

# **Videoportero analógico de 4 hilos**

**Guía de inicio rápido**



# Prefacio

## General






Este documento presenta principalmente la estructura, instalación, cableado y operaciones de menú del intercomunicador de video analógico de 4 hilos.

## Modelo

VTH1020J y VTH1020J-T

Las instrucciones de seguridad

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

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

## Revisión histórica

Versión	Contenido de la revisión	Tiempo de liberación
V1.1.0	<ul style="list-style-type: none"><li>Descripción agregada de la funciones de VTH1020J-T.</li><li>Se agregó la función FactoryReset.</li></ul>	Marzo 2021
V1.0.0	Primer lanzamiento.	Agosto de 2020

## Acerca del manual

El manual es solo para referencia. Si hay inconsistencia entre el manual y el producto real, prevalecerá el producto real.

No nos hacemos responsables de ninguna pérdida ocasionada por las operaciones que no cumplan con el manual. El manual se actualizaría de acuerdo con las leyes y regulaciones más recientes 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 existe 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 desviaciones en los datos técnicos, las funciones y la descripción de las operaciones, o errores en la impresión. Si hay alguna duda o disputa, nos reservamos el derecho a una explicación final.

**Actualice el software del lector o pruebe con otro software de lectura convencional si no puede abrir el manual (en formato PDF).**

Todas las marcas comerciales, marcas comerciales registradas y los nombres de empresas que aparecen en el manual son propiedad de sus respectivos propietarios.

Visite nuestro sitio web, póngase en contacto con el proveedor o el servicio de atención al cliente si surge algún problema al utilizar el dispositivo.

Si hay alguna duda o controversia, nos reservamos el derecho a una explicación final.

# Salvaguardias y advertencias importantes

La siguiente descripción es el método de aplicación correcto del dispositivo. Lea atentamente el manual antes de usarlo para evitar peligros y pérdidas materiales. Cumpla estrictamente con el manual durante la aplicación y consérvelo correctamente después de leerlo.

## Requisitos operativos

No exponga el dispositivo a la luz solar directa ni a fuentes de calor.

No instale el dispositivo en un área húmeda o polvorienta.

Instale el dispositivo horizontalmente en lugares estables para evitar que se caiga.

**No gotee ni salpique líquidos sobre el dispositivo; no coloque sobre el dispositivo nada lleno de líquido.**

Instale el dispositivo en lugares bien ventilados y no bloquee su abertura de ventilación. Utilice el dispositivo solo dentro del rango nominal de entrada y salida.

**No desmonte el dispositivo usted mismo.**

**El dispositivo debe utilizarse con cables de red apantallados.**

## requerimientos de energía

Utilice cables de alimentación recomendados en la región según su especificación nominal.

Utilice una fuente de alimentación que cumpla con los requisitos de SELV (voltaje de seguridad muy bajo) y suministre energía con un voltaje nominal que cumpla con la Fuente de energía limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas del dispositivo.

El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

## Actualización de dispositivo

No corte la fuente de alimentación durante la actualización del dispositivo. La fuente de alimentación se puede cortar solo después de que el dispositivo haya completado la actualización y se haya reiniciado.

# Tabla de contenido

Prefacio .....	I
Salvaguardias y advertencias importantes.....	
<b>III 1 Estructura .....</b>	<b>1</b>
1.1 Introducción.....	1
1.2 Características .....	1
1.3 Panel frontal .....	1
1.4 Panel trasero.....	3
<b>2 Instalación .....</b>	<b>4</b>
2.1 VTH .....	4
2.2 VTO .....	4
<b>3 Cableado.....</b>	<b>6</b>
3.1 Preparativos .....	6
3.1.1 Reglas de conexión de puertos.....	6
3.1.2 Especificaciones del cable .....	7
3.2 Cableado de un VTO y un VTH .....	7
3.3 Cableado de tres VTO y un VTH.....	8
3.4 Cableado de dos VTO y tres VTH.....	9
<b>4 Operaciones del menú.....</b>	<b>10</b>
4.1 Instantáneas .....	10
4.2 Hora.....	12
4.3 Restauración de la configuración predeterminada.....	12
<b>Appendix 1 Recomendaciones de ciberseguridad .....</b>	<b>14</b>

# 1 Estructura

## 1.1 Introducción

El videoportero analógico de 4 hilos consta de una estación de puerta ("VTO") y un monitor interior ("VTH"). Es aplicable a edificios, como edificios residenciales, para que las personas realicen llamadas de voz y video. El VTO se instala al aire libre y el VTH se instala en el interior.

## 1.2 Características

### VTH

Comunicación de video / voz en tiempo real

Se puede conectar a tres VTO Se puede conectar a cámaras (CVBS)

