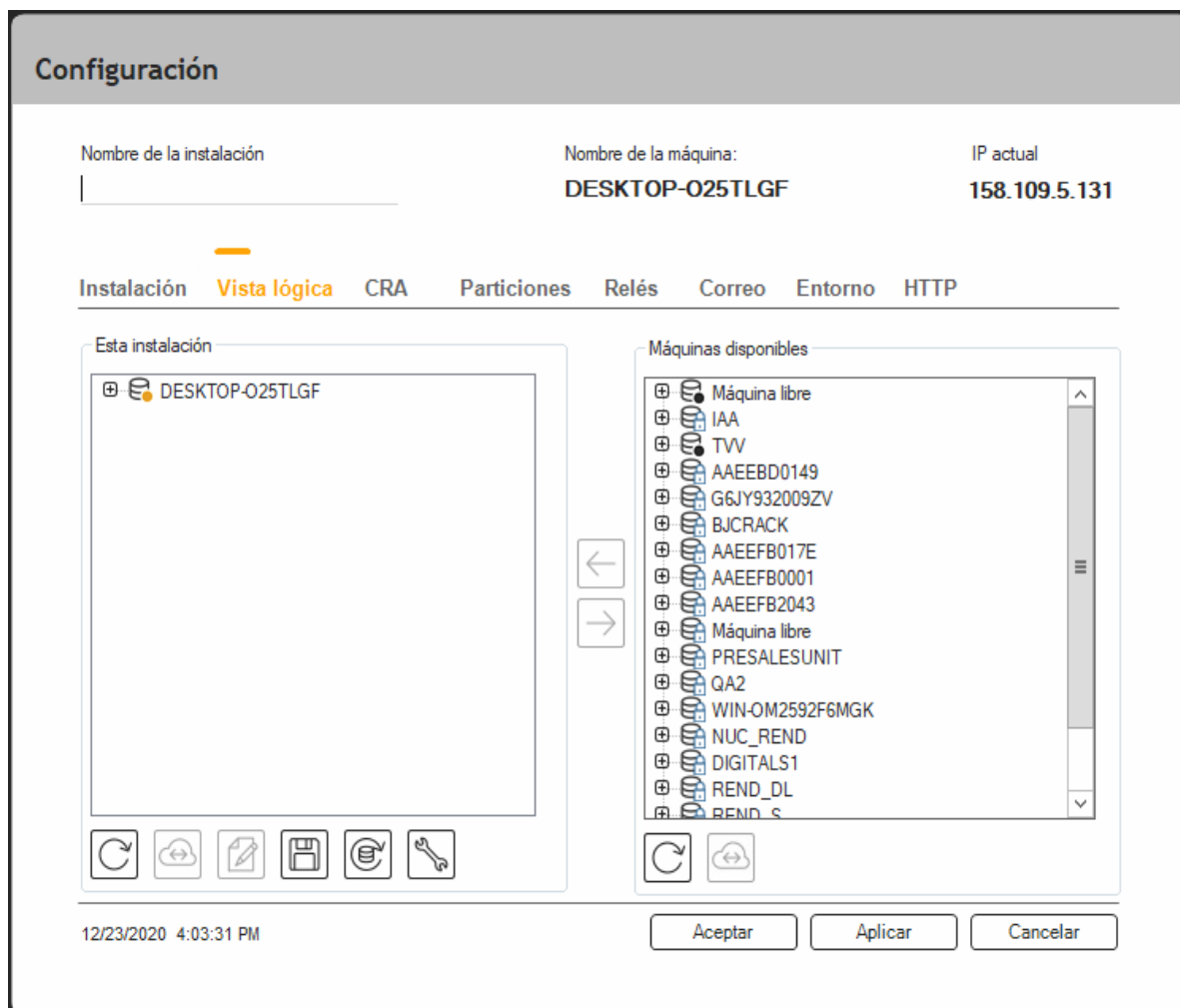
- **Cámaras disponibles:** el número de cámaras que pueden ser instaladas en el sistema.
- **Final de la licencia:** si es un equipo de demo, este campo indica la fecha de finalización de dicha licencia.
- **Actualiza:** obtén la información de licencia actualizada.
- **Modifica licencia:** se abre una ventana para la activación o modificación de la licencia sin conexión.

### 3.2.2 Vista lógica




*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Vista lógica”)*






Si la instalación está formada por un solo servidor, puedes continuar con el siguiente apartado de configuración.

En la pestaña “Vista lógica” podemos añadir o quitar equipos de nuestra instalación. Si la instalación está formada por más de un equipo, debes tener en cuenta los siguientes parámetros. Selecciona los equipos que aparecen en la parte derecha (**Máquinas disponibles**) que deben formar parte de la instalación (**Esta instalación**).








Los siguientes botones están disponibles:

-  **Flecha izquierda:** añadir un equipo de los disponibles en el panel de la derecha como Máquina disponible, obteniendo así capacidad para albergar más cámaras en el sistema. El equipo pasará al panel de la izquierda una vez le indiquemos la IP que deberá tener cuando lo solicite.
-  **Flecha derecha:** liberar un equipo esclavo del panel de la izquierda, pudiéndolo quitar físicamente cuando aparezca en el panel de la derecha como equipo libre.
-  **Doble flecha:** actualizar el panel ahora. El panel se actualiza automáticamente cada pocos segundos.

-  **Nube:** acceder remotamente al equipo seleccionado para modificar la configuración.
-  **Servidor y lápiz:** cambiar la IP del servidor esclavo seleccionado.
-  **Disco:** realizar una copia de seguridad de la configuración.
-  **Cilindro y flecha derecha:** restaurar un backup o reemplazar un servidor averiado de la instalación.
-  **Herramienta:** restaurar el servidor a los valores de fábrica. (Importante: si restauras el servidor a los valores de fábrica, perderás toda la información de cámaras y alarmas, incluidas las fotos y los vídeos de las alarmas generadas. Realiza esta acción bajo tu propia responsabilidad).

Los equipos que aparezcan en nuestra instalación pueden mostrar diferentes iconos de estado:

-  **Servidor master:** aparece este icono en el panel izquierdo indicando que el equipo en cuestión es el máster. Este equipo aparecerá una vez se haya configurado la pestaña de instalación y reiniciado el equipo.
-  **Servidor:** aparece este icono en el panel izquierdo indicando que el equipo en cuestión es un equipo esclavo que está funcionando correctamente. También aparece al lado derecho indicando que el equipo en cuestión puede añadirse a nuestra instalación.
-  **Servidor con símbolo de exclamación:** aparece este icono en el panel izquierdo indicando que el equipo en cuestión está en proceso de encendido o de apagado.
-  **Servidor con marca de prohibido:** aparece este icono en el panel izquierdo indicando que el servidor en cuestión está apagado o se ha retirado incorrectamente del sistema.
-  **Servidor con candado:** aparece este icono en el panel derecho indicando que el equipo en cuestión pertenece a otra instalación y que ya posee cámaras, por lo cual no puede utilizarse para nuestra instalación.

### 3.3 ACCESO

#### 3.3.1 Acceso al sistema

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”)*

El sistema te pedirá un nombre de usuario y una contraseña de acceso para ver y modificar cámaras. El nombre reservado al administrador del sistema es **admin**. La primera vez que se inicia el sistema, la contraseña por defecto se debe dejar en blanco para acceder al sistema.

Se recomienda modificar la contraseña de **admin** y configurar el sistema con varios tipos de usuarios para aumentar el nivel de seguridad de acceso al sistema.



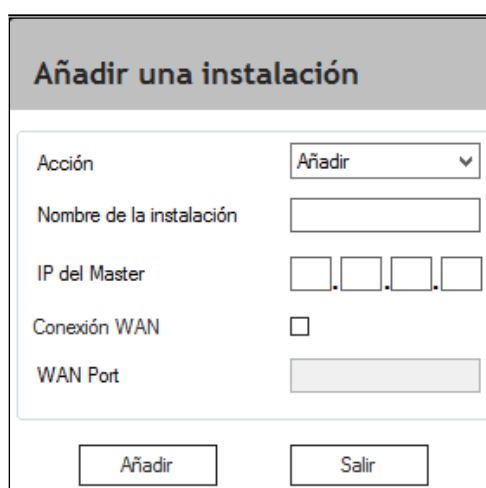
**Acceso**

Nombre de usuario:

Contraseña:

Instalación:

El sistema te permite gestionar otras instalaciones desde el mismo visor de cámaras. Esta opción solo es útil para equipos de vigilancia con el programa *ViewClient* instalado que quieran monitorizar instalaciones remotas. Para ello, en el menú desplegable “Instalación” selecciona la opción “Gestionar instalaciones”:



**Añadir una instalación**

Acción:

Nombre de la instalación:

IP del Master:

Conexión WAN:

WAN Port:

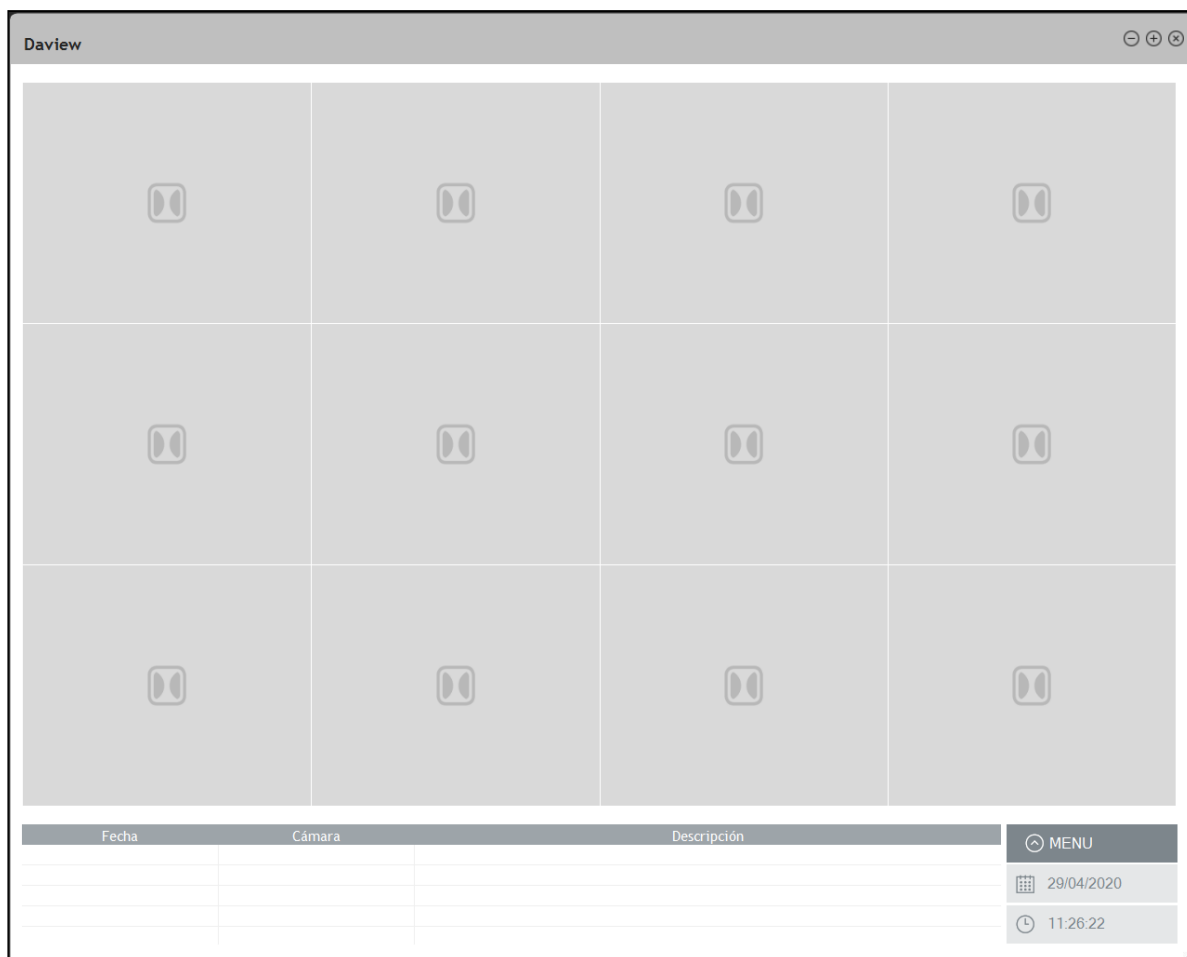
- **Acción:** te permite elegir entre Añadir, Modificar, Borrar y Añadir esta, para añadir automáticamente la instalación local.
- **Nombre de la instalación:** nombre local de la instalación.
- **IP del máster:** escribe la IP local del equipo máster de la instalación a la que te quieras conectar.
- **Conexión WAN:** marca la casilla si el servidor no se encuentra en tu red local.
- **WAN Port:** es el puerto necesario para la comunicación entre tu equipo y el servidor máster. Es necesario tener conocimientos avanzados de administración de redes y redirección SQL para usar este parámetro. Ponte en contacto con el administrador de red o con el proveedor del equipo para obtener este campo.

Al pulsar “Añadir”, podrás elegir el nuevo sitio creado desde el menú desplegable “Instalación”.

### 3.3.2 Visor

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña)

Después de unos segundos, el sistema habrá arrancado y en la pantalla aparecerá la interfaz gráfica, que tiene el aspecto siguiente:



La pantalla se divide en varios cuadrantes de visualización. La cantidad de estos cuadrantes se puede definir desde **Menú -> Visualización -> Distribución**.

Para asignar una cámara a un cuadrante, haz clic en el botón derecho del ratón sobre el cuadrante donde deseas ver la cámara y selecciona en el menú desplegable la cámara (o grupo de cámaras) que deseas visualizar.

Repite el proceso hasta que hayas asignado a cada cuadrante las imágenes de las cámaras deseadas.

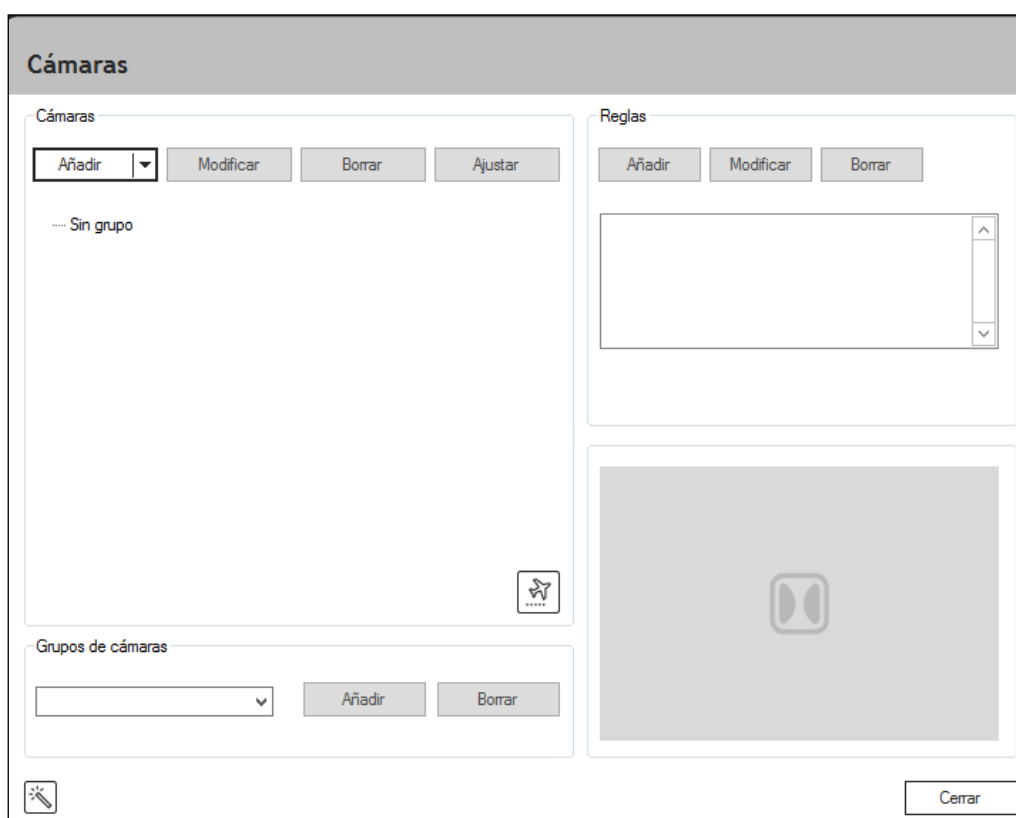
### 3.4 CÁMARAS

Lo primero que debemos hacer para configurar el sistema es definir las cámaras que se encuentran físicamente conectadas al sistema. Esta operación solo será necesaria cuando se instale el sistema por primera vez.

#### 3.4.1 Gestión de cámaras

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”)

Se abrirá la pantalla de gestión de cámaras con el siguiente aspecto:



En el área de cámaras, aparecerán las cámaras que estén definidas en el sistema (ninguna, durante la primera instalación). Recuerda que hasta que una cámara no esté definida, el sistema no podrá recibir las imágenes de la misma.

## 3.4.2 Cámara

### 3.4.2.1 Tipología de instalación

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Añadir”)

La primera vez que accedas al menú de cámaras se te pedirá que escojas el tipo de instalación que estás configurando entre “infraestructuras críticas”, “parque solar”, “industrial” y “residencial” mediante el siguiente formulario:

#### Seleccione el tipo de instalación

-  **Infraestructuras Críticas**  
Entorno de alta seguridad. Normalmente un sector crítico con un perímetro cerrado por las cámaras de seguridad. Caracterizado por zonas estériles de muy baja actividad. Habitualmente zonas sin oclusiones
-  **Industrial**  
Normalmente el perímetro de una empresa. Caracterizado por distancias medias y posiblemente de alta actividad, ya sea en el exterior del perímetro o en algunas zonas interiores. Posibles oclusiones por la presencia de material en el interior del perímetro. Posible presencia de luces exteriores.
-  **Parque solar**  
Normalmente el perímetro de una huerta solar o instalaciones con cámaras de largo alcance. Caracterizado por distancias largas y zonas estériles o de baja actividad. Habitualmente grandes áreas de detección con pocas oclusiones.
-  **Residencial**  
Normalmente el perímetro de una finca particular. Caracterizado por cámaras cercanas, con ópticas muy abiertas. Habitualmente con presencia de vegetación, piscina o animales domésticos.

Dependiendo del entorno que se ajuste más a tu instalación deberás escoger una u otra opción, que predefinirá las cámaras para que la detección se ajuste más al tipo de escena. Esta opción puede cambiarse luego desde el menú de cámara, aunque rara vez se debería utilizar, ya que es difícil que cambie el tipo de escena. Una vez escogido el tipo de instalación, en el menú de cámaras, aparecerá un dibujo recordatorio indicándolo, y con el botón abajo a la derecha es posible cambiarlo si así se desea.



### 3.4.2.2 Crear cámaras

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Añadir”)

Aparecerá la siguiente ventana:

Información de la cámara	
Nombre	cam1
ID máquina	G5YK513002ED
Entrada de vídeo	Análogo
Tipo	DFusion <input type="checkbox"/> Térmica
Análogo Canal	1 <input type="radio"/> PAL <input type="radio"/> NTSC
Cámara ONVIF virtual	
Transmisión (Puerto/URL)	<input type="checkbox"/> Activo 555 daview.sdp
Grupo	Sin grupo
Descripción	
Última modificación	
<input checked="" type="checkbox"/> Activa	<input type="button" value="Aceptar"/> <input type="button" value="Cancelar"/>

Los campos principales que debes rellenar para definir una cámara son los siguientes:

- **Nombre:** nombre de la cámara a definir libremente por el usuario.
- **ID máquina:** identificador del servidor que procesará esta cámara. Menú activo en instalaciones con más de un servidor.
- Las otras opciones del menú son **IP** (cámara IP con una dirección IP), **Análogo** (cámara analógica conectada al sistema mediante un conector BNC) o **Archivo de vídeo** (archivo de vídeo para análisis forenses).
- **Tipo:** (1) Estándar (cámara con reglas de videoanálisis), (2) Long Range (cámaras con características *long range* y reglas de videoanálisis), (3) videoverificación (cámara sin reglas de videoanálisis; las alarmas se generan por una entrada externa), (4) SmartPTZ (cámara de soporte PTZ o cámara de soporte fija), (5) DFUSIONPRO (cámaras Long Range con tecnología DeepFusion), (6) DFUSION (cámara estándar con tecnología DeepFusion), (7) ATKPRO (cámara PTZ con tecnología autotracking y DeepFusion). Si se elige “SmartPTZ (Cámara de soporte)”, no se pueden crear reglas de videoanálisis asociadas a esta cámara. En cambio, se pueden definir “presets” para esta cámara, que se utilizarán para grabar un vídeo adicional cuando una cámara con videoanálisis detecte un evento.

Algunas características adicionales pueden estar disponibles dependiendo de la solución adquirida:

- **Térmica:** habilita esta opción si conectas una cámara térmica. Si se habilita se aplicarán algoritmos específicos para este tipo de cámaras. Si activas esta opción, puedes elegir en “Funciones térmicas avanzadas” entre diferentes fabricantes de cámaras.
- **Funciones térmicas avanzadas:** podrás elegir entre diferentes fabricantes de cámaras para aplicar algoritmos específicos con un rendimiento superior.
- **Modo pasillo:** con la opción “Long range” activada, puedes elegir desde “Modo pasillo” entre diferentes opciones de rotación. Esta función aumenta la capacidad de detección en largas distancias y, al mismo tiempo, reduce la zona ciega debajo de la cámara.
- **Cámara ONVIF Virtual:**
  - Transmisión: activa esta opción para habilitar la transmisión de imágenes de vídeo a terceros usando el protocolo RTSP/H.264.
  - Puerto: el puerto TCP emisor para la transmisión de imágenes vía RTSP.
  - URL: la dirección URL para la retransmisión de imágenes vía RTSP.  
En este caso, la URL completa para acceder al flujo de vídeo sería la siguiente:  
rtsp://IP\_Servidor\_Daview:554/daview.sdp

Otros campos de cámara:

- **Grupo:** grupo al que asignarás la cámara (consulta el apartado “Definición de grupos de cámaras”)
- **Descripción:** descripción de la cámara, a definir libremente por el usuario.
- **Última modificación:** no es posible introducir el valor en este campo; el sistema lo actualiza automáticamente cuando se realiza una modificación en la configuración de la cámara una vez definida.
- **Activa:** (on/off) determina si la cámara se encuentra activada o desactivada. Se recomienda desactivar las cámaras que no estén siendo utilizadas.

Si estás configurando una cámara analógica, las siguientes opciones estarán disponibles:

- **Canal:** en el caso de cámaras analógicas conectadas a la capturadora de vídeo, debes seleccionar el canal de la capturadora al que ha sido conectado la cámara.

