

# Mini domo de velocidad híbrido de red térmica

Guía de inicio rápido








# Prefacio

## General

Este manual presenta las funciones y operaciones del dispositivo domo de velocidad minihíbrido de red térmica (en lo sucesivo, "la Cámara").

Las instrucciones de seguridad

Las siguientes palabras de advertencia categorizadas con un significado definido pueden aparecer en el manual.

Palabras de advertencia	Significado
 <b>PELIGRO</b>	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 <b>ADVERTENCIA</b>	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 <b>PRECAUCIÓN</b>	Indica un riesgo potencial que, si no se evita, podría provocar daños a la propiedad, pérdida de datos, menor rendimiento o resultados impredecibles.
 <b>CONSEJOS</b>	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 <b>NOTA</b>	Proporciona información adicional como énfasis y complemento del texto.

## Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.1	Nombre del producto actualizado.	diciembre 2020
V1.0.0	Primer lanzamiento.	enero 2019

## Aviso de protección de privacidad

Como usuario del dispositivo o controlador de datos, puede recopilar datos personales de otros, como la cara, las huellas dactilares, el número de placa del automóvil, la dirección de correo electrónico, el número de teléfono, el GPS, etc. Debe cumplir con las leyes y regulaciones locales de protección de la privacidad para proteger los derechos e intereses legítimos de otras personas mediante la implementación de medidas que incluyen, entre otras: proporcionar una identificación clara y visible para informar al sujeto de los datos sobre la existencia de un área de vigilancia y proporcionar información relacionada. contacto.

## Declaración de interfaz

Este manual presenta principalmente las funciones relevantes cuando utiliza el dispositivo. Las interfaces utilizadas para la fabricación, la devolución a la fábrica para su inspección y la localización de fallas no se describen en este documento.

manual. Póngase en contacto con el soporte técnico si necesita información sobre estas interfaces.

## Sobre el Manual

- El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.
- No somos responsables de ninguna pérdida causada por las operaciones que no cumplen con el manual.
- El manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las jurisdicciones relacionadas. Para obtener información detallada, consulte el manual en papel, el CD-ROM, el código QR o nuestro sitio web oficial. Si hay inconsistencia entre el manual en papel y la versión electrónica, prevalecerá la versión electrónica.
- Todos los diseños y el software están sujetos a cambios sin previo aviso por escrito. Las actualizaciones del producto pueden causar algunas diferencias entre el producto real y el manual. Póngase en contacto con el servicio de atención al cliente para obtener el programa más reciente y la documentación complementaria.
- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho de dar una explicación final.
- Actualice el software del lector o pruebe con otro software del lector convencional si no se puede abrir el manual (en formato PDF).
- Todas las marcas comerciales, marcas comerciales registradas y nombres de compañías en el manual son propiedad de sus respectivos dueños.
- Visite nuestro sitio web, comuníquese con el proveedor o el servicio al cliente si ocurre algún problema al usar el dispositivo.
- Si hay alguna duda o controversia, nos reservamos el derecho de la explicación final.

## Medidas de seguridad y advertencias importantes

Este capítulo describe el contenido que cubre el manejo adecuado del dispositivo, la prevención de riesgos y la prevención de daños a la propiedad. Lea este contenido detenidamente antes de utilizar el dispositivo, respételo cuando lo utilice y guárdelo para futuras consultas.

### Requisitos para profesionales de instalación y mantenimiento

Todos los profesionales de instalación y mantenimiento deben tener un certificado de calificación o experiencia en la instalación y mantenimiento de sistemas de circuito cerrado de televisión, aparatos eléctricos en entornos con gases explosivos y trabajos a gran altura. Además, tienen que adquirir los siguientes conocimientos y habilidades operativas.

- Conocimientos básicos y habilidades de instalación del sistema CCTV.
- Conocimientos básicos y habilidades de operación de cableado de bajo voltaje y conexión de cables de circuitos electrónicos de bajo voltaje.
- Conocimientos básicos y habilidades operativas de instalación y mantenimiento de aparatos eléctricos en sitios peligrosos.

### requerimientos de energía

- Toda la instalación y operación debe cumplir con el código de seguridad eléctrica local.
- Verifique si la fuente de alimentación es correcta antes de operar el dispositivo.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV y encienda la cámara con el voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Y consulte los requisitos de fuente de alimentación de la etiqueta de la cámara para su operación final.
- Instale un dispositivo fácil de usar para el apagado antes de instalar el cableado, que es para el apagado de emergencia cuando sea necesario.
- Evite pisotear o presionar el cable de alimentación, especialmente el enchufe, la toma de corriente y la unión del dispositivo.

### Requisitos del entorno de la aplicación

- Utilice el dispositivo dentro de la humedad (<95 % HR) y la altitud (<3000 m) permitidas.
- No utilice el dispositivo en entornos corrosivos, como zonas con mucha niebla salina (mar, playa y zonas costeras), entornos con gases ácidos y plantas químicas.
- No utilice el dispositivo en entornos con fuertes vibraciones, como barcos y vehículos.



Si aún desea utilizar cámaras térmicas en las tres condiciones mencionadas anteriormente, comuníquese con nuestro personal de ventas para comprar cámaras de modelo especial o cámaras personalizadas. Si usa cámaras en entornos inadecuados, no asumiremos los costes de los daños de la cámara.

- Por favor, no coloque el dispositivo en un lugar húmedo, polvoriento, extremadamente caliente y frío con radiación electromagnética fuerte o iluminación inestable.
- No bloquee la abertura de ventilación cerca del dispositivo para evitar la acumulación de calor.

para el dispositivo

- No instale el dispositivo cerca de un lugar con una fuente de calor, como un radiador, calentador, estufa u otro equipo de calefacción, para evitar incendios.
- No apunte la lente directamente a una fuente de radiación intensa (como el sol, el láser y el acero fundido, etc.), para evitar dañar el detector térmico.
- No permita que ningún líquido entre en el dispositivo, para evitar dañar los componentes internos; deje de usar el dispositivo inmediatamente y corte la alimentación, desconecte todos los cables que están conectados al dispositivo si entra líquido en el dispositivo y comuníquese con el centro de servicio al cliente local.
- Por favor, no meta ninguna materia extraña en el dispositivo en caso de que pueda causar un cortocircuito en el dispositivo, lo que puede causar daños al dispositivo o lesiones a personas.
- Utilice el paquete o material predeterminado de fábrica con la misma calidad para empacar el dispositivo cuando lo transporte.
- No presione, vibre ni empape el dispositivo durante el transporte, el almacenamiento y la instalación.

## Requisitos de operación y mantenimiento

- No toque el componente de disipación de calor del dispositivo en caso de que se quemé.
- Por favor, no desmonte el dispositivo; no hay ninguna parte que pueda ser reparada por los propios usuarios. Puede causar fugas de agua o una mala imagen del dispositivo si se desmonta de forma no profesional.
- Se recomienda usar el dispositivo junto con un pararrayos, que es para mejorar el efecto de la protección contra rayos, debe cumplir con la regulación de protección contra rayos para aplicaciones al aire libre.
- No toque el dispositivo fotosensible con las manos. Para limpiar el polvo y la suciedad de la lente, se puede utilizar un soplador de aire. Para una mayor limpieza, vierta un poco de alcohol en un paño seco con el que pueda limpiar suavemente la suciedad.
- Limpie el cuerpo del dispositivo con un paño suave y seco. Para cualquier suciedad difícil de quitar, tome un paño limpio y suave, humedézcalo con un poco de detergente neutro y limpie suavemente el polvo con él; después de eso, limpie todos los líquidos del dispositivo con otro paño seco. Nunca utilice disolventes volátiles como alcohol, benceno y diluyentes, ni ningún limpiador que sea fuerte y abrasivo. De lo contrario, el revestimiento de la superficie del dispositivo se dañará y su rendimiento laboral se verá afectado.