Plug-and-play

### VTO

Comunicación de voz en tiempo real

Iluminación IR autoadaptable

## 1.3 Panel frontal

Figure 1-1 Panel frontal

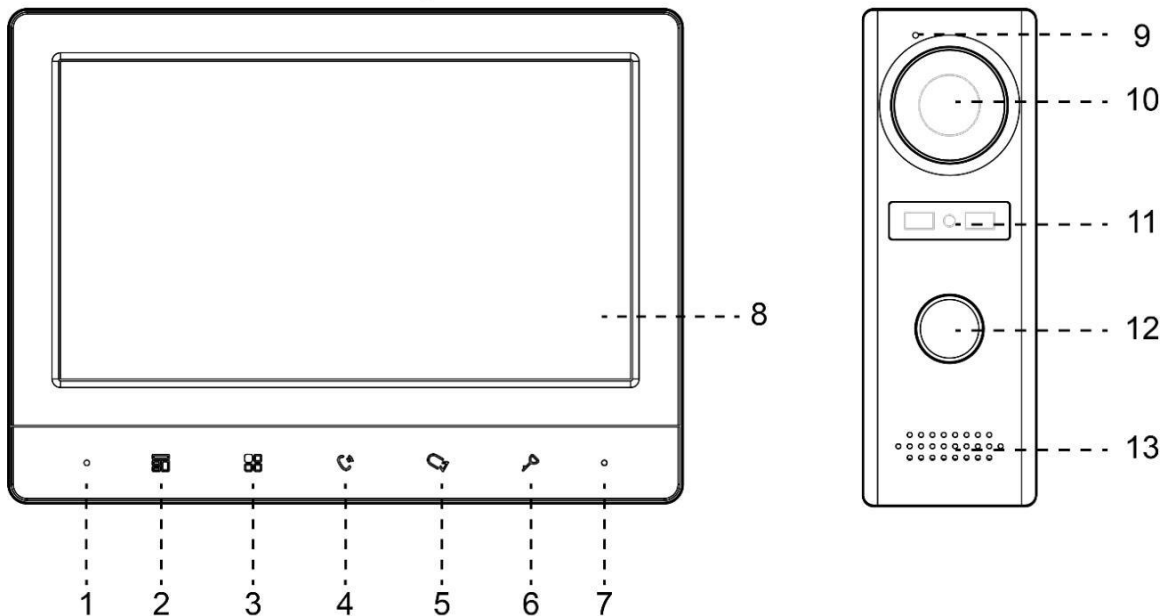







Tabla 1-1 Panel frontal

No.	Icono	Descripción
1	-	<b>Micrófono.</b>
2		<ul style="list-style-type: none"> <li>● Presione para colgar la llamada entrante.</li> <li>● Tome instantáneas durante la supervisión (solo compatible con</li> </ul>
3		<p>VTH1020J-T). Active la pantalla y abra el menú.</p> <p>Para saber cómo operar el menú, consulte "4 Operaciones de</p>
4		<p>menú". Cuando alguien llama desde el VTO:</p> <ul style="list-style-type: none"> <li>● Presione una vez para comunicarse por voz con la persona. Presione</li> <li>● dos veces rápidamente para colgar.</li> </ul>
5		<p><b>Cuando alguien llama desde el VTO:</b></p> <ul style="list-style-type: none"> <li>● Presione para hablar con la persona (solo compatible con VTH1020J).</li> <li>● Presione para tomar instantáneas (solo compatible con VTH1020J-T).</li> </ul> <p>Cuando nadie llama:</p> <ul style="list-style-type: none"> <li>● Presione una, dos, tres y cuatro veces para ver video en vivo de: VTO1, VTO2, cámara analógica 1 y cámara analógica 2 respectivamente.</li> <li>● En cualquier video en vivo, presione para tomar instantáneas (solo compatible con VTH1020J-T).</li> </ul>
6		Cuando alguien está llamando, presione para abrir la puerta donde está instalado el VTO. Indicador
7	-	de encendido.
8	-	<b>Pantalla LCD.</b>
9	-	<b>Micrófono.</b>
10	-	<b>Cámara integrada.</b>
11	-	Indicador de encendido.
12	-	<p>Botón de llamada.</p> <p>Presione una vez para llamar al VTH.</p> <p>Mantenga pulsado durante 10 segundos para cambiar el tipo de campana del VTO. El indicador de encendido parpadeará.</p> <p>Mantenga pulsado durante 15 segundos para subir el volumen del timbre del VTO. El indicador de encendido parpadeará. Cuando el volumen alcanza el máximo, este paso lo establecerá al mínimo. Repita este paso para configurar el volumen apropiado.</p> <p>Mantenga pulsado durante 20 segundos para cambiar a DWDR (rango dinámico amplio digital) / modo normal para el VTO. El indicador de encendido parpadeará.</p>
13	-	<b>Altavoz.</b>