En caso de seleccionar **Fichero** como entrada de vídeo, deberás completar los siguientes campos:

- **Fichero:** selecciona el archivo de vídeo desde una carpeta del disco duro del equipo. Aparecerá un cuadro de diálogo que te permitirá hacer dicha selección.
- **Fotogramas por segundo:** el número de imágenes por segundo que el sistema procesará para la detección de incidentes. Se recomienda un mínimo de seis imágenes por segundo para la detección de incidentes inteligente y detección de movimiento.

Después de configurar la cámara, haz clic en **Aceptar** y la ventana de la cámara se cerrará. En la sección de cámaras, aparecerá la cámara que acabas de definir.

### 3.4.2.3 Crear una cámara IP

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Añadir”)

**Información de la cámara**

Nombre  1

ID máquina

Entrada de vídeo

Tipo   Térmica

IP

Usuario/Contraseña   →

Modelo

Dirección IP  🔍

Protocolo de transmisión  RTSP  HTTP

Puertos RTSP/HTTP   →

URL

Canal

Cámara ONVIF virtual

Transmisión (Puerto/URL)  Activo

Grupo

Descripción

Última modificación

Activa

Si has elegido como Entrada de vídeo: **IP**, las siguientes opciones están disponibles:

- **Usuario/Contraseña:** introduce el usuario y la contraseña de la cámara IP. Se pueden comprobar los detalles de usuario pulsando el botón que aparece a su derecha.
- **Modelo:** selecciona el fabricante de la cámara entre los disponibles del desplegable.
- **Dirección IP:** en caso de usar cámaras IP, se debe definir la dirección IP asignada a la cámara. Consulta el manual de instrucciones de la cámara para determinar cuál es la dirección IP de la misma.
- **Protocolo de transmisión:** debes elegir entre el protocolo RTSP y el protocolo HTTP.
- **Puertos RTSP / HTTP:** son los puertos de comunicaciones asignados a la cámara para la transmisión de imágenes. Los puertos comúnmente utilizados son el 554 (RTSP) y el 80 (HTTP). Se puede hacer un test de la IP y el puerto pulsando el botón que aparece a su derecha.
- **URL:** para las cámaras que transmiten por RTSP, la URL identifica la dirección del flujo de vídeo que deseamos obtener. Este campo se rellenará automáticamente al seleccionar el modelo de cámara IP. Si tu modelo de cámara no aparece en la lista o quieres especificar otra URL, selecciona “Genérico” en la lista de modelos de cámaras, para pasar a editar el campo URL.

- **Canal:** se puede utilizar para especificar el canal o el flujo de vídeo en la dirección URL como un parámetro. Si la URL contiene '#' en la cadena, esto será sustituido por el número de canal.

La mayoría de cámaras IP aceptan varios flujos de vídeo. Si la instalación tiene un DVR, se debe utilizar el flujo principal en alta resolución para el grabador y un flujo secundario para el videoanálisis.

Para optimizar el ancho de banda de la red y la calidad de imagen, entra en los parámetros de configuración de la cámara y modifica el flujo de vídeo secundario según las especificaciones recomendadas a continuación:

- Protocolo: H264
- Resolución: 4CIF (704x576) o VGA (640x480)
- Imágenes por segundo: 15 fps
- *Bitrate:* ~768 kbps – 1024 kbps

#### 3.4.2.4 Crear una cámara ONVIF

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Añadir”)*

En caso de trabajar con cámaras ONVIF, el proceso se simplifica, ya que el propio sistema será capaz de listar las cámaras y extraer la información necesaria.

Para añadir una cámara ONVIF al sistema, se solicita la siguiente información:

- **Usuario / Contraseña:** introduce el usuario y la contraseña de la cámara IP.
- **Modelo:** selecciona ONVIF.
- **Dirección IP:** elige la dirección IP de la lista.
- **URL:** elige la dirección URL de la lista.

Recuerda que para que una cámara ONVIF pueda ser encontrada, esta debe estar configurada en la misma red que el equipo.

Algunas cámaras requieren autenticación para poder acceder a las URL. Si una vez seleccionada la IP, el campo URL no aparece activo, será necesario introducir usuario y contraseña para obtener las URL. Aparecerá un mensaje de error avisando de que la cámara requiere autenticación.

### 3.4.2.5 Eliminar una cámara

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Borrar”)*

Para eliminar una cámara del sistema, haz clic en la cámara que quieras suprimir, para repetir a continuación la misma acción sobre el botón **Borrar**.

**Atención:** Cuando elimines una cámara del sistema, estás eliminando además toda la información disponible sobre esta cámara, así como **todas las alarmas y secuencias de vídeo** que han sido grabadas con esa cámara.

### 3.4.2.6 Modificar una cámara

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Modificar”)*

Para modificar una cámara del sistema, haz clic en la cámara que quieras editar, para repetir a continuación la misma acción sobre el botón **Modificar**.

De esta forma, la pantalla con la información de la cámara volverá a abrirse, permitiéndote modificar los datos definidos anteriormente sobre la cámara seleccionada.

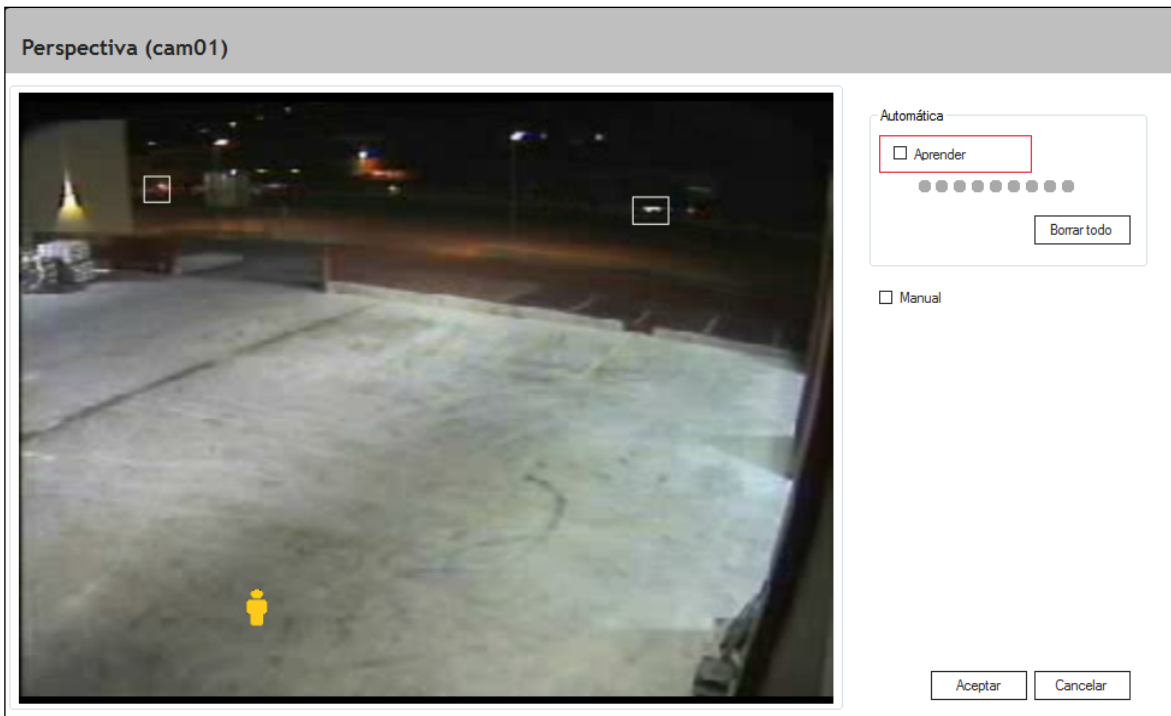
Después de haber definido todas las cámaras conectadas al sistema repitiendo la operación descrita arriba, cierra la ventana de cámaras para volver a la pantalla principal.

## 3.4.3 Herramienta de calibración de zoom

### 3.4.3.1 Tamaño mínimo

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar”, marca “Perspectiva”, botón “Siguiente”)*

Para calibrar la necesidad de zoom en cada cámara, el sistema te mostrará el dibujo de una persona que te servirá como indicador del tamaño mínimo que debe tener una persona en esa zona de la cámara.



Sigue los siguientes pasos para calibrar el zoom de la cámara:

- Desactiva **Aprender** tal y como se marca en el gráfico.
- Sitúa la persona en la parte más alejada donde quieras detectar intrusos.
- Con el ratón, acerca la persona dibujada en amarillo a la persona real.
- Si la persona real es igual o más grande que el dibujo en ese lugar, el zoom es correcto.
- Si la persona real es más pequeña que el dibujo en ese lugar, aumenta el zoom hasta conseguir el objetivo descrito en el punto anterior.

Cuando no sea posible aumentar el zoom de la cámara, es posible aumentar los parámetros de sensibilidad de la solución para que el sistema detecte objetos más pequeños que el dibujo de la persona.

**Atención:** El aumento de la sensibilidad también puede aumentar el número de falsas alarmas.

#### 3.4.4 Perspectiva de la cámara

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón "Cámaras", introduce usuario/contraseña, "MENÚ", "CÁMARAS", selecciona una cámara, botón "Ajustar", marca "Perspectiva", botón "Siguiente")*

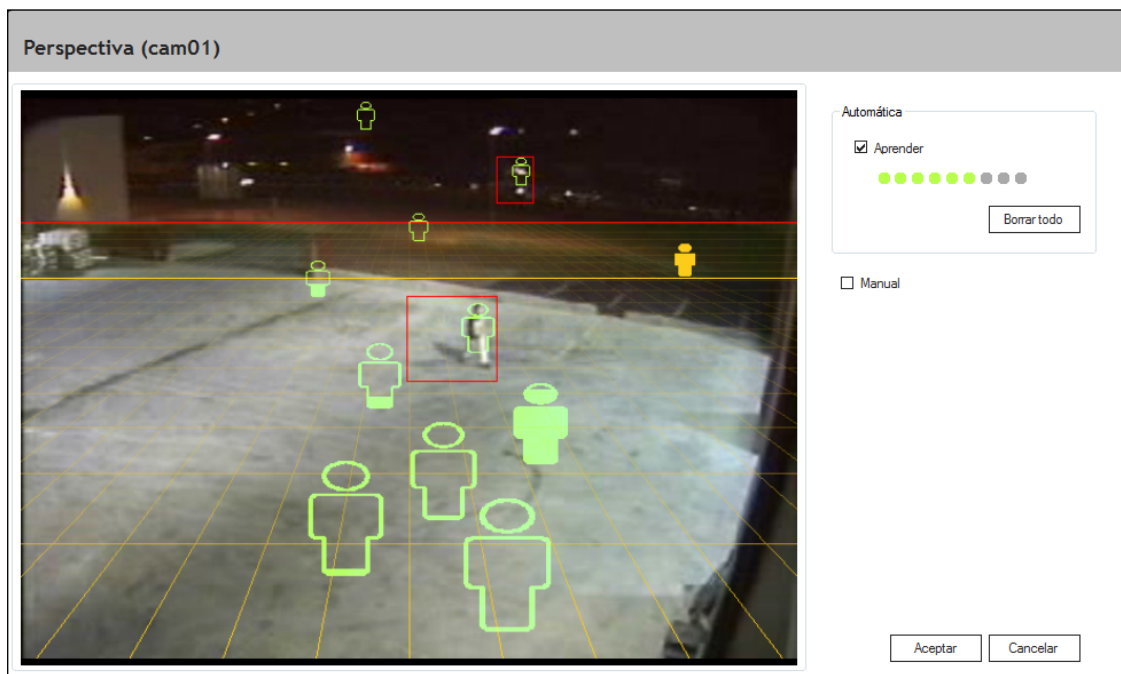
El objetivo de esta pantalla es que el sistema aprenda la profundidad de la escena y pueda saber el tamaño de una persona en cada punto de la imagen. Hay dos modos de funcionamiento: el automático y el manual. El modo automático es el que aparece seleccionado por defecto al entrar en esta pantalla. Cuando el sistema está en este modo, la casilla **Aprender** aparece seleccionada.

### 3.4.4.1 Modo Perspectiva automática

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar”, marca “Perspectiva”, botón “Siguiente”)

En este modo, el sistema aprenderá automáticamente la perspectiva de la escena. Una persona deberá pasearse por toda la imagen. Es recomendable que la persona pasee primero por las zonas más próximas a la cámara y, una vez el sistema lo haya detectado, se vaya alejando de la cámara haciendo eses. Es muy importante que la persona llegue encuadrada hasta la posición más lejana donde queremos que el sistema detecte. También es importante evitar las oclusiones durante el proceso de aprendizaje de tal modo que el sistema siempre vea el cuerpo entero de la persona.

Durante el proceso de aprendizaje, el sistema irá mostrando la perspectiva estimada mediante el dibujo de unas personas que indican el tamaño estimado de estas en distintos puntos de la imagen.



Los dibujos de las personas se irán rellenando a medida que se vaya llenando la barra de progreso del aprendizaje. Una muestra no rellenada indicará un número insuficiente de muestras en un nivel; una muestra rellenada a medias indicará que es recomendable adquirir más muestras en aquel nivel, y una muestra completamente rellenada indicará que ya se han adquirido suficientes muestras. El modelo también nos mostrará dos líneas de horizonte. La de color rojo indicará el límite teórico de detección del equipo. Es importante que esta línea esté por encima de la región que se quiere vigilar, ya que más allá de esta línea el sistema no detectará. La de color amarillo indicará el límite óptimo de detección del equipo. Si estos horizontes se muestran demasiado bajos, se deberán tomar más muestras por encima de estas líneas de horizonte y, en caso de que la situación persista, aumentar el zoom de la cámara.

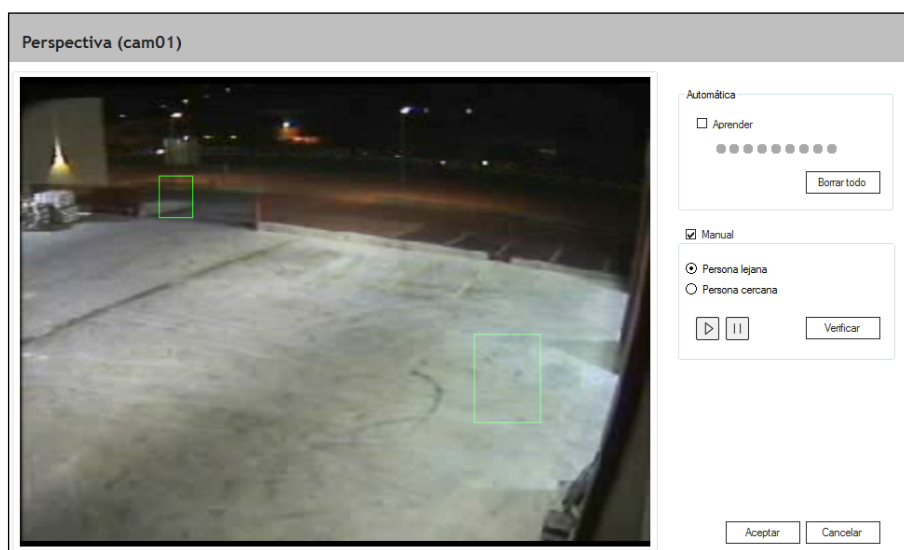
En caso de querer pausar la adquisición de muestras durante el proceso de aprendizaje, se debe desactivar la casilla **Aprender**. Pausar la adquisición de muestras puede ser necesario si entran objetos no deseados en la escena (animales, vehículos, etc.), que

pueden distorsionar el modelo aprendido. Para retomar la adquisición de muestras, marca de nuevo la casilla **Aprender**. Si quieres borrar todas las muestras adquiridas y empezar de cero todo el proceso, pulsa el botón **Borrar todo**. El sistema saldrá automáticamente de la pantalla de perspectiva y deberás volver a entrar para aceptar un nuevo modelo.

### 3.4.4.2 Modo Perspectiva manual

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar”, marca “Perspectiva”, botón “Siguiente”)*

Puede suceder que el sistema no sea capaz de aprender un modelo apropiado de perspectiva. En este caso se puede recurrir al modo manual. Para activar el modo manual, desactiva la casilla **Aprender** y activa la casilla **Manual**. Después, selecciona la casilla **Persona lejana** y con el ratón dibuja un rectángulo que recuadre completamente a una persona en la posición más lejana donde se quiera detectar. Repite el mismo procedimiento seleccionando la casilla **Persona cercana** y dibuja el rectángulo en la posición más cercana posible. El rectángulo se debe dibujar de tal modo que el límite superior toque a la parte superior de la cabeza de una persona, y que el límite inferior toque a los pies de la persona. Lo mismo debe suceder para los límites laterales. Una vez dibujados los dos rectángulos, pulsa el botón **Verificar** para comprobar con el ratón que el modelo se ajusta en todas las partes de la imagen al tamaño de una persona.



En caso de querer pausar la imagen durante el proceso de aprendizaje manual, puedes utilizar el botón de **Pausa**. Para volver a la imagen en movimiento, utiliza el botón **Reproducir**.

Si quieres borrar las muestras dibujadas y empezar de cero todo el proceso, pulsa el botón **Borrar todo**. El sistema saldrá automáticamente de la pantalla de perspectiva y deberás volver a entrar para aceptar un nuevo modelo.



### 3.4.5 Creación de reglas

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas)

Una regla es una situación que en caso de producirse generaría una alarma en el sistema. Una regla lleva siempre asociada una respuesta del sistema. Un ejemplo de regla y alarma asociada sería el siguiente:

En caso de detectar:

<movimiento> en la cámara <1>

Generar la siguiente respuesta:

alarma <sonora> y <maximizar cámara>

La primera pantalla de definición de reglas tiene el aspecto siguiente:

The screenshot shows a web form titled "Regla: Datos Generales (paso 1)". It contains the following elements:

- Nombre:** A text input field.
- Activo:** A checked checkbox.
- Creado el:** A date/time field showing "29/04/2020 11:53:18".
- Sin Partición:** An unchecked checkbox.
- Última modificación:** A date/time field.
- Partición:** A dropdown menu currently showing "1".
- Descripción:** A large text area for entering a description.
- Buttons:** "Cancelar" and "Siguiente" buttons at the bottom right.

Los campos a rellenar son los siguientes:

- **Nombre:** nombre de la regla. Es aconsejable poner un nombre significativo para evitar confusiones con otras reglas del sistema.
- **Creado el:** se muestra automáticamente la fecha de creación.
- **Última modificación:** se muestra automáticamente la última fecha de modificación de la regla.
- **Descripción:** permite introducir una descripción de la regla para ser identificada.
- **Activo:** opción que permite activar/desactivar la regla. Para que la regla sea tenida en cuenta por el sistema, debe estar activada.
- **Sin partición:** permite configurar la regla para que esté activa sin depender de una entrada externa.
- **Partición:** permite relacionar cada regla con una entrada externa.

### 3.4.6 Tipos de detección

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”)

Una vez completado el paso 1, haz clic en **Siguiente**. La pantalla de configuración te mostrará el paso 2:

**Regla: Tipo de detección (paso 2)**

Detectar:

Súper-regla

Intruso + que está en la imagen

Merodeando más de: 0 segundos Crear/Modificar zona

Horario:

Siempre

Personalizada

Cancelar Atrás Siguiente

Para crear una regla, se debe definir el tipo de detección y en qué lugar de la imagen de la cámara se encuentra.

Puedes elegir el tipo de detección a efectuar. El sistema te permite elegir entre las siguientes opciones:

- **Movimiento:** cualquier movimiento de píxel generará un evento.
- **Persona:** únicamente se creará un evento si una persona es detectada (los vehículos no serán detectados).
- **Vehículo:** únicamente se creará un evento si un vehículo es detectado (las personas no serán detectadas).
- **Todo:** crear una regla para detectar cualquier tipo de movimiento con cierta relevancia. Podrían ser personas, vehículos, animales o cualquier otra cosa.
- **Intruso:** generación de eventos provocados por personas o vehículos.
- **Objeto:** crear una regla para detectar objetos abandonados o robados.
- **Aglomeración:** crear una regla para detectar aglomeración con un cierto umbral.
- **Entrada externa:** crear una regla para detectar la activación de:
  - entradas externas del sistema
  - entradas de una cámara o dispositivo externo

A continuación, puedes escoger la acción entre las siguientes opciones:

- **Está en:** se refiere al área de la imagen de la cámara
- **Entra en:** se refiere a moverse de un área de la imagen a otra área de la imagen en una dirección, la opuesta (**Sale de**) o en ambas (**Entrar / Salir**)
- **Desaparecer de:** se refiere a un intruso que se ve por última vez en un área específica de la imagen.
- **Abandonado en:** se refiere a un objeto abandonado en un área específica de la imagen.
- **Robado de:** se refiere a un objeto robado de un área específica de la imagen.

Y, finalmente, puedes definir la localización entre estas opciones:

- **La imagen:** toda la imagen.
- **Región de interés:** puedes modificar la región de interés pulsando la ventana **Crear / Modificar zona**. Aparecerá una nueva ventana con la imagen de la cámara seleccionada donde se puede definir la zona de exclusión de la imagen.

La detección de un evento puede pedir que la detección dure un mínimo de segundos como requisito para generar la alarma. Para habilitar esta opción debes marcar la casilla **Merodeando más de** y poner en el cuadro el número de **segundos** deseado.

La combinación de reglas permite dos tipos de acciones. Desde el mismo paso 2 de la ventana **Creación de reglas**:

- **Aparece en:** se refiere a un intruso que se ve por primera vez en un área específica de la imagen. Esta es una condición previa que se puede combinar con todas las otras reglas expuestas en el punto anterior. El aspecto más significativo de esta combinación es que el sujeto detectado en la condición previa debe ser el mismo que provoque cualquiera de las combinaciones posteriores posibles.

Regla: Tipo de detección (paso 2)

Detectar:

Súper-regla

Intruso que aparece en la imagen y está en la imagen

Merodeando más de: 0 segundos

Horario:

Siempre

Personalizada

Cancelar Atrás Siguiente

- **Súper-regla:** se refiere a que una regla ya creada sea la condición previa para activar esta nueva regla durante el tiempo que se establezca. El aspecto más significativo de esta combinación es que el sujeto detectado en la condición previa es independiente del que provoque cualquiera de las combinaciones posteriores posibles.