### ADVERTENCIA

- Modifique la contraseña predeterminada después de iniciar sesión, en caso de que se la roben.
- Utilice los accesorios regulados por el fabricante, y el dispositivo debe ser instalado y mantenido por profesionales.
- La conexión a tierra interna y externa debe ser estable.
- No proporcione dos o más modos de fuente de alimentación al dispositivo, de lo contrario, puede causar daños al dispositivo.
- Se reserva un cable de control de aproximadamente 2,5 m de largo cuando el dispositivo se entrega fuera de fábrica, debe usar un tubo flexible a prueba de explosiones o un cable blindado para proteger cuando el cable de control está conectado al gabinete de control a prueba de explosiones.
- Corte la alimentación antes de realizar el mantenimiento y la revisión del dispositivo. Está prohibido abrir la tapa.

con energía en el entorno de explosión.

- Asegúrese de que todos los componentes y piezas a prueba de explosiones estén completos sin grietas y que no haya ningún defecto que pueda afectar el rendimiento a prueba de explosiones.
- Póngase en contacto con el distribuidor local o el centro de servicio más cercano si el dispositivo no funciona normalmente, no desmonte ni modifique el dispositivo.

# Tabla de contenido

<b>Prefacio</b> .....	<b>I Medidas de seguridad y advertencias importantes</b> .....
<b>la caja</b> .....	<b>III 1 Desembalaje de la caja</b> .....
	<b>7</b>
<b>2 Diseño</b> .....	<b>8</b>
2.1 Dimensiones .....	8
2.1.1 Cámara .....	8
2.1.2 Soportes .....	8
2.2 Cableado .....	10
<b>3 Configuración general</b> .....	<b>12</b>
3.1 Inicializar la cámara.....	12
3.2 Modificación de la dirección IP .....	13
3.3 Vídeo en directo.....	13
<b>4 Instalación</b> .....	<b>15</b>
4.1 Preparación de cables .....	15
4.2 Instalación de la cámara .....	15
4.2.1 (Opcional) Instalación de la tarjeta SD .....	15
4.2.2 Fijación de la cámara .....	dieciséis
4.2.3 Conexión de los puertos de cable.....	20
4.2.4 Instalación del conector a prueba de agua.....	20
<b>5 Configuración de la alarma</b> .....	<b>21</b>
<b>Apéndice 1 Recomendaciones sobre ciberseguridad</b> .....	<b>23</b>

# 1 Desembalaje de la caja

Consulte la siguiente lista de verificación y verifique el paquete. Si encuentra daños en el dispositivo o alguna pérdida, comuníquese con el servicio posventa.

Figura 1-1 Lista de verificación

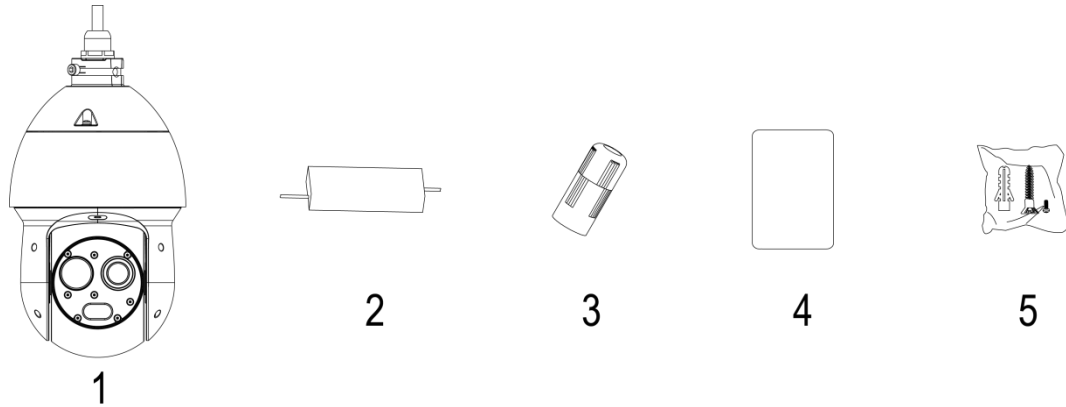


Tabla 1-1 Descripción de la lista de verificación

No.	Nombre	No.	Nombre	No.	Nombre
1	Cámara	2	Cable de energía	3	Conector impermeable
4	Guía de inicio rápido	5	Bolsa de tornillos	—	—

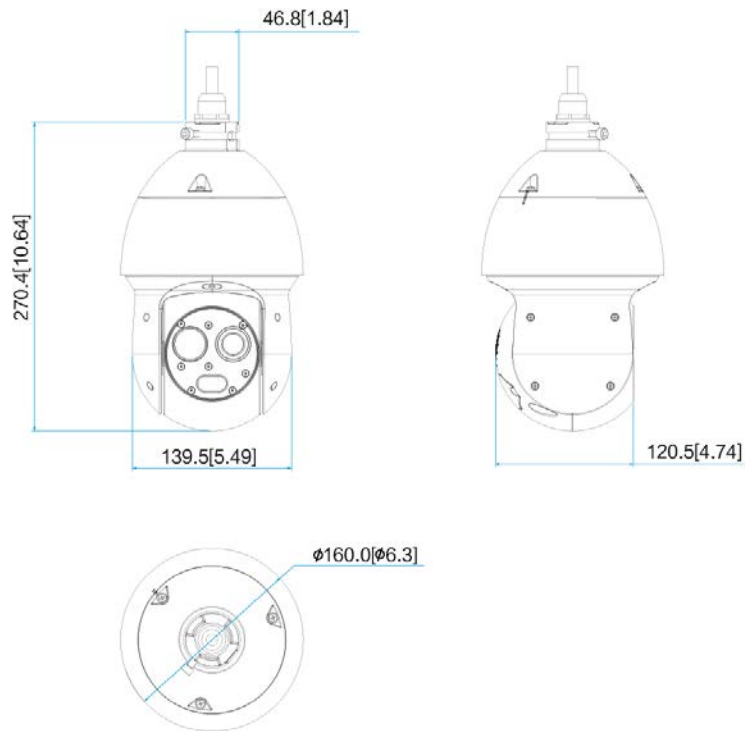


# 2 diseño

## 2.1 Dimensiones

### 2.1.1 Cámara

Figura 2-1 Dimensiones (mm [pulgadas])



### 2.1.2 Soportes



- No proporcionamos soportes en la caja de embalaje y, si los necesita, cómprelos por separado.
- Los soportes para diferentes métodos de instalación son los siguientes.