## 1.4 Panel trasero

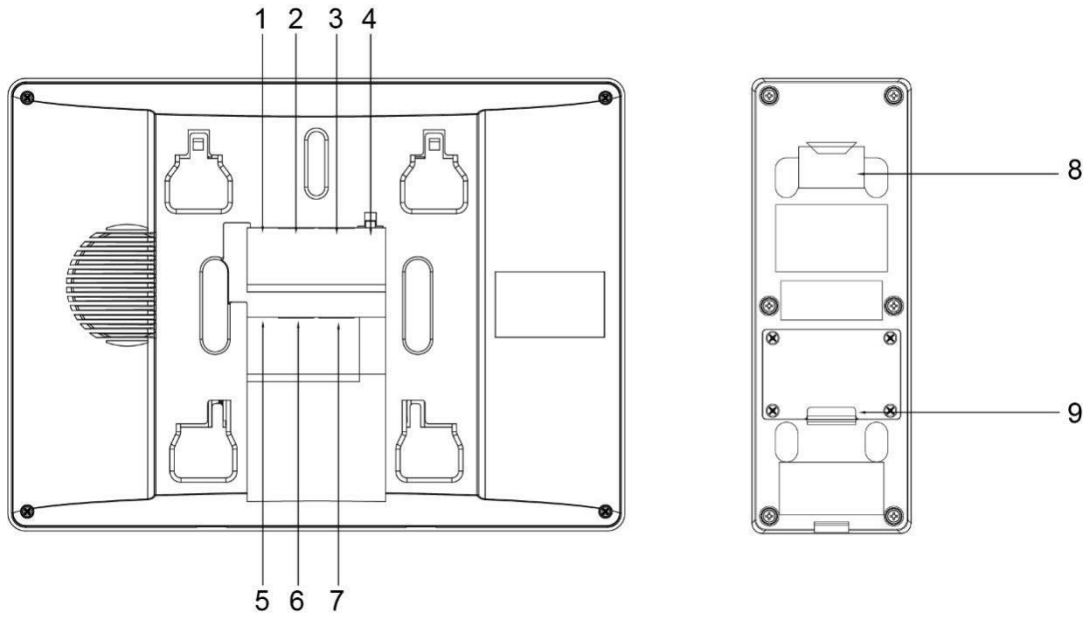


Tabla 1-2 Panel trasero

No.	Descripción	No.	Descripción
1	Puerto de cámara analógica 1.	6	Puerto en cascada VTH 1.
2	Puerto VTO 1.	7	Puerto en cascada VTH 2.
3	Puerto VTO 2.	8	Ranura colgante VTO.
4	Entrada de alimentación.	9	Alambres
5	Puerto de cámara analógica 2.	-	-

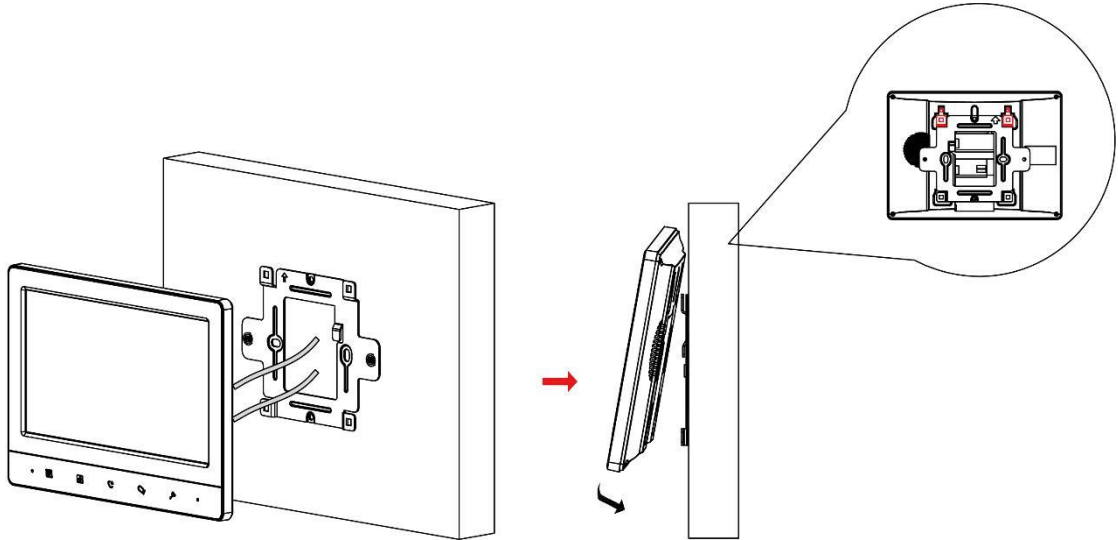


## 2 Instalación

### 2.1 VTH

Fije el soporte en la pared con tornillos, cuelgue el VTH en el soporte y luego aplique sellador de silicona en el espacio entre el dispositivo y la pared.

Figure 2-1 Instalación VTH



### 2.2 VTO

Instale el soporte VTO en la pared y luego cuelgue el VTO en el soporte; o instale la cubierta VTO en la pared y luego cuelgue el VTO en la cubierta. Finalmente, aplique sellador de silicona en el espacio entre el dispositivo y la pared.

