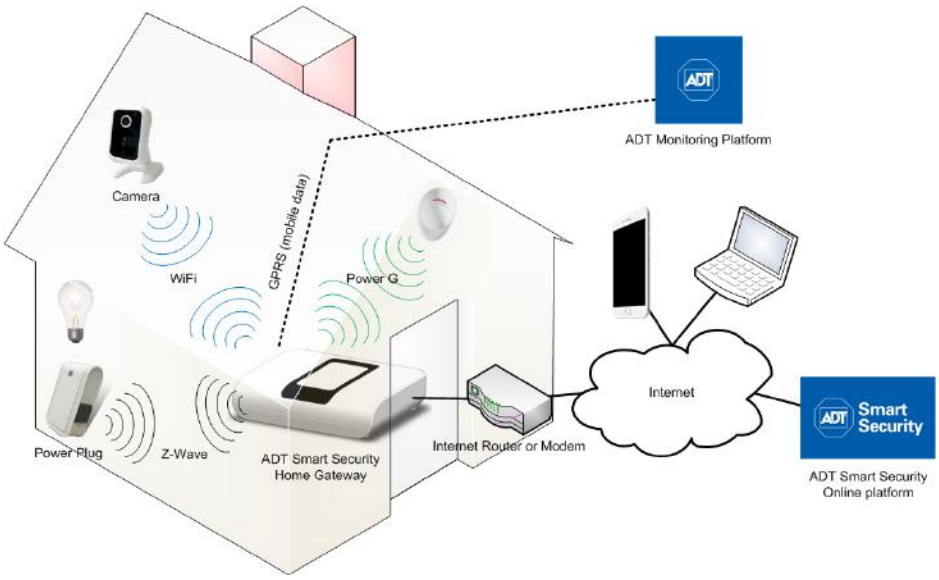
Manual del Usuario
para Portal Web y Aplicación Móvil

CONTENIDO

1. INTRODUCCIÓN

La solución ADT Smart Security extiende el concepto del sistema de alarma de seguridad del hogar.



Este sistema añade servicios interactivos de ADT Smart Security, que suministran acceso y control remoto usando un dispositivo móvil o un explorador Web Internet para permitir la transmisión y grabación de video en vivo, control de luces y monitorización de la energía. Todo esto es provisto sin afectar la disponibilidad y desempeño del panel de alarmas de seguridad.

El panel de alarmas se basa en diversos sensores (sensores de movimiento, sensores de contacto de puerta o ventana, etc.) para detectar intrusiones no solicitadas o peligros para la seguridad. Estos sensores pueden ser conectados al panel de alarmas mediante cables o de manera inalámbrica. La solución ADT Smart Security provee dispositivos adicionales para gestionar los elementos interactivos, tales como enchufes de alimentación eléctrica o cámaras de video controlables de manera inalámbrica. Esta solución también brinda nuevas maneras de controlar el armado o desarmado del panel de alarmas. Ahora es posible realizar dichas acciones usando un ordenador o un smartphone con acceso a la Internet, que otorga el control al propietario de la casa dondequiera que esté, ya sea en la casa o afuera.

2. KIT DE ADT SMART SECURITY

Un kit de ADT Smart Security puede contener varios ítems:

- Un panel de alarmas que incluye también un gateway para los servicios interactivos de Smart Security (Visonic Powermaster 360)
- Uno o varios dispositivos Visonic PowerG (sensores de movimiento PIR inalámbricos, sensores de contacto de puertas/ventanas, etc.)
- Una o varias cámaras PowerG PIR (opcional)
- Uno o varios dispositivos interactivos (enchufes de alimentación, etc.)
- Una o varias cámaras IP.

Estos kits pueden ser adquiridos contactando a ADT.

La instalación de estos ítems debe ser realizada por un instalador ADT autorizado.

3. ACTIVACIÓN DE SU CUENTA

3.1. ¿Qué es una cuenta?

