

# Grabador de video en red

## Guía de inicio rápido



# Prefacio

## General

Esta guía de inicio rápido (en lo sucesivo, "el Manual") presenta las funciones y operaciones del dispositivo NVR (en lo sucesivo, "el NVR").

## Instrucciones de seguridad

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

Palabras de advertencia	Sentido
 <b>DANGER</b>	Indica un peligro de alto potencial que, si no se evita, provocará la muerte o lesiones graves.
 <b>WARNING</b>	Indica un peligro potencial medio o bajo que, si no se evita, podría provocar lesiones leves o moderadas.
 <b>CAUTION</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>TIPS</b>	Proporciona métodos para ayudarlo a resolver un problema o ahorrarle tiempo.
 <b>NOTE</b>	Proporciona información adicional como énfasis y complemento del texto.

## Revisión histórica

Versión	Contenido de revisión	Tiempo de liberación
V1.0.0	Primer lanzamiento.	julio 2020

## Aviso de protección de privacidad

Como usuario de NVR o controlador de datos, puede recopilar datos personales de otros, como rostro, huellas dactilares, número de placa del automóvil, dirección de correo electrónico, número de teléfono, GPS. 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 del área de vigilancia y proporcionar información relacionada. contacto.

## 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 cumplan con el Manual.
- El Manual se actualizaría de acuerdo con las últimas leyes y reglamentos de las regiones 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. Contacta el

servicio al cliente para el último programa y documentación complementaria.

- Todavía puede haber desviación en los datos técnicos, descripción de funciones y operaciones, o errores en la impresión. Si tiene alguna duda o disputa, consulte nuestra explicación final.
- Actualice el software del lector o pruebe con otro software de 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 NVR.
- Si hay alguna duda o controversia, consulte nuestra explicación final.

## Medidas de seguridad y advertencias importantes

La siguiente descripción es el método de aplicación correcto del NVR. Lea atentamente el Manual antes de su uso para evitar peligros y pérdidas materiales. Siga estrictamente el Manual durante la aplicación y consérvelo correctamente después de leerlo.

### Requisitos operativos

- Instale las cámaras PoE en interiores.
- No coloque ni instale el NVR en un área expuesta a la luz solar directa o cerca de un dispositivo generador de calor.
- No instale el NVR en un área húmeda, polvorienta o fuliginosa.
- Mantenga su instalación horizontal, o instálelo en lugares estables, y evite que se caiga.
- No gotee ni salpique líquidos sobre el NVR; no coloque en el NVR nada lleno de líquidos para evitar que los líquidos fluyan hacia el NVR.
- Instale el NVR en lugares bien ventilados; no bloquee su abertura de ventilación.
- Use el NVR solo dentro del rango nominal de entrada y salida.
- No desmonte el NVR arbitrariamente.
- Transporte, use y almacene el NVR dentro del rango permitido de humedad y temperatura.

### requerimientos de energía

- Use baterías de acuerdo con los requisitos. ¡De lo contrario, puede provocar incendios, explosiones o quemar las baterías!
- Para reemplazar las baterías, solo se puede usar el mismo tipo de baterías.
- Deseche las baterías agotadas de acuerdo con las instrucciones.
- Utilice cables eléctricos dentro de las especificaciones nominales recomendadas por las normas locales.
- Utilice un adaptador de corriente estándar compatible con este NVR. De lo contrario, el usuario asumirá las lesiones personales resultantes o los daños al NVR.
- Utilice una fuente de alimentación que cumpla con los requisitos SELV (voltaje extra bajo de seguridad) y suministre energía con un voltaje nominal que cumpla con la fuente de alimentación limitada en IEC60950-1. Para conocer los requisitos específicos de la fuente de alimentación, consulte las etiquetas de los dispositivos.
- Los productos con estructura de categoría I se conectarán a la toma de salida de la red eléctrica, que está equipada con protección a tierra.
- El acoplador de electrodomésticos es un dispositivo de desconexión. Durante el uso normal, mantenga un ángulo que facilite la operación.

# Tabla de contenido

Prefacio.....	YO Medidas de
seguridad y advertencias importantes.....	III 1 Operaciones
locales.....	1
1.1 Iniciar el NVR.....	1
1.2 Inicialización del NVR.....	1
1.3 Configuración de la red.....	4
1.4 Adición de cámara IP.....	6
1.4.1 Inicialización de la cámara IP.....	6
1.4.2 Agregar cámara IP por resultado de búsqueda.....	10
1.4.3 Adición manual de cámaras IP.....	12
1.5 Configuración del horario de almacenamiento de video grabado.....	15
1.6 Configuración de ajustes de P2P.....	17
1.6.1 Habilitación de la función P2P.....	17
1.6.2 Adición del NVR al cliente de teléfono inteligente.....	18
1.7 Detección de movimiento inteligente.....	19
1.8 Vista en vivo.....	21
1.9 Reproducción de grabación.....	23
2 Iniciar sesión en la Web.....	25
Apéndice 1 Recomendaciones sobre ciberseguridad.....	26

# 1 Operaciones locales



Se pueden encontrar ligeras diferencias en las interfaces de diferentes modelos. Las siguientes cifras son para solo referencia. Prevalecerá el producto real.

## 1.1 Iniciar el NVR

Antes de iniciar el NVR, asegúrese de que:

- El voltaje de entrada nominal coincide con los requisitos de energía del NVR.
- La conexión del cable de alimentación está lista.
- Para la seguridad del dispositivo, primero conecte el NVR al adaptador de corriente y luego conéctelo a la toma de corriente.
- Utilice siempre corriente estable. Se recomienda utilizar UPS como fuente de alimentación.

## 1.2 Inicialización del NVR

Este tema muestra cómo inicializar el NVR antes de usarlo.

### Información de contexto

Al iniciar por primera vez, debe configurar la información de la contraseña para **administración** (por defecto). Para garantizar la seguridad del dispositivo, le recomendamos encarecidamente que conserve correctamente la contraseña de inicio de sesión y la modifique periódicamente.

### Procedimiento

Paso 1 Encienda el NVR.

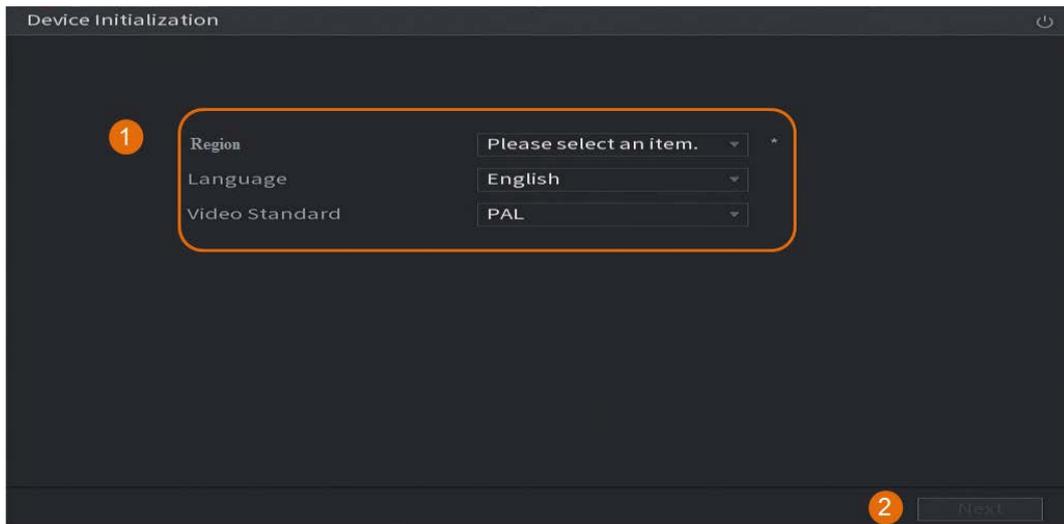
El sistema ingresa a la interfaz de inicialización del dispositivo.

Paso 2 En las listas desplegables, seleccione la región, el idioma y el estándar de video según sea necesario.



Puede cambiar esta configuración en las páginas de configuración del NVR después de la inicialización.

Figura 1-1 Establecer ubicación, idioma y estándar de video

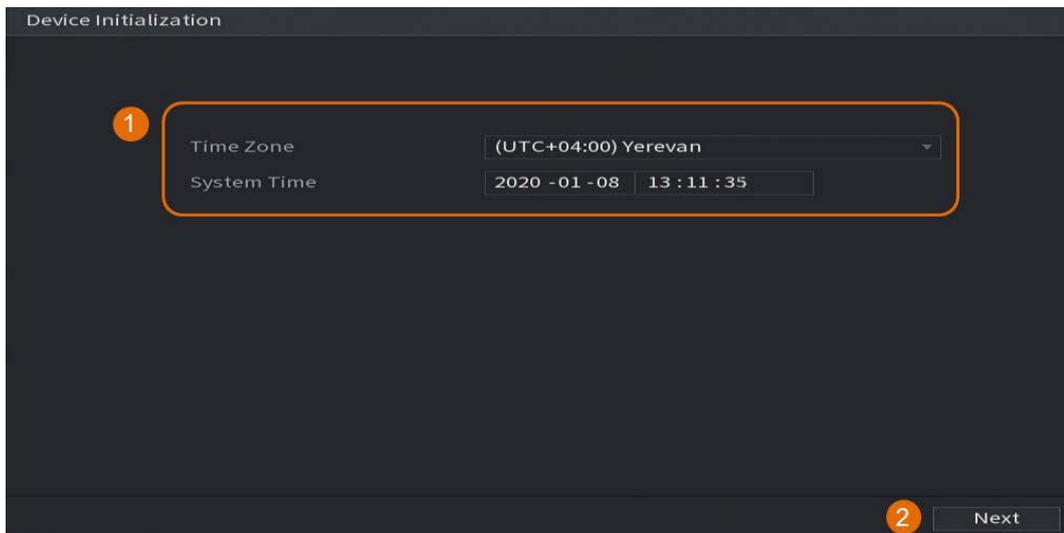


**Paso 3** Hacer clic **próximo**.

**Paso 4** Lea el Acuerdo de licencia de software y seleccione **He leído y estoy de acuerdo con todos los términos** y luego haga clic en **próximo**.