Figure 2-2 Instalación de VTO

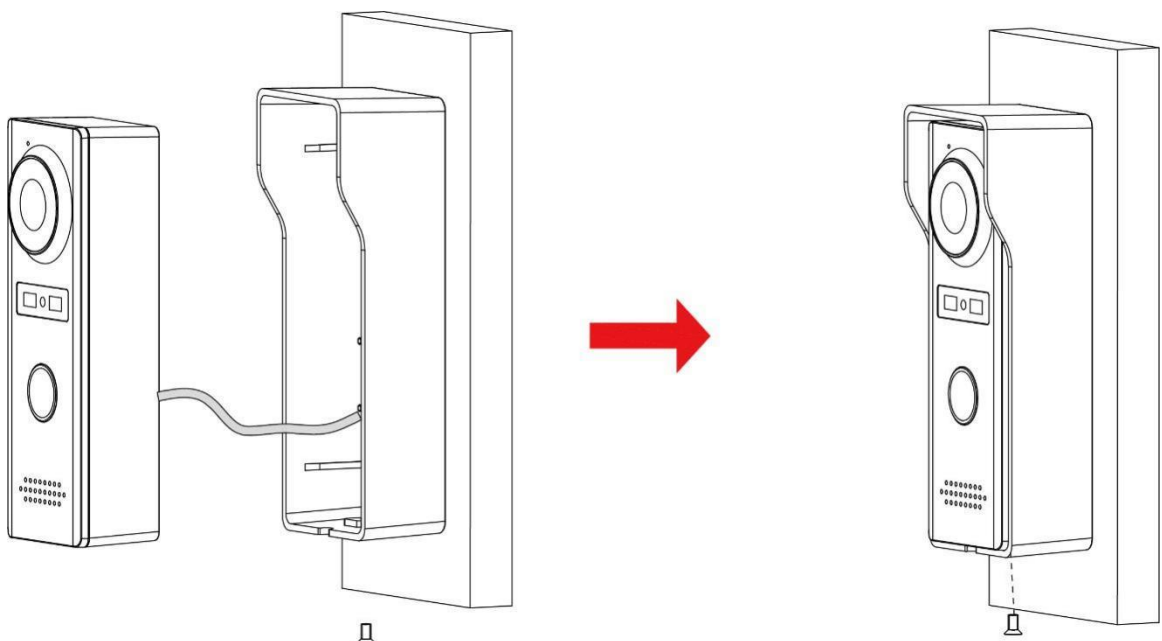
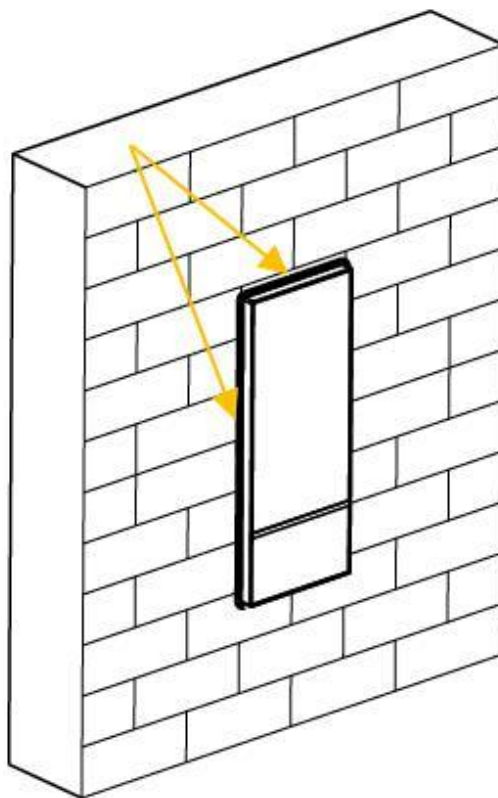


Figure 2-3 Aplique sellador de silicona en el espacio entre el dispositivo y la pared.