Figura 2-2 Soporte de montaje en pared (mm [pulgadas])

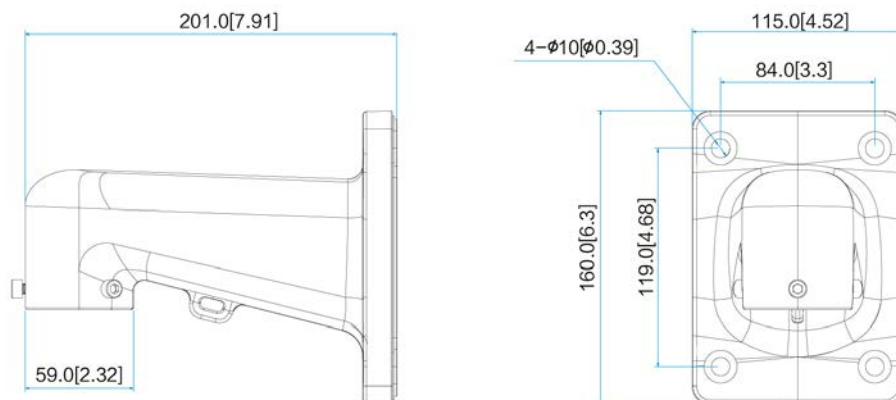


Figura 2-3 Soporte de montaje en poste (mm [pulgadas])

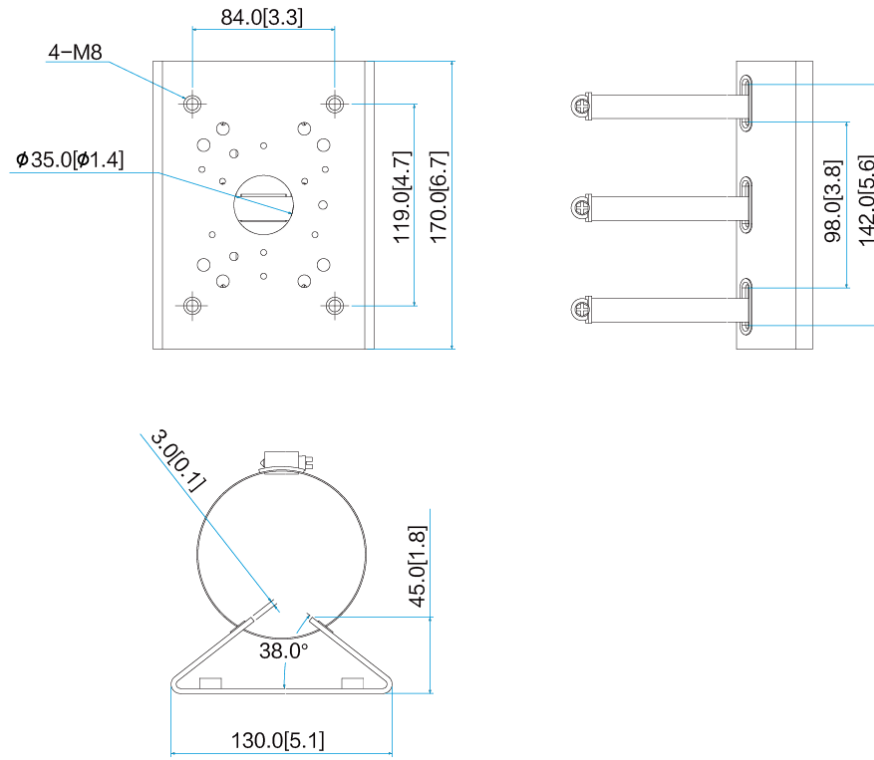


Figura 2-4 Soporte de montaje en esquina (mm [pulgadas])

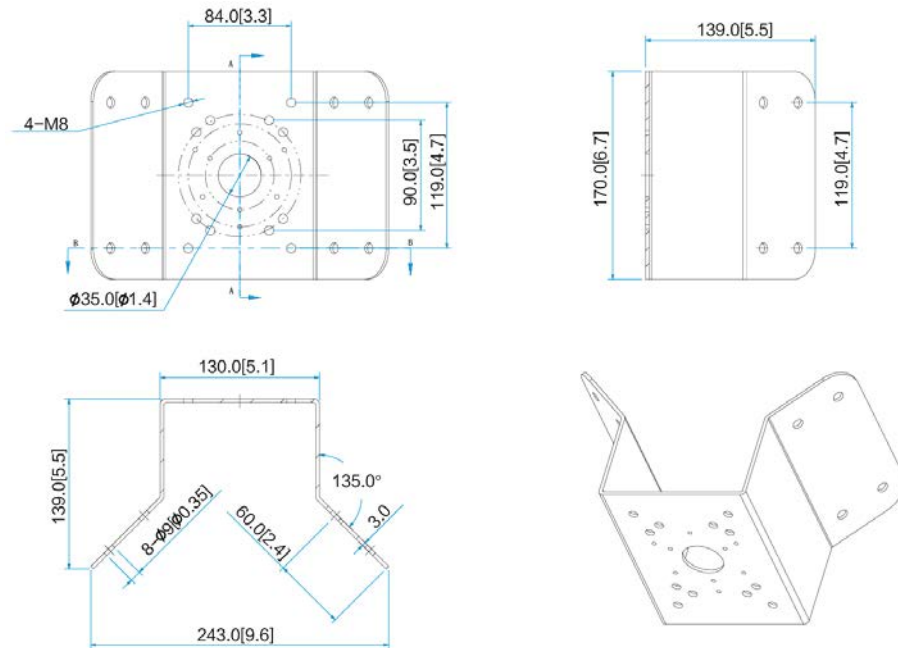
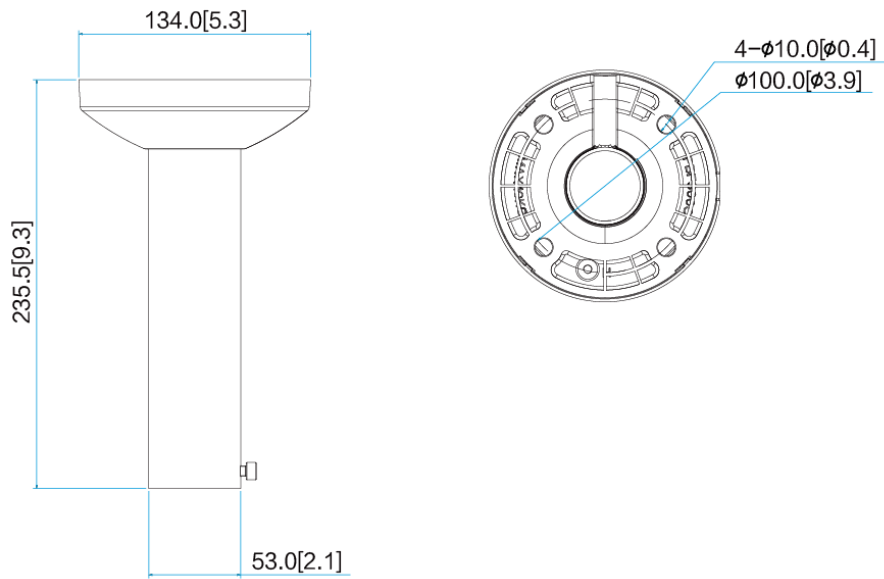


Figura 2-5 Soporte de montaje en techo (mm [pulgadas])

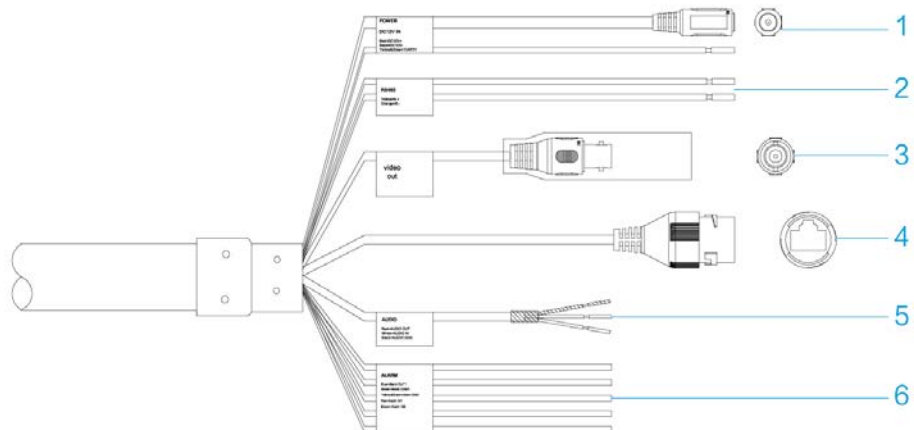


## 2.2 cable



El tipo de cable puede variar con diferentes cámaras y prevalecerá el producto real.