**Paso 5** Seleccione la zona horaria y configure la hora del sistema, y luego haga clic en **próximo**.

Figura 1-2 Configurar la zona horaria y la hora del sistema



**Paso 6** Configure la información de la contraseña para el administrador del dispositivo y luego haga clic en **próximo**.

Figura 1-3 Configurar información de contraseña

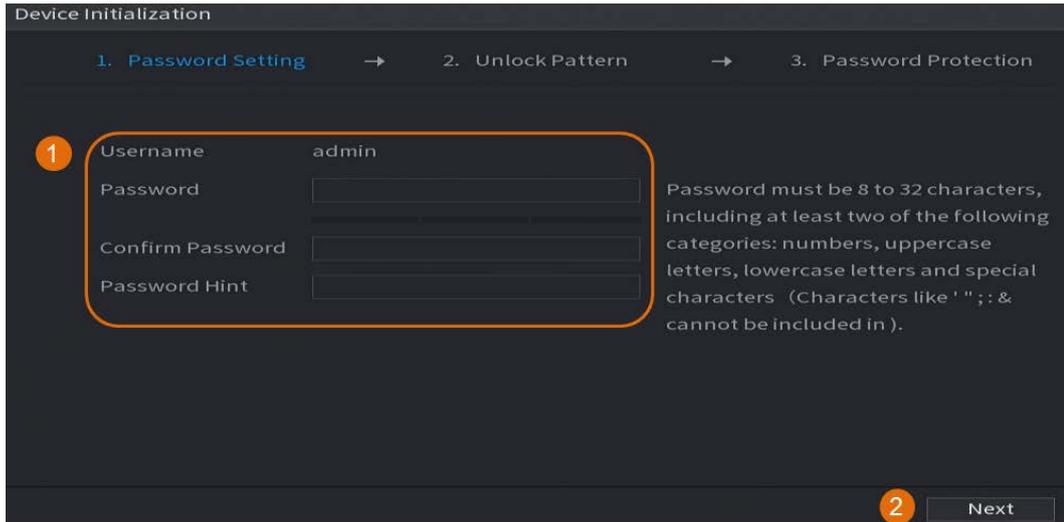
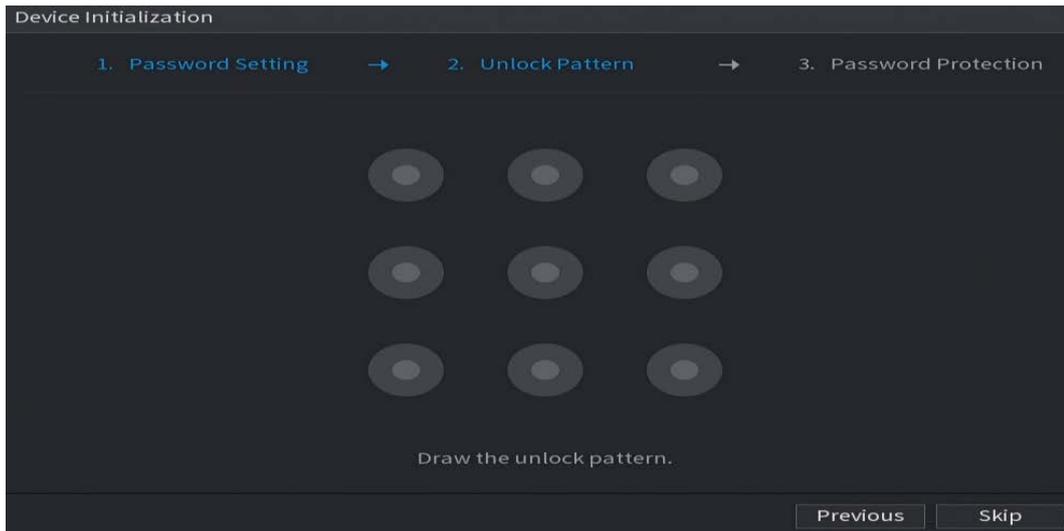


Tabla 1-1 Información de contraseña

Parámetro	Descripción
Nombre de usuario	Por defecto, el usuario es <b>administración</b> y no puedes cambiarlo.
Clave	Introduzca una nueva contraseña para el administrador del dispositivo en <b>Clave</b> y confirme la contraseña en el siguiente campo.
Confirmar contraseña	 La nueva contraseña se puede configurar de 8 caracteres a 32 caracteres y contiene al menos dos tipos de números, letras y caracteres especiales (excluyendo "", "", "", ":", "." y "&").
Pista de la contraseña	Ingresa una pregunta rápida que lo ayudará a recordar la contraseña de su dispositivo.  En la interfaz de inicio de sesión, haga clic en  y se mostrará el aviso para ayudarlo a restablecer la contraseña.

**Paso 7** (Opcional) Use el mouse para dibujar un patrón de desbloqueo y luego vuelva a dibujarlo para confirmarlo.

Figura 1-4 Dibujar un patrón de desbloqueo

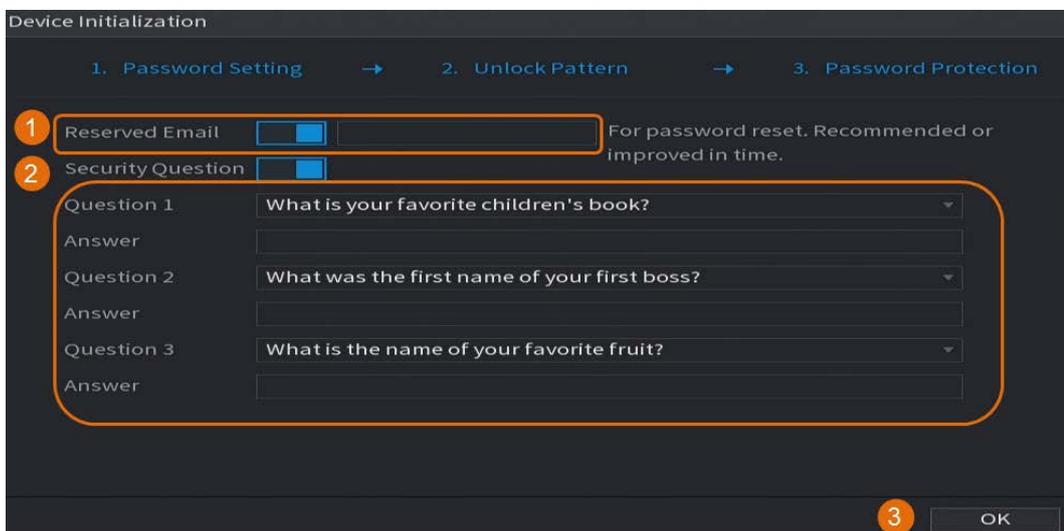


- El patrón que desea establecer debe cruzar al menos cuatro puntos.
- Si no desea configurar el patrón de desbloqueo, haga clic en **Saltar**.
- Una vez que haya configurado el patrón de desbloqueo, se utilizará como predeterminado método de autenticación. Si omite esta configuración, ingrese la contraseña para iniciar sesión.

**Paso 8** (Opcional) Aplicar correo electrónico reservado y preguntas de seguridad al NVR.

- Habilitar **Correo electrónico reservado** e ingrese la dirección de correo electrónico.
- Habilitar **Pregunta de seguridad** y seleccione preguntas de las listas desplegables para **Pregunta 1**, **Pregunta 2**, y **Pregunta 3** y luego ingrese las respuestas a esas preguntas.

Figura 1-5 Aplicar correo electrónico reservado y preguntas de seguridad



**Paso 9** Hacer clic **OK**.

## 1.3 Configuración de la red

Puede configurar los ajustes de red básicos, como el modo de red, la versión de IP y la dirección IP para el NVR.

**Paso 1** Seleccione **Menú principal > LA RED > TCP/IP**.

**Paso 2** Configurar parámetros.



También puede configurar los parámetros de red en el Asistente de inicio.