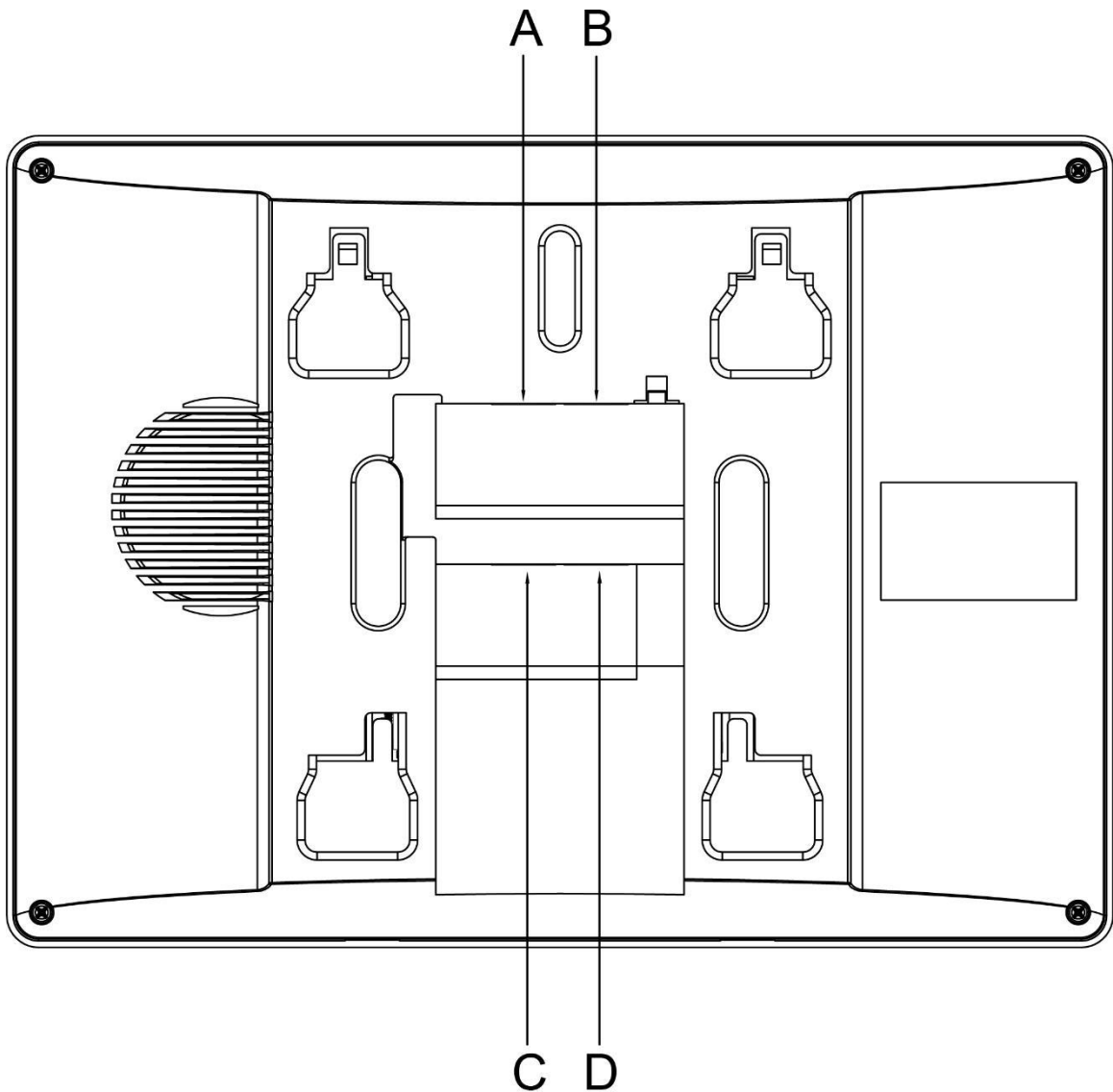
## 3 Cableado

Como máximo, se pueden conectar 2 VTO y 3 VTH en un sistema de comunicación.

### 3.1 Preparativos

#### 3.1.1 Reglas de conexión de puertos

Figure 3-1 Reglas de conexión de puertos



El puerto A de un VTH se puede conectar al puerto C de otro VTH para realizar la comunicación de datos. El puerto B de un VTH se puede conectar al puerto D de otro VTH para realizar la comunicación de datos. El puerto A de un VTH no se puede conectar al puerto B o D de otro VTH para realizar la comunicación de datos. El puerto C de un VTH no se puede conectar al puerto B o D de otro VTH para realizar la comunicación de datos.

### 3.1.2 Especificaciones del cable

Dependiendo de la distancia entre el VTO y el VTH, debe seleccionar cables RVV4 de diferentes especificaciones.

Tabla 3-1 Especificaciones del cable

Distancia de transmisión (TD)	Especificación del cable RVV4
TD ≤ 10 m	RVV4 × 0,3 mm <sup>2</sup>
10 m <TD ≤ 30 m	RVV4 × 0,5 mm <sup>2</sup>
30 m <TD ≤ 50 m	RVV4 × 0,75 mm <sup>2</sup>



Si la distancia entre el VTO y el VTH es superior a 50 m, utilice cables coaxiales.

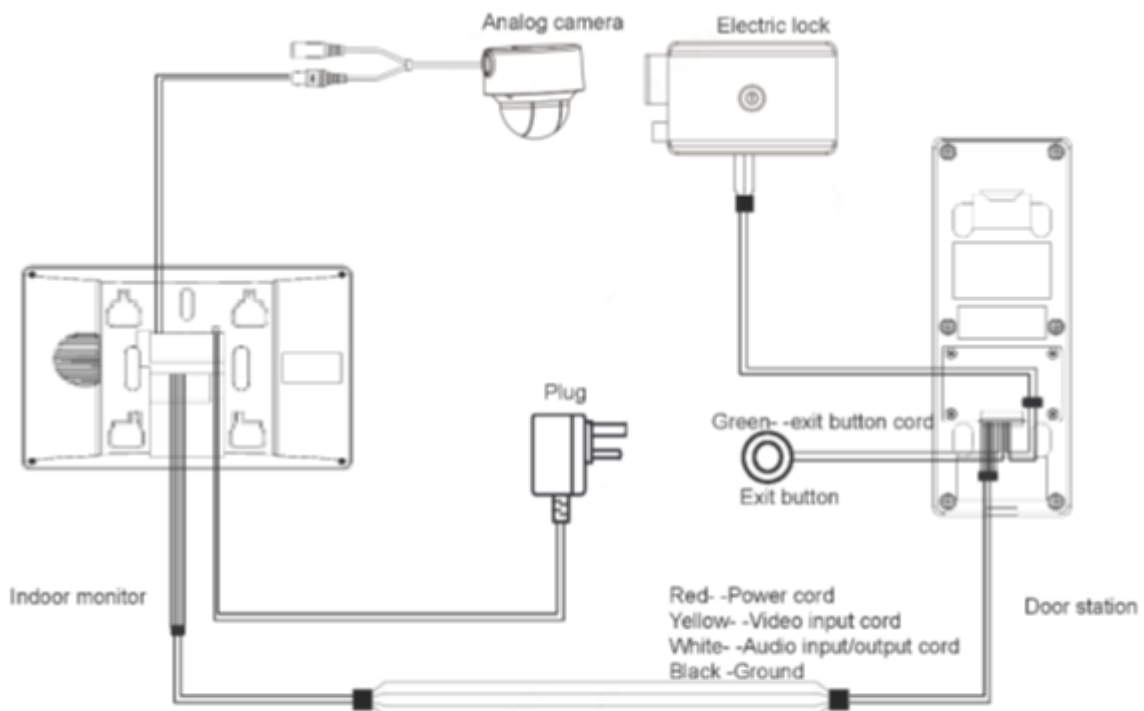


No tire de los cables con violencia.

Durante el cableado, envuelva las uniones del cable con cinta aislante de goma para evitar cortocircuitos.