**Regla: Tipo de detección (paso 2)**

Detectar:

Súper-regla  y durante los próximos  segundos

+ que

Merodeando más de:  segundos

Horario:

Siempre

Personalizada

Filtros adicionales pueden estar disponibles:

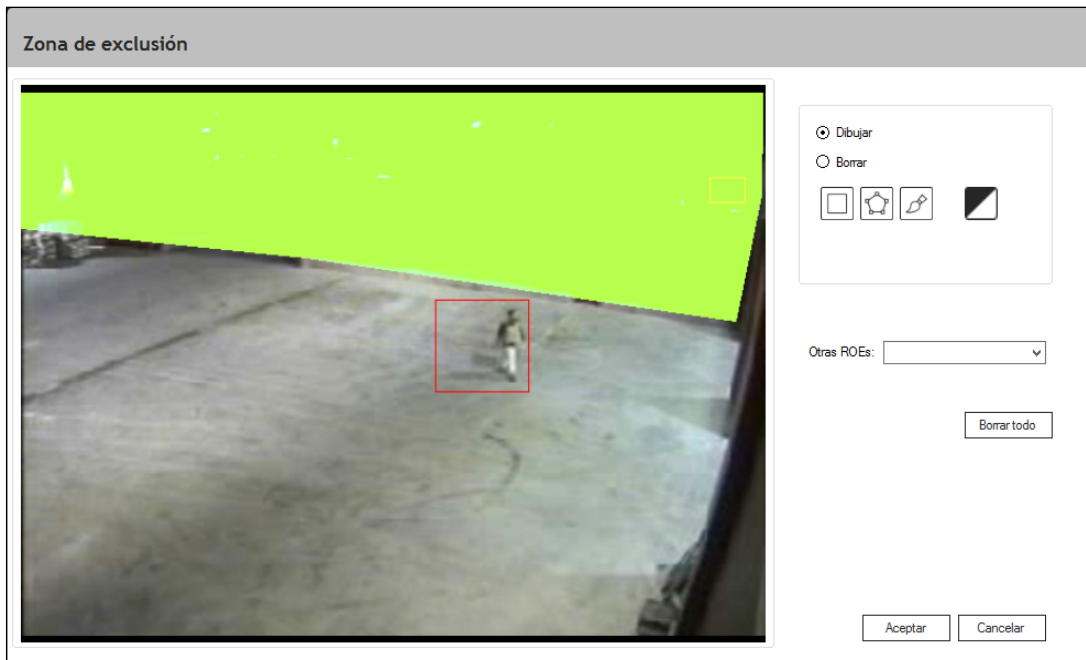
- **Más rápido que:** activará una alarma si el intruso se mueve más rápido que una velocidad específica. Las unidades de velocidad son múltiplos de la velocidad de persona estándar. En escenarios llenos de gente, el intruso debe verse claramente durante un cierto período de tiempo. De lo contrario, la regla de velocidad no activará una alarma.
- **Más grande que:** activará una alarma si el intruso es más grande que un tamaño mínimo específico. Las unidades de tamaño son múltiplos del tamaño de persona estándar. En escenarios llenos de gente, el intruso debe verse claramente durante un cierto período de tiempo. De lo contrario, el filtro de tamaño no activará una alarma.

### 3.4.7 Zona de exclusión de regla

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, botón “Crear/Modificar zona”)*

La zona de exclusión es muy útil para no generar alarmas en zonas de la cámara donde hay actividad pero no queremos que se genere un evento.

También puede utilizarse para reducir el número de falsos positivos en algún área en particular de la imagen. El área sombreada será definida como área de exclusión, es decir, el movimiento que tenga lugar en esta área no generará ninguna alarma.



Las herramientas para pintar zonas de exclusión son las siguientes:

- **Herramienta rectángulo:** nos permite definir áreas rectangulares en la pantalla. Se define la zona de exclusión haciendo clic con el ratón sobre la imagen de la cámara y arrastrando el ratón, soltando el botón del ratón terminaremos de definir el área sombreada.
- **Herramienta polígono:** nos permite definir áreas sombreadas de forma poligonal. En este caso, debemos hacer clic con el ratón en los vértices del polígono hasta que volvamos a hacer clic en el primer vértice del polígono cerrándolo. El polígono se cierra y se rellena automáticamente definiendo un área sombreada.
- **Herramienta pincel:** permite definir áreas sombreadas como si estuviésemos arrastrando un pincel por la pantalla mientras mantenemos apretado el botón izquierdo del ratón. Al seleccionar la herramienta pincel, aparece en la pantalla una ventana que permite modificar el grosor del pincel que estamos utilizando.

Otras opciones están disponibles en la misma ventana:

- Los **colores** permiten definir diferentes tonos para la región de exclusión, solamente se usan para una mejor visualización de la misma, no afecta al comportamiento.
- El **control de acción** te permite definir si vas a usar las herramientas para dibujar la región de exclusión o para borrar una parte de ella. También puedes usar el botón **Borrar todo** para borrar toda la región que haya dibujada, o utilizar la opción "Otras ROEs" para escoger entre las ROEs que el equipo tenga definidas para otras cámaras y reglas.

### 3.4.8 Respuestas de regla

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, botón “Siguiente”)

En esta pantalla se selecciona la respuesta del sistema cuando se produce la alarma.

#### Regla: Respuesta (paso 3)

<b>Alarma</b> <input type="checkbox"/> Notificación a la CRA <input checked="" type="checkbox"/> Generar alarma <input checked="" type="checkbox"/> Guardar vídeo <input checked="" type="checkbox"/> Remarcar objetos en los videos <input checked="" type="checkbox"/> Remarcar objetos en directo <input type="checkbox"/> Hot spot Gravedad <input type="text" value="1"/> Retardo de desactivación (seg) <input type="text" value="0"/>	<b>Accionar relé</b> <input type="checkbox"/> Habilitar Dispositivo <input type="text"/> Relés <input type="text"/> Aplicar retardo de desactivación <input type="radio"/> Sí <input checked="" type="radio"/> No Tiempo máximo de activación <input type="text" value="30"/>
<b>Reproducir sonido</b> <input type="checkbox"/> Habilitar <input type="checkbox"/> Repetir sonido hasta aceptar alarma <input type="radio"/> Altavoz PC <input type="radio"/> Archivo <input type="text"/>	<b>Enviar correo electrónico</b> <input type="checkbox"/> Habilitar Destinatario <input type="text"/> Asunto <input type="text"/> Mensaje <input type="text"/>
<b>SmartPTZ</b> <input type="checkbox"/> Habilitar Cámara <input type="text"/> Preset <input type="text" value="No preset"/> Volver a preset <input type="text" value="No preset"/> <input type="checkbox"/> Habilitar Auto-Tracking	<b>HTTP</b> <input type="checkbox"/> Habilitar URL <input type="text"/> <input type="button" value="Test"/> <input type="checkbox"/> Usar autenticación <input checked="" type="radio"/> Basic <input type="radio"/> Digest Usuario <input type="text"/> Contraseña <input type="text"/>

Opciones relacionadas con alarmas:

- **Notificación a la CRA:** cuando se desea enviar las alarmas generadas a una Central Receptora de Alarmas (CRA).
- **Generar alarma:** activa el registro de detecciones. Normalmente activado.
- **Guardar vídeo:** guarda el vídeo resultante de cada alarma.
- **Remarcar objetos en los vídeos:** el sistema recuadra los elementos que han activado la alarma, para facilitar la identificación en pantalla. Opción válida para los vídeos grabados.
- **Remarcar objetos en directo:** el sistema recuadra los objetos que han activado la alarma para facilitar la identificación en pantalla. Opción válida para las imágenes en directo.
- **Hot Spot:** esta respuesta cambia los visores del sistema al modo **Hot Spot** cuando se genera la alarma. La cámara donde se genera la alarma ocupará toda la pantalla, y el resto de visores desaparecerán momentáneamente.
- **Gravedad:** corresponde a la gravedad de la alarma. Es un elemento útil para filtrar posteriormente las alarmas cuando se realizan búsquedas.

- **Retardo de desactivación:** es el tiempo en segundos que dejará pasar el sistema antes de enviar la alarma a la CRA. También puede denominarse *retardo de entrada*, ya que es el tiempo que tiene el usuario para entrar y desactivar el sistema sin notificar a la CRA.

Acción de respuesta de activación de relés:

- **Habilitar:** selecciona para activar dispositivos externos mediante relés. Se puede escoger de qué dispositivo se activará el relé. Los dispositivos disponibles son: el propio servidor de vídeo análisis, la cámara donde está definida la regla (si esta es ONVIF y posee salidas de relés) y dispositivos externos añadidos en el menú de cámaras (consulta el apartado 3.5 “Dispositivos”).
- **Aplicar retardo de desactivación:** selecciona **Sí** para sincronizar la activación del relé con la notificación de la alarma a la CRA.
- **Tiempo máximo de activación:** se puede seleccionar la duración máxima del relé rellenando este campo. Si no, se aplicará la duración máxima común.

Acción de respuesta de posicionamiento SmartPTZ:

- **Habilitar:** selecciona esta opción para mover automáticamente una **cámara ONVIF PTZ** a una nueva posición cuando se detecta un evento. Después de moverse a la nueva posición predefinida anteriormente, se obtiene un segundo vídeo, llamado también *vídeo de soporte*, para una verificación complementaria.
- **Habilitar Autotracking:** si este control está activado, después de mover la cámara PTZ a la posición del **Preset** seleccionado, si se detecta algo en la escena será seguido (*tracking*) por la cámara PTZ seleccionada. El seguimiento vendrá determinado por los parámetros de Autotracking previamente dados.
- **Volver a preset:** si se ha seleccionado la opción de Autotracking, posicionará la cámara PTZ al preset seleccionado una vez acabe el Autotracking.

Acción de respuesta de reproducción de sonidos:

- **Habilitar:** selecciona para reproducir un sonido cada vez que se genera la alarma. El sonido puede ser generado por el **Altavoz de PC** (el ordenador genera un pitido con el altavoz interno) o por un **Fichero** (permite reproducir un fichero WAV cualquiera. El sistema incluye un conjunto de ficheros WAV que pueden ser utilizados, aunque el usuario es libre de seleccionar cualquier otro fichero WAV que desee).
- **Parar sonido al aceptar alarma:** cuando se selecciona esta opción, el sistema generará un sonido cada vez que se produzca una alarma que no se detendrá hasta que el personal de seguridad la haya aceptado o validado.

Acción de respuesta de envío de mensajes de correo electrónico:

- **Habilitar:** selecciona esta opción para enviar un correo con la imagen, el vídeo o el enlace de la alarma al destinatario especificado con un mensaje opcional. Debes introducir los datos de la conexión al servidor de correo SMTP desde la sección de **Configuración** del equipo, en la pestaña **Correo**. Se te solicitará información adicional.

Acción de respuesta de envío por HTTP:

- **Habilitar:** selecciona esta opción para enviar una petición HTTP de tipo GET a la URL especificada. La conexión con la URL especificada se podrá testear mediante el botón **Test**, que pintará el fondo del textbox de la URL de verde o rojo según si la conexión se ha podido establecer o no.
- **Utilizar autenticación:** seleccionando esta opción se permitirá añadir credenciales de autenticación a la conexión utilizada hacia la URL indicada. Se puede indicar si el tipo de autenticación debe ser Basic o Digest.

Una vez seleccionadas las opciones deseadas, es necesario hacer clic en el botón **Finalizar** para que la regla sea definida en el sistema.

Con esta acción, volvemos a la pantalla de definición de cámaras que deberemos **Cerrar** para volver a pantalla principal. Después de unos segundos, el sistema comenzará a realizar las detecciones programadas por la regla y a generar las alarmas correspondientes.

Este proceso puede repetirse para añadir reglas adicionales en cada cámara.

### 3.5 DISPOSITIVOS

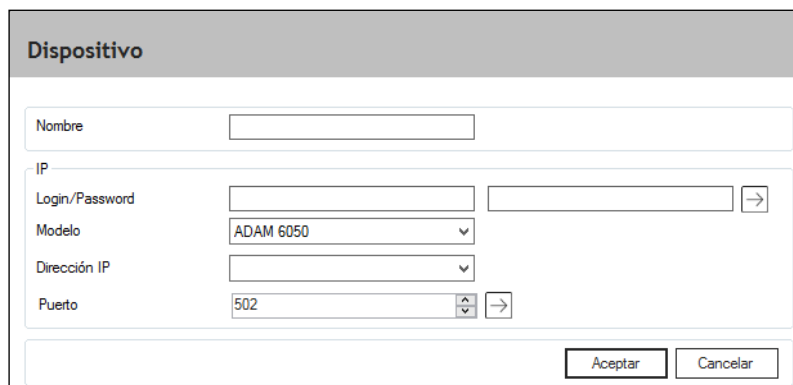
Aparte de las cámaras, también se pueden añadir dispositivos externos admitidos por el sistema.

Añadir dispositivos al sistema sirve para poder activar sus relés de salida ante la generación de alarmas (consulta el apartado [3.4.8. "Respuestas de regla"](#)).

#### 3.5.1 Creación de dispositivos

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón "Cámaras", introduce usuario/contraseña, "MENÚ", "CÁMARAS", aprieta en la flecha del botón "Añadir", selecciona "Dispositivo")*

Se abrirá la pantalla de creación de dispositivos con el siguiente aspecto:



El formulario, titulado "Dispositivo", contiene los siguientes campos:

- Nombre: un campo de texto.
- IP: un campo de texto.
- Login/Password: dos campos de texto con un botón de flecha a la derecha.
- Modelo: un menú desplegable con "ADAM 6050" seleccionado.
- Dirección IP: un menú desplegable.
- Puerto: un menú desplegable con "502" seleccionado y un botón de flecha a la derecha.

En la parte inferior derecha del formulario hay dos botones: "Aceptar" y "Cancelar".

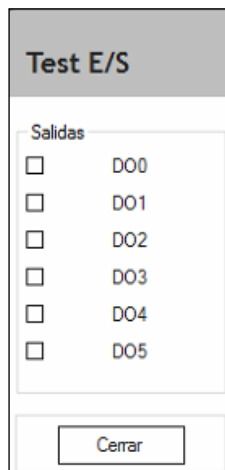
Recuerda que hasta que un dispositivo no esté definido, el sistema no podrá utilizar sus relés de salida a través de reglas de cámara.



### 3.5.2 Testeo de dispositivos

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona un dispositivo creado, aprieta el botón “Test E/S”)

Se abrirá una pantalla que permite el testeo de las salidas del dispositivo:



The screenshot shows a mobile application interface titled "Test E/S". Below the title is a section labeled "Salidas" containing a list of six digital outputs: D00, D01, D02, D03, D04, and D05. Each output name is preceded by an unchecked checkbox. At the bottom of the screen, there is a button labeled "Cerrar".

Salidas
<input type="checkbox"/> D00
<input type="checkbox"/> D01
<input type="checkbox"/> D02
<input type="checkbox"/> D03
<input type="checkbox"/> D04
<input type="checkbox"/> D05

Cerrar

## 4 CONFIGURACIÓN AVANZADA

### 4.1 CONFIGURACIÓN

#### 4.1.1 Central Receptora de Alarmas (CRA)

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “CRA”)

Si necesitas configurar el equipo para enviar las alarmas a una Central Receptora de Alarmas (CRA) o Centro de Control (CC), accede a la pestaña de **CRA**.

Configuración

Nombre de la instalación: Davantis      Nombre de la máquina: G5YK513002ED      IP actual: 198.164.1.109

Instalación   Vista lógica   **CRA**   Particiones   Relés   Correo   Entorno   HTTP

**CRA 1**

Enviar alarmas

Tipo de receptora: DAVANTIS

	IPs/DNSs	Puertos
primaria	12.34.56.78	9034
secundaria	12.34.56.78	9034

Código abonado: 4589

Actualizar automáticamente la IP pública en la CRA

**CRA 2**

Enviar alarmas

Tipo de receptora: DAVANTIS

	IPs/DNSs	Puertos
primaria		9034
secundaria		9034

Código abonado:

Actualizar automáticamente la IP pública en la CRA

29/04/2020 12:08:24      Aceptar   Aplicar   Cancelar

Desde la pestaña CRA, puedes introducir la siguiente información:

- **Enviar alarmas (CRA 1):** activa esta opción para enviar alarmas a un sistema de terceros.
- **Tipo de receptora:** elige el protocolo de envío de las alarmas.
- **Primaria:** el campo de la izquierda es la dirección IP primaria de la CRA, y el de la derecha, el puerto TCP. A parte de IP también se admiten nombres de dominio.
- **Secundaria:** el campo de la izquierda es la dirección IP secundaria de la CRA, y el de la derecha, el puerto TCP. Esta dirección IP se usará cuando la IP primaria falle. En caso de que la CRA no disponga de dos conexiones o IP públicas diferentes, introduce la misma que la primaria.
- **Código abonado:** es el identificador único del abonado o instalación. Normalmente lo asigna la CRA para identificar las alarmas que provengan de este abonado.

- **Actualizar automáticamente la IP pública en la CRA:** si la instalación tiene una conexión con IP dinámica, activa esta opción para notificar periódicamente la dirección IP pública de la instalación y actualizarla en la CRA.
- **Enviar alarmas (CRA 2):** activa esta casilla en caso de querer enviar cada alarma con redundancia a otra destinación. Deberás introducir las direcciones IP de la nueva destinación. De esta forma, las alarmas serán enviadas simultáneamente a la CRA 1 y CRA 2.

#### 4.1.2 Particiones

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Particiones”)

En la pestaña “Particiones” podemos definir el comportamiento del sistema según las señales de un dispositivo externo, como por ejemplo una alarma o un sensor.

Las siguientes opciones están disponibles:

- **Detectar alarmas:** existen dos opciones:
  - Detectar “**Siempre**” implica que las reglas de detección funcionarán aunque la partición a la que pertenecen esté desarmada con la particularidad de que no enviarán las alarmas a CRA ni activarán el relé, aunque estas opciones estuvieran activas en la configuración de la regla. Con la partición armada, las alarmas generadas sí que se enviarían a CRA y activarían el relé, siempre que estas opciones de respuesta estuvieran configuradas en la regla.

- Detectar “**Solo cuando se activa la alarma**” se refiere a que las reglas no funcionarán cuando la partición a la que pertenecen esté desarmada. Y como en la otra opción, con la partición armada, las alarmas generadas sí que se enviarían a CRA y activarían el relé, siempre que estas opciones de respuesta estuvieran configuradas en la regla.

Elige **Siempre** si quieres almacenar los vídeos de la actividad cotidiana, o **Solo cuando se activa la alarma** para optimizar la capacidad de almacenamiento.

- **Retardo de detección:** es el tiempo en segundos desde que se activa una partición hasta que empieza a detectar, o que empieza a enviar alarmas a CRA, en caso de **Detectar alarmas siempre**. También puede denominarse *retardo de salida*, ya que es el tiempo que tiene el usuario para salir de la instalación sin notificar a la CRA.
- **Datos del dispositivo externo:** las entradas y salidas externas pueden provenir de un dispositivo interno, un dispositivo USB, un dispositivo externo IP, o mediante el **Panel software**. Si estás utilizando el dispositivo INTERNAL TYPE-C puedes elegir entre 4 y 8 entradas.
- **Estado de las particiones (N/A, N/C):** elige si la señal de entrada es del tipo normalmente abierta o normalmente cerrada.
- **Cuál es mi dispositivo:** botón situado al lado del tipo de dispositivo. Abre un documento con información sobre los diferentes dispositivos compatibles con el sistema.

En los recuadros numerados del 1 al 8, podrás ver el estado de las entradas en tiempo real (en rojo las activas y en gris, las inactivas). Si cambias el estado de N/C a N/A o viceversa, deberás aplicar los cambios para ver el nuevo estado.

### 4.1.3 Relés

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Relés”)

En la pestaña “Relés” configuraremos la salida de relés del sistema si hemos adquirido el módulo adicional de salidas.

Se pueden configurar hasta 4 salidas externas por instalación, las cuales podrán ser activadas remotamente desde la CRA. Es decir, lo que definamos aquí va a ser la información que tendrán los operadores de la CRA en el caso de haberla contratado. Para cada salida tenemos:

- **Relé X (Y/N):** marca la casilla del relé X para permitir su activación remota.
- **Desplegable de tipo:** selecciona aquí el tipo de dispositivo que activará el relé (una luz, un aviso sonoro...).
- **Botón de test:** pulsa el botón para verificar la correcta activación/desactivación del dispositivo. El botón estará activo una vez se haya habilitado el relé para su activación remota.
- **Descripción:** información adicional que verán los operadores de la CRA sobre la salida en cuestión. Añade una breve descripción en el cuadro contiguo.
- **Duración máxima:** marca la casilla para establecer un tiempo máximo de activación del relé. Una vez marcada, deberás introducir el tiempo máximo de activación deseado.

El panel de **Testeo de relés** se utiliza para probar si los relés se activan correctamente en todos los equipos de la instalación. Selecciona el equipo que desees en **Máquina** y luego haz clic en el botón correspondiente para activar el relé seleccionado.

#### 4.1.4 Correo

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Correo”)*

Si deseas enviar alarmas mediante correo electrónico, desde la pestaña **Correo**, deberás configurar los parámetros de la cuenta de correo que se utilizará para enviar estas notificaciones de alarmas.

### Configuración

Nombre de la instalación <b>Davantis</b>	Nombre de la máquina: <b>G5YK513002ED</b>	IP actual <b>198.164.1.109</b>
---	--	-----------------------------------

—

**Instalación** **Vista lógica** **CRA** **Particiones** **Relés** **Correo** **Entorno** **HTTP**

<b>Servidor SMTP:</b> Nombre <input type="text" value="smtp.example.com"/> Puerto <input type="text" value="25"/> <input checked="" type="checkbox"/> Usar autenticación <input checked="" type="checkbox"/> Encriptación TLS	<b>Cuentas de correo</b> De <input type="text" value="user@example.com"/> Destino por defecto <input type="text" value="admin@example.com"/> Asunto por defecto <input type="text"/>
<b>Autenticación</b> Usuario <input type="text" value="user@example.com"/> Contraseña <input type="password" value="*****"/>	<b>Test</b> <input type="button" value="Envía"/> <input type="text"/> <input type="button" value="Comprueba"/> <input type="text"/>

29/04/2020 12:12:37

En la sección del Servidor SMTP debes rellenar la siguiente información:

- **Nombre:** aquí debes introducir el nombre del servidor de correo saliente (SMTP).
- **Puerto:** el puerto SMTP, por defecto, es el 25. Si tu servidor requiere una conexión segura (SSL), el puerto por defecto es el 995, aunque otros proveedores como Gmail utilizan el 587.
- **Usar autenticación:** activa esta opción si tu servidor SMTP requiere autenticación.
- **Encriptación TLS:** activa esta opción si tu servidor SMTP utiliza el método de encriptación TLS.

En la sección “Autenticación” debes rellenar la siguiente información:

- **Usuario:** introduce tu nombre de usuario del servidor de correo saliente (SMTP).
- **Contraseña:** introduce tu contraseña de usuario.

En la sección “Cuentas de correo” debes rellenar la siguiente información:

- **De:** es el correo electrónico de la cuenta de origen. Es posible que el usuario y el correo electrónico sean iguales.
- **Destino por defecto:** es el destinatario de envío por defecto. Esta información se utiliza para rellenar los campos automáticamente durante la creación de las reglas de las alarmas, aunque se puede modificar la regla para enviar a un destinatario diferente.
- **Asunto por defecto:** es el asunto o tema del correo que le aparecerá al destinatario cuando reciba las notificaciones de alarma.

En la sección “Test”, tienes disponibles las siguientes opciones para verificar los datos introducidos.

- **Envía:** utiliza el botón **Envía** para testear la configuración. Se enviará un correo electrónico desde la cuenta de origen configurada al “Destino por defecto”.
- **Comprueba:** utiliza este botón para verificar si el correo se ha enviado correctamente.