Figura 1-6 TCP/IP

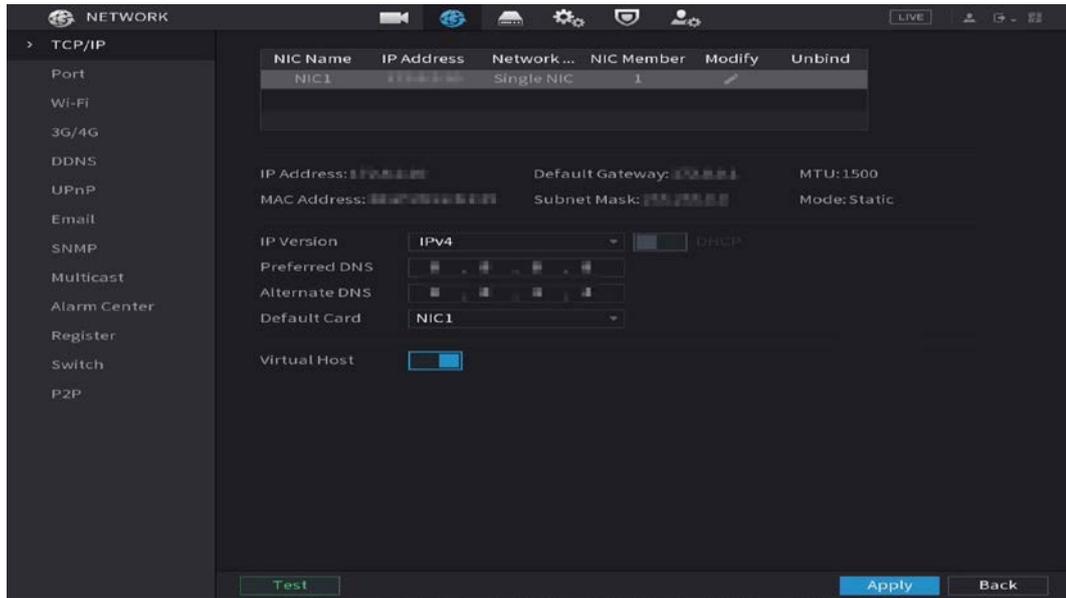


Tabla 1-2 Parámetros de TCP/IP

Parámetro	Descripción
Versión IP	En el <b>Versión IP</b> lista, puede seleccionar <b>IPv4</b> o <b>IPv6</b> . Ambas versiones son compatibles para el acceso.
Dirección MAC	Muestra la dirección MAC del NVR.
DHCP	Habilite la función DHCP. La dirección IP, la máscara de subred y la puerta de enlace predeterminada no están disponibles para la configuración una vez que se habilita DHCP. <ul style="list-style-type: none"> <li>● Si DHCP es efectivo, la información obtenida se mostrará en la <b>Dirección IP</b>, <b>Máscara de subred</b> y <b>Puerta de enlace predeterminada</b>. Si no, todos los valores muestran 0.0.0.0.</li> <li>● Si la conexión PPPoE se realiza correctamente, la dirección IP, la máscara de subred, la puerta de enlace predeterminada y el DHCP no estarán disponibles para la configuración.</li> </ul>
Dirección IP	Ingrese la dirección IP y configure la máscara de subred correspondiente y la puerta de enlace predeterminada.  <p>La dirección IP y la puerta de enlace predeterminada deben estar en la misma red segmento.</p>
Máscara de subred	
Puerta de enlace predeterminada	
DNS preferido	Introduzca la dirección IP de DNS.
DNS alternativo	Ingrese la dirección IP del DNS alternativo.

Parámetro	Descripción
MTU	<p>Introduzca un valor para la tarjeta de red. El valor varía de 1280 bytes a 1500 bytes. El valor predeterminado es 1500.</p> <p>Los valores de MTU sugeridos son los siguientes.</p> <ul style="list-style-type: none"> <li>● 1500: El mayor valor del paquete de información de Ethernet. Este valor generalmente se selecciona si no hay una conexión PPPoE o VPN, y también es el valor predeterminado de algunos enrutadores, adaptadores de red y conmutadores.</li> <li>● 1492: valor optimizado para PPPoE.</li> <li>● 1468: Valor optimizado para DHCP.</li> <li>● 1450: valor optimizado para VPN.</li> </ul>
Prueba	Hacer clic <b>Prueba</b> para probar si la dirección IP y la puerta de enlace ingresadas están interconectadas.

**Paso 3** Hacer clic **OK**.

## 1.4 Adición de cámara IP

Puede agregar una cámara IP por resultado de búsqueda o ingresando manualmente la información de IP.



Las cámaras que desee agregar deben estar en la misma red que el NVR.

### 1.4.1 Inicialización de la cámara IP

El tema muestra cómo inicializar cámaras nuevas o las cámaras después de restaurar los valores predeterminados de fábrica.

#### Información de contexto

La cámara IP debe inicializarse antes de conectarse a un NVR; de lo contrario, la conexión fallará. La inicialización cambiará la contraseña de inicio de sesión y la dirección IP de la cámara IP.



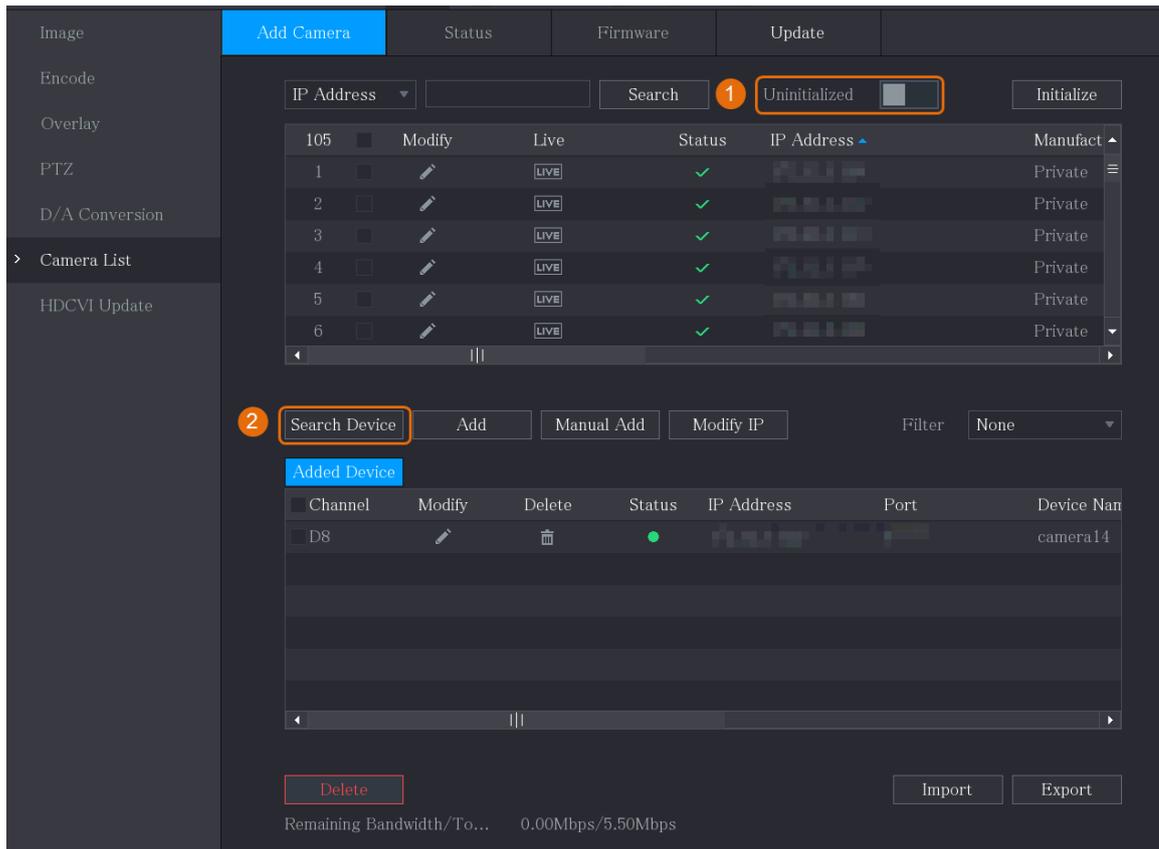
Cuando conecte una cámara al NVR a través del puerto PoE, el NVR inicializará automáticamente el cámara. Y la cámara adopta la contraseña y la información de correo electrónico del NVR de forma predeterminada.