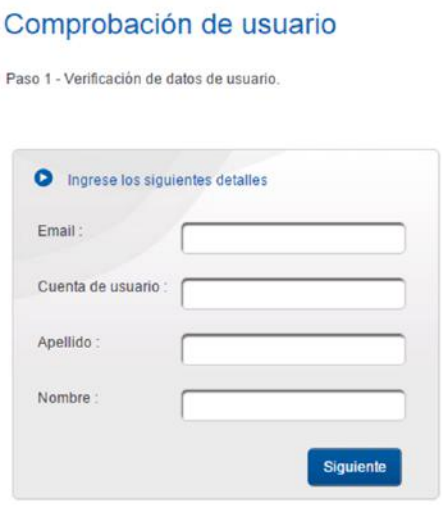
Una cuenta es necesaria para poder manejar el gateway del hogar, sus accesorios emparejados, y los servicios asociados de la casa. El gateway puede ser controlado mediante una interfaz de portal Web o una aplicación móvil. Como resultado, el gateway requiere una conexión Internet en el hogar para habilitar la comunicación con el mundo exterior. Esto permite al usuario utilizar los servicios interactivos de ADT Smart Security desde cualquier lugar del mundo, mientras disponga de acceso a Internet en el ordenador o en el smartphone en uso. Las cuentas de usuario están aseguradas para garantizar que únicamente los usuarios legítimos puedan acceder a sus propios gateways.

3.2. Registro de la cuenta

Una vez efectuado el contrato con ADT, usted recibirá un email de “Confirmación de Registro” enviado a la dirección electrónica que fue comunicada a ADT a la firma del contrato. En este email se le solicitará que haga clic en un enlace de registro para activar su cuenta y definir su contraseña y las preguntas de seguridad.

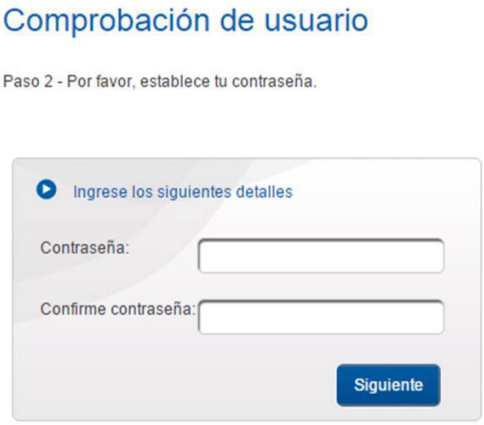
Para garantizar la seguridad de su cuenta, el enlace de registro es válido por siete días. Si por alguna razón usted no recibió el email o no pudo hacer clic en el enlace de registro antes de que expire el período de validez de siete días, usted deberá llamar al servicio de Atención al Cliente de ADT y solicitarles que verifiquen su dirección de email y reenviar el correo electrónico de registro.

Al hacer clic en el enlace de registro, su explorador abrirá la siguiente página:



El propósito de las preguntas es asegurarse de que la persona que activa la cuenta es la misma persona que se ha suscripto al servicio. Para los cuatro campos de verificación del usuario, usted debe ingresar la misma información que ha provisto a ADT al firmar el contrato, y luego debe hacer clic en el botón “Verificar usuario”.

Si toda la información de verificación de usuario ingresada coincide con la información del contrato, se presenta una página nueva para crear su contraseña personal:



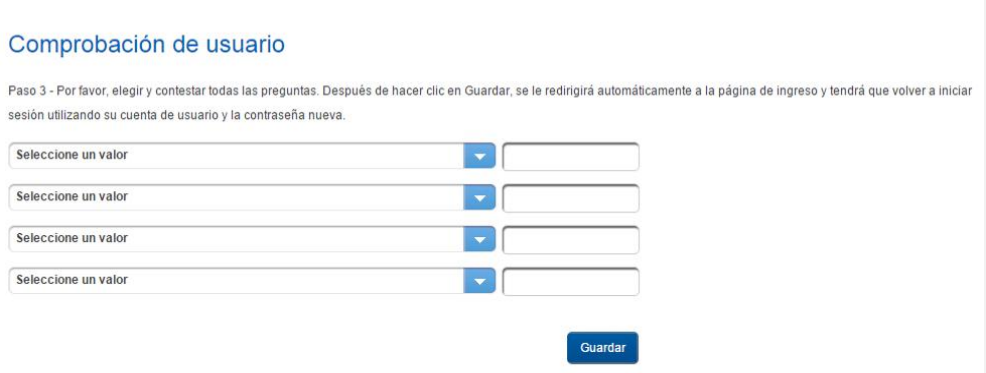
Esta contraseña será requerida para usar tanto el portal Web de autoservicio como la aplicación móvil.