Si desconoces los datos de configuración de tu cuenta de correo, contacta con tu proveedor de correo electrónico.

#### 4.1.5 Entorno

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “Entorno”)

En la pestaña “Entorno” se puede definir la configuración horaria del equipo.

**Configuración**

Nombre de la instalación: **Davantis**      Nombre de la máquina: **G5YK513002ED**      IP actual: **198.164.1.109**

Instalación   Vista lógica   CRA   Particiones   Relés   Correo   **Entorno**   HTTP

Sincronizar

Sincroniza fecha y hora con:    CRA    Servidor NTP   **Sincronizar ahora**

Fecha

Fecha actual: 29/04/2020

Año con 4 dígitos  
 Siempre 2 dígitos en los meses  
 Siempre 2 dígitos en los días

La semana empieza en: lunes

Orden: Día   Mes   Año

Separador de fecha: /

Hora

Hora actual: 12:14:17

Siempre 2 dígitos en las horas  
 Siempre 2 dígitos en los minutos  
 Siempre 2 dígitos en los segundos

12 h    24 h   12 h    Antes    Después

Añadir AM/PM

Separador de tiempo: :

Huso horario: (UTC+01:00) Brussels, Copenhagen, Madrid, Paris

29/04/2020 12:14:17   **Aceptar**   **Aplicar**   **Cancelar**

Para sincronizar la hora automáticamente con la CRA (requiere tener el equipo conectado a una CRA) o con un servidor NTP, selecciona la casilla **Sincroniza fecha y hora con:**, escoge la opción que desees y pulsa **Sincronizar ahora**. Para la opción de servidor NTP se puede introducir una dirección o escoger entre una serie de opciones por defecto.

Alternativamente, se puede definir la hora y la fecha manualmente, usando las opciones disponibles en las secciones **Fecha** y **Hora**. Selecciona la zona horaria correspondiente a tu localidad para ajustar automáticamente el horario del equipo.

#### 4.1.6 HTTP

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Configuración”, introduce usuario/contraseña, pestaña “HTTP”)

En la pestaña “HTTP” se puede definir la configuración por defecto para la característica HTTP de la pantalla de respuesta de la creación/modificación de las reglas de la cámara.

**Configuración**

Nombre de la instalación: **Davantis**      Nombre de la máquina: **G5YK513002ED**      IP actual: **198.164.1.109**

Instalación   Vista lógica   CRA   Particiones   Relés   Correo   Entorno   **HTTP**

Conexión

Servidor de alarma (por defecto):       Test

Tipo de autenticación:    Basic    Digest

Usuario (por defecto):

Contraseña (por defecto):

29/04/2020 12:17:21      Aceptar   Aplicar   Cancelar

En la sección “Autenticación” debes rellenar la siguiente información:

- **Usuario:** introduce tu nombre de usuario del servidor.
- **Contraseña:** introduce tu contraseña de usuario.

En la sección “Conexión” debes rellenar la siguiente información:

- **Servidor de alarma:** es la dirección HTTP.

Será necesario pulsar el botón **Aplicar** para que los cambios tengan efecto.



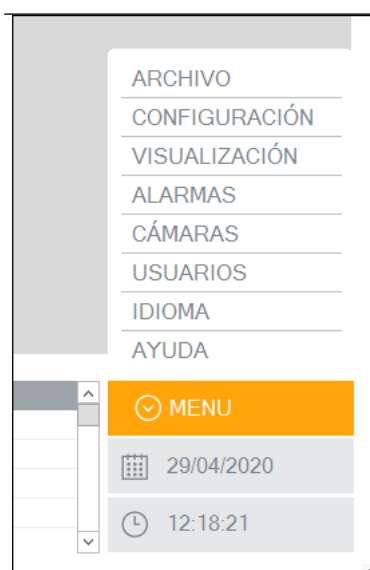
## 4.2 CÁMARAS

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña)

### 4.2.1 Menú de opciones

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”)

La barra de menú se encuentra en la parte inferior derecha de la pantalla principal. Si haces clic sobre el botón **Menú**, te aparecerán los siguientes botones u opciones:



#### 4.2.1.1 Archivo

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ARCHIVO”)

En el menú “Archivo”, tenemos la opción **Reiniciar**, que implica reiniciar todos los equipos a la vez. Seleccionando la opción **Salir**, se cierra la interfaz gráfica del cuadrante de cámaras de la aplicación. En este último caso, una vez situados en la pantalla principal, las reglas de detección definidas seguirán funcionando en el servidor y el sistema seguirá detectando las alarmas definidas a pesar de que las cámaras no estén siendo visualizadas.

#### 4.2.1.2 Configuración

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CONFIGURACIÓN”)

Consulta la sección “Configuración general” para más información.

### 4.2.1.3 Visualización

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “VISUALIZACIÓN”)*

Las siguientes opciones están disponibles en este menú:

- **Distribución:** permite el acceso a la pantalla de diseño del cuadrante de cámaras. Puedes elegir entre 1 y 4 filas y entre 1 y 4 columnas, por lo que se puede ver de forma simultánea un máximo de 16 cámaras.
- **Pantalla completa:** cambia el panel de monitorización seleccionado al modo de pantalla completa. La interfaz gráfica desaparecerá, dejando solo los paneles de monitoreo actualmente en el área de la pantalla visible. Para volver a la interfaz gráfica, pulsa la tecla Escape (Esc) en tu teclado.
- **Seleccionar:** te permite seleccionar una de las vistas predefinidas. Vistas de cámara son grupos de cámaras que se utilizan para mostrar rápidamente conjuntos de cámaras.
- **Añadir/Borrar:** te permite guardar la vista actual (el seguimiento de paneles y la configuración de selección de cámara) o borrar la vista actual.
- **Mapa de colores:** para imágenes térmicas, puedes elegir entre ver las imágenes en escala de grises o ver imágenes que solicitan un mapa de color para aumentar el contraste de ciertas temperaturas.

### 4.2.1.4 Alarmas

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)*

Consulta la sección “Buscador de alarmas” para más información.

### 4.2.1.5 Cámaras

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”)*

Consulta la sección “Cámaras” para más información.

### 4.2.1.6 Usuarios

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “USUARIOS”)*

El menú “Usuarios” tiene las siguientes opciones disponibles:

- **Gestionar:** permite añadir, modificar o eliminar los usuarios
- **Perfiles:** permite añadir o eliminar las acciones disponibles a cada perfil.
- **Registro:** muestra el registro de actividad de cada operador en el sistema.

Si se selecciona **Gestionar** aparece la siguiente ventana, donde podrás ver los usuarios existentes:

Usuarios		
Usuario	Password	Perfil
admin	*****	Administrador

Añadir    Modificar    Eliminar    Aceptar

Puedes añadir, modificar o eliminar todos los datos de los usuarios: perfil de seguridad, nombre de usuario y contraseña.

Gestión de usuarios	
Por favor introduzca sus datos	
Contraseña:	<input type="password"/>
Datos del usuario	
Perfil	<input type="text" value="▼"/>
Nombre de usuario:	<input type="text"/>
Nueva Contraseña:	<input type="text"/>
Confirmar Contraseña:	<input type="text"/>
Aceptar	Cancelar

Los 3 niveles de seguridad son los siguientes: Instalador (sin restricciones), Administrador (con todas las opciones disponibles excepto “Ajustar cámaras”) y Usuario (con opciones más limitadas). Aparte, el sistema dispone de dos perfiles alternativos, Usuario2 e Invitado2, con algunas opciones extra para los perfiles Usuario e Invitado, respectivamente.

La opción **Perfiles** nos permite definir nuevos perfiles de usuario, con opciones personalizadas para cada uno de ellos.

### Perfil

Nuevo perfil:

Perfil	Nivel de acceso
<b>Invitado</b>	1
<b>Usuario</b>	2
<b>Administrador</b>	3
Invitado2	3
Usuario2	3

Permisos:

Actividad
<input type="checkbox"/> Modificar configuración del sistema
<input type="checkbox"/> Encender y parar cámaras
<input type="checkbox"/> Ver histórico de imágenes y datos
<input type="checkbox"/> Exportar grabaciones de video
<input type="checkbox"/> Exportar históricos de datos

Para crear un nuevo perfil, deberás escribir el nombre del nuevo perfil (o seleccionar uno de la lista para modificarlo). A continuación deberás seleccionar de la lista los permisos que tendrá el nuevo perfil. En función de los permisos que elijas, se le asignará un “Nivel de Acceso” al perfil. Los perfiles Invitado, Usuario y Administrador son propios del sistema, y no se podrán modificar ni borrar.

Seleccionando **Registro** aparece la siguiente ventana:

### Registro

Fecha	Operador	Tipo	Comando

De:   Operador:

Para:   Tipo:

Podrás ver el registro de acciones clasificadas según el **operador**, filtrar por los **tipos** definidos (general, cámaras y reglas), y según periodos de tiempo seleccionados por **calendario**.

#### 4.2.1.7 Idioma

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “IDIOMA”)*

La opción “Idioma” permite cambiar el idioma de la aplicación. Permite seleccionar entre alemán, catalán, español, francés, inglés, italiano y portugués. Para que se aplique el cambio de idioma, se deberá cerrar la aplicación y volver a arrancar la interfaz gráfica.

#### 4.2.1.8 Ayuda

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “AYUDA”)*

- **Ayuda:** abre una ventana nueva donde se puede consultar este manual.
- **Información del equipo:** muestra estadísticas sobre el espacio disponible en disco, así como el tiempo total de grabaciones en el equipo.
- **Ver los términos de uso:** podrás visualizar las condiciones generales de contratación.
- **Acerca de...:** muestra en pantalla tanto la versión del software como información del fabricante.

#### 4.2.2 Configuración general

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CONFIGURACIÓN”)*

Desde el menú “Configuración” se permite modificar algunos parámetros globales.

## Configuración

**Servidor**

Vida de las alarmas (días)

Vida de las alarmas protegidas (días)

Gravedad (alarmas del sistema)

Nivel de visualización de alarma

Pérdida señal vídeo (seg)

Formato de vídeo

Grabación vídeo (fps)

Tiempo de pre-alarma (seg)

Tiempo de post-alarma (seg)

Duración del vídeo SmartPTZ (seg)

Cortar alarmas (seg)

Sólo cortar las enviadas a CRA

Superponer fecha y hora en directo y en grabaciones

**Modo de visualización**

Ver el nombre de la cámara por pantalla

Ver la resolución de la cámara por pantalla

Ver el tipo de las reglas por pantalla

Ver pre-alarmas

Ver trayectorias

Mantener proporciones de las imágenes

Deshabilitar botón de minimizar

Mostrar panel de entradas por software

Ver información de las reglas por pantalla

Mostrar el contador en tiempo real

Contraste

Tiempo de hot-spot  segundos

Últimas alarmas  minutos

**Color de las alarmas**

Tipo de alarma	Color
Movimiento	<span style="background-color: yellow; border: 1px solid #ccc; display: inline-block; width: 20px; height: 15px;"></span> <input type="button" value="🔍"/>

Restaurar los colores por defecto

**Correo electrónico**

Adjuntar imagen  Sí  Link  No

Adjuntar vídeo  Sí  Link  No

Enviar estado de las zonas a:

**App**

Activar notificaciones push

Habilitar compatibilidad con versiones anteriores

**Protocolos**

Activar suscripción Xtension

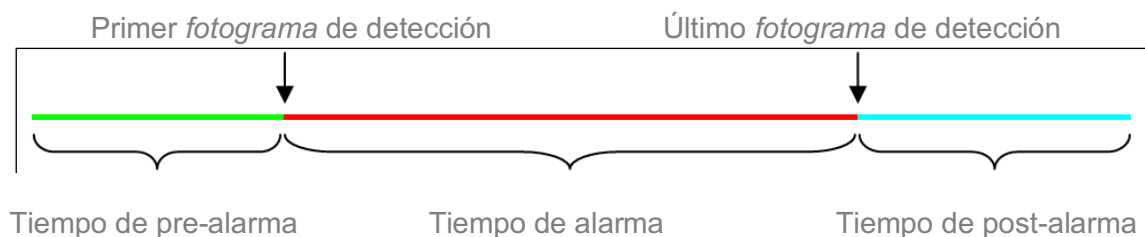
Activar ONVIF

Los parámetros del servidor que se pueden modificar son los siguientes:

- **Vida de las alarmas (días):** establece el tiempo de vida de las alarmas en el sistema.
- **Vida de las alarmas protegidas (días):** establece un tiempo de vida máximo de las alarmas protegidas en el sistema.
- **Gravedad (alarmas del sistema):** gravedad de las alarmas generadas por el sistema (pérdida de conexión, pérdida de señal de cámaras...).
- **Nivel visualización alarmas:** visualización de las alarmas a partir de un determinado nivel de gravedad en el área de alarmas recientes.
- **Pérdida señal vídeo (seg):** tiempo en segundos sin señal de una cámara para generar alarma de pérdida de señal.

- **Formato de vídeo:** formato del fichero de grabación. Esta opción no estará disponible para los servidores que tengan configurado el envío de alarmas a una CRA con sistema Daview AMS, ya que en estos casos, la opción del formato de vídeo viene determinado por la CRA.
- **Grabación vídeo (fps):** posibilidad de indicar (fps) de los vídeos grabados.
- **Tiempo de pre-alarma (seg):** tiempo de grabación de pre-alarma.
- **Tiempo de post-alarma (seg):** tiempo de grabación de post-alarma.
- **Duración del vídeo SmartPTZ (seg):** tiempo de grabación del vídeo SmartPTZ.
- **Cortar alarmas (seg):** tiempo máximo de grabación de alarma incluyendo tiempo de pre-alarma.
- **Solo cortar las enviabiles a CRA:** el vídeo de las alarmas solo se cortará si la regla que lo ha generado debe enviarse a la CRA.

El tiempo de grabación de una alarma consiste en el tiempo de pre-alarma, tiempo de alarma y el tiempo de post-alarma como se muestra en el siguiente diagrama.



Por ejemplo, con 3 segundos de pre-alarma y 7 segundos de post-alarma, si el intruso permanece detectado en la escena durante 30 segundos:

- Si desactivas la opción "Cortar alarmas", tendrás toda la alarma de 40 segundos de tiempo de grabación ( $3\text{ s} + 30\text{ s} + 7\text{ s} = 40\text{ s}$ ).
- Si el tiempo de corte está activado, obtendrás solo los primeros segundos del vídeo de alarma.

En la sección de "Correo electrónico" se pueden modificar los siguientes parámetros:

- **Adjuntar imagen:** permite seleccionar qué se adjuntará en el correo de notificación de alarma. Se puede enviar la imagen, el enlace o nada.
- **Adjuntar vídeo:** permite seleccionar si se adjunta el fichero del vídeo de la alarma en el correo electrónico. Por defecto, no se adjuntará para agilizar el envío.
- **Enviar estado de las zonas a:** al seleccionarlo, permite enviar el estado de las zonas a una dirección de correo electrónico determinada.

En la sección "Modo de visualización" se pueden modificar los siguientes parámetros:

- **Contraste:** puedes elegir entre estándar, maximizada, más oscuro, más claro o más igualado contraste.

- **Ver el nombre de la cámara por pantalla:** mostrar o no los nombres de las cámaras.
- **Ver información de las reglas por pantalla:** mostrar o no información adicional relacionada con reglas tales como flechas.
- **Ver el tipo de las reglas por pantalla:** muestra el nombre de tipo de regla (por ejemplo, intruso, persona, etc.).
- **Ver pre-alarmas:** esto te permite ver la detección del sistema. Solo se utiliza para la visualización, no se generan alarmas.
- **Ver trayectorias:** esto te permite ver las trayectorias de las detecciones superpuestas en la pantalla.
- **Mantener proporciones de las imágenes:** para mantener las proporciones de la imagen según la resolución de la pantalla del monitor.
- **Deshabilitar botón de minimizar:** quitar el botón de minimizar de la aplicación.
- **Mostrar panel de entrada por software:** permite al usuario armar y desarmar el sistema utilizando esta aplicación.
- **Mostrar contador tiempo real:** si se ha creado una regla Contador, se muestra en tiempo real un contador en una esquina de la imagen.
- **Tiempo de Hot Spot:** el tiempo en segundos que este modo estará activo.
- **Últimas alarmas:** tiempo máximo que permanecerán los eventos en la sección de alarmas recientes.

En la sección “Color” se pueden modificar los siguientes parámetros:

- **Tipo de alarma y color:** la posibilidad de asignar un color a cada tipo de alarma.
- **Restaurar los colores por defecto:** opción para restaurar los colores por defecto según la configuración de fábrica.

En la sección “App” se puede modificar el siguiente parámetro:

- **Activar notificaciones push:** permite habilitar/deshabilitar el envío de notificaciones push de la instalación.
- **Habilitar compatibilidad con versiones anteriores:** permite habilitar la compatibilidad con las aplicaciones que utilizan la versión 2.5 o inferior.

En la sección “Protocolos” se puede modificar el siguiente parámetro:

- **Xtension:** activa/desactiva las peticiones de la funcionalidad Xtension.
- **ONVIF:** activa/desactiva el protocolo ONVIF como dispositivo servidor.



### 4.2.3 Gestión de cámaras

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”)*

Los grupos de cámaras ayudan al usuario a organizar las cámaras. Estos grupos se usan generalmente para agrupar cámaras de una misma zona, planta o edificio.

Los pasos para crear un grupo de cámaras son los siguientes:

1. Haz clic en el campo **Grupo** e introduce el nombre del grupo de cámaras que desees crear.
2. Presiona el botón **Añadir** y el grupo de cámaras se creará automáticamente.

A partir de este momento, cuando se defina o se modifique una cámara, podrá ser incluida en los grupos de cámaras existentes.

Para eliminar un grupo de cámaras, selecciona el nombre del grupo en el menú desplegable “Grupo” y pulsa el botón **Borrar**. El grupo se eliminará automáticamente. Se permitirá borrar un grupo siempre que este no tenga ninguna cámara asignada. Para llevar a cabo el proceso, accede a Modificar cámara y deja la sección en blanco de grupo.

Las vistas de cámaras son similares a los grupos de cámaras, pero solo se usan para organizar las cámaras que se mostrarán en la pantalla de cámaras en directo. Las vistas de cámaras no tienen por qué coincidir con los grupos de cámaras.

### 4.2.4 Horarios de regla

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, botón “Crear/modificar horario”)*

Seleccionando **Personalizado** en Horario, aparecerá una nueva opción que te permitirá definir el tiempo en el cual esta regla estará activa.

Haciendo clic en **Crear/modificar horario** aparecerá otra nueva pantalla donde definir las franjas horarias en las que se activará la alarma para cada día de la semana. Seleccionando **activación** / **desactivación** según convenga y haciendo clic sobre las celdas de la pantalla, se configuran los horarios en los que la alarma estará activa. Cada celda representa una fracción de hora de 15 minutos. Las alarmas durante periodos no activos son ignoradas por el sistema y no generan ningún aviso.

El botón **Guarda el horario** permite guardar y poner nombre a un horario para ser eventualmente utilizado en otras reglas. En caso de tener seleccionado un horario, este botón permite eliminar el horario.

**Creación de horarios**

hora	lunes	martes	miércoles	jueves	viernes	sábado	domingo
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00	■	■	■	■	■	■	■
10:00	■	■	■	■	■	■	■
11:00	■	■	■	■	■	■	■
12:00	■	■	■	■	■	■	■
13:00	■	■	■	■	■	■	■
14:00	■	■	■	■	■	■	■
15:00	■	■	■	■	■	■	■
16:00	■	■	■	■	■	■	■
17:00	■	■	■	■	■	■	■
18:00	■	■	■	■	■	■	■
19:00							
20:00							
21:00							
22:00							
23:00							

activación

desactivación

Activo  Inactivo

En la imagen se muestra un ejemplo de horario en el que el sistema estará activo de lunes a viernes, desde las 8:30 h hasta las 19:00 h.

Tras definir los horarios y guardarlos, haz clic en la pantalla Reglas (paso 2), y selecciona **Aceptar**.

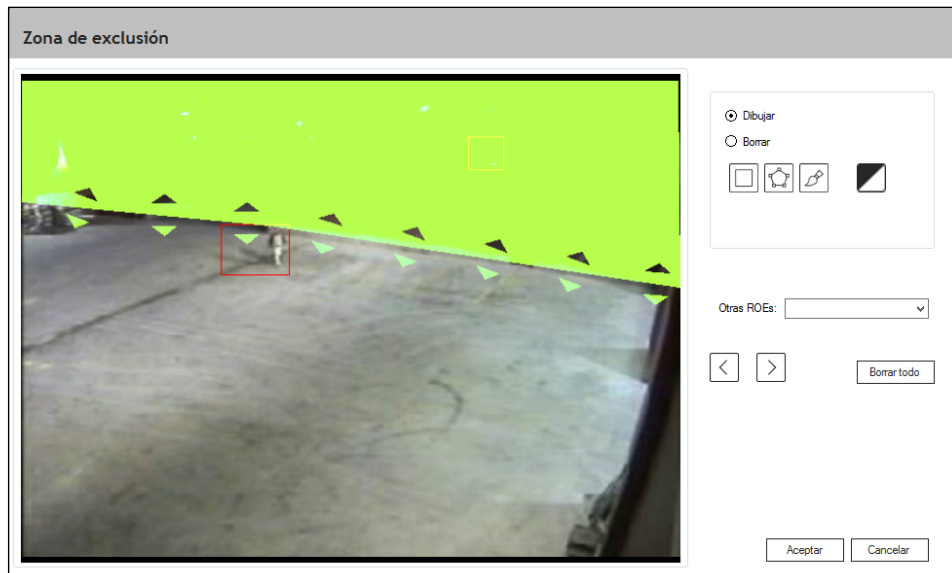
#### 4.2.5 Regla Entrar / Salir

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón "Cámaras", introduce usuario/contraseña, "MENÚ", "CÁMARAS", selecciona una cámara, botón "Añadir" de la sección de Reglas, botón "Siguiente", botón "Crear / modificar zona")*

Las alarmas pueden ser generadas cuando un intruso entra o sale de una región predefinida en la imagen.

Entrar en una región significa que el intruso debe ser visto y analizado antes de entrar en la región especificada, debe ser visto al entrar en la región y debe ser visto una vez que haya entrado en la región.

La detección puede ser generada en un sentido, en el sentido opuesto o en ambos. La regla **Entrar** se activa cuando el intruso se mueve desde el área verde (zona de exclusión) al área no verde. La regla **Salir** se activa cuando el intruso se mueve del área no verde al área verde. Y por último, la regla **Entrar / Salir** se activa en ambos casos.