#### Procedimiento

**Paso 1** Seleccione **Menú principal > Cámara > Lista de cámaras > Agregar cámara**.

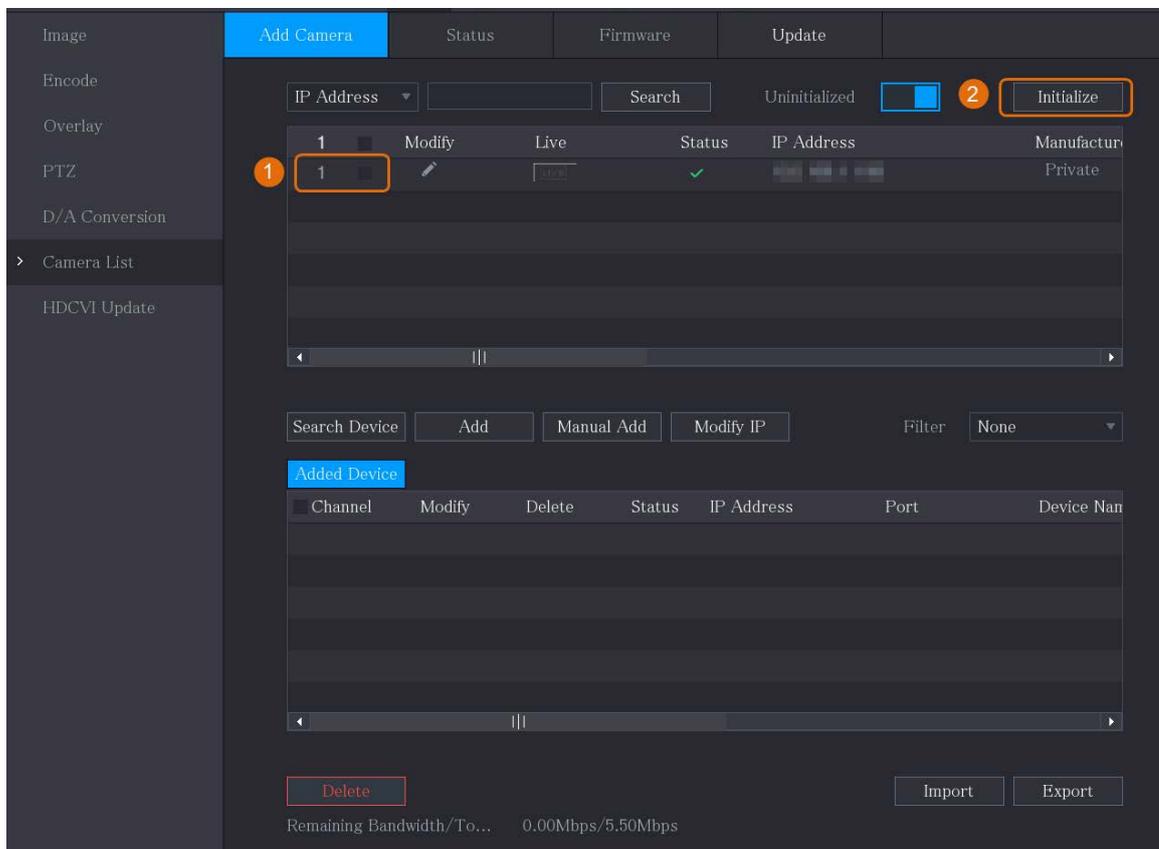
**Paso 2** Habilite **no inicializado** y luego haga clic en **Dispositivo de búsqueda**.

Figura 1-7 Buscar dispositivo no inicializado



**Paso 3** Seleccione la cámara que desea inicializar y luego haga clic en **Inicializar**.

Figura 1-8 Inicializar la cámara



**Paso 4** Aplique la contraseña y la información de correo electrónico a la cámara IP.

- Utilice la configuración del NVR.

1. Seleccione **Usando la contraseña actual del dispositivo y la información de correo electrónico.**



Esta casilla de verificación está seleccionada por defecto.

Figura 1-9 Aplicar la configuración del dispositivo

The screenshot shows a dark-themed 'Enter Password' screen. At the top, the title 'Enter Password' is visible. Below it, there is a radio button option labeled 'Using current device password and email info.' which is selected, indicated by a checkmark and a blue circle. A red circle with the number '1' is placed to the left of this option. At the bottom right, there is a 'Next' button, with a red circle containing the number '2' next to it.

2. Haga clic en **próximo.**

● Establecer manualmente la contraseña y la información de correo electrónico.

1. Cancelar **Usando la contraseña actual del dispositivo y la información de correo electrónico.**

Figura 1-10 Establecer contraseña

The screenshot shows the 'Enter Password' screen with the 'Using current device password and email info.' option unselected. A red circle with the number '1' is next to this option. Below it, a rounded rectangular area is highlighted with a red border, containing a form with the following fields: 'User' with the value 'admin', 'Password' with an empty input field, and 'Confirm Password' with an empty input field. A red circle with the number '2' is next to the 'User' field. Below the password fields, there is a text instruction: '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 ' ' ; : & )'. At the bottom right, there is a 'Next' button, with a red circle containing the number '3' next to it.

2. Establecer contraseña.



Figura 1-12 Configurar dirección IP

NETWORK

Checked Device No.: 1

DHCP

STATIC

IP Address  Incremental Value

Subnet Mask

Default Gateway

1	IP Address
1	<input type="text"/>

Back Next Skip

- Paso 6** Hacer clic **próximo**.  
Espere de 1 a 2 minutos para que se complete la inicialización.
- Paso 7** Hacer clic **Acabado**.

## 1.4.2 Agregar cámara IP por resultado de búsqueda

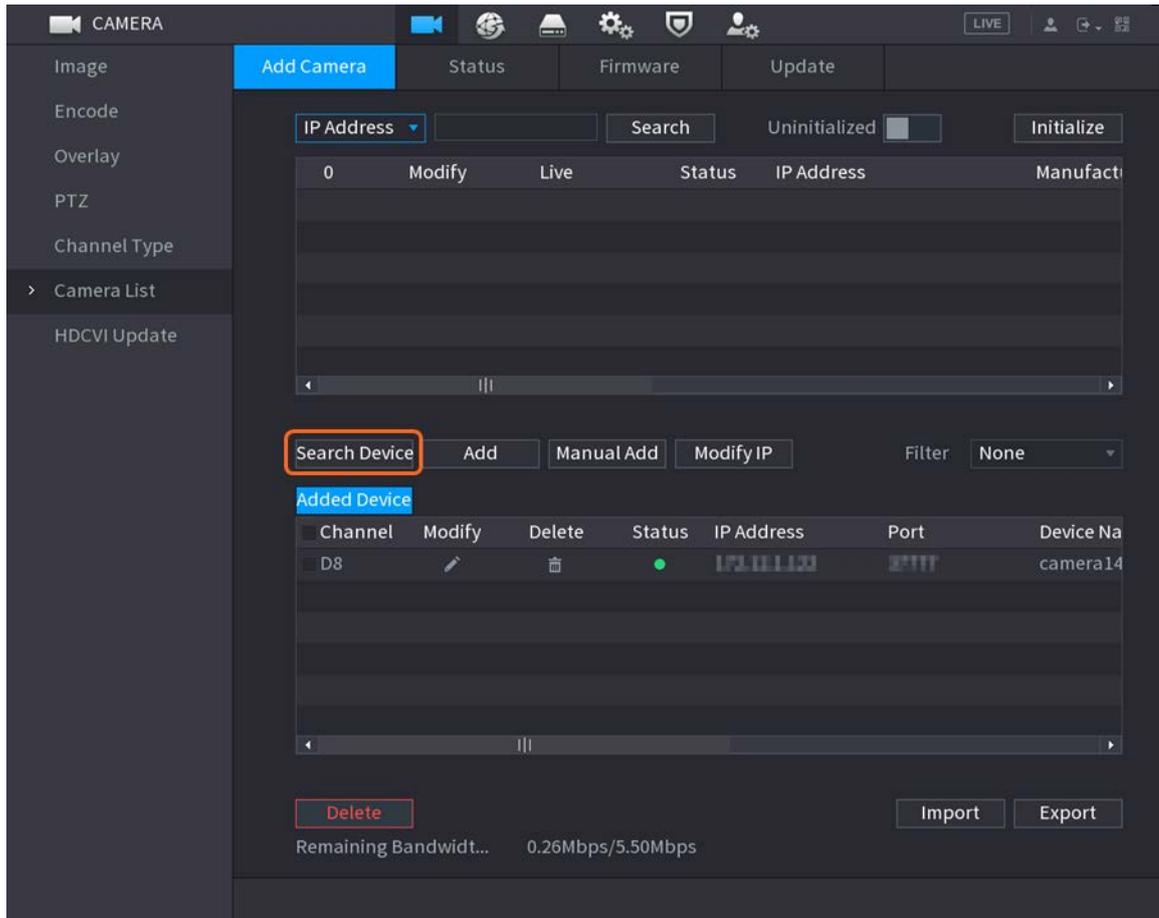
requisitos previos

Asegúrese de que las cámaras que desea agregar ya se hayan inicializado y conectado a la red correcta.

Procedimiento

- Paso 1** Seleccione **Menú principal > CÁMARA > Lista de cámaras > Agregar cámara**. Hacer clic
- Paso 2** **Dispositivo de búsqueda**.

Figura 1-13 Dispositivo de búsqueda



**Paso 3** Añadir cámaras IP.

- Agregar haciendo doble clic: haga doble clic en la cámara de destino para agregarla a **Dispositivo agregado** lista.