Figura 2-6 Puertos de cables



Consulte la Tabla 2-1 para obtener más detalles sobre la función del cable.


Tabla 2-1 Descripción de los puertos de cable

número de serie	Puerto	Nombre del puerto	conector	Función descriptiva
1	12V CC	Entrada de alimentación Puerto	—	Entradas de alimentación de 12 V CC.
	TIERRA	Tierra Terminal	—	Terminal de tierra
2	RS485_A (Amarillo)	Puerto RS485	—	Puerto RS485, control PTZ, etc.
	RS485_B (Naranja)			

número de serie	Puerto	Nombre del puerto	conector	Función descriptiva
3	SALIDA DE VIDEO	Vídeo analógico producción	BNC	En general, emite una señal de video analógica, se puede conectar a un monitor de TV para verificar la imagen.
4	LAN	puerto de red	Puerto Ethernet	Conéctese a un cable Ethernet estándar.
5	ENTRADA DE AUDIO (Rojo)	Entrada de audio Puerto	rca	Entrada de señal de audio, recepción de señal de audio analógica desde la captación de sonido y otros dispositivos.
	SALIDA DE AUDIO (Blanco)	Salida de audio Puerto	rca	Salida de señal de audio al altavoz y otros dispositivos.
	TIERRA DE AUDIO (Negro)	Audio tierra Terminal	—	terminal puesto a tierra.
6	E/S	puerto de E/S	Varios externo alarma aparatos	Incluye entrada de alarma, salida. Consulte la Tabla 2-2 para obtener más detalles.

Consulte la Tabla 2-2 para conocer la introducción de la función del puerto de E/S.

Tabla 2-2 Descripción del puerto de E/S

Puerto	Nombre del puerto de cable	Función descriptiva
puerto de E/S	ALARMA_SALIDA1 (Azul)	Puertos de salida de alarma, señal de alarma de salida al dispositivo de alarma. 
	ALARM_COM1 (Verde)	ALARM_OUT1 solo se puede usar con ALARM_COM1 cuando se conecta a un dispositivo de alarma.
	ALARMA_IN1 (Rojo)	Puertos de entrada de alarma, recibe la señal de encendido y apagado de una fuente de alarma externa.
	ALARMA_IN2 (Marrón)	
	ALARMA_GND (amarillo y verde)	terminal puesto a tierra.

# 3 Configuración general

## 3.1 Inicializar cámara

Debe inicializar su cámara y configurar la contraseña de usuario cuando inicie sesión por primera vez. Puede usar ConfigTool o web para lograr la inicialización. Aquí se toma como ejemplo la inicialización por web.



- No puede usar la cámara si la cámara no está inicializada.
- Para proteger los datos de la cámara, mantenga bien la contraseña de administrador después de la inicialización y modifíquela regularmente.
- Puede implementar la inicialización del dispositivo solo cuando la dirección IP de su cámara (192.168.1.108 por predeterminado) y la dirección IP de su PC están en el mismo segmento de red.

**Paso 1** Abra el navegador IE, ingrese la dirección IP predeterminada de la cámara en la barra de direcciones y luego presione **Ingresar**.



La dirección IP predeterminada de fábrica es: 192.168.1.1087.

Él **Inicialización del dispositivo** se muestra la interfaz. Consulte la Figura 3-1.

Figura 3-1 Inicialización de la cámara

The screenshot shows a web form titled "Device Initialization". It contains the following elements:

- Username:** A text input field with "admin" entered.
- Password:** A text input field with a strength indicator below it showing "Weak", "Middle", and "Strong" buttons.
- Confirm Password:** A text input field.
- Instructions:** "Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like " " ; : & )"
- Email Address:** A text input field with a checked checkbox next to it.
- Reset Note:** "To reset password, please input properly or update in time."
- Save Button:** A button labeled "Save" at the bottom center.

**Paso 2** Establezca la contraseña de inicio de sesión de administrador. Consulte la Tabla 3-1 para obtener más información.

Tabla 3-1 Descripción de la contraseña

Parámetro	Descripción
Clave	La contraseña puede configurarse de 8 a 32 caracteres que no estén en blanco, que pueden estar compuestos por números, letras y caracteres especiales (excepto " " , "!" , " ; " , " : " y "& " ), y tiene debe contener al menos dos tipos de caracteres. Configure la contraseña con alta seguridad de acuerdo con la solicitud de intensidad de la contraseña.
Confirmar Clave	
Dirección de correo electrónico	Para restablecer la contraseña, ingrese la dirección de correo electrónico correctamente y actualícela a tiempo.

**Paso 3** Hacer clic **Guardar** para finalizar la inicialización.

## 3.2 Modificación de la dirección IP

Para que la cámara tenga acceso a la red, planifique la dirección IP razonablemente de acuerdo con el entorno de red real.

**Paso 1** Inicie sesión en la interfaz web de la cámara en el navegador IE.



- La dirección IP predeterminada de fábrica es: 192.168.1.108.
- El usuario predeterminado es administrador; la contraseña se establece durante la inicialización del dispositivo.

**Paso 2** Seleccione **Configuración > Red > TCP/IP** y el sistema mostrará la interfaz de “TCP/IP”, que se muestra en la Figura 3-2.

Figura 3-2 TCP/IP

**Paso 3** Configure la información relevante de la dirección IP y haga clic en **Guardar**.

## 3.3 Vídeo en directo



Diferentes dispositivos pueden tener diferentes interfaces WEB, la figura en este documento es solo para referencia, por favor refiérase al documento *Manual de operaciones WEB* en el disco y la interfaz real para más detalles.

**Paso 4** Inicie sesión en la interfaz web de la cámara en el navegador IE.



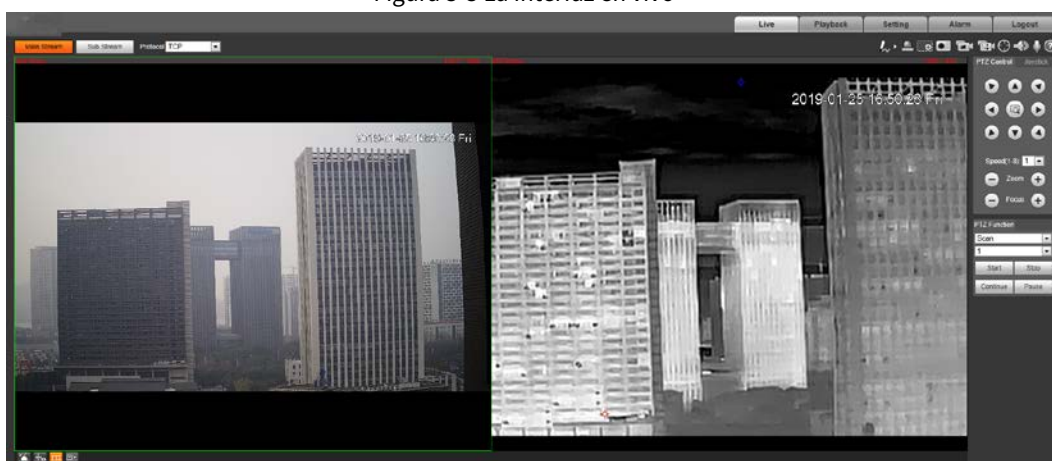
- La dirección IP es la que ha sido modificada.
- El usuario predeterminado es administrador; la contraseña se ha establecido durante la inicialización del dispositivo.