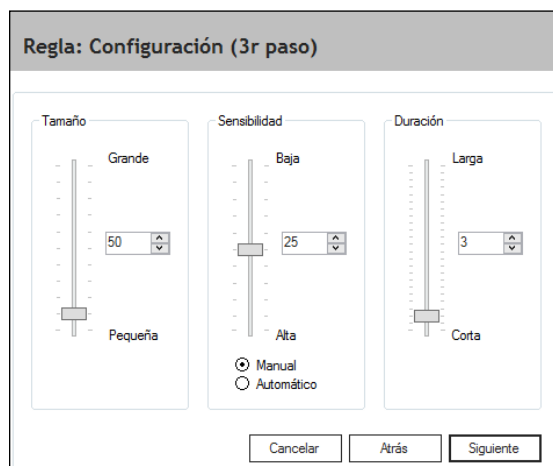
La regla **Entrar / Salir** permite una detección “anti-flujo”. Es decir, personas que se muevan en la dirección opuesta al flujo esperado puedan generar una alarma.

En escenarios llenos de gente, la persona o vehículo que se mueve de una región a otra en una dirección específica, debe ser claramente visto antes, durante y después de moverse a la nueva región. De lo contrario, la alarma puede no ser generada.

#### 4.2.6 Regla Movimiento

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, seleccionar detectar “Movimiento”, botón “Siguiente”)*

**Atención:** El tercer paso de la configuración únicamente será accesible cuando se haya seleccionado el tipo de regla de “Movimiento”. En los otros casos, el sistema irá directamente al paso **Respuesta**.



Los parámetros de movimiento se configuran de la siguiente forma:

- haciendo clic y arrastrando cada uno de los controles deslizantes arriba o abajo para cambiar el parámetro
- cambiando directamente el número en la ventana donde se muestra el valor de cada parámetro
- haciendo clic sobre las flechas de arriba/abajo al lado de cada valor de parámetro

Los parámetros a configurar son los siguientes:

**Tamaño:** representa el número total de píxeles o puntos de la pantalla que deben cambiar para activar la detección de movimiento. Por encima de este número de píxeles la detección se activará, y por debajo no se activará.

Por ejemplo, una persona en movimiento que en la pantalla representa un cambio de 45 píxeles con respecto a la imagen anterior, necesitará que el parámetro **Tamaño** esté como mínimo a 45 píxeles para poder ser detectado. Con el parámetro de tamaño a 45, una persona de 50 píxeles será detectada, un árbol que represente 83 píxeles también, pero un perro que represente 18 píxeles, no.

**Sensibilidad:** la sensibilidad es el cambio mínimo que debe sufrir un píxel para que se considere que ha habido movimiento.

Un parámetro de sensibilidad demasiado bajo hará nuestro sistema sensible al más ligero cambio en la escena, aunque también nos dará falsas alarmas por pequeños cambios de luz.

Un parámetro de sensibilidad demasiado alto, hará nuestro sistema más inmune a los cambios ligeros de luz, pero es posible que objetos en movimiento de color muy parecido al fondo se escapen de la detección.

**Modo Automático:** el sistema ajusta automáticamente la sensibilidad.

**Duración:** este parámetro representa el número de imágenes consecutivas en que el sistema debe detectar movimiento para activar la alarma.

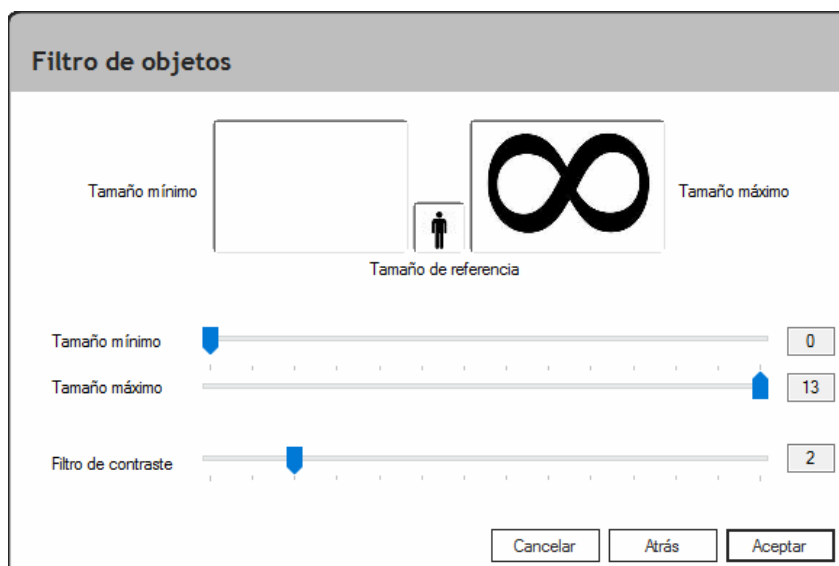
Por ejemplo, con un sistema funcionando a 6 imágenes por segundo, y con el parámetro duración configurado a 4 imágenes, un pájaro que permanece en la escena durante 3 imágenes (1/2 segundo) no será detectado, pero sí lo será una motocicleta que permanece en la pantalla durante 12 imágenes (2 segundos).

#### 4.2.7 Regla Objeto abandonado/robado

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón "Cámaras", introduce usuario/contraseña, "MENÚ", "CÁMARAS", selecciona una cámara, botón "Añadir" de la sección de Reglas, botón "Siguiente", seleccionar detectar "Objeto", botón "Siguiente")*

**Atención:** El filtro de tamaño de objeto únicamente será accesible cuando se haya seleccionado el tipo de regla **Objeto**. En los otros casos, el sistema irá directamente al paso **Respuesta**.

**Atención:** La regla Objeto abandonado/robado es una característica opcional y solo está disponible en ciertas soluciones.



Cuando se defina una regla de objeto abandonado o de objeto robado se deberá especificar el rango de tamaños del objeto que queremos detectar. Por defecto no hay ninguna restricción de tamaño. Los tamaños mínimos y máximos especificados serán siempre en relación al tamaño de persona definido en la perspectiva de la cámara.

- **Tamaño mínimo y máximo:** los diferentes tamaños de objetos que se pueden especificar se sitúan entre la posición 0 y la 13. En estos dos límites no se aplica ninguna restricción al tamaño del objeto.
- **Filtro de contraste:** por defecto este filtro no debe modificarse. Si se producen falsas alarmas en la detección de objetos por culpa de cambios de iluminación en la escena, deberemos subir el filtro de contraste. Si, por el contrario, el sistema tiene dificultades para detectar objetos poco contrastados con el fondo, deberemos bajar el filtro de contraste.

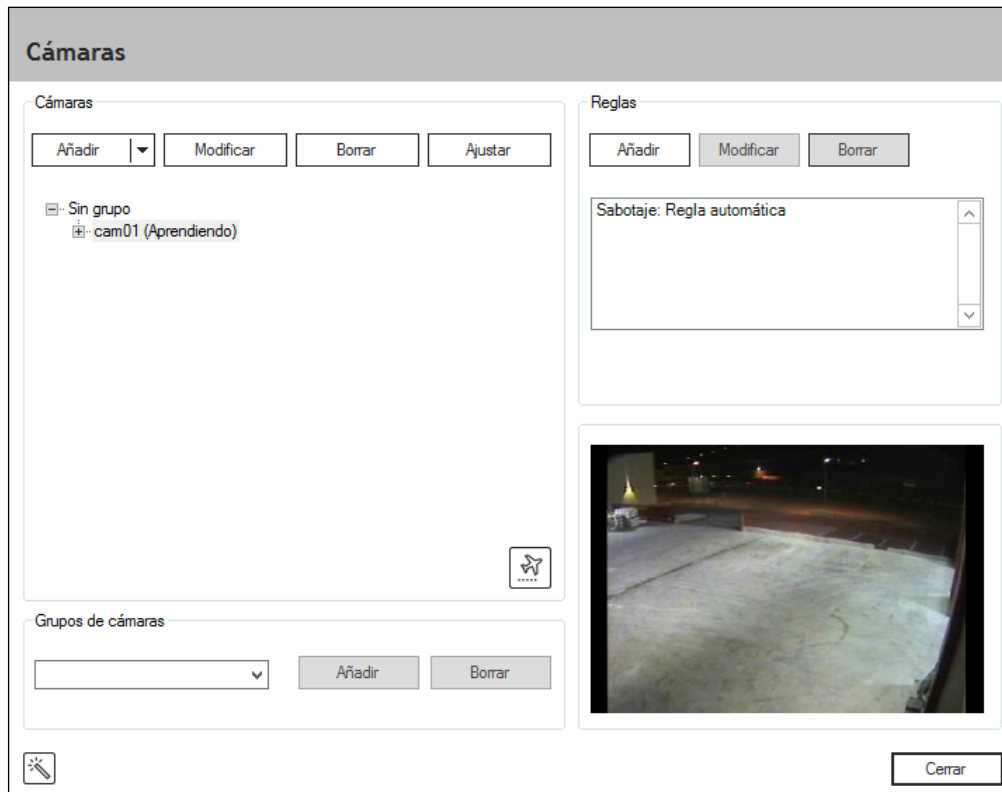
En escenas concurridas, el objeto abandonado debe ser visto claramente durante un cierto período de tiempo; si no, puede ser que la alarma no se genere. Para reglas de objeto robado, el espacio libre donde estaba el objeto debe ser visto claramente durante un cierto período de tiempo; si no, puede ser que la alarma no se genere.

#### 4.2.8 Regla Sabotaje

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, seleccionar detectar “Sabotaje”)*

La regla de sabotaje es la que se encarga de detectar cualquier cambio brusco en la imagen de la cámara. Esta regla generará una alarma cuando se detecte un cambio brusco en la imagen de la cámara, como cambios de escena o alteraciones voluntarias de la imagen.

Esta regla se generará **automáticamente** al crear una cámara, por lo tanto no es necesario crearla posteriormente. Por defecto, la regla no estará asociada a ninguna partición. Es altamente recomendable mantenerla no asignada a particiones, ya que en este estado estará funcionando siempre, y generará alarmas aun cuando el sistema no esté armado.



La sensibilidad de esta regla puede ajustarse desde el parámetro Sabotaje. Consulta la sección “Parámetros” para más información.

#### 4.2.9 Regla Aglomeración

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiente”, seleccionar detectar “Aglomeración”, botón “Siguiente”)*

**Atención:** Esta característica es opcional y solo está disponible en ciertas soluciones.

La regla Aglomeración te permite detectar los niveles de ocupación de la cámara a partir de un cierto umbral. El umbral de densidad se representa con un porcentaje de ocupación de la imagen de entre 0% y 100%.

Como en muchas otras reglas, puede especificar la región de la cámara donde desea medir el nivel de ocupación.

La regla Aglomeración se basa en la detección de movimiento. Por lo tanto, si todos los elementos de la escena permanecen estáticos, la alarma puede que no se active o que el promedio de aglomeración muestre una cantidad inferior a la esperada.

La sensibilidad y la duración pueden ajustarse de manera similar a la de una regla de movimiento. Consulte la sección “Regla Movimiento” para más información.

**Regla: Configuración (3r paso)**

Densidad (%)

Alta

50

Baja

Sensibilidad

Baja

10

Alta

Duración

Larga

3

Corta

Manual  
 Automático

Cancelar Atrás Siguiete

La información sobre la aglomeración puede comprobarse de tres maneras:

- mostrando un contador en tiempo real en la ventana principal que muestre el porcentaje de densidad.
- generando una alarma cada X minutos con el porcentaje de densidad promedio en la escena.
- generando una alarma cuando se alcanza un umbral de porcentaje de densidad.

#### 4.2.10 Regla Entrada externa

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Añadir” de la sección de Reglas, botón “Siguiete”, seleccionar detectar “Entrada externa”, botón “Siguiete”)*

Esta regla permite detectar cambios de estado de entradas externas. Se puede escoger entre dos tipos de entradas:

- las propias entradas del sistema.
- las entradas de una cámara o dispositivo externo.

#### Entradas del sistema:

Las alarmas solo se generarán cuando las entradas se activen. El estado lógico de las entradas se puede ver en el menú de Configuración (consulta la sección “Configuración”).

Se pueden generar alarmas con entradas de un equipo máster o uno esclavo. En un equipo máster, si la entrada se usa como partición (para armado y desarmado) no se podrá usar para generar alarmas de entrada externa.

## **Entradas de una cámara o dispositivo externo:**

Para que una cámara o dispositivo externo genere alarmas por entrada externa, estos deben ser compatibles con el sistema (consulta la sección “Gestión de cámaras” para añadir una cámara).

Una vez que la cámara o dispositivo estén añadidos al sistema se podrán seleccionar las entradas deseadas para generar alarmas solamente si están disponibles en el dispositivo.

### **4.2.11 Región de exclusión**

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar” de la sección de Cámaras, seleccionar “Región de exclusión”, botón “Siguiente”)*

Los ajustes de cámaras son esenciales para una correcta detección y para minimizar el número de falsas alarmas.

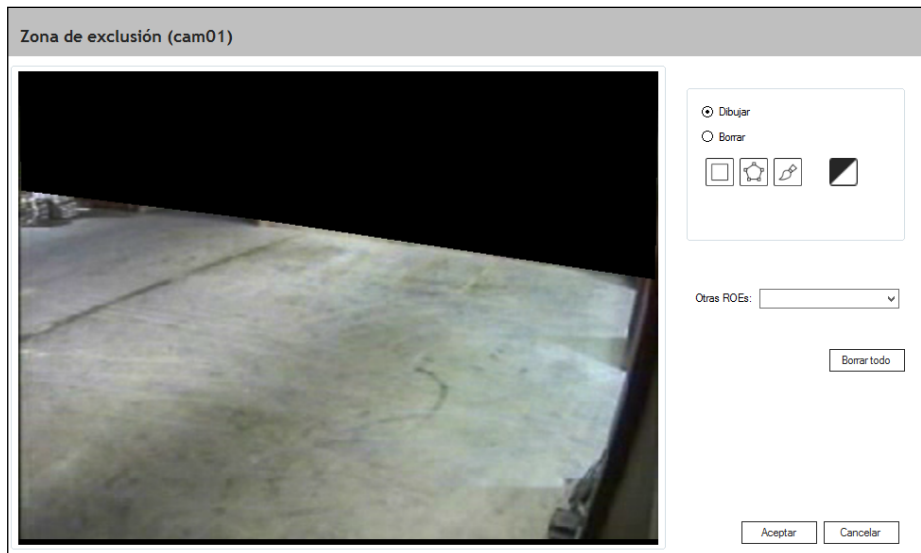
Hay cinco tipos de ajustes de cámara:

- Región de exclusión
- Perspectiva
- Parámetros
- Máscara de privacidad
- Virtual IR ®

Es importante tener en cuenta que cualquier cambio en estos cinco ajustes se aplica a la cámara, y, por lo tanto, todas las reglas de detección asociadas a esa cámara se verán afectadas.

El objetivo de la región de exclusión es anular aquellas zonas que el sistema no deberá analizar. La zona marcada será enmascarada y ayudará a mejorar el rendimiento del equipo. Para el sistema la región de exclusión será una zona negra. En consecuencia, cualquier parte de un objeto (persona o vehículo) que quede dentro de la zona exclusión será eliminada por el sistema y, por lo tanto, será imposible que el sistema pueda detectar aquel objeto. La región de exclusión está pensada para eliminar zonas donde es imposible la presencia de un intruso, como por ejemplo zonas de cielo, paredes de edificios (sin llegar nunca hasta al suelo, ya que entonces no se detectaría a una persona que caminara pegada a la pared), carreteras, zonas que no se quieren vigilar, etc. En caso de duda, es mejor no marcar ninguna región de exclusión.





Las herramientas para dibujar la región de exclusión son las mismas que las herramientas para dibujar la región de exclusión de una regla, aunque no hay que confundir ambas regiones. Mientras que la región de exclusión de cámara elimina cualquier análisis en aquella zona, la región de exclusión de regla solo indica las zonas que activarán una alarma y las zonas que no. Si una persona tiene todo el cuerpo excepto los pies en una región de exclusión de regla, el sistema detectará a la persona y lanzará una alarma. En cambio, si una persona tiene todo el cuerpo excepto los pies en una región de exclusión de cámara, el sistema no detectará nada.

Las herramientas para pintar zonas de exclusión son las siguientes:

- La **herramienta rectángulo** nos permite definir áreas rectangulares en la pantalla. Se define la zona de exclusión haciendo clic con el ratón sobre la imagen de la cámara y arrastrando el ratón; soltando el botón del ratón terminaremos de definir el área sombreada.
- La **herramienta polígono** nos permite definir áreas sombreadas de forma poligonal. En este caso, debemos hacer clic con el ratón en los vértices del polígono hasta que volvamos a hacer clic en el primer vértice del polígono cerrándolo. El polígono se cierra y se rellena automáticamente definiendo un área sombreada.
- La **herramienta pincel** permite definir áreas sombreadas como si estuviésemos arrastrando un pincel por la pantalla mientras mantenemos apretado el botón izquierdo del ratón. Al seleccionar la herramienta pincel, aparece en la pantalla una ventana que permite modificar el grosor del pincel que estamos utilizando.

Otras opciones están disponibles en la misma ventana:

- El **botón Negro / Blanco** permite modificar el color de la región de exclusión entre negro o blanco. Solamente se usa para una mejor visualización de la misma; no afecta al comportamiento.
- El **control de acción** te permite definir si vas a usar las herramientas para definir la región de exclusión o para borrar una parte de ella. También puedes usar el botón **Borrar todo** para borrar toda la región que haya dibujada, o utilizar la opción “Otras ROEs” para escoger entre las ROEs que el equipo tenga definidas para otras cámaras y reglas.

## 4.2.12 Parámetros

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar” de la sección de Cámaras, seleccionar “Parámetros”, botón “Siguiente”)

Una vez se ha creado la cámara, se ha ajustado la perspectiva y se han creado las reglas, el equipo debería estar listo para detectar intrusos en el área especificada. La configuración estándar que se utiliza por defecto ha sido validada bajo condiciones climatológicas adversas en un gran número de escenas diferentes y debería satisfacer las necesidades del cliente sin necesidad de realizar ningún otro ajuste. Sin embargo, en algunas escenas con características muy concretas, podría ser que el nivel de falsas alarmas que proporcionara el sistema con la configuración estándar no cumpliera con el nivel de exigencia del cliente. En este caso, se puede tratar de reducir el nivel de falsas alarmas ajustando alguno de los parámetros que se presentan en la pantalla de configuración de parámetros.

**Parámetros (cam1)**

Configuraciones predefinidas

Extra sensible     Estándar     Muy filtrada

**DeepFusion**

Apariencia	bajo	<input type="range"/>	alto	4
Potenciar detecciones	si	<input type="range"/>	no	1
Animales	bajo	<input type="range"/>	alto	1

**Filtros avanzados**

Detección de intrusos	rápida	<input type="range"/>	fiable	5
Tamaño mínimo	bajo	<input type="range"/>	alto	2
Distancia	bajo	<input type="range"/>	alto	5
Tiempo	bajo	<input type="range"/>	alto	5
Movimiento oscilatorio	bajo	<input type="range"/>	alto	2
Objetos rápidos	bajo	<input type="range"/>	alto	3
Intensidad	bajo	<input type="range"/>	alto	7
Sabotaje	bajo	<input type="range"/>	alto	4

Aceptar    Cancelar

La primera vez que se entre en esta pantalla, el sistema mostrará los parámetros por defecto. La pantalla también presenta dos configuraciones típicas predefinidas que el usuario puede escoger en función de sus necesidades o las características de la escena. También se debe tener en cuenta que el filtro de sabotaje afectará exclusivamente a las reglas de sabotaje y que los únicos controles que afectan a las reglas de objeto abandonado u objeto robado son los filtros de intensidad y color.

**Atención:** El procedimiento de ajuste de los parámetros es crucial para conseguir su correcta configuración. Una mala selección de parámetros puede llevar al sistema a un funcionamiento inadecuado. Sigue atentamente las instrucciones de este manual.

### 4.2.12.1 Procedimiento de ajuste

Para ajustar las cámaras correctamente, el técnico deberá efectuar como mínimo dos visitas a la instalación del cliente.

En la primera visita el técnico deberá:

1. crear las cámaras
2. definir nuevas reglas o modificar las existentes para cada cámara
3. configurar la perspectiva y las regiones de interés de cada cámara

**Durante la primera visita, los parámetros de configuración de la cámara no deben modificarse a menos que sea necesario para garantizar detecciones en condiciones difíciles.**

En la segunda visita, como mínimo 24 horas después de la primera, el técnico deberá:

1. analizar las falsas alarmas que ha generado cada cámara desde la última visita
2. ajustar la configuración de las reglas para reducir el efecto de las falsas alarmas
3. ajustar los parámetros de configuración de la cámara si aún es necesario

A continuación se detallan cada uno de los pasos:

#### **Análisis de falsas alarmas**

Abrir el visor de alarmas y, por cada cámara, revisar las alarmas que ha generado el sistema desde la última visita. Es importante analizar las distintas causas que han generado falsas alarmas, agruparlas y anotar el número de falsas alarmas que hay de cada tipo. Se empezará a atacar primero el tipo de falsa alarma que haya generado más falsas alarmas.

#### **Ajuste de la configuración de las reglas**

La primera estrategia para reducir el número de falsas alarmas es ampliar la región de exclusión. Si la región donde se han producido falsas alarmas es una región que no nos interesa vigilar, se deberá eliminar con la región de exclusión del menú de configuración de reglas. Si las falsas alarmas se producen en una pared, seguramente también las podremos eliminar con la región de exclusión. Es importante recordar que la región de exclusión solo tiene en cuenta la posición de los pies de la persona o la parte inferior del vehículo, por lo tanto, mientras los pies de la persona no estén dentro de la región de exclusión, el sistema seguirá detectando la intrusión. En el caso concreto de una pared, es recomendable hacer llegar la región de exclusión hasta la altura de las rodillas de una persona. Otra posibilidad es que las falsas alarmas se produzcan en un lugar que se quiere vigilar, pero que para llegar a él se deba pasar necesariamente por una zona que está siendo vigilada por el sistema. En este caso, también se podría excluir la zona que produce falsas alarmas, dado que el sistema detectaría la intrusión antes que el intruso llegara a dicha zona.

Finalmente, si aún quedan falsas alarmas que no se han podido eliminar siguiendo esta estrategia, se deberá pasar al ajuste de los parámetros de configuración de la cámara.

## Ajuste de los parámetros de configuración de la cámara

Los fenómenos que pueden hacer que el sistema genere una falsa alarma son diversos. Así pues, también hay distintas estrategias para abordarlas. A continuación se definen a grandes rasgos los efectos que tiene cada barra de control sobre la capacidad de detección del sistema. En general, los controles en posiciones bajas harán el sistema más sensible y a la vez más propenso a dar falsas alarmas. Por lo contrario, los controles en posiciones altas harán que el sistema filtre más falsas alarmas, pero a la vez puede retrasar la detección de una intrusión.

### 4.2.12.2 Filtros de falsas alarmas

En general, estos controles son útiles para aumentar la fiabilidad de la detección y filtrar falsas alarmas provocadas por animales, árboles, viento, movimiento de la cámara, etc. Sin embargo, en algunos casos, pueden afectar la capacidad de detección del sistema. Por lo tanto, si se han modificado estos parámetros es importante asegurarse de que el sistema siga detectando correctamente cualquier tipo de intrusión.