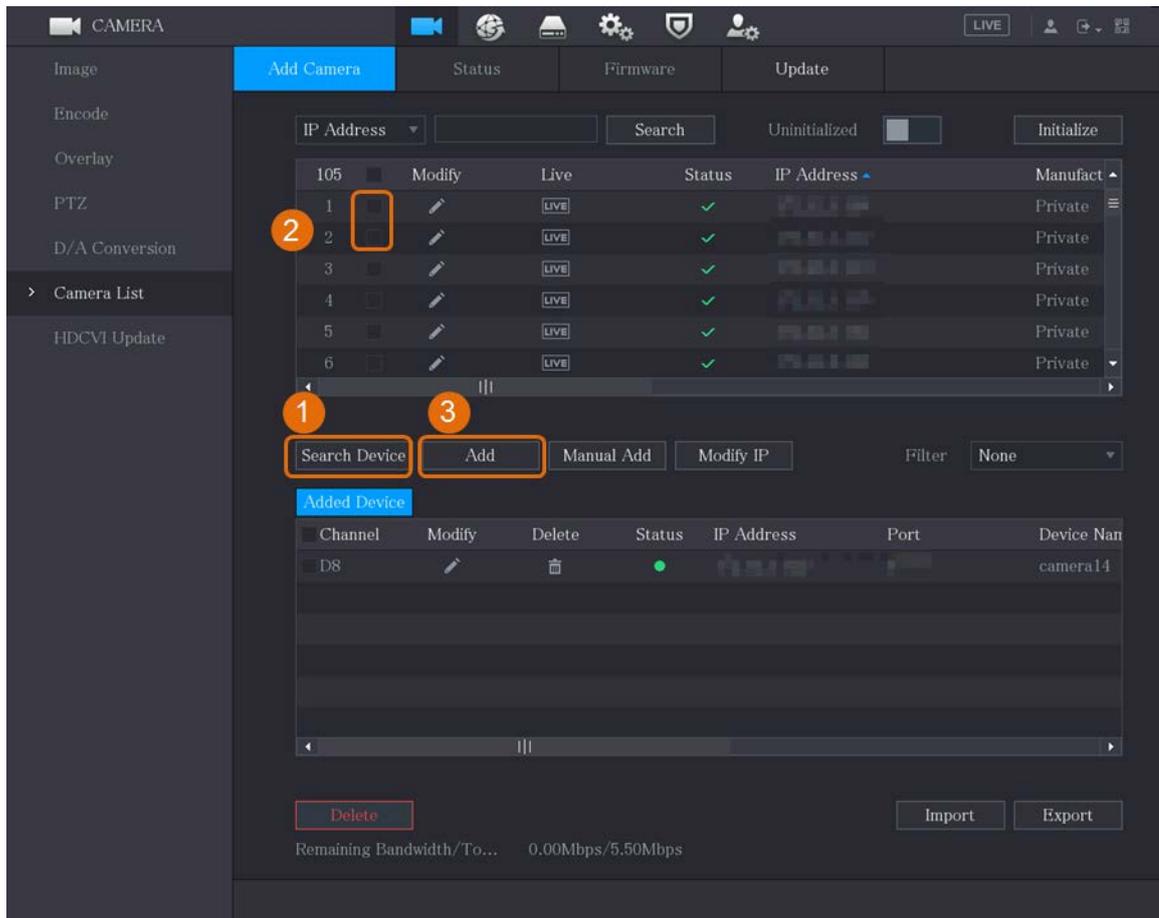
Puede agregar solo una cámara por resultado de búsqueda a la vez.

- Agregar por casilla de verificación: seleccione la casilla de verificación de la cámara de destino y luego haga clic en **Agregar** para agregarlo a **Dispositivo agregado** lista.



Puede seleccionar más de una casilla de verificación y agregar cámaras en lotes.

Figura 1-14 Agregar cámara IP por resultado de búsqueda



Resultado

- Si el estado de la cámara agregada es verde (●), indica que la cámara se ha agregado correctamente a la (NVR).
- Si el estado de la cámara agregada es rojo (●), indica falla de conexión entre la cámara y el NVR. Verifique los parámetros de la cámara, como la contraseña, el protocolo y el número de canal, y luego intente agregarlo nuevamente.

### 1.4.3 Adición manual de cámaras IP

Puede agregar una cámara IP por información de IP a la vez.

requisitos previos

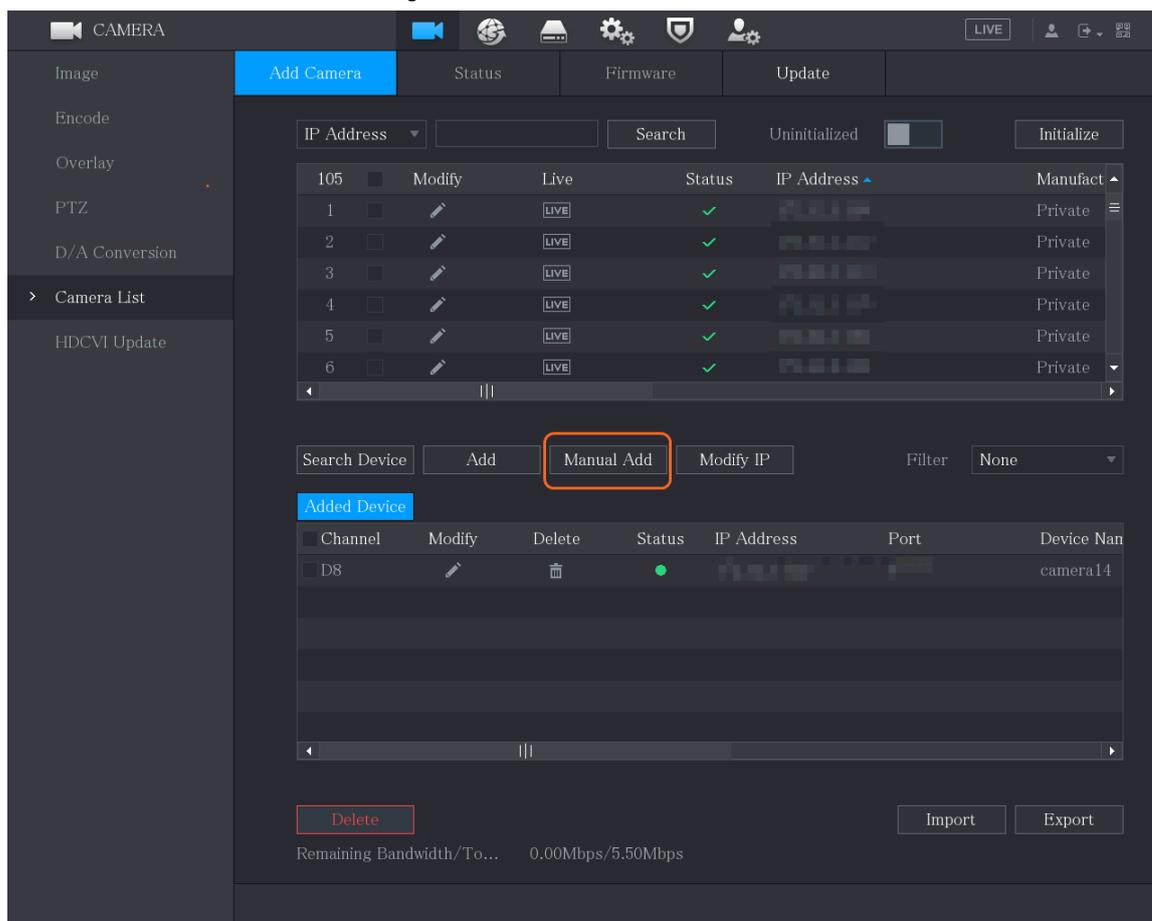
Asegúrese de que las cámaras que desea agregar ya se hayan inicializado y conectado a la red correcta.

Procedimiento

**Paso 1** Seleccione **Menú principal > CÁMARA > Lista de cámaras > Agregar cámara**.

**Paso 2** Hacer clic **Adición manual**.

Figura 1-15 Adición manual



**Paso 3** En el **Adición manual** cuadro de diálogo, configurar parámetros.

Figura 1-16 Configurar parámetros de adición manual

Tabla 1-4 Parámetros de adición manual

Parámetro	Descripción
Canal	Desde el <b>Canal</b> lista desplegable, seleccione el canal que desea usar en el NVR para conectar el dispositivo remoto.
Fabricante	Desde el <b>Fabricante</b> lista desplegable, seleccione el fabricante del dispositivo remoto.
Dirección IP	En el <b>Dirección IP</b> campo, ingrese la dirección IP de la cámara IP.  Cambie el valor predeterminado (192.168.0.0) al que el sistema no puede conectarse.
Puerto RTSP	El valor predeterminado es 554. Puede cambiar el valor según sea necesario.
Puerto HTTP	El valor predeterminado es 80. Puede cambiar el valor según sea necesario.  Si ingresa otro valor, por ejemplo, 70, debe ingresar 70 después de la dirección IP al iniciar sesión en el NVR mediante el navegador.
Puerto TCP	El valor predeterminado es 37777. Puede cambiar el valor según sea necesario.
Nombre de usuario	Introduzca el nombre de usuario del dispositivo remoto.
Clave	Ingrese la contraseña del usuario para el dispositivo remoto.
Nº de canal remoto	Ingrese el número de canal remoto del dispositivo remoto que desea agregar.
Estrategia del decodificador	En el <b>Estrategia del decodificador</b> lista, seleccione <b>Defecto</b> , <b>Tiempo real</b> , o <b>Fluido</b> según sea necesario.

Parámetro	Descripción
Tipo de protocolo	<ul style="list-style-type: none"> <li>● Si la cámara IP se agrega a través de un protocolo privado, seleccione<b>TCP</b>.</li> <li>● Si la cámara IP se agrega a través del protocolo ONVIF, la selección<b>Auto, TCP, UDP, o MULTIDIFUSIÓN</b>.</li> <li>● Si la cámara IP se agrega a través de otros fabricantes, seleccione<b>TCP o UDP</b>.</li> </ul>
Cifrado	<p>Si la cámara IP se agrega a través del protocolo ONVIF, habilitar la <b>Cifrado</b> casilla de verificación proporcionará protección de cifrado a los datos que se transmiten.</p> <p></p> <p>Para usar esta función, la función HTTPS debe estar habilitada para la cámara IP remota.</p>

**Paso 4** Hacer clic **OK**.

## 1.5 Configuración del horario de almacenamiento de video grabado

De forma predeterminada, todas las cámaras graban videos de forma continua las 24 horas del día. Puede modificar la configuración según sea necesario.



También puede configurar la programación de almacenamiento en el Asistente de inicio.