**Paso 5** Hacer clic **Acceso** y el sistema mostrará la interfaz principal WEB, que se muestra en la Figura 3-3.



Le pedirá que instale el complemento para el primer inicio de sesión del sistema, guarde e instale el complemento según indicación. La interfaz WEB se actualizará automáticamente después de que finalice la instalación del complemento. completado, luego aparecerá el video en vivo.

Figura 3-3 La interfaz en vivo



# 4 Instalación



- Asegúrese de que la superficie de montaje sea lo suficientemente fuerte para sostener al menos ocho veces la cámara peso.
- La siguiente figura es solo de referencia y prevalecerá el producto real.

## 4.1 Preparación de cables

### Selección del cable de video necesario

- 75 ohmios
- Cable completo con conductor de cobre. Escudo 95% cobre tejido.

Tabla 4-1 Cable de vídeo

modelo internacional	Distancia máxima de transmisión (pies/m)
RG59/U	750 pies/229 m
RG6/U	1000 pies/305 m
RG11/U	1500 pies/457 m

### Selección del cable de alimentación necesario



Se recomienda instalar la potencia correspondiente a menos de 5 m del dispositivo si está permitido; pero si no, entonces necesita extender el cable de alimentación, pero tiene que garantizar el voltaje del dispositivo puerto de entrada (cable de salida de domo híbrido térmico) no es inferior a  $12\text{ V} \pm 20\% \text{ CC}$ .

### Selección del cable de señal necesario

Se recomienda que todos los cables de señal (audio, entrada y salida de alarma y RS-485, etc.) utilicen un cable de 0,56 mm (24 AWG) y superior como cable de señal de alambre alargado.

## 4.2 Instalación de la cámara

### 4.2.1 (Opcional) Instalación de la tarjeta SD



- Corte la alimentación del dispositivo antes de instalar la tarjeta SD.
- Tenga cuidado y no confunda la ranura de la tarjeta Micro SD con el orificio de reinicio. Mantenga presionado el botón de reinicio para De 4 a 5 segundos y restablecerá su cámara.
- Verifique si el anillo impermeable está instalado correctamente antes de cerrar la tapa, de lo contrario, afectará el rendimiento a prueba de agua del dispositivo.



Figura 4-1 Instalación de la tarjeta SD

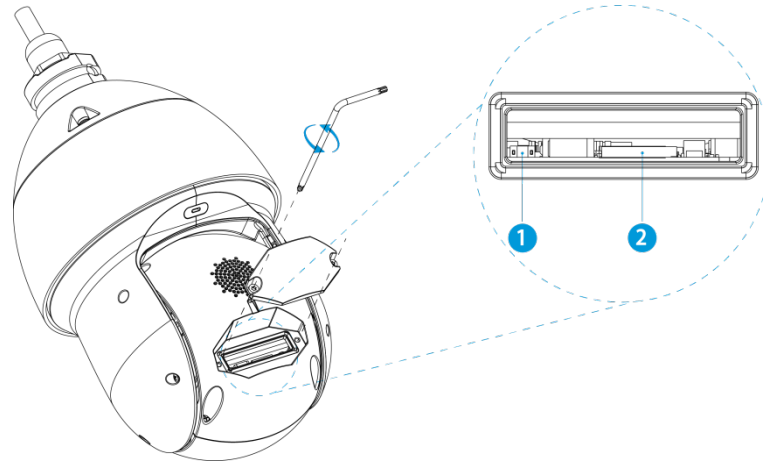


Tabla 4-2 Lista de componentes de la cámara

No.	Nombre	No.	Nombre
1	Restablecer agujero	2	Ranura para tarjeta MicroSD

## 4.2.2 Cámara de fijación

El domo de velocidad híbrido admite cuatro modos de instalación: montaje en pared, montaje colgante, montaje en esquina y montaje en poste.



No proporcionamos soportes en la caja de embalaje y, si los necesita, cómprelos por separado. Para las dimensiones de los soportes adecuadas para su cámara, consulte “2.1.2 Soportes” .