Hay limitaciones de caracteres en la contraseña para evitar que los usuarios puedan elegir credenciales que puedan ser fáciles de adivinar, como “123456”, “contraseña”, “qwerty”, etc. Por lo tanto su contraseña debe cumplir con los siguientes requerimientos de complejidad:

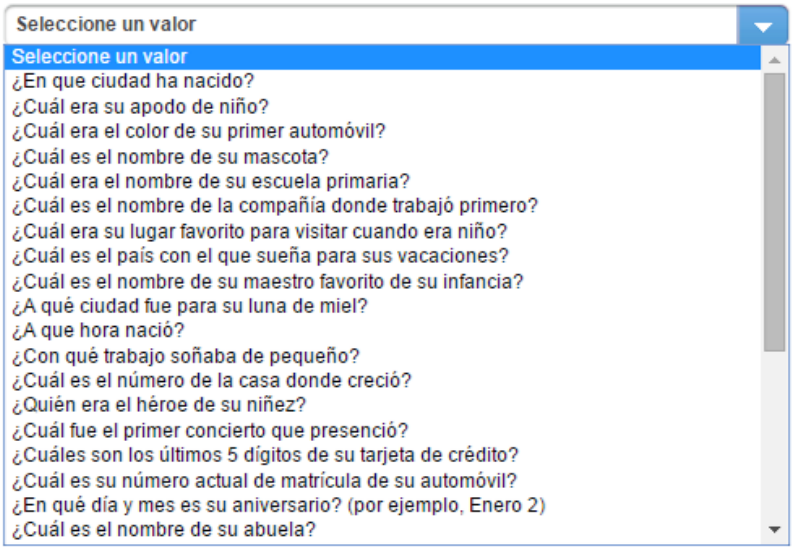
- Las letras mayúsculas y minúsculas son consideradas como caracteres diferentes, y como a resultado “hola” no es lo mismo que “Hola”.
- Longitud de la contraseña: 8 caracteres o más
- La contraseña debe contener solamente los siguientes caracteres alfanuméricos: ‘A’..‘Z’, ‘a’..‘z’, ‘0’..’9’, ‘_’ (subrayado), ‘-‘ (guión)
- La contraseña debe contener por lo menos una letra mayúscula
- La contraseña debe contener por lo menos una letra minúscula
- La contraseña debe contener por lo menos un carácter numérico
- Al inicio de la contraseña, está prohibido que haya tres o más caracteres idénticos juntos
- Al inicio, en el medio o al final de la contraseña, está prohibido que haya cinco caracteres consecutivos, tanto alfabéticos (por ejemplo, “ABCDE”) como numerales (por ejemplo, “12345”)
- La contraseña no puede ser idéntica al nombre de usuario
- No puede ser idéntica a las dos contraseñas previamente provistas.

Después de hacer clic en el botón “Siguiente”, si su nueva contraseña es válida, tiene que elegir y contestar sus preguntas de seguridad. Estas preguntas de seguridad son necesarias en caso que el usuario olvide su contraseña y deba recuperarla. El sistema también debe confirmar que un pedido de recuperación de contraseña provenga del dueño legítimo de la cuenta y no de otra persona.

En caso de recuperación de contraseña, se le solicita al usuario brindar respuestas a algunas preguntas personales. Estas preguntas son seleccionadas aleatoriamente de un conjunto de preguntas que el usuario ha elegido previamente y para las cuales proveyó respuestas. Ésta es la etapa que aquí describimos:



El usuario debe elegir preguntas de un conjunto predefinido. Puede accederse a estas preguntas, expandiendo la lista desplegable en el campo de cada pregunta.