## 3.2 Cableado OneVTO y OneVTH

Figure 3-2 Cableado (1)

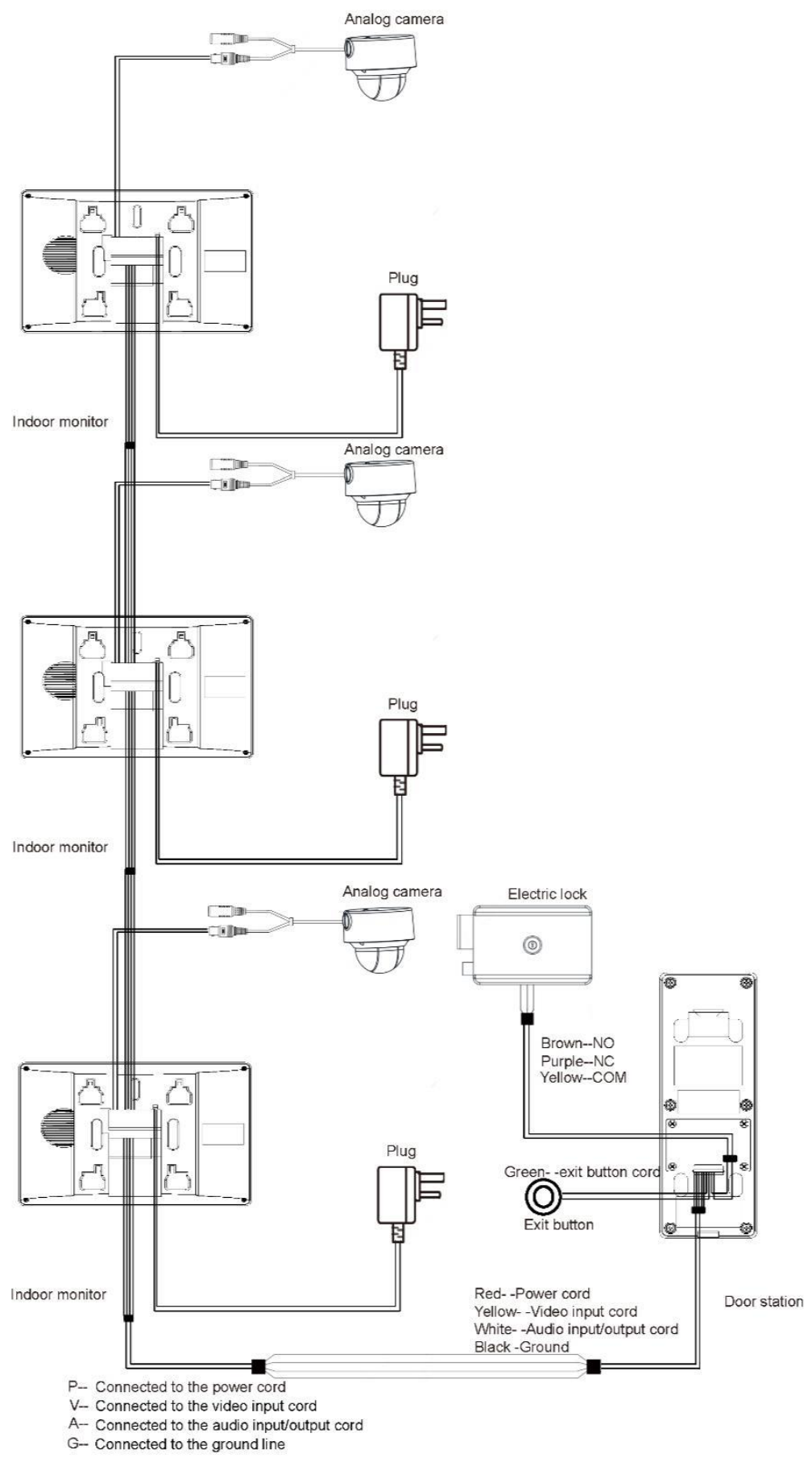


P- Connected to the power cord  
V- Connected to the video input cord  
A- Connected to the audio input/output cord  
G- Connected to the ground line

<b>ROJO</b>	- + 12V DC (alimentado desde el monitor)
<b>AMARILLO</b>	Video de la cámara
<b>BLANCO</b>	Audio
<b>NEGRO</b>	Masa
<b>VERDE</b>	Botón de salida (cortocircuito a tierra)
<b>NARANJA</b>	Interruptor de láminas (cortocircuito a tierra)
<b>VIOLETA</b>	Relé Contacto NA
<b>AZUL</b>	Contacto de relé COM
<b>MARRON</b>	Contacto de relé NC