Existen dos grupos de parámetros: **DeepFusion** y **Filtros avanzados**. Mientras que los **Filtros avanzados** están disponibles para toda nuestra gama de soluciones, los parámetros de **DeepFusion** solo están disponibles para la gama **DFUSION** y la gama Daview con funcionalidad **\_Xtension**.

En las soluciones **DFUSION** y **\_Xtension**, los parámetros **DeepFusion** deben ser la primera opción a la hora de ajustar el sistema.

#### 4.2.12.2.1 DeepFusion

La primera barra de control, **Apariencia**, regula cuánto dependerá el sistema de la apariencia de los objetos para generar una alarma. Cuanto más a la derecha, más evidencias necesitará el sistema de que el objeto es una persona o un vehículo para generar una alarma. En la posición más baja, el sistema sólo usará información de apariencia muy básica para tomar una decisión. En caso de tener falsas alarmas, para escenas en buenas condiciones (vista completa del objeto, escena abierta, bien iluminada con tiempo suficiente para observar el objeto), aumentar este control disminuirá el número de alarmas no deseadas sin comprometer la capacidad de detección del sistema. En caso de querer detectar objetos que se muevan de manera coherente durante algún tiempo sin tener en cuenta su apariencia, se debe establecer este filtro en la posición más baja.

**Advertencia:** por encima de la posición 7, si el sistema está procesando un flujo de vídeo de baja resolución, puede ignorar objetos muy pequeños en canales día/noche.

La segunda barra de control, **Potenciar detecciones** (solo disponible para DeepFusion), regula si los objetos que no han cumplido un criterio mínimo de tiempo o distancia pueden generar una alarma si su apariencia es similar a la de una persona o un vehículo. La activación de este control ayuda a detectar en condiciones difíciles. Por otro lado, si el sistema detecta constantemente un objeto como intruso cuando no lo es, se puede desactivar esta opción ya que el sistema podría estar malinterpretando el objeto como una persona o un vehículo. En caso de desactivar esta opción, el técnico deberá asegurarse de que el sistema continúe detectando correctamente cualquier intrusión bajo cualquier posible condición.

La tercera barra, **Animales**, filtrará los objetos que tengan apariencia de animal. Una vez más, cuanto más a la derecha de la barra, más estricto será el sistema. Conviene distinguir el filtro de animales del **DeepFusion** del filtro de animales de **Filtros avanzados** en el

siguiente apartado. Mientras que el primero se basa en apariencia, como hemos dicho, el segundo utilizará criterios de medidas, según la perspectiva.

#### 4.2.12.2 Filtros avanzados

La primera barra de control, **Detección de intrusos**, regula la fiabilidad de las detecciones. Aumentando este control se le permite al sistema tener más tiempo para decidir si el objeto que está analizando es una persona, un vehículo o, por lo contrario, es una falsa alarma. Aumentar este control reduce directamente el número de falsas alarmas. En consecuencia, es una herramienta muy potente para luchar contra las falsas alarmas y, junto al filtro de distancia, debe ser la primera opción para cualquier técnico que se encuentre con un problema de falsas alarmas. En estos casos, es recomendable situar el filtro entre la posición 15 y la 18. Si una vez situado el control en esta posición se siguen teniendo falsas alarmas y se observa que al sistema aún se le podría dar más tiempo para decidir, se puede situar el control en la posición 19 o 20, pero solo de forma excepcional. Por el contrario, si lo que se desea es que el sistema detecte más rápido, se puede llegar a situar el control en la posición 13 o 14. Para infraestructuras críticas, instalaciones con cámaras térmicas o cualquier otro entorno de alta seguridad con intrusiones difíciles (por ejemplo, intrusos arrastrándose u otras situaciones parecidas), se recomienda ajustar el control a la posición 5, y, solo en circunstancias excepcionales, a los valores alrededor de 2.

La segunda barra de control de este grupo, **Filtro de animales** (también llamado **Tamaño mínimo** en canales DFUSION), está especialmente pensada para eliminar falsas alarmas provocadas por pequeños animales (gatos, perros, etc.) o cualquier otro tipo de objeto pequeño que se desplace por el suelo (bolsas de plástico, papeles, etc.). Cuanto más alto se sitúe el control, más grandes respecto al tamaño de una persona serán las falsas alarmas que el sistema tendrá capacidad de filtrar. En caso de que haya falsas alarmas provocadas por gatos o perros, es recomendable situar la barra de control en la posición 3 o 4.

El **filtro de tamaño máximo** solo está disponible para cámaras térmicas. Permite filtrar objetos según su tamaño. Cuánto más alta sea la posición del filtro, menores serán los objetos detectados por el sistema. En caso de tener falsas alarmas provocadas por objetos grandes como aviones o camiones, se recomienda mover el filtro a una posición más alta.

La tercera barra de control, **filtro de distancia**, regula la distancia mínima que debe moverse un objeto antes de que el sistema detecte una intrusión. Si se aumenta el filtro de distancia, un objeto deberá recorrer más distancia antes de que el sistema detecte una intrusión. Para calcular la distancia, el sistema tiene en cuenta la perspectiva de la escena. Este filtro es útil para filtrar falsas alarmas producidas por árboles, viento, leves movimientos de la cámara, sombras, etc. En caso de tener falsas alarmas de este tipo, se recomienda situar este filtro en la posición 9 o 10. A estas posiciones al objeto se le exigirá haber recorrido como mínimo dos metros antes de ser detectado. En escenas con muchas oclusiones, con poca iluminación o poco contraste, se recomienda situar la barra de control entre los valores 4 y 7. Si se tienen problemas de falsas alarmas y la zona a vigilar está despejada, se puede subir este control hasta la posición 11 o 12.

La cuarta barra de control, **filtro de tiempo**, regula indirectamente el tiempo que tardará el sistema a detectar una intrusión. Si se aumenta el filtro de tiempo, el sistema tardará más en detectar una intrusión. Este control puede ser útil para filtrar falsas alarmas de corta duración (1 o 2 segundos), como por ejemplo falsas alarmas producidas por cambios de iluminación, luces que se encienden o se apagan o luces de coches. Sin embargo, solo se debe tocar este parámetro en escenas abiertas donde el sistema tenga tiempo suficiente para detectar la intrusión. En cámaras muy cercanas o en cámaras donde los objetos estén muy poco tiempo en la escena, no es recomendable aumentar este parámetro, y en casos muy extremos donde se quieran detectar objetos que son visibles muy poco tiempo, se

recomienda situar este filtro en la posición 3 o 4. Situando este control en la posición 10, aproximadamente se le exigirá al objeto haber estado en la escena como mínimo dos segundos. Si se tienen problemas de falsas alarmas se puede llegar a situar este control a la posición 12 o 13.

El **filtro de movimiento oscilatorio** está activado por defecto en la configuración y está especialmente diseñado para filtrar pequeños movimientos oscilatorios como los que puede producir la rama de un árbol moviéndose por el viento. Este filtro solo se debe desactivar en casos excepcionales donde se desee que el sistema detecte muy rápidamente cualquier objeto que entre en la escena, como por ejemplo en cámaras muy cercanas con personas o vehículos moviéndose muy rápido y que son visibles durante muy poco tiempo. Si se desactiva este filtro, el nivel de falsas alarmas del sistema subirá.

La siguiente barra de control, **Filtro de objetos rápidos**, no deberá tocarse en la gran mayoría de escenas típicas de videovigilancia. Solamente deberá aumentarse ligeramente en escenas donde los objetos se desplacen muy rápidamente, o en escenas donde los objetos estén muy próximos a la cámara y su tamaño ocupe una parte significativa de la imagen (por ejemplo si un coche ocupa más de la mitad de la imagen). En estos casos se deberá situar el control en la posición 1 o 2. Este control no está pensado para regular el nivel de falsas alarmas del sistema, sin embargo, aumentarlo sin necesidad puede provocar un aumento de falsas alarmas.

El siguiente control afecta a la capacidad del sistema de filtrar cambios de **intensidad** y afecta indistintamente a cámaras en color y a cámaras en blanco y negro. Este filtro se aumentará cuando el sistema detecte falsas alarmas en escenas donde aparentemente no hay ningún objeto en movimiento y no se detecte ninguna distorsión de color, o cuando se observe que la cámara es muy ruidosa (por ejemplo, de noche). En este caso se puede subir el filtro hasta la posición 9. Es posible que, al aumentar el filtro de intensidad, en zonas oscuras, las personas o los vehículos no queden recuadrados en su totalidad. Si observas este efecto, disminuye un poco el nivel de filtrado hasta encontrar el punto óptimo en el que los objetos se recuadran de forma entera pero no se generan falsas alarmas. En cámaras muy oscuras también puede suceder que con la configuración por defecto el sistema no recuadre enteramente a la persona o vehículo. En este caso, se puede disminuir el filtro hasta la posición 5 o 4. Solo en casos extremos donde se necesite una sensibilidad máxima se debe llegar a las posiciones 2 o 3.

El **filtro de color** afecta a la capacidad del sistema de filtrar cambios de color en la imagen. Consecuentemente, este control no tiene ningún efecto en cámaras en blanco y negro, o en cámaras en color en modo noche. Se aumentará este filtro cuando el sistema detecte falsas alarmas en escenas donde aparentemente no hay ningún objeto en movimiento y la cámara no se mueva por el viento. Si observando atentamente la falsa alarma se detectan distorsiones de color (normalmente tonos amarillos, verdes, azules o rosas), deberemos aumentar el filtro de color (por ejemplo hasta la posición 7 u 8). Si por el contrario, se ha aumentado demasiado el filtro de color, se observará que los vehículos o personas que antes el sistema recuadraba correctamente pasan a no recuadrarse completamente. En este caso, disminuye un poco el filtro de color.

El **filtro de sabotaje** regula la sensibilidad de detección de la regla de sabotaje. Se considerará un sabotaje cualquier cambio significativo en la imagen que se prolongue durante el tiempo especificado. Una alarma de sabotaje puede ser producida tanto por un objeto que tape el objetivo de la cámara como por un desplazamiento significativo del objetivo. En caso de que la regla de sabotaje genere falsas alarmas (por ejemplo, por cambios de iluminación) deberá desplazar el filtro de sabotaje hacia la derecha.

La última barra del control, el **Estabilizador de cámara**, activará o desactivará el estabilizador de cámara. Aparece únicamente en la solución Long Range, y su utilización

aumenta la capacidad de detección en larga distancia y reduce las falsas alarmas causadas por la vibración de la cámara.

#### **4.2.12.3 Configuraciones predefinidas**

Juntamente con la posibilidad de ajustar algunos parámetros para reducir el número de falsas alarmas, el sistema también le proporciona la opción de escoger entre tres configuraciones predefinidas.

##### **Configuración estándar**

Esta configuración es la que llevan todas las cámaras por defecto. Es una configuración validada en una gran cantidad de escenarios distintos y debería satisfacer los requerimientos del cliente en la mayoría de situaciones.

##### **Extra sensible**

Esta configuración está pensada para cámaras más o menos cercanas, que enfocan a la calle. Al ser una cámara cercana donde los vehículos están poco tiempo presentes en la escena, se ha aumentado la tolerancia en el seguimiento de objetos, y como no interesa diferenciar entre personas y vehículos se ha activado la detección rápida para la regla Intruso. También se asume que no habrá demasiada vegetación o que esta podrá ser anulada con una región de exclusión o con una barrera virtual. En consecuencia, se ha hecho la detección de intrusos más rápida y se ha desactivado el filtro de movimiento oscilatorio. Es una configuración muy sensible.

##### **Muy filtrada**

La tercera configuración predefinida es la más indicada para entornos de poca actividad y con buen contraste de cámara. Es la más indicada para escenas abiertas con poca actividad, que permiten un tiempo de detección mayor.

#### 4.2.12.4 Guía rápida de solución de problemas

La tabla que se muestra a continuación pretende ser una guía rápida para técnicos que necesitan solucionar problemas de falsas alarmas o que necesitan ajustar la rapidez de la detección. A continuación se listan un conjunto de problemas habituales y la estrategia que se debe seguir para solucionarlos.

Problema	Solución
El sistema genera falsas alarmas en sitios donde no se mueve nada. Se observan pequeñas <b>distorsiones de color</b> .	Sube el filtro de color al nivel 6 u 7. Si se siguen generando falsas alarmas, súbelo hasta el nivel 8 o 9.
En una cámara en color, el sistema genera falsas alarmas alrededor de <b>contornos</b> de objetos en sitios donde no se mueve nada. Por ejemplo, en el tronco de un árbol, en una farola o en el palo de una señal de tráfico.	Sube el filtro de color al nivel 6 o 7. Si se siguen generando falsas alarmas, aumentalo hasta el nivel 8 o 9.
En una cámara en blanco y negro se generan falsas alarmas en sitios donde no se mueve nada. Mirando atentamente la imagen, se observa <b>ruido</b> en la imagen.	Sube el filtro de intensidad al nivel 8. Si siguen apareciendo falsas alarmas, aumentalo hasta el nivel 9 o 10.
Después de aumentar el filtro de color o intensidad, el sistema no recuadra correctamente a los objetos o tiene problemas de detección en ciertas zonas de la imagen.	Disminuye el filtro que se había modificado. Encuentra el punto óptimo entre calidad de la detección y falsas alarmas.
El sistema no recuadra correctamente a las personas en <b>zonas muy oscuras</b> o con poco contraste.	Disminuye el filtro de intensidad hasta el nivel 5 o 4.
El sistema detecta falsas alarmas en <b>árboles</b> movidos por el viento.	Aumenta la detección de intrusos hasta el nivel 16 o 17. Aumenta también el filtro de distancia hasta el nivel 7 o 8. Asegúrate de que el filtro de movimiento oscilatorio esté activado.
El sistema detecta falsas alarmas por <b>luces de coches</b> que no están en la escena.	Aumenta el filtro de tiempo hasta el nivel 8 o 9, o usa solo la regla de persona.
El sistema detecta <b>insectos</b> delante de la cámara.	Aumenta la detección de intrusos hasta el nivel 16 o 17. Si es posible, usa solo reglas de persona.
El sistema detecta los objetos tarde, cuando están a punto de salir de la imagen.	Disminuye la detección de intrusos hasta el nivel 12 o 13. Si no es suficiente, baja la detección de intrusos al nivel 4 o 5. Aumenta el filtro de objetos rápidos hasta el nivel 4 o 5. Si el problema persiste, sitúa el filtro de tiempo a la posición 2 y mueve el filtro de movimiento oscilatorio a la posición 0.

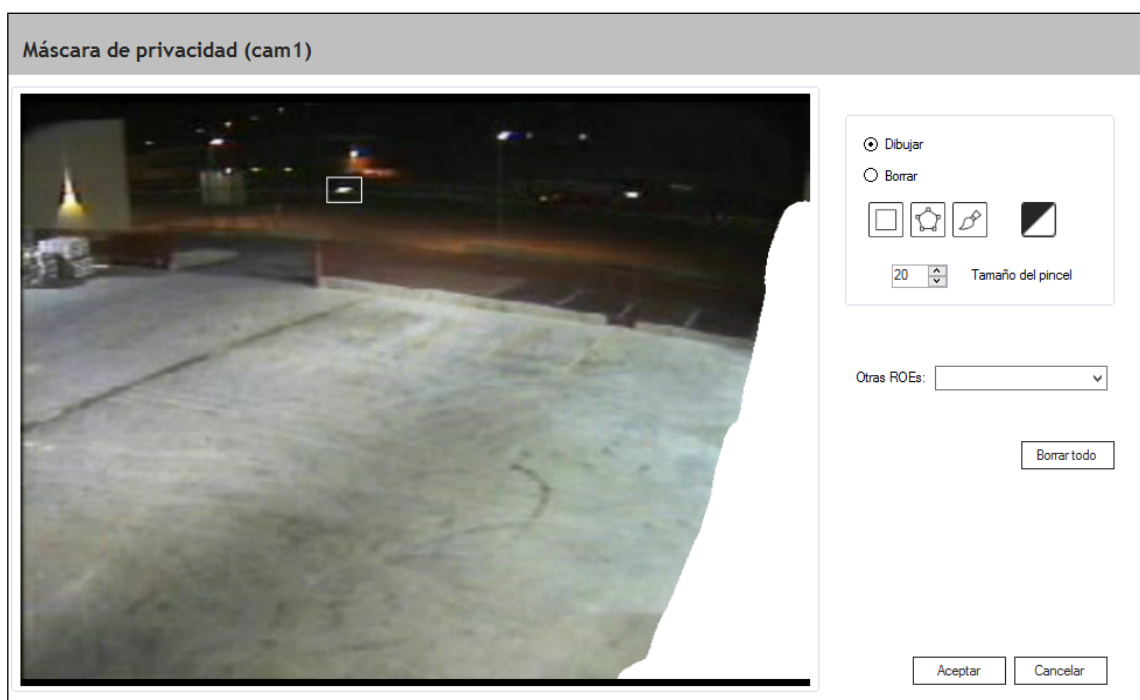


El sistema detecta falsas alarmas por culpa de <b>sombras</b> de árboles proyectadas en el suelo.	Aumenta el filtro de distancia hasta la posición 9 o 10. Aumenta la detección de intrusos hasta el nivel 16 o 17 y aumenta el filtro de animales hasta el nivel 4.
La <b>imagen se mueve</b> o aparece <b>distorsionada</b> . Presencia de interferencias o problemas de sincronismo.	Fija bien la cámara, arregla los problemas de señal. Si no es posible, aumenta la detección de intrusos al nivel máximo que permita la escena.
El sistema detecta gatos, perros u otros <b>animales</b> .	Aumenta el filtro de animales hasta el nivel 3 o 4.
El sistema detecta falsas alarmas cuando hay un cambio de iluminación debido a las <b>nubes</b> .	Aumenta el filtro de intensidad. Sitúa el control al nivel 8 o 9.
El sistema detecta falsas alarmas en una <b>piscina</b> .	Si es posible, excluye la piscina de la zona de detección. Aumenta el filtro de distancia hasta la posición 7, 8 o 9, y aumenta la detección de intrusos hasta el nivel 16 o 17.
El sistema detecta falsas alarmas por culpa de los <b>aspersores</b> .	Usa reglas solo de persona o solo de vehículo, si es posible. Aumenta la detección de intrusos hasta el nivel 16, 17 o 18.
El sistema detecta falsas alarmas cuando se enciende o se apaga una <b>farola</b> .	Intentar excluir la farola con la zona de exclusión. Si no es posible, aumenta el filtro de tiempo hasta la posición 6, 8 o incluso 10. Si es posible, aumenta el filtro de intensidad hasta el nivel 8 o 9.
El sistema no detecta en zonas aparentemente sencillas.	Revisa las regiones de exclusión, tanto la de la cámara como las de las reglas.
El sistema no detecta la entrada/salida de una zona.	Asegúrate de que el objeto es visible antes y después de cruzar el perímetro. Comprueba que el sentido de cruce está correctamente configurado.
El sistema detecta <b>gotas de lluvia</b> en la cámara.	Si es posible, restringe las zonas de detección y evita el uso de la regla de intruso.
El sistema no detecta en <b>zonas muy lejanas</b> .	Valida que la perspectiva esté bien configurada. Si la zona donde no se detecta está por encima de la línea de horizonte, aumenta el zoom de la cámara.
El sistema detecta vehículos como personas o personas como vehículos.	Valida que la perspectiva esté bien configurada. Asegúrate de que el tamaño de las cajas se ajuste al de una persona en todas las partes de la imagen. Si la perspectiva está bien configurada, aumenta la detección de intrusos hasta la posición 17, 18 o 19.
Los cambios de iluminación producen falsas <b>alarmas de sabotaje</b> .	Desplaza el filtro de sabotaje una o dos posiciones hacia la derecha.
Los camiones cuando pasan por delante de la cámara generan falsas <b>alarmas de sabotaje</b> .	En la segunda pantalla de creación de la regla, aumenta el tiempo de detección de sabotaje.

### 4.2.13 Máscara de privacidad

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar” de la sección de Cámaras, seleccionar “Privacidad”, botón “Siguiente”)

El objetivo de la máscara de privacidad es excluir las áreas de la cámara que el operador no puede ver por razones de privacidad. Estas áreas son analizadas por el sistema, pero las imágenes que se muestran al operador localmente o remotamente tendrán estas partes de la imagen pintadas en blanco.



### 4.2.14 Virtual IR

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar” de la sección de Cámaras, seleccionar “Virtual IR”, botón “Siguiente”)

Virtual IR<sup>®</sup> tan solo está disponible para cámaras específicas. Su finalidad es mejorar el contraste en una determinada región de la imagen. Esta región tiene forma elíptica y se conoce como Foco. Hay dos opciones disponibles (posición del Foco: Manual/Auto):

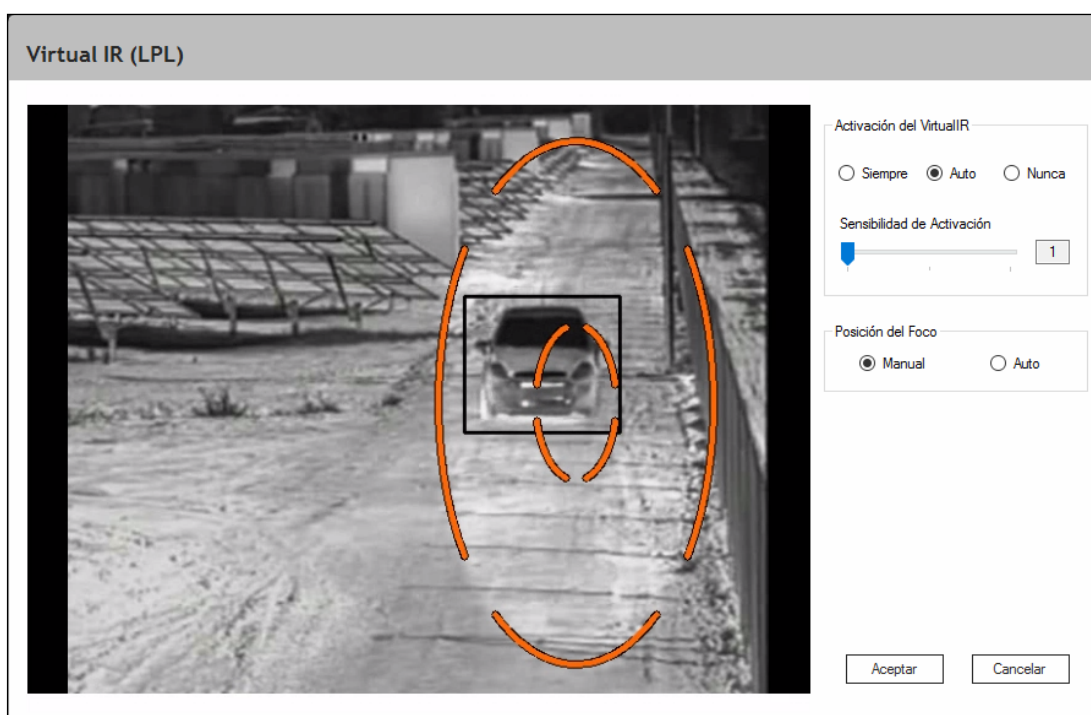
- **Manual:** el usuario puede dibujar libremente el Foco elíptico.
- **Auto:** el sistema propone de forma automática el Foco teniendo en cuenta la perspectiva de la escena, así como la ROE de cámara y las ROEs de las reglas de intrusión. Para usar el modo Auto, es imprescindible que se haya definido primero la perspectiva.