El usuario debe elegir las preguntas basándose en el criterio siguiente:

- Conoce las respuestas.
- Las respuestas no están disponibles en las redes sociales (Facebook, Twitter, etc.) o, por lo menos, no están fácilmente disponibles.

Una vez recuperada la contraseña, las respuestas ingresadas por el usuario serán cotejadas contra las respuestas guardadas en esta etapa. El usuario también puede modificar las preguntas y respuestas más tarde, cuando ya estén registradas en su cuenta.

Las respuestas no son almacenadas abiertamente en el sistema para revisión por ninguno que no sea el dueño de la cuenta. Por lo tanto, nadie en la sección de Atención al Cliente o en el departamento de TI puede leer las respuestas a las preguntas de seguridad de una cuenta. Es importante que los usuarios elijan preguntas para las cuales puedan responder fácilmente y sin dudas.

Una vez completadas las preguntas de seguridad, la cuenta está lista para ser usada.

Antes de poder utilizar su kit ADT Smart Security, un instalador ADT vendrá a su hogar para activar el kit e instalar todos los accesorios.

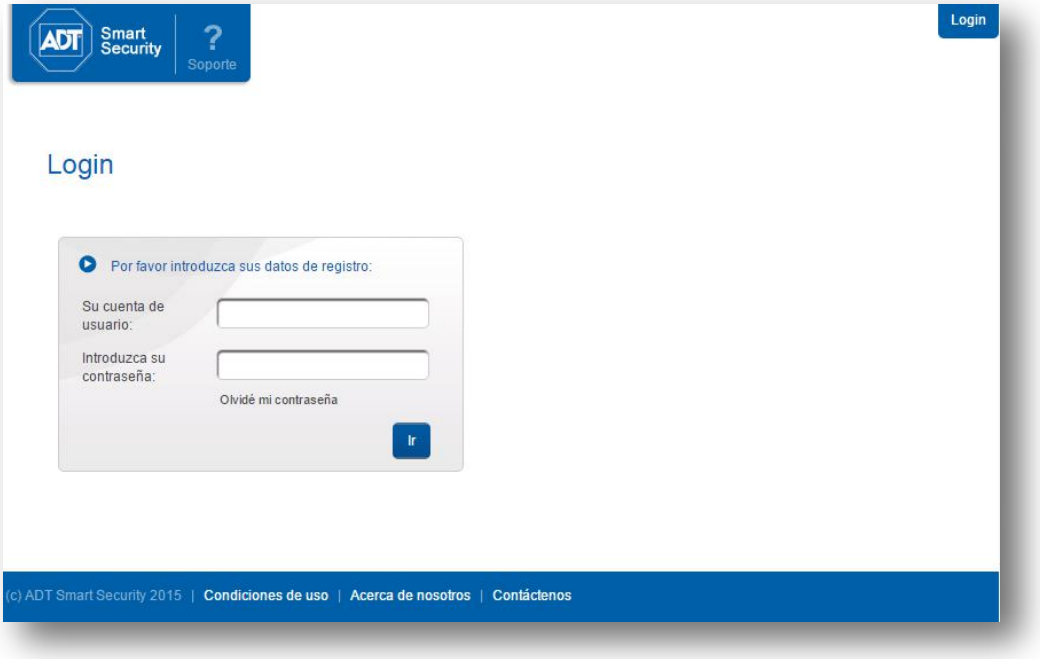
3.3. Activación de la cuenta

Una vez que su cuenta haya sido registrada y que su contraseña de usuario haya sido definida, se requiere efectuar unos pocos pasos más para poder usar su kit:

- Acepte el Convenio de Licencia de usuario Final
- Active el ADT Home Box e ingrese los accesorios