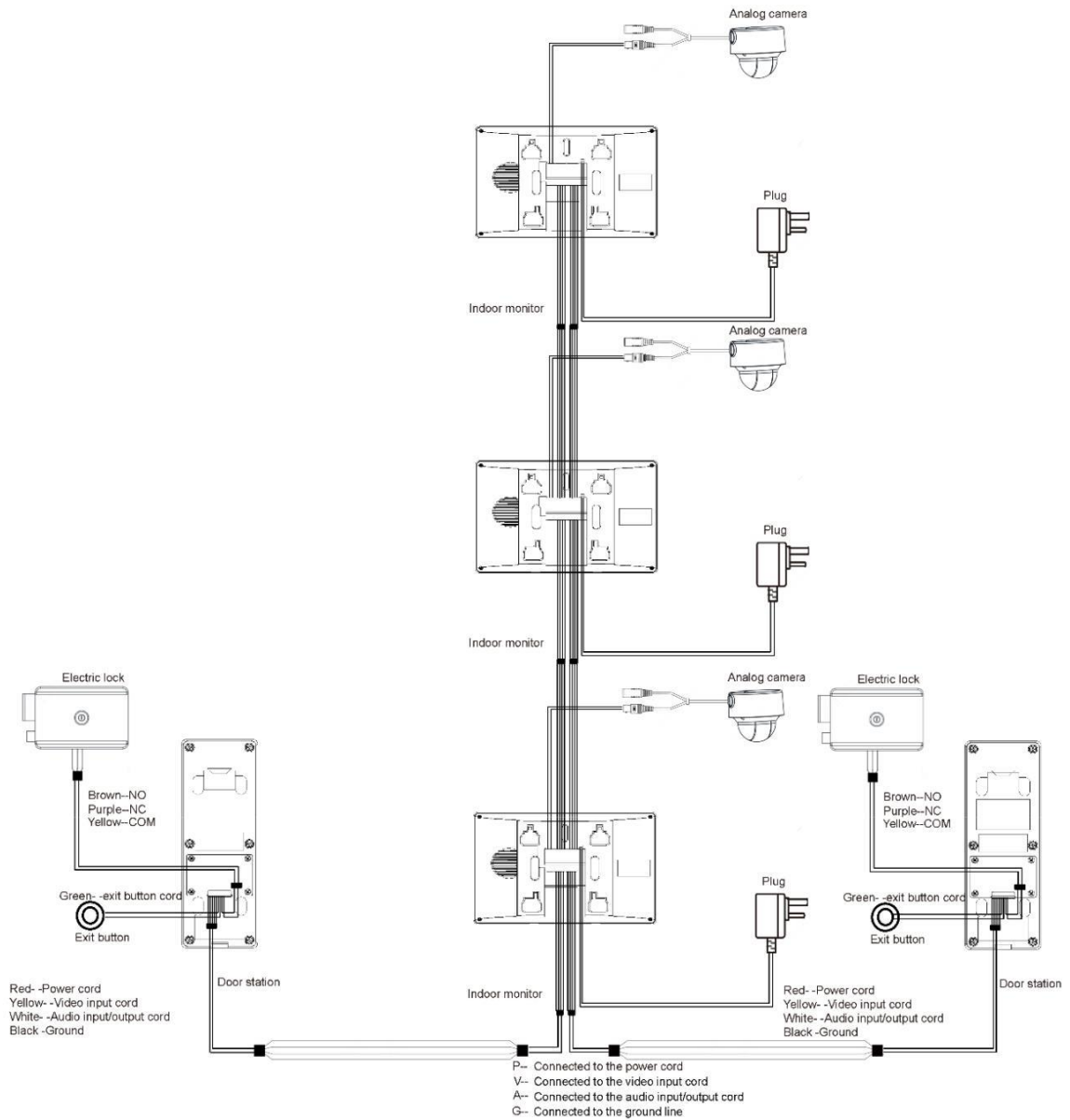
### 3.3 Wiring Three VTOs y One VTH

Figure 3-3 Cableado (2)



## 3.4 Cableado Dos VTOs y Tres VTHs

Figure 3-4 Cableado (3)



Las cámaras analógicas recomendadas (CVBS) son de la serie HAC 1230.

## 4 Operaciones de menú

Puede configurar las funciones del VTH, como volumen, brillo y más.



Solo VTH1020J-T admite el Instantáneas y Hora funciones. Todas las configuraciones se guardarán después de salir del menú.

Figure 4-1 Menú

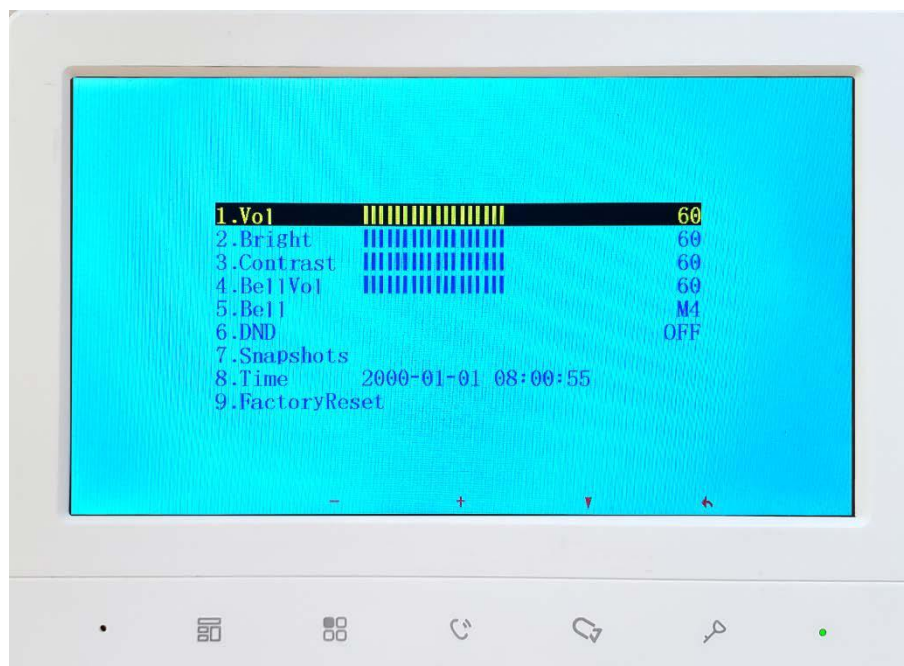


Tabla 4-1 Operaciones del menú

Icono	Función
	Se utiliza para confirmar su operación cuando está utilizando el Instantáneas y Hora funciones (solo compatible con VTH1020J-T).
	Ajustar Vol (volumen), Brillante (brillo), Contraste y BellVol (volumen de la campana), cambiar campana y apaga DND (No molestar). Aparecer
	Vol (volumen), Brillante (brillo), Contraste y BellVol (volumen de la campana), cambiar Campana, apagar DND (no molestar) y ajustar la hora.
	Selecciona un artículo.
	<ul style="list-style-type: none"> <li>● Salga del menú y bloquee la pantalla.</li> <li>● Vuelve a la interfaz anterior.</li> </ul>

### 4.1 Instantáneas

Puede tomar instantáneas durante el monitoreo y ver las instantáneas que ha tomado.