Virtual IR<sup>®</sup> viene activado por defecto en el modo Activación del Virtual IR: Auto. Vale la pena mencionar que en esta opción el efecto del Virtual IR<sup>®</sup> depende de los valores

térmicos dentro del Foco. Es posible, por tanto, que dicho efecto no sea evidente en algún momento. Sin embargo, cuando las condiciones térmicas (intensidad de la imagen) sean favorables, tales efectos resultaran gradualmente visibles.

Si queremos forzar que Virtual IR ® esté siempre activo, independientemente de las condiciones térmicas, podemos usar el modo Activación del Virtual IR: Siempre. Por el contrario, si no queremos usar esta herramienta en ningún caso, podemos poner el modo Activación del Virtual IR: Nunca.

En el caso que seleccionemos el modo Activación del Virtual IR: Auto tenemos, además, la posibilidad de especificar el grado de sensibilidad con la cual el Foco se activa, mediante la barra de progreso Sensibilidad de Activación yendo de izquierda a derecha, de menos sensible a más, respectivamente.



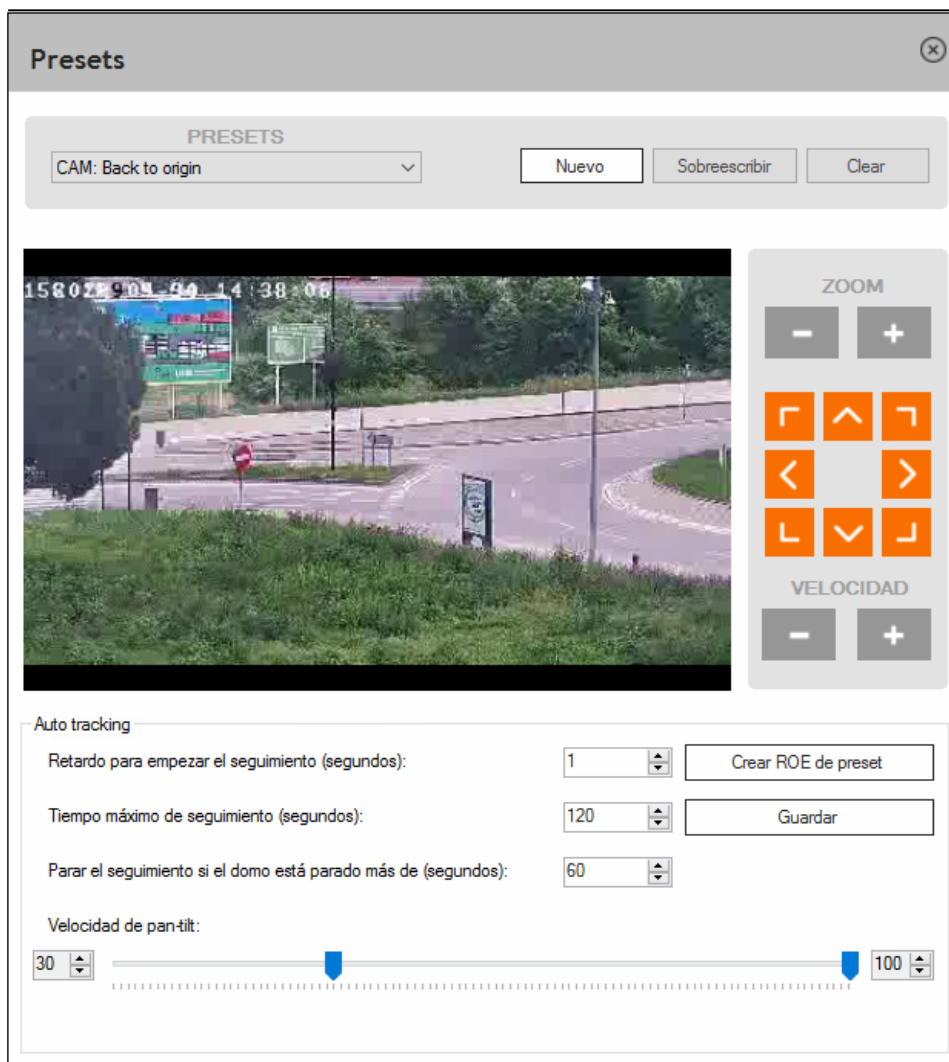
#### 4.2.15 Posicionamientos PTZ

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Presets”.*

*Si la característica de Autotracking está disponible, desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara, botón “Ajustar”, selecciona “Presets”, “Siguiente”)*

**Atención:** Autotracking es una característica opcional y solo está disponible en ciertas soluciones.

La ventana Presets te permite definir varios posicionamientos o presets de una cámara creada del tipo SmartPTZ o ATKPRO. Estos presets se utilizarán para mover y hacer zoom a la cámara PTZ cuando una cámara fija con análisis detecte un evento. Este evento contará con 2 vídeos asociados: uno proveniente de la cámara fija que ha generado la alarma y otro, para facilitar la verificación del primero, generado por la cámara PTZ.



Puedes mover la posición de la cámara usando las siguientes opciones:

- **Las flechas:** para mover hacia arriba, abajo, izquierda, derecha, arriba-izquierda, arriba-derecha, abajo-izquierda o abajo-derecha.
- **Zoom:** para acercar o alejar.
- **Velocidad:** puedes optar por graduar la velocidad de movimiento del domo al utilizar las flechas de dirección.

Una vez elegida la posición correcta del posicionamiento, y siempre que la cámara sea compatible con esta opción, puedes pulsar **Nuevo**, introducir un nombre para este preset y pulsar el botón **Guardar** para guardar el preset.

Si quieres modificar un preset ya establecido, elige el nombre del preset del desplegable, sitúate en la nueva posición y utiliza el botón **Sobrescribir** para guardar la nueva posición con el mismo nombre.

Si quieres eliminar un preset ya creado, elige el nombre del preset del desplegable y pulsa el botón **Borrar**.

Asimismo, el sistema muestra tanto los presets creados por el usuario a través del software así como los creados internamente en la cámara. Los primeros se mostrarán con el prefijo "DAV:" mientras que los segundos, con "CAM:". El listado estará ordenado alfabéticamente, mostrando primero los creados a través del software.

Además, en las soluciones donde Autotracking esté disponible, en la sección de **Autotracking** se podrán configurar los siguientes parámetros:

- **Retardo para empezar el seguimiento:** tiempo de espera (en segundos) antes de empezar el seguimiento. Este tiempo empieza a contabilizar en el momento en que la cámara PTZ comienza a moverse a la posición de preset seleccionada. Está pensado para dar tiempo a la cámara a posicionarse en el preset deseado antes de que el Autotracking coja el control.
- **Tiempo máximo de seguimiento:** cancela el seguimiento si se supera el tiempo máximo de seguimiento.
- **Parar el seguimiento si el domo no se mueve más de:** cancela el seguimiento si la cámara PTZ ha estado estática durante este periodo de tiempo.
- **Velocidad de Pan-Tilt:** controla la velocidad mínima y máxima de movimiento de la cámara PTZ durante el seguimiento. La cámara PTZ se moverá a la velocidad mínima cuando el intruso esté cerca del centro de la imagen y más rápidamente a medida que se vaya alejando, llegando a la velocidad máxima cuando el intruso esté en los límites de la imagen. Si se pierde habitualmente el seguimiento de los objetos que se mueven rápidamente, se pueden aumentar las velocidades mínima y máxima. Si, en cambio, los movimientos de la cámara son demasiado bruscos, se pueden disminuir estas velocidades.

Dentro de la sección de Autotracking, también se puede configurar una región de interés para cada preset pulsando el botón **Crear ROE de preset**. Esta región sirve para definir el área de búsqueda de los objetos a seguir antes de iniciar el seguimiento, una vez la cámara ya se ha posicionado en el preset especificado. Una vez la cámara PTZ se mueve y comienza a seguir el intruso, esta región ya no se utiliza. La región de interés se define siguiendo la misma metodología que las otras áreas, marcándose con color las zonas excluidas. La región de interés se puede usar, por ejemplo, para excluir zonas externas al perímetro donde pueda haber objetos en movimiento que puedan distraer el seguimiento de un intruso en el interior del perímetro.

**Atención:** Para activar el Autotracking, marca la casilla "Habilitar Autotracking" a la respuesta de reglas (consulta la sección 0).

**Atención:** Para facilitar el proceso de configuración, mientras la ventana de **Presets** esté abierta el sistema ignorará las peticiones de posicionar preset o de Autotracking que vengan accionadas como respuesta a una regla.

## 4.2.16 Calibración del Zoom

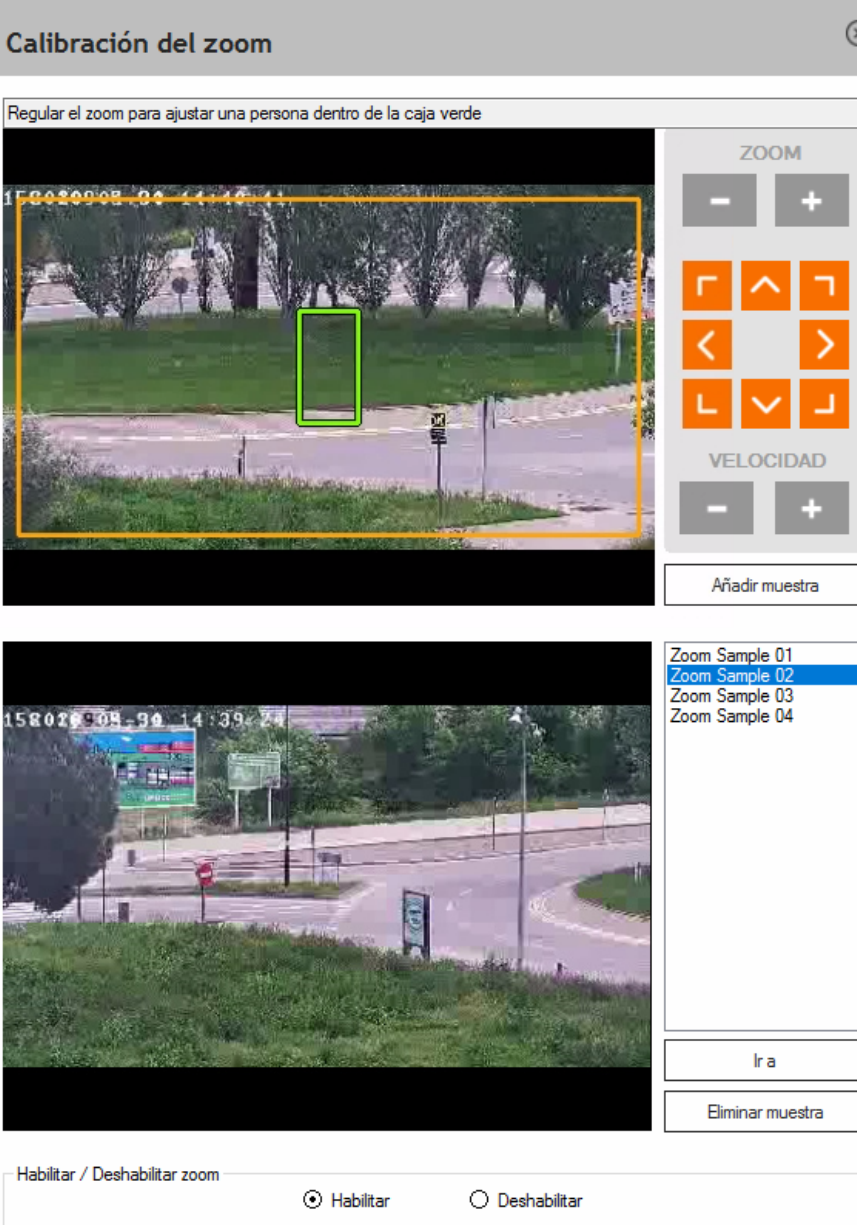
(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, selecciona una cámara ATKPRO, botón “Ajustar”, opción “Calibración del Zoom”)

**Atención:** Autotracking es una característica opcional y solo está disponible en ciertas soluciones.

Su finalidad es definir, de forma manual, el nivel de Zoom para un conjunto representativo de coordenadas Pan (eje horizontal) y Tilt (eje vertical), que cubran la escena de interés. De esta forma, cuando la PTZ siga un objeto de interés irá ajustando el nivel de Zoom de forma automática. Cabe tener en cuenta que dicha calibración es opcional. Así pues, si se omite este paso o si se deshabilita mediante el control en la parte inferior de la pantalla, la PTZ tan solo aplicará Pan y Tilt para el seguimiento, pero no Zoom.

### Calibración del zoom

Regular el zoom para ajustar una persona dentro de la caja verde



ZOOM

VELOCIDAD

Añadir muestra

Zoom Sample 01  
Zoom Sample 02  
Zoom Sample 03  
Zoom Sample 04

Ir a

Eliminar muestra

Habilitar / Deshabilitar zoom

Habilitar  Deshabilitar

Para adquirir muestras de Zoom, mueve los controles PTZ para incluir (aproximadamente) una persona entera dentro del cuadro verde. Puedes mover la posición de la cámara usando las siguientes opciones:

- **Las flechas:** para mover hacia arriba, abajo, izquierda, derecha, arriba-izquierda, arriba-derecha, abajo-izquierda o abajo-derecha.
- **Zoom:** para acercar o alejar.
- **Velocidad:** puedes optar por graduar la velocidad de movimiento del domo al utilizar las flechas de dirección.

Una vez elegida la posición correcta, puedes guardar la muestra pulsando el botón **Añadir muestra**. Esta acción añadirá una entrada a la lista ("Zoom Sample XXX") y guardará una captura de imagen para más información. Puedes repetir este proceso tantas veces como haga falta.

También puedes seleccionar cualquier elemento de la lista de Muestras. Una vez seleccionada una muestra, la imagen asociada aparecerá en la ventana inferior y tendrás la posibilidad de mover la PTZ a la posición donde la muestra fue adquirida (botón **Ir a**) o bien eliminarla (botón **Eliminar muestra**).

Para calibrar correctamente el Zoom en una determinada escena, se deben añadir muestras de tal forma que se cubra, aproximadamente, toda la zona donde los posibles objetos a seguir se puedan mover.

**Atención:** Para facilitar el proceso de configuración, mientras la ventana de **Calibración de zoom** esté abierta, el sistema ignorará las peticiones de posicionar preset o de autotracking que vengan accionadas como respuesta a una regla.

#### 4.2.17 Vista conceptual

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón "Cámaras", introduce usuario/contraseña, "MENÚ", "CÁMARAS", botón "Varita mágica")*

La varita mágica situada en la esquina inferior izquierda de la ventana de cámaras abre la Vista conceptual. Presionándola una vez se hayan creado las cámaras y las reglas, se abre una nueva ventana que le permite ver y modificar algunas de las características principales de las cámaras y las reglas, así como tener una vista general de la instalación.

La Vista conceptual contiene varias pestañas, cada una de las cuales tiene diferentes opciones de configuración de cámara y/o regla. Todos los cambios realizados en una pestaña o subpestaña se guardan al presionar "Aceptar" o "Aplicar", pero si cambias una opción temporalmente en una pestaña, el cambio temporal se mantiene al cambiar a otra pestaña e incluso se refleja en las otras pestañas que hacen referencia a la misma información.

### 4.2.17.1 Reglas

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Varita mágica”, pestaña “Reglas”)

**Vista conceptual**

Reglas | Cámaras | CRA | Particiones | Relés

Regla	Cámara
Sabotaje	cam01
Sabotaje	cam1
Intruso	cam1

Respuesta | **ROEs**

**Alarma**

- Notificación a la CRA
- Generar alarma
- Guardar vídeo
- Remarcar objetos en los videos
- Remarcar objetos en directo
- Hot spot

Gravedad: 1

Retardo de desactivación (seg): 0

**Reproducir sonido**

- Habilitar
- Repetir sonido hasta aceptar alarma
- Altavoz PC
- Fichero

**SmartPTZ**

- Habilitar
- Camera: [dropdown] Preset: [dropdown]
- Habilitar Auto-Tracking Back to preset: [dropdown]

**Accionar relé**

- Habilitar
- Dispositivo: [dropdown] Relé: [dropdown]
- Aplicar retardo de desactivación:  Sí  No
- Tiempo máximo de activación: 30

**Enviar correo electrónico**

- Habilitar
- Para: [input]
- Asunto: [input]
- Mensaje: [text area]

**HTTP**

- Habilitar
- URL: [input] [Test]
- Usar autenticación  Basic  Digest
- Usuario: [input]
- Contraseña: [input]

Aceptar | Aplicar | Cancelar

En la primera pestaña, “**Reglas**”, puedes acceder a la última ventana de la configuración de cada regla (explicada anteriormente) y a la ventana de configuración de tu ROE (región de exclusión) a través de la subpestaña “ROEs”. La funcionalidad de estas ventanas se ha explicado anteriormente en sus respectivas secciones.



### 4.2.17.2 Cámaras

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Varita mágica”, pestaña “Cámaras”)

En la segunda pestaña, “Cámaras”, puedes acceder a la ventana de configuración de los parámetros de la cámara y a la región de exclusión de cámara (ROEs).

**Vista conceptual**

Reglas **Cámaras** CRA Particiones Relés

**Cámara**

cam01  
cam1

**Parámetros** ROEs

Configuraciones predefinidas

Extra sensible  Estándar  Muy filtrada

Filtros avanzados

Detección de intrusos	rápida		fiable	5
Animales	bajo		alto	2
Distancia	bajo		alto	5
Tiempo	bajo		alto	5
Movimiento oscilatorio	bajo		alto	2
Objetos rápidos	bajo		alto	3
Intensidad	bajo		alto	7
Color	bajo		alto	4
Sabotaje	bajo		alto	4

Aceptar Aplicar Cancelar

### 4.2.17.3 CRA

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Varita mágica”, pestaña “CRA”)

En la tercera pestaña, “CRA”, hay dos listas. La lista de la izquierda contiene las reglas que *NO envían* la alarma a la CRA y la de la derecha las reglas que *SÍ la envían*. Esta ventana permite modificar el comportamiento de la regla arrastrándola de una lista a otra.

**Vista conceptual**

Reglas | Cámaras | **CRA** | Particiones | Relés

No envían		Envían	
Regla	Cámara	Regla	Cámara
		Sabotaje	cam01
		Sabotaje	cam1
		Intruso	cam1

Aceptar | Aplicar | Cancelar

#### 4.2.17.4 Particiones

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Varita mágica”, pestaña “Particiones”)

La cuarta pestaña, “**Particiones**”, está dividida en 9 listas que representan las 9 posibles particiones aceptadas por el sistema: desde “Sin partición” hasta las 8 entradas externas representadas por la “Partición 1” a la “Partición 8”. Las reglas se muestran en su correspondiente partición, la cual se puede modificar arrastrando cada regla de una partición a otra.

**Vista conceptual**

Reglas Cámaras CRA **Particiones** Relés

Sin Partición		Partición 1		Partición 2	
Regla	Cámara	Regla	Cámara	Regla	Cámara
		Sabotaje	cam01		
		Sabotaje	cam1		
		Intruso	cam1		

Partición 3		Partición 4		Partición 5	
Regla	Cámara	Regla	Cámara	Regla	Cámara

Partición 6		Partición 7		Partición 8	
Regla	Cámara	Regla	Cámara	Regla	Cámara

Aceptar Aplicar Cancelar

#### 4.2.17.5 Relés

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “CÁMARAS”, botón “Varita mágica”, pestaña “Relés”)

La pestaña “**Relés**” también está dividida en 9 listas que representan los 9 casos posibles de activación de relés aceptados por el sistema. Desde “Sin relé” hasta los relés representados por “Relé 1” hasta “Relé 8”. Igual que en las pestañas anteriores, las reglas se muestran en su correspondiente lista. Para modificar el relé que activa cada regla se debe arrastrar la regla de una lista a otra.

**Vista conceptual**

Reglas Cámaras CRA Particiones **Relés**

Sin relé		Relé 1		Relé 2	
Regla	Cámara	Regla	Cámara	Regla	Cámara
Sabotaje	cam01				
Sabotaje	cam1				
Intruso	cam1				

Relé 3		Relé 4		Relé 5	
Regla	Cámara	Regla	Cámara	Regla	Cámara

Relé 6		Relé 7		Relé 8	
Regla	Cámara	Regla	Cámara	Regla	Cámara

Aceptar Aplicar Cancelar

### 4.3 ASISTENCIA

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Asistencia”, introduce usuario/contraseña)*

Para permitir el acceso remoto al equipo, debes hacer clic en el botón **Asistencia** y, a continuación, hacer clic en **Autorizo a conectarse al equipo remotamente para tareas de mantenimiento** y facilitar a tu interlocutor el código proporcionado en pantalla.

### 4.4 APAGAR

*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Apagar”, introduce usuario/contraseña)*

Aparecerá un menú con tres opciones:

- **Reiniciar:** cerrar e iniciar el servidor de forma automática.
- **Apagar:** para detener completamente el equipo. No volverá a estar activo hasta que se vuelva a iniciar el equipo manualmente.
- **Cancelar:** cerrar la ventana de opciones de apagado y volver a la pantalla principal del sistema.

## 5 ALARMAS

### 5.1 BUSCADOR DE ALARMAS

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)

El visor de alarmas te permite visualizar eventos o alarmas detectadas por el sistema. El sistema guarda unos segundos/minutos cuando se genera una alarma y posteriormente desde el visor de alarmas se puede buscar y reproducir esta grabación.

El visor de alarmas se puede abrir a través del menú o haciendo doble clic en la alarma que quieras que se muestre en la lista de alarmas recientes.

El visor de alarmas tiene el siguiente aspecto:

Visor de alarmas

Cámara: Todas las cámaras | Evento: Todos los eventos | Regla: Todas las reglas

Desde el: April de 2020 (29) | Hasta el: April de 2020 (29)

0:00:00 | 23:59:59

Gravedad: 1

Fecha	Cámara	Evento	Regla	Gravedad
0				

Proteger | Elimina | Exporta | Aceptar alarma | Cerrar

#### 5.1.1 Buscador de alarmas

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)

Por defecto, los menús de filtrado se encuentran en posición **Todos/Todas**, lo cual indica que no realizarán ningún filtrado y que seleccionarán las incidencias de todas las cámaras, de todos los eventos y de todas las reglas.