Procedimiento

**Paso 1** Seleccione **Menú principal > ALMACENAMIENTO > Calendario > Registro**.

Figura 1-17 Horario de grabación



**Paso 2** Configurar parámetros.

Tabla 1-5 Parámetros de registro

Parámetro	Descripción
Canal	Desde el <b>Canal</b> lista desplegable, seleccione el canal para cambiar la configuración de grabación de video.
Grabar antes	En el <b>Grabar antes</b> campo, configure el tiempo para capturar video adicional que ocurre antes de un evento para proporcionar contexto a una grabación. Rango de valores: 0 a 30 s.
Redundancia	<p>Permite a los usuarios configurar uno de los discos duros como disco duro redundante para guardar los archivos grabados en diferentes discos duros. En caso de falla del disco duro, puede encontrar la grabación de respaldo en el disco duro redundante.</p> <ul style="list-style-type: none"> <li>● Seleccione <b>Menú principal &gt; ALMACENAMIENTO &gt; Administrador de discos</b>, a continuación, establezca un disco duro como disco duro redundante.</li> <li>● Seleccione <b>Menú principal &gt; ALMACENAMIENTO &gt; Calendario &gt; Registro</b>, a continuación, seleccione el <b>Redundancia</b> casilla de verificación</li> </ul> <ul style="list-style-type: none"> <li>◇ Si el canal seleccionado no está grabando, la función de redundancia tendrá efecto la próxima vez que grabe sin importar si selecciona la casilla de verificación o no.</li> <li>◇ Si el canal seleccionado está grabando, los archivos grabados actuales se empaquetarán y luego comenzarán a grabar de acuerdo con el nuevo horario.</li> </ul> <p></p> <ul style="list-style-type: none"> <li>● Esta función está disponible en modelos seleccionados.</li> <li>● El HDD redundante solo realiza una copia de seguridad de los videos grabados, pero no de las instantáneas.</li> </ul>
Tipo de evento	<p>Seleccione la casilla de verificación de los tipos de eventos.</p> <ul style="list-style-type: none"> <li>● <b>General:</b> Grabación general significa que el NVR graba todos los videos durante el período de tiempo especificado. La grabación general está representada por el color verde.</li> <li>● <b>Movimiento:</b> La grabación de movimiento significa que el NVR graba video solo cuando se activa la detección de movimiento. La grabación de movimiento está representada por el color amarillo.</li> <li>● <b>Alarma:</b> Grabación de alarma significa que el NVR graba video cuando se activa una alarma. La grabación de alarma está representada por el color rojo.</li> <li>● <b>MAMÁ:</b> La grabación de M&amp;A combina grabación de movimiento y grabación de alarma. El dispositivo graba video cuando se activa la detección de movimiento o cualquier alarma. El registro de fusiones y adquisiciones está representado por el color naranja.</li> <li>● <b>Inteligente:</b> Grabación inteligente significa que el NVR graba video cuando se activa la detección inteligente. La grabación inteligente está representada por el color azul.</li> <li>● <b>TPV:</b> La grabación de POS significa que el NVR graba video cuando la máquina POS se usa para realizar un pago. La grabación de POS está representada por el color púrpura.</li> </ul>
Período	Define un período durante el cual la configuración de grabación configurada está activa. El sistema solo activa la alarma en el período definido.

Parámetro	Descripción
Copiar a	Hacer clic <b>Copiar a</b> para copiar la configuración a otros canales.

**Paso 3** Establece el horario dibujando o editando.

- Dibujar: mantenga presionado el botón izquierdo del mouse y arrastre el mouse para dibujar el período.
- Edición: Haga clic  para configurar el período y luego haga clic en **OK**.

**Paso 4** Hacer clic **Aplicar**.



El cronograma de grabación configurado puede entrar en vigencia solo cuando la función de grabación automática está activada. activado. Para obtener detalles sobre cómo habilitar la grabación automática, consulte el Manual del usuario.

## 1.6 Configuración de ajustes de P2P

Puede usar el código QR para conectar un teléfono inteligente al NVR para su administración.



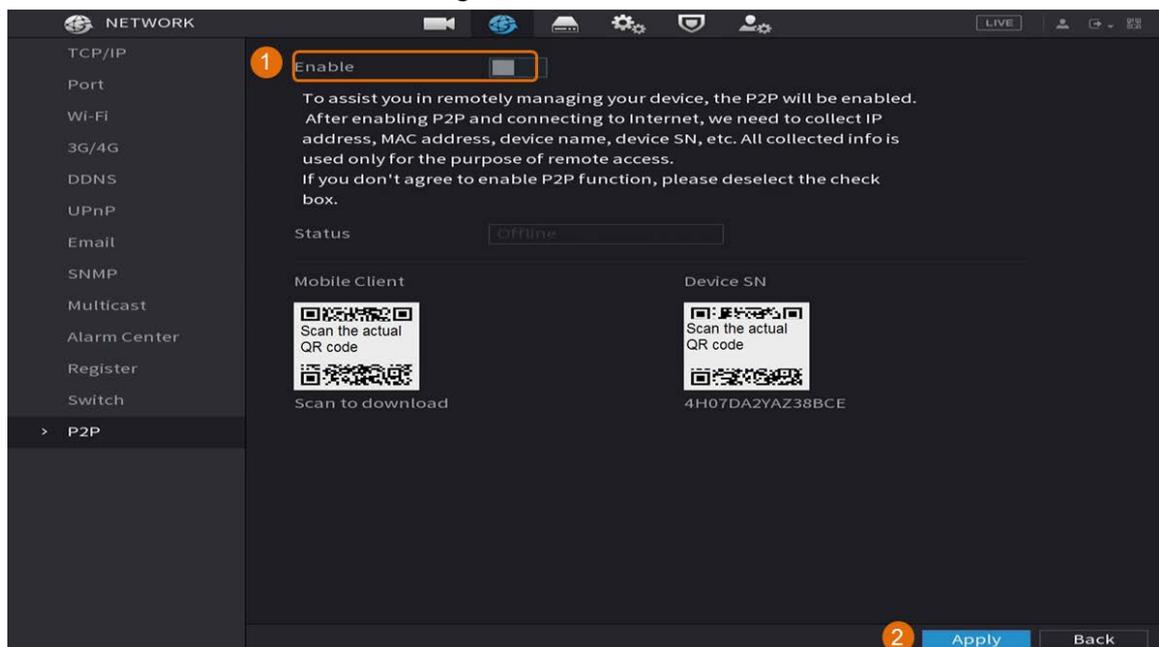
Asegúrese de que el NVR se haya conectado a Internet y, en caso afirmativo, en el **Estado** caja del P2P interfaz, muestra **En línea**.

### 1.6.1 Habilitación de la función P2P

Debe ingresar a la interfaz P2P para habilitar la función P2P y escanear el código QR para descargar la aplicación del teléfono inteligente.

**Paso 1** Seleccione **Menú principal > LA RED > P2P**.

Figura 1-18 P2P



**Paso 2** Hacer clic **Habilitar** para habilitar la función P2P.

**Paso 3** Hacer clic **Aplicar**

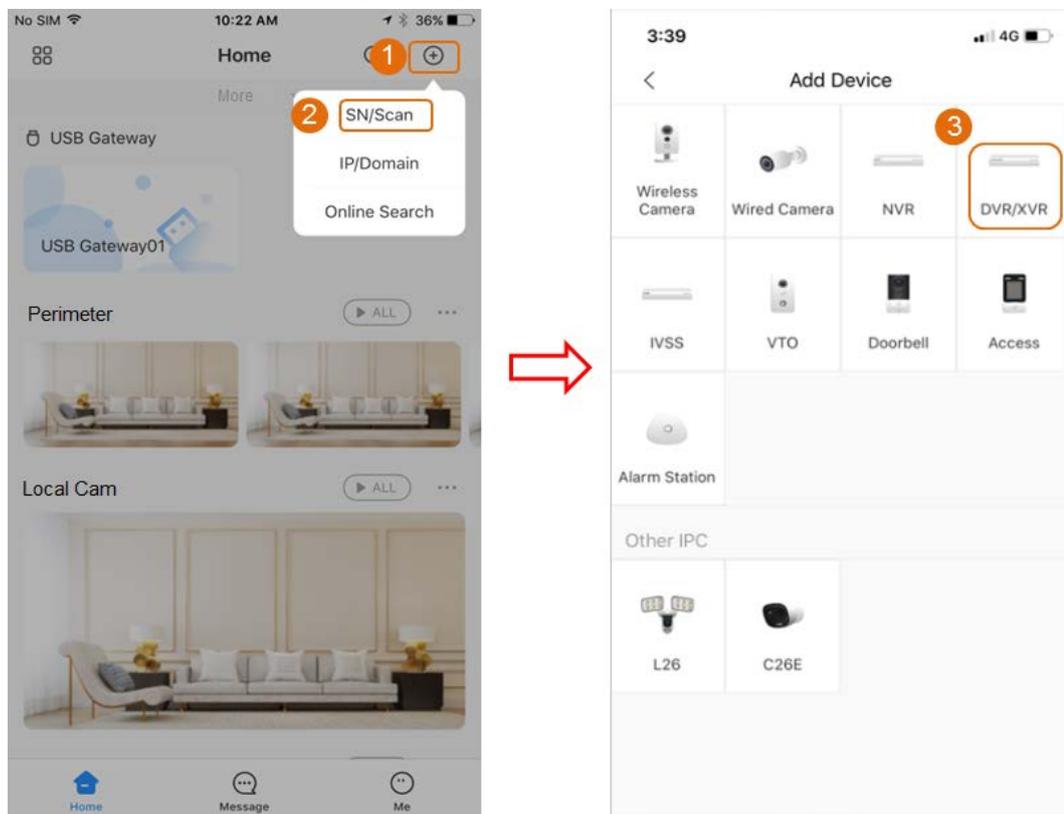
## 1.6.2 Adición del NVR al cliente de teléfono inteligente

Este tema toma la adición del NVR al cliente de teléfono inteligente como un ejemplo para la administración de teléfonos inteligentes. Paso 1

Abra la aplicación y toque .