Figura 4-2 Instalación de montaje en pared

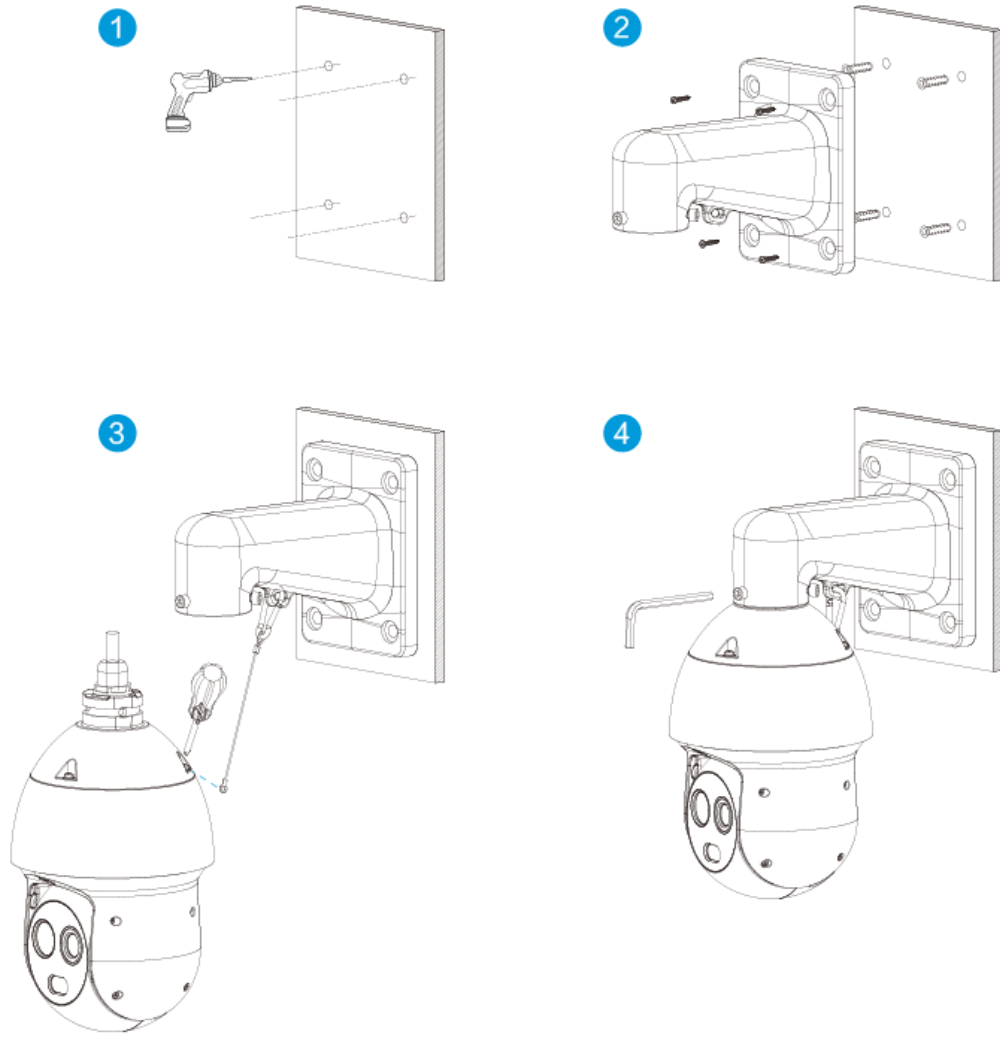


Figura 4-3 Instalación de montaje en poste

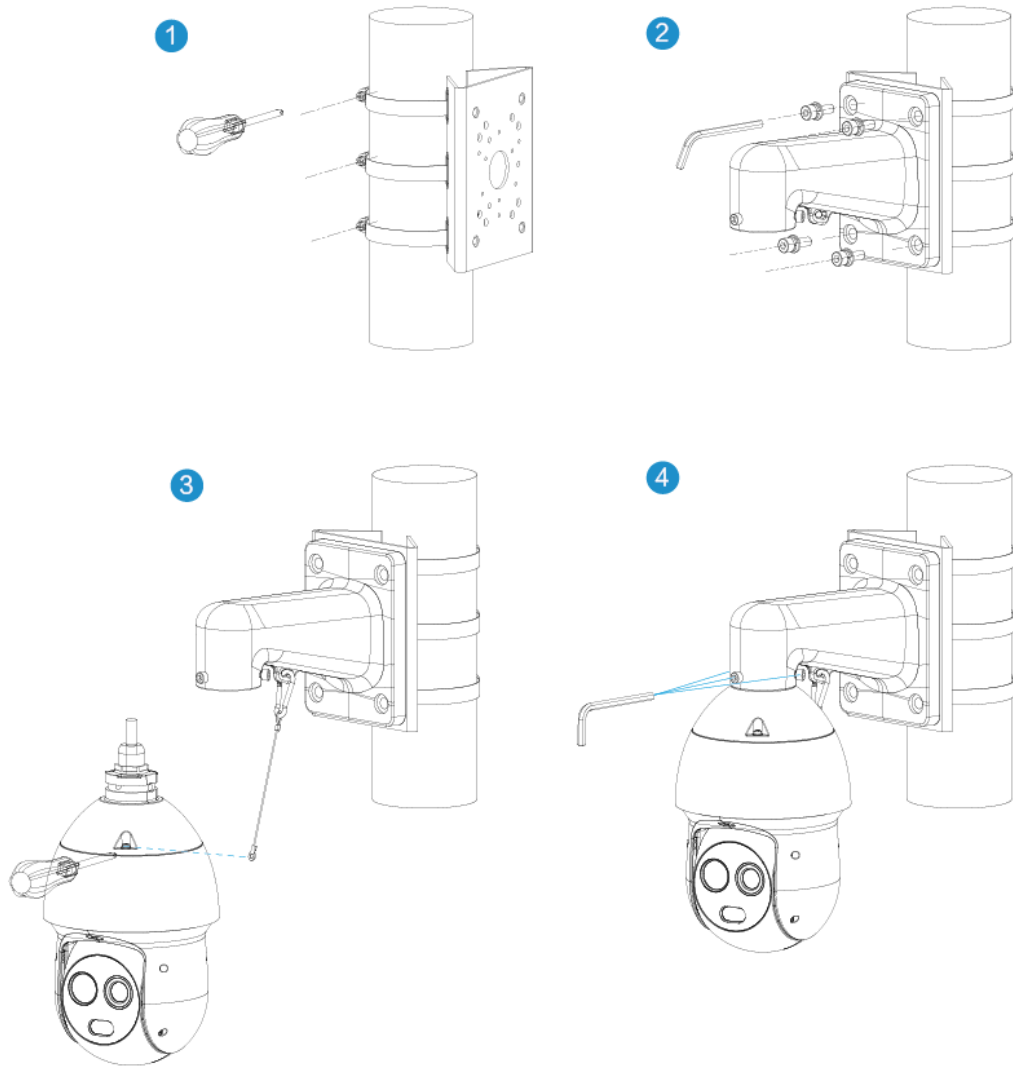


Figura 4-4 Instalación de montaje en esquina

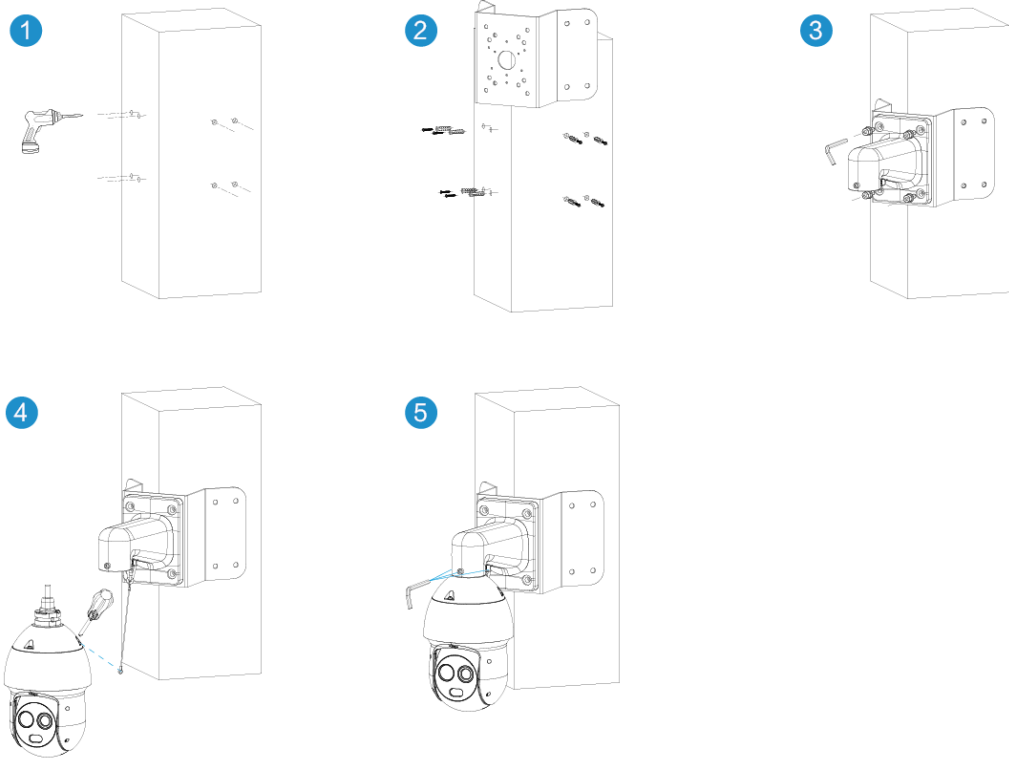
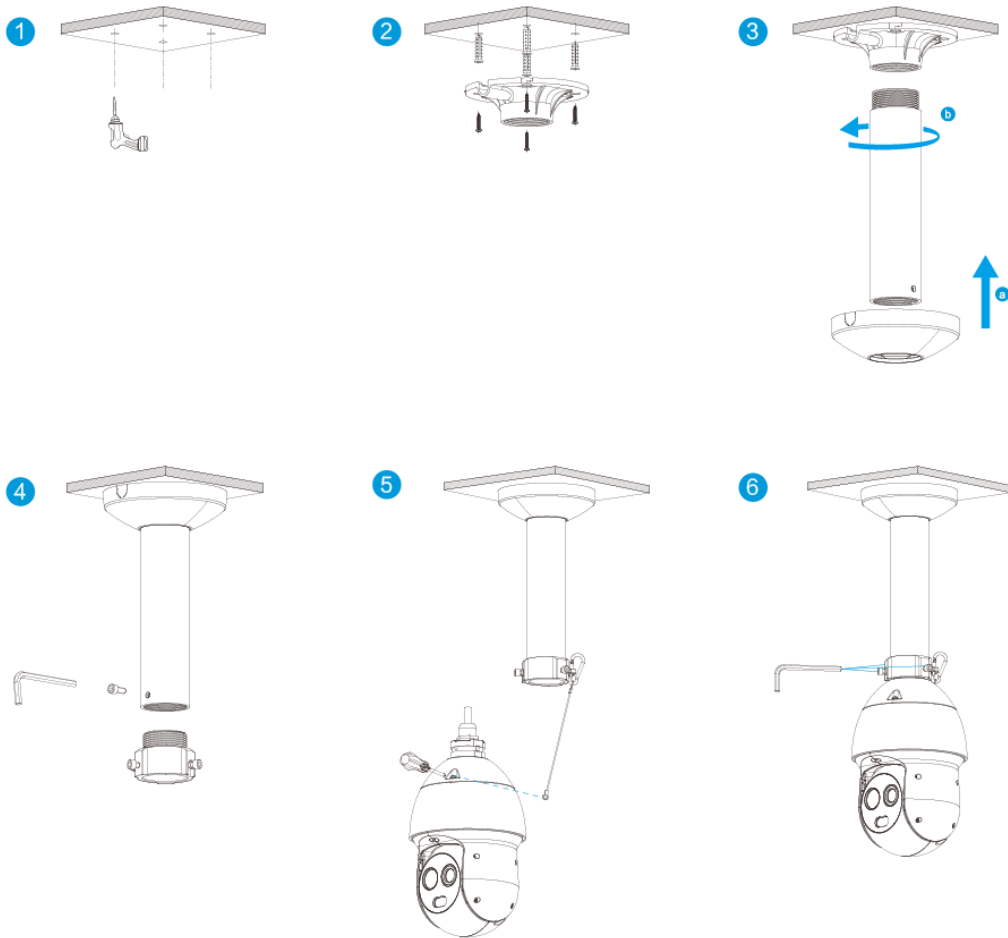