El VTH puede almacenar hasta 200 instantáneas. Si el almacenamiento está lleno, se sobrescribirán los anteriores.

## Tomando instantáneas

Durante el seguimiento.

**Step 1** Presione  para ir a la imagen de monitoreo que desee.

**Step 2** presiona , y entonces Exitoso aparecerá en la pantalla.

Cuando un VTO está llamando o en una llamada con un VTO, presione , y entonces Exitoso aparecerá en el pantalla.



Si la llamada dura más de 1 segundo, se tomará una instantánea automáticamente.

## Visualización de instantáneas

**Step 1** presiona  para abrir el menú.

**Step 2** presiona , Seleccione Instantáneas, y luego presione .

Figure 4-2 Lista de instantáneas



**Step 3** presiona  para seleccionar el que necesita y luego presione .






Para eliminar una instantánea, presione , Detele? aparecerá en la pantalla, y luego presione  a

confirmar.





Figure 4-3 Ver una instantánea



**Step 4** prensa  o  para ver la instantánea anterior o siguiente. O puedes presionar  volver a la lista de instantáneas y luego seleccione la que necesita.



Para eliminar una instantánea, presione , Detele? aparecerá en la pantalla, y luego presione  a confirmar.

## 4.2 Hora

**Step 1** prensa  para abrir el menú.

**Step 2** prensa  para seleccionar la parte del tiempo que desee.

**Step 3** prensa  para o  para ajustar el número.


## 4.3 Restaurar la configuración predeterminada

**Step 1** prensa  para abrir el menú.

**Step 2** prensa  para seleccionar FactoryReset.

Figure 4-4 Confirma tu operación



**Step 3** prensa  y luego el dispositivo se reiniciará.

# Appendix 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 muestran 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. Utilice contraseñas seguras

Consulte las siguientes sugerencias para establecer contraseñas:

**La longitud no debe ser inferior a 8 caracteres;**

**Incluya al menos dos tipos de personajes; los tipos de caracteres incluyen letras mayúsculas y minúsculas, números y símbolos;**

**No incluya 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 cliente inTime

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 "búsqueda automática de actualizaciones" para obtener información oportuna de las actualizaciones de firmware publicadas por el fabricante.

**Le sugerimos que descargue y utilice la última versión del software cliente.**

Recomendaciones "Es bueno 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 de computadoras especial y gabinete, e implemente permisos de control de acceso bien hechos y administración de claves para evitar que el personal no autorizado lleve a cabo contactos físicos, como daños en el hardware, conexión no autorizada de dispositivos extraíbles (como un disco flash USB). , puerto serie), etc.

## 2. Cambie las contraseñas con regularidad

Le sugerimos que cambie las contraseñas con regularidad para reducir el riesgo de ser adivinado o descifrado.

## 3. Establecer y actualizar la información de restablecimiento de contraseñas

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 sobre protección de contraseña. Si la información cambia, modifíquela a tiempo. Al configurar las preguntas de protección por contraseña, se sugiere no utilizar aquellas que se puedan adivinar fácilmente.

## 4. Habilite el 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 con la contraseña incorrecta varias veces, 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 en cualquier conjunto de números entre 1024 ~ 65535, reduciendo el riesgo de que personas ajenas puedan adivinar qué puertos está utilizando.

## 6. Habilite 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 que vincule la dirección IP y MAC de la puerta de enlace al dispositivo, reduciendo así el riesgo de suplantación de ARP.

## 8. Asignar cuentas y privilegios de forma razonable

De acuerdo con los requisitos comerciales y de administración, agregue usuarios de manera razonable y asígneles un conjunto mínimo de permisos.

## 9. Desactive los servicios innecesarios y elija los 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 de correo. **FTP:** elija SFTP y configure contraseñas seguras.

**Punto de acceso AP:** elija el modo de cifrado WPA2-PSK y configure contraseñas seguras.

## 10. Transmisión encriptada de audio y video

Si su contenido de datos de audio y video es muy importante o sensible, 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 cifrada provocará una pérdida en la eficiencia de la transmisión.

## 11. Auditoría segura

**Verificar usuarios en línea:** le sugerimos que verifique a los usuarios en línea con regularidad para ver si el dispositivo está conectado sin autorización.

**Verificar el registro del dispositivo:** al ver los registros, puede conocer las direcciones IP que se utilizaron 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 que habilite la función de registro de red para asegurarse de que los registros críticos estén sincronizados 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:

Desactive la función de asignación de puertos del enrutador para evitar el acceso directo a los dispositivos de la intranet desde la 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 utilizar VLAN, red GAP 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 permitidos para acceder al dispositivo.