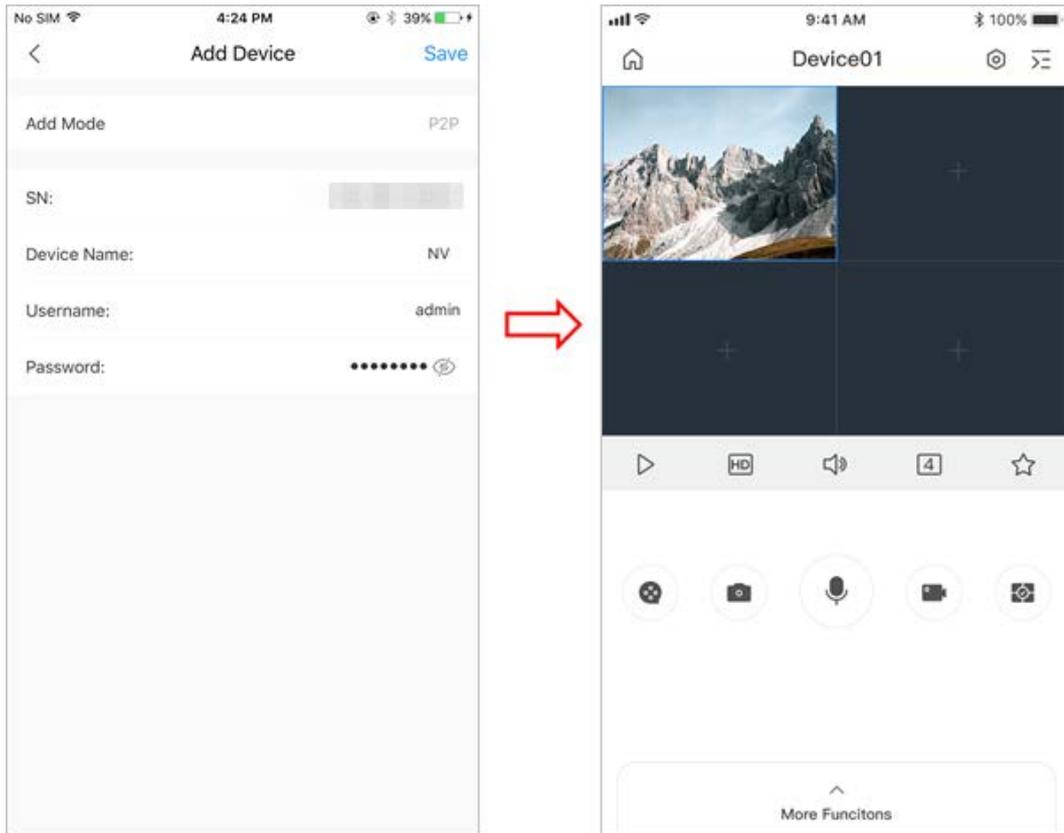
Paso 2 Seleccionar **NS/escaneo**.

Figura 1-19 Agregar dispositivo



Paso 3 Seleccione , ingrese un nombre y una contraseña para el NVR y luego toque **Ahorrar**.

Figura 1-20 Iniciar vista en vivo



## 1.7 Detección de movimiento inteligente

Este tema muestra cómo configurar la detección de movimiento inteligente (SMD).

### Información de contexto

La detección de movimiento inteligente (SMD) es una función de monitoreo ideal para áreas poco pobladas donde desea una alerta de humanos o vehículos en cualquier lugar de la escena sin tener que establecer reglas y trazar líneas.

#### Procedimiento

Paso 1 Seleccione **Menú principal > AI > Parámetro > SMD**.

Figura 1-21 SMD

The screenshot shows a configuration interface for SMD linkage. The settings are as follows:

- Channel: D1 (dropdown)
- Enable:  (toggle)
- Sensitivity: Medium (dropdown)
- Effective Target:  Human,  Motor Vehicle
- Schedule: Setting (button)
- Anti-Dither: 0 sec. (input)
- Alarm-out Port: Setting (button)
- Post-Alarm: 0 sec. (input)
- Show Message:  (checkbox)
- Report Alarm:  (checkbox)
- Send Email:  (checkbox)
- Record Channel: Setting (button)
- PTZ Linkage: Setting (button)
- Post-Record: 10 sec. (input)
- Tour: Setting (button)
- Picture Storage:  (checkbox)
- Buzzer:  (checkbox)
- Log:  (checkbox)
- Alarm Tone: None (dropdown)

SMD linkage configuration synchronizes with MD linkage configuration.

**Paso 2** Seleccione y habilite un canal y luego configure los parámetros.

Tabla 1-6

Parámetro	Descripción
Sensibilidad	Cuanto mayor sea el valor, más fácil será activar una alarma. Pero al mismo tiempo, la falsa alarma puede ocurrir. Se recomienda el valor predeterminado.
Objetivo efectivo	Elija humano o vehículo de motor o ambos.
Calendario	Configure el período y en el rango de tiempo establecido, el elemento de configuración correspondiente se vinculará para iniciar la alarma.
Anti-interpolación	Indica el tiempo transcurrido desde el final de la detección de movimiento hasta el final de la acción de enlace de alarma. El rango es de 0 a 600 segundos.
Puerto de salida de alarma	El dispositivo de alarma (como luces, sirenas, etc.) está conectado al puerto de salida de alarma. Cuando ocurre una alarma, el dispositivo NVR transmite la información de alarma al dispositivo de alarma.
Post-Alarma	Cuando finaliza la alarma, la alarma se prolonga durante un período de tiempo. El rango de tiempo es de 0 segundos a 300 segundos.
Mostrar mensaje	Marque la casilla para habilitar un mensaje emergente en su PC host local.
Reportar alarma	<p>Seleccione la casilla de verificación. Cuando ocurre una alarma, el dispositivo NVR carga una señal de alarma a la red (incluido el centro de alarma).</p> <p></p> <ul style="list-style-type: none"> <li>● Esta función está disponible en modelos seleccionados.</li> <li>● Primero debe configurar el centro de alarma.</li> </ul>

Parámetro	Descripción
Enviar correo electrónico	<p>Seleccione la casilla de verificación. Cuando ocurre una alarma, el dispositivo NVR envía un correo electrónico al buzón establecido para notificar al usuario.</p>  <p>Primero debe configurar el correo electrónico.</p>
Grabar canal	<p>Seleccione la casilla de verificación y seleccione el canal de grabación necesario (admite múltiples opciones). Cuando ocurre una alarma, el dispositivo NVR activa el canal para grabar.</p>  <p>Primero debe habilitar la grabación inteligente y la grabación automática.</p>
Post-grabación	<p>Al final de la alarma, la grabación se extiende por un período de tiempo. El rango de tiempo es de 10 segundos a 300 segundos.</p>
Enlace PTZ	<p>Seleccione la casilla de verificación y haga clic en Configuración para seleccionar el canal y la acción PTZ. Cuando ocurre una alarma, el dispositivo NVR asocia el canal para realizar la acción PTZ correspondiente. Por ejemplo, active el PTZ en el canal uno para volver al punto preestablecido X.</p>  <ul style="list-style-type: none"> <li>● La alarma Tripwire admite la activación del punto preestablecido PTZ únicamente.</li> <li>● Primero debe configurar las acciones PTZ correspondientes.</li> </ul>
Recorrido	<p>Seleccione la casilla de verificación y seleccione el canal para el recorrido. Cuando ocurre una alarma, la interfaz local del dispositivo NVR muestra la pantalla del canal seleccionado.</p>  <ul style="list-style-type: none"> <li>● Primero debe configurar el intervalo de tiempo y el modo para el recorrido.</li> <li>● Una vez que finaliza el recorrido, la interfaz de vista previa se restaura al modo de pantalla dividida antes del recorrido.</li> </ul>
Almacenamiento de imágenes	<p>Seleccione la casilla de verificación Instantánea para tomar una instantánea del canal seleccionado.</p>  <p>Para utilizar esta función, seleccione <b>Menú principal &gt; CÁMARA &gt; Codificar &gt; Instantánea</b>, Seleccione <b>Evento en Escribelista</b>.</p>
Zumbador	<p>Seleccione la casilla de verificación para activar el zumbador cuando se produzca una alarma.</p>
Tono de alarma	<p>Marque la casilla y luego seleccione el archivo de audio correspondiente de la lista desplegable. El sistema reproduce el archivo de audio cuando se produce la alarma.</p>  <p>Primero debe agregar el archivo de audio.</p>

**Paso 3** Hacer clic **Aplicar**.

## 1.8 Vista en vivo

Después de iniciar sesión, el sistema pasa al modo de vista en vivo de múltiples canales de forma predeterminada. Puede ver el video de monitoreo de cada canal. Tenga en cuenta que el número de ventanas mostradas puede variar según el modelo.

modelar.

Para ingresar a la pantalla de vista en vivo desde otras interfaces, haga clic en  en la parte superior derecha de la pantalla.