Los filtros disponibles en el buscador de alarmas son los siguientes:

- **Cámara:** selecciona una cámara del desplegable si deseas ver únicamente las alarmas de esa cámara específica.
- **Evento:** selecciona un evento si deseas ver únicamente alarmas de un tipo determinado.
- **Regla:** selecciona una regla si deseas ver únicamente las alarmas generadas por una regla específica de detección.
- **Desde el:** introduce fecha y hora para filtrar por calendario. El sistema no mostrará alarmas previas a la fecha y hora introducidas.
- **Hasta el:** introduce fecha y hora para filtrar por calendario. El sistema no mostrará alarmas posteriores a la fecha y hora introducidas.
- **Gravedad:** modifica el nivel de gravedad si deseas ver únicamente alarmas con nivel de gravedad igual o superior al especificado. Las alarmas con inferior gravedad de la seleccionada no se mostrarán en la búsqueda.

Una vez haya configurado todas las opciones de filtrado de alarmas, presiona el botón **Buscar** para iniciar la búsqueda.

**Atención:** Si la búsqueda encuentra más de 1.000 alarmas, el sistema mostrará únicamente las 1.000 primeras de la búsqueda (empezando por las más recientes).

La información disponible para cada alarma es la siguiente:

<b>Fecha</b>	Fecha y hora en la cual la incidencia fue detectada.
<b>Cámara</b>	Nombre de la cámara dónde se detectó la incidencia.
<b>Regla</b>	Nombre de la regla que generó la alarma.
<b>Evento</b>	Tipo de evento definido en la regla (detección de persona, vehículo, intruso, movimiento, sabotaje, etc.).
<b>Gravedad</b>	Gravedad de la alarma.

### 5.1.2 Acciones de alarmas

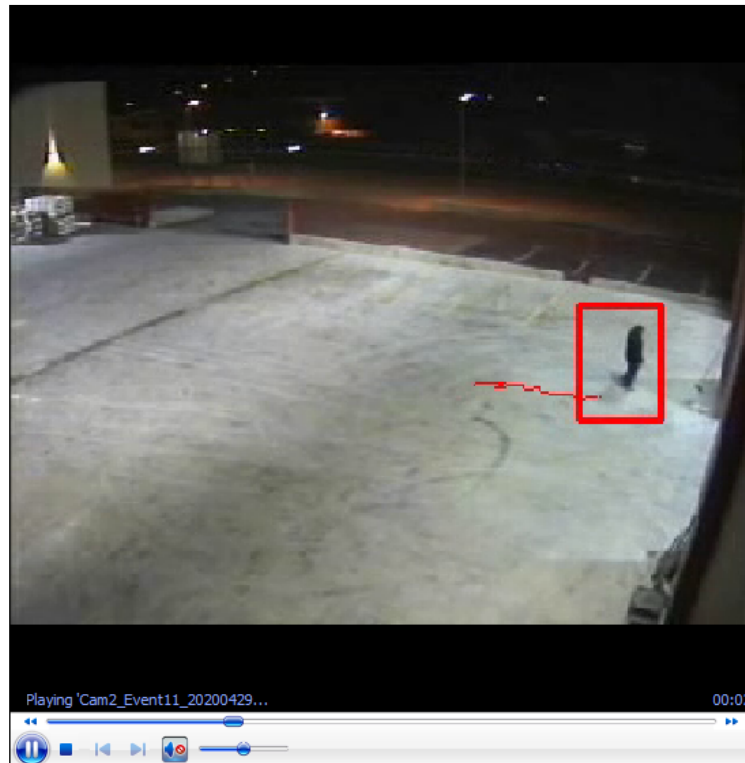
*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)*

#### 5.1.2.1 Mostrando una alarma

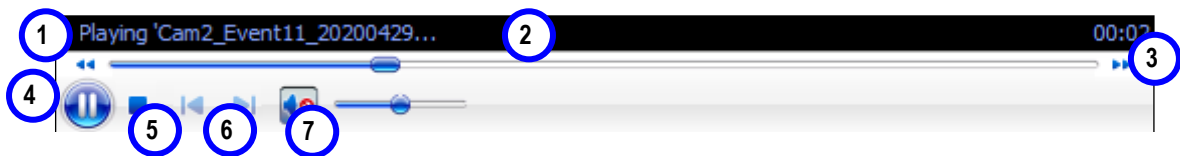
*(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)*

Para visualizar una alarma, haz clic en el listado de incidencias/alarmas encontradas (6). En el visor se mostrará la imagen del momento de la detección. Para ver el vídeo de la incidencia, haz doble clic sobre el listado de alarmas o sobre el visor de vídeos.

El visor de vídeos comenzará a reproducir el vídeo de la alarma.



Utiliza los controles del panel de vídeo para reproducir el vídeo:



1. **Botón de retroceso rápido:** equivalente a la tecla de rebobinado de un reproductor estándar. Reproduce las imágenes a cámara rápida y marcha atrás.
2. **Barra de posicionamiento:** permite situarse en un momento dentro del vídeo de forma instantánea. Haz clic y arrastra la barra para posicionarte dentro del vídeo.
3. **Botón de avance rápido:** equivalente a la tecla de avance rápido de un reproductor estándar. Reproduce las imágenes a cámara rápida.
4. **Botón de reproducción:** inicia o pausa la reproducción del vídeo seleccionado.
5. **Botón de parada:** detiene la reproducción del vídeo seleccionado.
6. **Botones de anterior y siguiente vídeo:** desactivados en esta aplicación.
7. **Teclas de volumen:** desactivadas en esta aplicación.

**Repetición continua de vídeo:** para visualizar repetidamente una secuencia de vídeo o incidencia, selecciona la opción **“Repetir vídeo”** debajo del visor de vídeos. La misma secuencia se visualizará indefinidamente hasta que cierres el visor de vídeos o deselecciones esta opción.



### 5.1.2.2 Otras acciones

(¿Cómo se llega a esta pantalla? Desde la pantalla principal, haz clic en el botón “Cámaras”, introduce usuario/contraseña, “MENÚ”, “ALARMAS”)

Los siguientes botones están disponibles para realizar otras acciones:



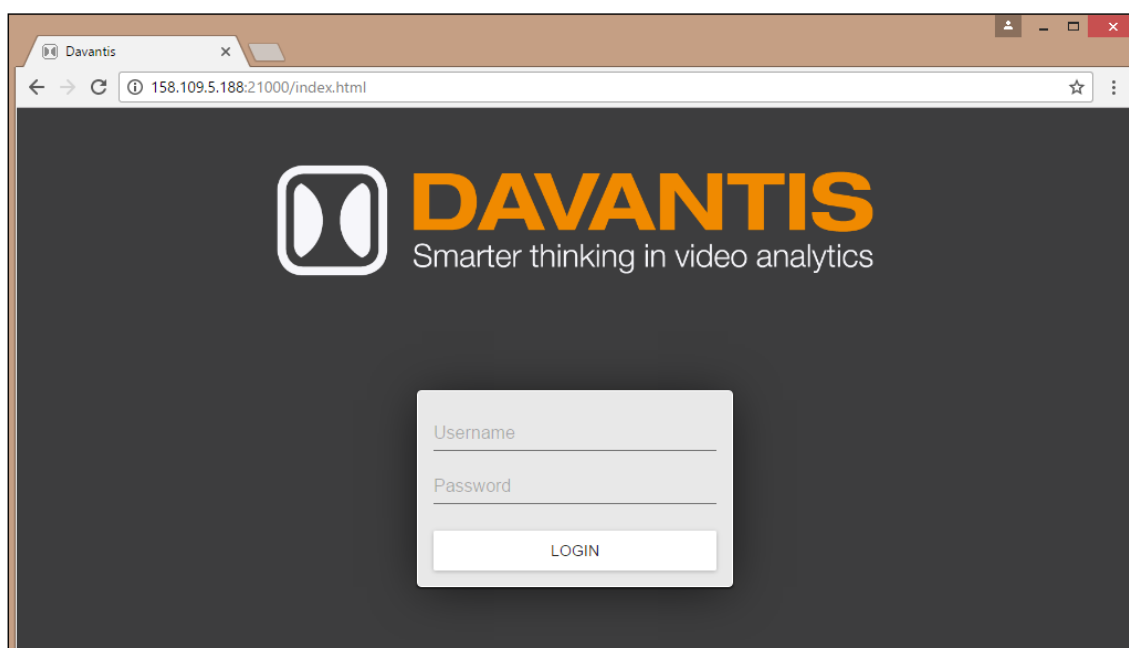
- **Exportar lista de alarmas:** para exportar la lista de alarmas de la búsqueda actual a un fichero .csv, presiona el botón de la esquina inferior izquierda y selecciona la ubicación de destino del fichero.
- **Proteger:** el personal de vigilancia tiene la opción de proteger alarmas de especial interés. Cuando seleccionas una alarma y pulsas el botón **Proteger**, esta alarma se define como una “Alarma protegida” marcada en amarillo y tendrá una consideración especial ya que su tiempo de vida máximo podrá ser diferente de las otras alarmas.
- **Elimina:** para eliminar una alarma del sistema, selecciona la alarma que deseas eliminar y pulsa el botón **Elimina**. Esa alarma se eliminará automáticamente de la lista de alarmas junto con la foto y el vídeo del evento.
- **Exporta:** para exportar un vídeo de una alarma, inserta una memoria USB en un puerto USB libre del equipo, selecciona la alarma de la lista y pulsa el botón **Exporta**. Hay dos formas de exportar una alarma: (1) **Alarma completa firmada:** un fichero binario .sig se exportará junto al fichero del vídeo para verificar la autenticidad del vídeo. Este proceso se usa para proteger el vídeo de copia, manipulación o fraude. (2) **Solo vídeo:** para exportar el fichero del vídeo únicamente. Al pulsar el botón, se abrirá una ventana de exploración de archivos para seleccionar la unidad USB y presionar **Guardar**.
- **Aceptar alarma:** las alarmas se muestran en **ROJO** cuando no han sido validadas y en **NEGRO** cuando lo han sido. Validar una alarma significa confirmar al sistema que la alarma ha sido visualizada por el personal responsable de la vigilancia. Para aceptar una alarma, selecciona la alarma que deseas aceptar, y presiona el botón **Aceptar alarma** para que la alarma sea automáticamente aceptada y se cambie a color negro. En caso de que las reglas tengan configurada la opción de “sonido y aceptación”, el sistema reproducirá el sonido hasta que el personal de seguridad acepte la alarma.

**ATENCIÓN:** Al eliminar una alarma, se perderán todos los datos de la alarma seleccionada. Solo los perfiles en modo administrador podrán realizar dicha acción.

## 6 ACCESO REMOTO WEB

La finalidad del acceso web remoto de los servidores es proporcionar a los clientes una herramienta rápida para ver cámaras en directo y alarmas recientes desde un navegador web.

Para acceder al web, abra un navegador (Google Chrome, Firefox o Internet Explorer 11) e introduzca en la barra de direcciones: `http://IP-pública:puerto-videos`. Por defecto el puerto web (vídeos) es el 21000 TCP. Este puerto debe estar abierto en el router para poder acceder desde internet. Por ejemplo: “`http://158.109.5.188:21000`”.



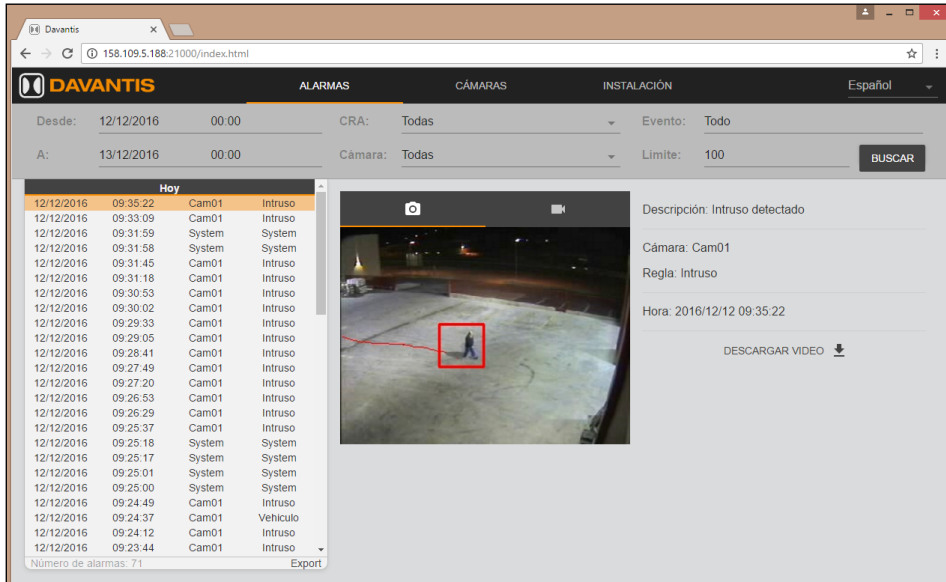
Introduce tu usuario y contraseña y haz clic en **Login**. Ten en cuenta que los usuarios y contraseñas serán los mismos que cuando se accede directamente al sistema.

Opciones disponibles:

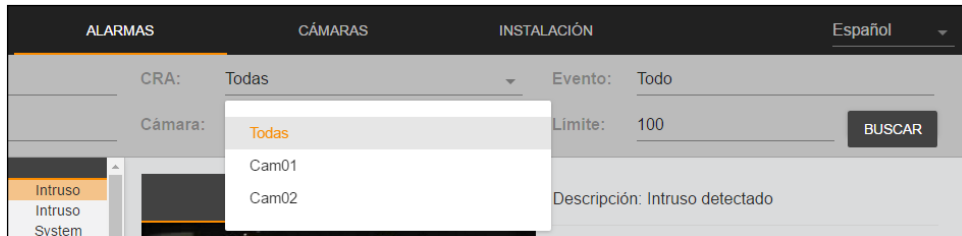
- ALARMAS: ver alarmas recientes usando un calendario y otros filtros.
- CÁMARAS: ver una cámara en directo o varias a la vez.
- INSTALACIÓN: muestra información básica de la instalación.

## 6.1 ALARMAS

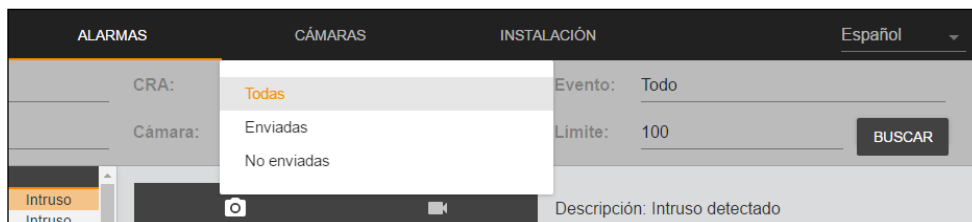
En la sección “Alarmas” se puede ver la foto y el vídeo de la alarma, normalmente 3 segundos antes y 7 después de la detección. Haz clic en la fecha para abrir el calendario, selecciona el periodo que deseas filtrar y, a continuación, haz clic en **Buscar**.



Para realizar una búsqueda por cámara, haz clic en el desplegable de cámaras, selecciona la cámara por la que deseas filtrar y haz clic en **Buscar**:



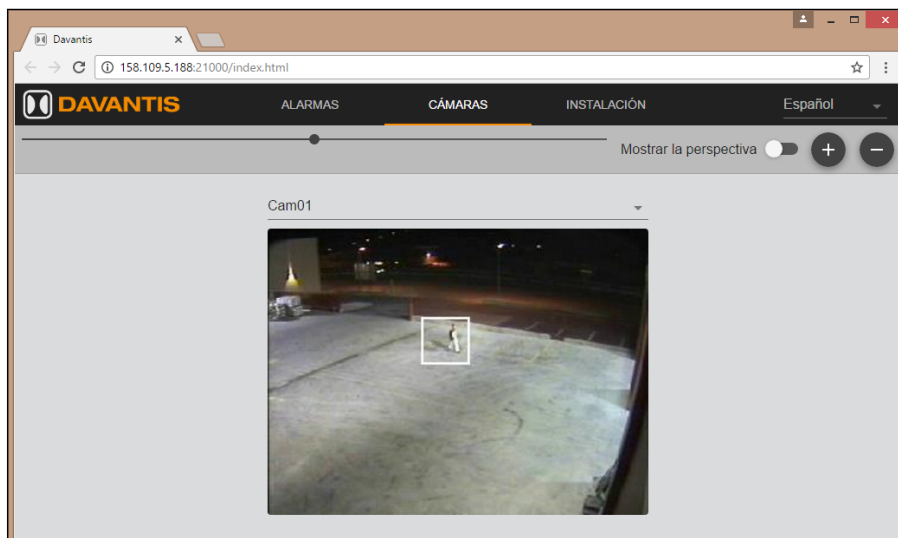
También es posible mostrar solo las alarmas “Enviadas” o “No enviadas” a la CRA. Una alarma se marca como “Enviada” cuando el sistema ha recibido la confirmación de la CRA.



Y por último, es posible filtrar por “Evento”: Intruso, Persona, Vehículo, Envío a CRA activado/desactivado y otras alarmas de sistema. En esta lista solo aparecerán los eventos ocurridos dentro del periodo de búsqueda.

## 6.2 CÁMARAS

Cuando entres en la sección “Cámaras”, la primera cámara se mostrará en directo. Abre el desplegable para seleccionar otra cámara de la lista.



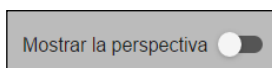
En esta página están disponibles las siguientes herramientas:

### Zoom:

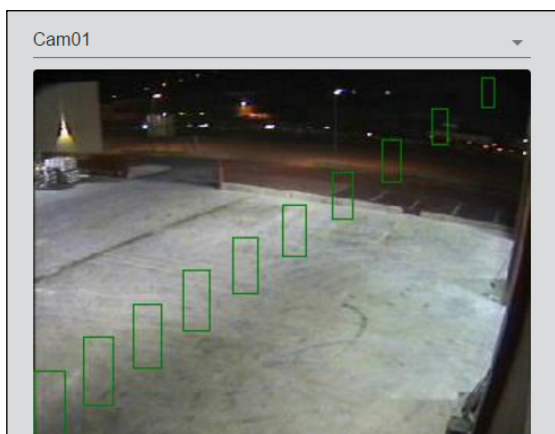


Mueve el zoom a la izquierda para reducir el tamaño de la cámara o a la derecha para ampliarlo.

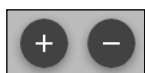
### Perspectiva:



Si activas esta opción (mover a la derecha), la perspectiva entrenada por el sistema se mostrará en las cámaras disponibles.



## Añadir/eliminar cámaras:



Si deseas ver más cámaras a la vez, haz clic en el botón “+” para añadir una cámara más a la página o haz clic en el botón “-” para eliminar la última cámara de la página.

## 6.3 INSTALACIÓN

En la sección “Instalación” se puede ver información básica de la instalación.



Información disponible:

- El nombre de la instalación
- El número de cámaras creadas
- El huso horario
- La IP pública y los puertos TCP

Y también la información de los equipos en el sistema:

- Número de serie
- Información de licencia
- Dirección IP local

En caso de tratarse de una instalación de más de un equipo, se podrá ver la información de todos los equipos de la instalación.

## 7 GAMA DE SOLUCIONES Y CARACTERÍSTICAS

Algunas de las características descritas en este documento solo están disponibles en las soluciones seleccionadas.

### 7.1 DAVIEW MINI

Las siguientes características están disponibles en las soluciones DFUSION, DFUSIONPRO, Daview S y Daview LR pero no están disponibles en la solución Daview MINI:

- Algoritmos específicos para cámaras térmicas.
- Cámara virtual ONVIF/RTSP.
- Servidores apilables desde la Vista lógica.
- Visor de cámaras en directo.
- 

### 7.2 DAVIEW S

La solución Daview S incluye todas las características descritas en este documento excepto las características que están disponibles únicamente en las soluciones DFUSION, DFUSIONPRO, Daview LR y Daview Smart Cities.

### 7.3 DAVIEW LR

Daview LR incluye todas las características disponibles en la solución Daview S más las siguientes características exclusivas:

- Mayor distancia de detección basada en análisis a mayor resolución.
- Las cámaras pueden configurarse en modo “Pasillo” / “Corridor View”.
- Estabilizador de imagen para mejorar el reconocimiento de objetos pequeños a grandes distancias y reducir las falsas alarmas generadas por las vibraciones de la cámara.
- Característica SmartPTZ para que las alarmas puedan ser verificadas usando un vídeo de soporte con un zoom ampliado.

### 7.4 DFUSION

La solución DFUSION incluye todas las características descritas en este documento excepto las características que están disponibles únicamente en las soluciones DFUSIONPRO, Daview LR y Daview Smart Cities.

## 7.5 DFUSIONPRO

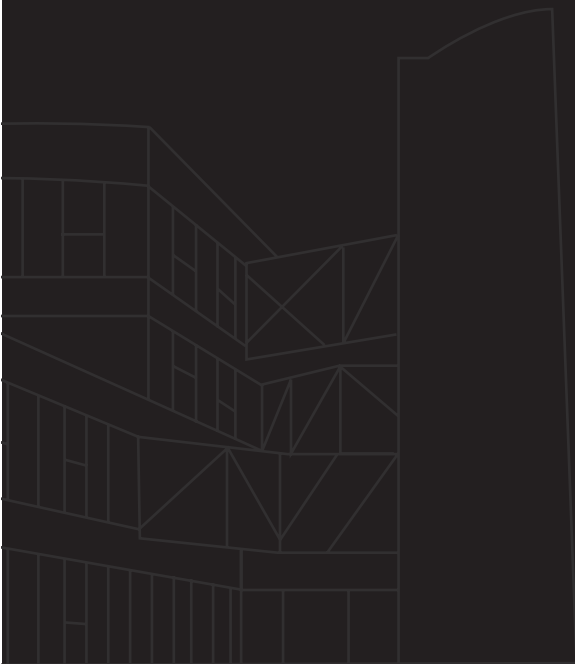
DFUSIONPRO incluye todas las características disponibles en la solución DFUSION más las siguientes características exclusivas:

- Mayor distancia de detección basado en análisis a mayor resolución.
- Las cámaras pueden configurarse en modo “Pasillo” / “Corridor View”.
- Estabilizador de imagen para mejorar el reconocimiento de objetos pequeños a grandes distancias y reducir las falsas alarmas generadas por las vibraciones de la cámara.
- Característica SmartPTZ para que las alarmas puedan ser verificadas usando un vídeo de soporte con un zoom ampliado.

## 7.6 DAVIEW SMART CITIES

Puede haber funciones adicionales en algunos proyectos Smart Cities.

- Objeto abandonado y objeto robado.
- Filtros de velocidad y tamaño.
- Aglomeración.
- Contador de personas.



**DAVANTIS TECHNOLOGIES SL**

Barcelona · España

Madrid · España

Niza · Francia

Luedinghausen · Alemania

Bogotá · Colombia

Singapur

**DAVANTIS TECHNOLOGIES INC**

Washington DC · USA

---

[info@davantis.com](mailto:info@davantis.com)  
[www.davantis.com](http://www.davantis.com)