Figura 4-5 Instalación de montaje en techo

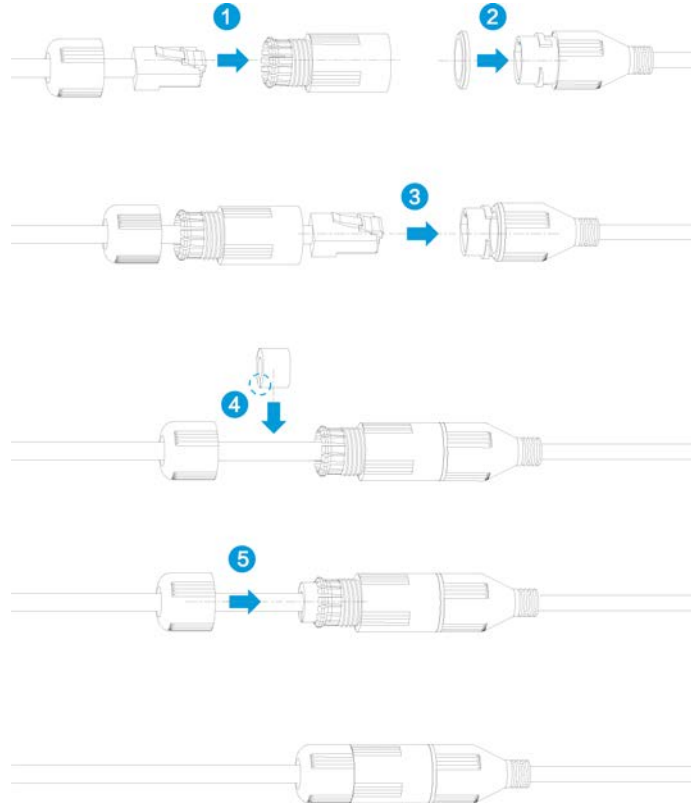


### 4.2.3 Puertos de cable de conexión

Consulte “2.2 Cable” y conecte cada puerto de cable a los cables correspondientes. Luego use la cinta aislante para sellar cada puerto para evitar fugas de agua.

### 4.2.4 Instalación del conector a prueba de agua para el puerto de red

Figura 4-6 Instalación del conector a prueba de agua para el puerto de red



## 5 Configuración de alarma



Tiene que cortar la energía primero al conectar los cables.

### Descripción de la conexión de entrada y salida de alarma

**Paso 6** Conecte el dispositivo de entrada de alarma al puerto de entrada de alarma del cable de E/S.

**Paso 7** Conecte el dispositivo de salida de alarma al puerto de salida de alarma del cable de E/S. La salida de alarma es una salida de interruptor de relé, y el puerto de salida de alarma solo se puede conectar a ningún dispositivo de alarma.

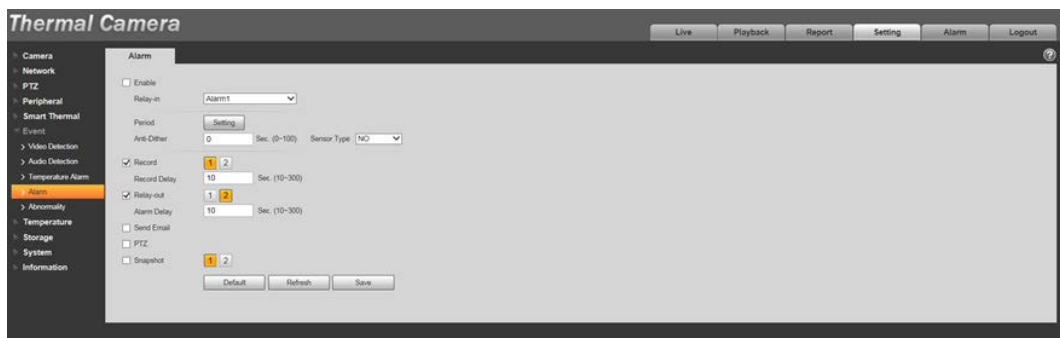
**Paso 8** Abra la interfaz web, seleccione **Configuración > Evento > Alarma**.

**Paso 9** Realice los ajustes correspondientes a la entrada y salida de la alarma en la interfaz de configuración de alarmas y, a continuación, haga clic en **Guardar**.

Vea la Figura 5-1 para el **Alarma** interfaz.

- La entrada de alarma corresponde al puerto de entrada de alarma del cable de E/S del dispositivo. Es para configurar el NO y NC correspondiente de acuerdo con la señal de nivel alto y bajo generada por el dispositivo de entrada de alarma cuando ocurre la alarma.
- La salida de alarma corresponde al puerto de salida de alarma del cable de E/S del dispositivo.