Figura 1-22 Vista en vivo



Pantalla de visualización en vivo

Puede ver el video en vivo de las cámaras conectadas a través de cada canal en la pantalla.

- De manera predeterminada, la hora del sistema, el nombre del canal y el número del canal se muestran en la ventana de cada canal. Este ajuste se puede configurar seleccionando **Menú principal > CÁMARA > Cubrir > Cubrir**.
- La figura en la esquina inferior derecha representa el número de canal. Si se cambia la posición del canal o se modifica el nombre del canal, puede reconocer el número del canal por esta figura y luego realizar operaciones como consulta de grabación y reproducción.

Para los iconos que se muestran en cada canal, consulte la Tabla 1-7.

Tabla 1-7 Descripción del icono

Icono	Descripción
	El video se está grabando.
	La detección de movimiento ocurre en la escena.
	Se detecta pérdida de video.
	La monitorización del canal está bloqueada.

## 1.9 Reproducción de grabación

Para reproducir una grabación, puede seleccionar **Menú principal** > **Reproducción** o haga clic derecho en la interfaz de vista en vivo y seleccione **Búsqueda**.

Figura 1-23 Interfaz principal de reproducción



Para obtener detalles sobre las instrucciones sobre la interfaz principal de reproducción, consulte *Manual de usuario*.

### Reproducción instantánea

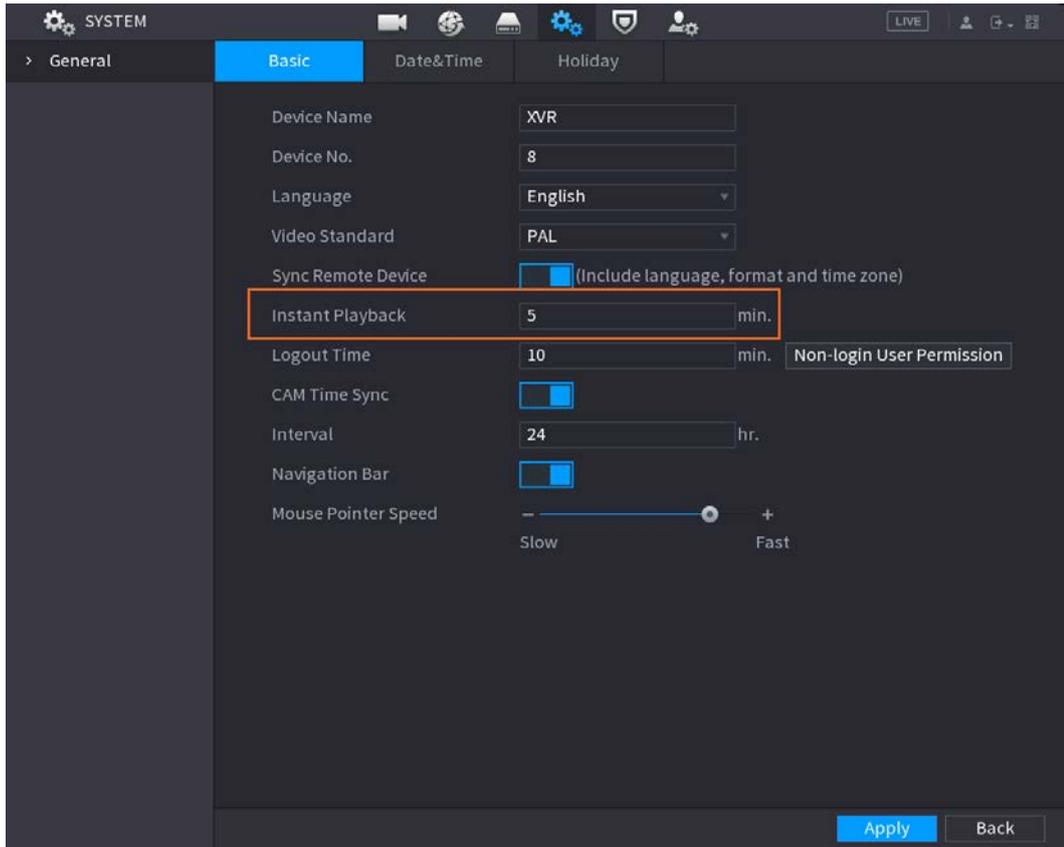
Puede reproducir los 5 a 60 minutos anteriores del video grabado.

Al hacer clic en **Se** muestra la interfaz de reproducción instantánea. La reproducción instantánea tiene las siguientes características:

- Mueva el control deslizante para elegir el momento en que desea comenzar a jugar.
- Reproducir, pausar y cerrar la reproducción.
- La información como el nombre del canal y el ícono de estado de grabación están protegidos durante la reproducción instantánea y no se mostrarán hasta que se salga.
- Durante la reproducción, no se permite el cambio de diseño de división de pantalla.

Para cambiar el tiempo de reproducción, seleccione **Menú principal** > **SISTEMA** > **General** > **Básico**, en el **Juego instantáneo** cuadro, ingrese el tiempo que desea reproducir.

Figura 1-24 Establecer el tiempo de reproducción instantánea



#### Reproducción de búsqueda inteligente

Durante la reproducción, puede analizar un área determinada para averiguar si se produjo algún evento de detección de movimiento. El sistema mostrará las imágenes con eventos de movimiento del video grabado.



Esta función es solo para algunos productos de serie.

Para usar la función de búsqueda inteligente, debe habilitar la detección de movimiento para el canal seleccionando **Menú principal>ALARMA>Detección de vídeo>Detección de movimiento.**

## 2 Iniciar sesión en la Web

La web proporciona la mayoría de las funciones en la GUI local. Puede iniciar sesión en la web para administrar el NVR según sea necesario.

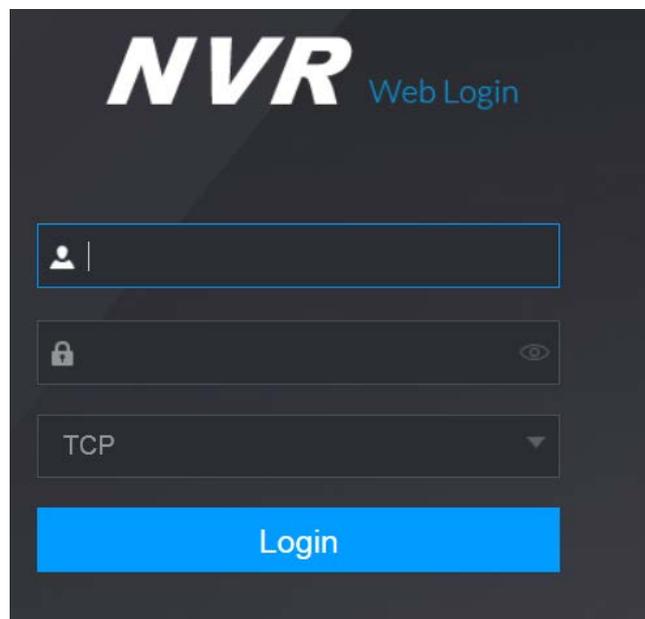


Se pueden encontrar ligeras diferencias en las interfaces de diferentes modelos. Las siguientes cifras son para solo referencia. El producto real prevalecerá.

### Procedimiento

- Paso 1** Abra el navegador e ingrese la dirección IP del NVR, y luego presione la tecla Enter. Introduzca el nombre de usuario y la contraseña.
- Paso 2**

Figura 2-1 Inicio de sesión



- La cuenta de administrador predeterminada es **administración**. La contraseña es la que estaba configurado durante la configuración inicial. Para proteger su cuenta, se recomienda mantener la contraseña correctamente y cámbiela regularmente.
- Hacer clic  para mostrar la contraseña.

- Paso 3** Hacer clic **Acceso**.

# Apéndice 1 Recomendaciones sobre 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 a realizar para la seguridad de la red de equipos básicos:

### 1. Usa 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 equipo (como NVR, DVR, cámara IP, etc.) para garantizar que el sistema esté equipado con los últimos parches y correcciones de seguridad. Cuando el equipo está conectado a la red pública, se recomienda habilitar el **comprobación automática de actualizaciones** función 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 equipo:

### 1. Protección Física

Le sugerimos que realice protección física a los equipos, especialmente a los dispositivos de almacenamiento. Por ejemplo, coloque el equipo en un gabinete y una sala de computadoras especiales, e implemente una administración de claves y un permiso de control de acceso bien hecho para evitar que el personal no autorizado realice contactos físicos, como dañar el hardware, la conexión no autorizada de equipos extraíbles (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 equipo 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. Habilitar lista de permitidos

Le sugerimos que habilite la función de lista de permitidos para evitar que todos, excepto aquellos con direcciones IP específicas, accedan al sistema. Por lo tanto, asegúrese de agregar la dirección IP de su computadora y la dirección IP del equipo adjunto a la lista de permitidos.

## 8. Enlace de dirección MAC

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

## 9. 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.

## 10. 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.

## 11. 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.

## 12. Auditoría segura

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

## 13. Registro de red

Debido a la limitada capacidad de almacenamiento del equipo, 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.

## 14. Construya un entorno de red seguro

Para garantizar mejor la seguridad de los equipos 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 red.

- Establezca el sistema de autenticación de acceso 802.1x para reducir el riesgo de acceso no autorizado a redes privadas.

15. Se recomienda que habilite el firewall de su dispositivo o la función de lista de bloqueo y lista de permitidos para reducir el riesgo de que su dispositivo sea atacado.