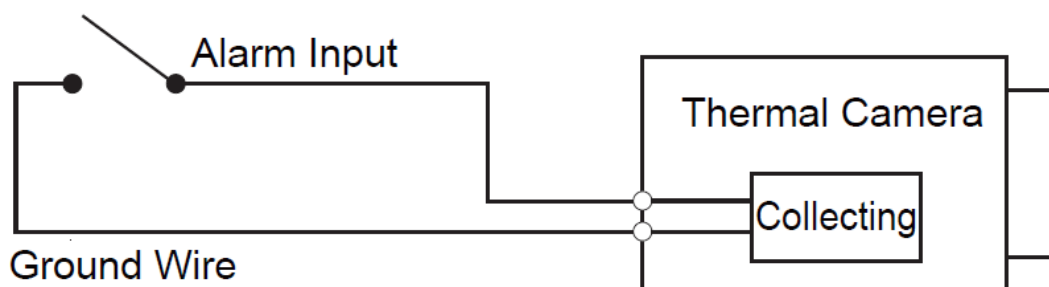
Figura 5-1 La interfaz de alarma



### Cifras de entrada y salida de alarma

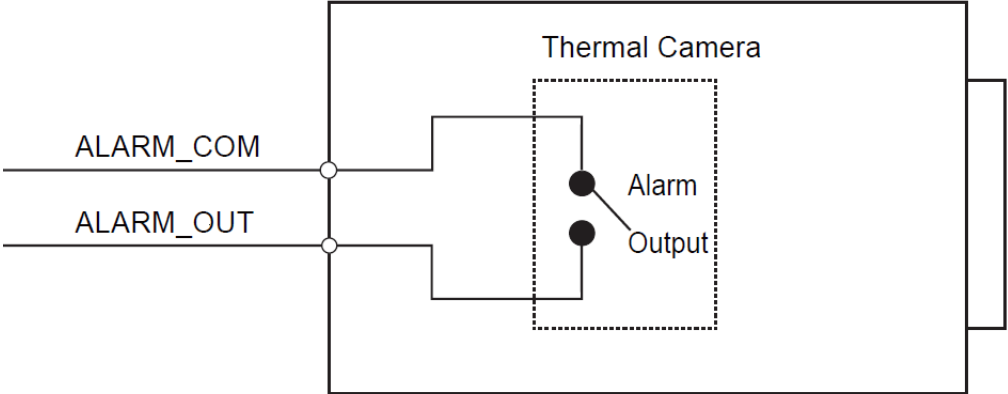
Entrada de alarma: la señal de entrada está inactiva o conectada a tierra; el dispositivo puede recopilar diferentes estados del puerto de entrada de alarma. La señal de entrada está conectada a 3,3 V o inactiva, el dispositivo recopila la lógica "1"; la señal de entrada está conectada a tierra, el dispositivo recoge la lógica "0".

Figura 5-2 Entrada de alarma



Salida de alarma: los puertos ALARM\_OUT y ALARM\_COM forman un conmutador que se puede utilizar para proporcionar una salida de alarma. Normalmente, el interruptor está encendido y estará apagado cuando haya una salida de alarma.

Figura 5-3 Salida de alarma



# Apéndice 1 Recomendaciones de ciberseguridad

La ciberseguridad es más que una palabra de moda: es algo que pertenece a todos los dispositivos que están conectados a Internet. La videovigilancia IP no es inmune a los riesgos cibernéticos, pero tomar medidas básicas para proteger y fortalecer las redes y los dispositivos en red los hará menos susceptibles a los ataques. A continuación se presentan algunos consejos y recomendaciones sobre cómo crear un sistema de seguridad más seguro.

## **Acciones obligatorias que se deben tomar para la seguridad básica de la red del dispositivo: 1. Use contraseñas seguras**

Consulte las siguientes sugerencias para establecer contraseñas:

- La longitud no debe ser inferior a 8 caracteres;
- Incluya al menos dos tipos de caracteres; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;
- No contenga el nombre de la cuenta o el nombre de la cuenta en orden inverso;
- No utilice caracteres continuos, como 123, abc, etc.;
- No utilice caracteres superpuestos, como 111, aaa, etc.;

## **2. Actualice el firmware y el software del cliente a tiempo**

- De acuerdo con el procedimiento estándar en la industria tecnológica, recomendamos mantener actualizado el firmware de su dispositivo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el dispositivo está conectado a la red pública, se recomienda habilitar la función de "verificación automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware lanzadas por el fabricante.
- Le sugerimos que descargue y utilice la última versión del software del cliente.

## **Recomendaciones "agradables de tener" para mejorar la seguridad de la red de su**

### **dispositivo: 1. Protección física**

Le sugerimos que realice una protección física al dispositivo, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el dispositivo en una sala y gabinete de computadoras especiales, e implemente un permiso de control de acceso y una administración de claves bien hechos para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de un dispositivo extraíble (como un disco flash USB), puerto serie), etc.

### **2. Cambie las contraseñas regularmente**

Le sugerimos que cambie las contraseñas regularmente para reducir el riesgo de ser adivinadas o descifradas.

### **3. Establezca y actualice la información de restablecimiento de contraseñas a tiempo**

El dispositivo admite la función de restablecimiento de contraseña. Configure la información relacionada para restablecer la contraseña a tiempo, incluido el buzón del usuario final y las preguntas de protección de contraseña. Si la información cambia, modifíquela a tiempo. Al establecer preguntas de protección de contraseña, se sugiere no utilizar aquellas que se pueden adivinar fácilmente.

### **4. Habilitar bloqueo de cuenta**

La función de bloqueo de cuenta está habilitada de forma predeterminada y le recomendamos que la mantenga activada para garantizar la seguridad de la cuenta. Si un atacante intenta iniciar sesión varias veces con la contraseña incorrecta, la cuenta correspondiente y la dirección IP de origen se bloquearán.

### **5. Cambiar HTTP predeterminado y otros puertos de servicio**

Le sugerimos que cambie el HTTP predeterminado y otros puertos de servicio a cualquier conjunto de números entre 1024 y 65535, lo que reduce el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.



## 6. Habilitar HTTPS

Le sugerimos que habilite HTTPS, para que visite el servicio web a través de un canal de comunicación seguro.

## 7. Enlace de dirección MAC

Le recomendamos vincular la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de identidad ARP.

## 8. Asigne cuentas y privilegios de manera razonable

De acuerdo con los requisitos comerciales y de gestión, agregue usuarios razonablemente y asígneles un conjunto mínimo de permisos.

## 9. Deshabilite los servicios innecesarios y elija modos seguros

Si no es necesario, se recomienda desactivar algunos servicios como SNMP, SMTP, UPnP, etc., para reducir los riesgos.

Si es necesario, se recomienda encarecidamente que utilice modos seguros, incluidos, entre otros, los siguientes servicios:

- SNMP: elija SNMP v3 y configure contraseñas de cifrado y contraseñas de autenticación seguras.
- SMTP: Elija TLS para acceder al servidor de buzones.
- FTP: elija SFTP y configure contraseñas seguras.
- Punto de acceso AP: elija el modo de encriptación WPA2-PSK y configure contraseñas seguras.

## 10. Transmisión encriptada de audio y video

Si el contenido de sus datos de audio y video es muy importante o confidencial, le recomendamos que utilice la función de transmisión encriptada para reducir el riesgo de robo de datos de audio y video durante la transmisión.

Recordatorio: la transmisión encriptada causará cierta pérdida en la eficiencia de la transmisión.

## 11. Auditoría segura

- Verifique a los usuarios en línea: le sugerimos que verifique a los usuarios en línea regularmente para ver si el dispositivo está conectado sin autorización.
- Verifique el registro del dispositivo: al ver los registros, puede conocer las direcciones IP que se usaron para iniciar sesión en sus dispositivos y sus operaciones clave.

## 12. Registro de red

Debido a la capacidad de almacenamiento limitada del dispositivo, el registro almacenado es limitado. Si necesita guardar el registro durante mucho tiempo, se recomienda habilitar la función de registro de red para asegurarse de que los registros críticos se sincronizan con el servidor de registro de red para su seguimiento.

## 13. Construya un entorno de red seguro

Para garantizar mejor la seguridad del dispositivo y reducir los posibles riesgos cibernéticos, recomendamos:

- Deshabilite la función de mapeo de puertos del enrutador para evitar el acceso directo a los dispositivos de intranet desde una red externa.
- La red debe dividirse y aislarse de acuerdo con las necesidades reales de la red. Si no hay requisitos de comunicación entre dos subredes, se sugiere usar VLAN, GAP de red y otras tecnologías para dividir la red, a fin de lograr el efecto de aislamiento de la red.
- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.
- Habilite la función de filtrado de direcciones IP/MAC para limitar el rango de hosts que pueden acceder al dispositivo.