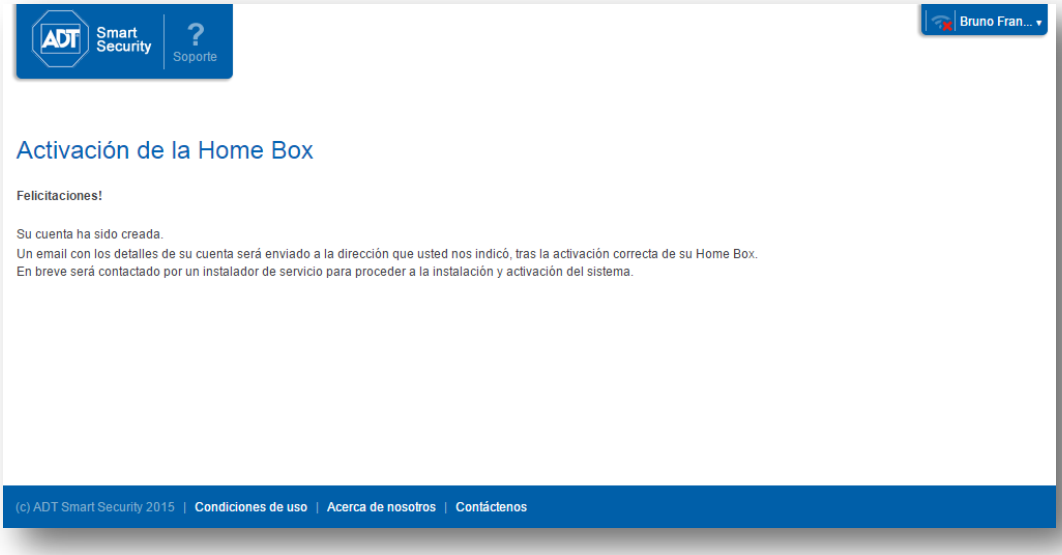
El primer paso es hacer login al portal Web de ADT Smart Security:

- Abra un explorador Web y vaya a la página Web del sitio de ADT Smart Security: https://smartsecurity.adt.com.ar/selfcare



Ingrese su nombre de usuario y la contraseña que usted acaba de crear en el paso previo.

En caso su kit no fuera activado por un instalador ADT, se mostrara la pantalla siguiente:



Si su kit fuera instalado y activado, Usted tiene que aceptar el Convenio de Licencia de Usuario Final.

4. EL PORTAL WEB DE AUTOSERVICIO

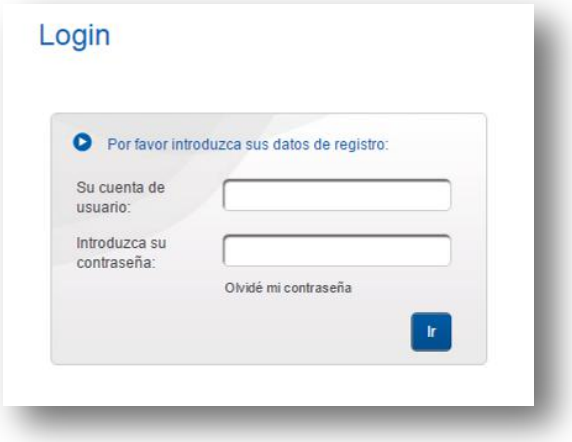
El portal Web de autoservicio es la interfaz Web para gestionar su kit ADT Smart Security del hogar desde dentro de la casa o desde ubicaciones remotas. Requiere un explorador Web para acceder al mismo. ADT recomienda los siguientes exploradores Web para disponer de la mejor experiencia de usuario posible:

- Microsoft Internet Explorer versiones 10 y 11, y Microsoft Edge
- Mozilla Firefox (versiones recientes)
- Google Chrome (versiones recientes)
- Apple Safari (versión reciente).

4.1. Reseña

El portal Web de autoservicio permite a los usuarios establecer y utilizar su gateway, accesorios y todos los servicios del hogar a los que se hayan suscrito, incluyendo Dispositivos, Visualización de video e imágenes, e Iluminación.
El acceso al portal Web de autoservicio comienza con la ejecución de un explorador Web y conectándose a la URL de autoservicio:

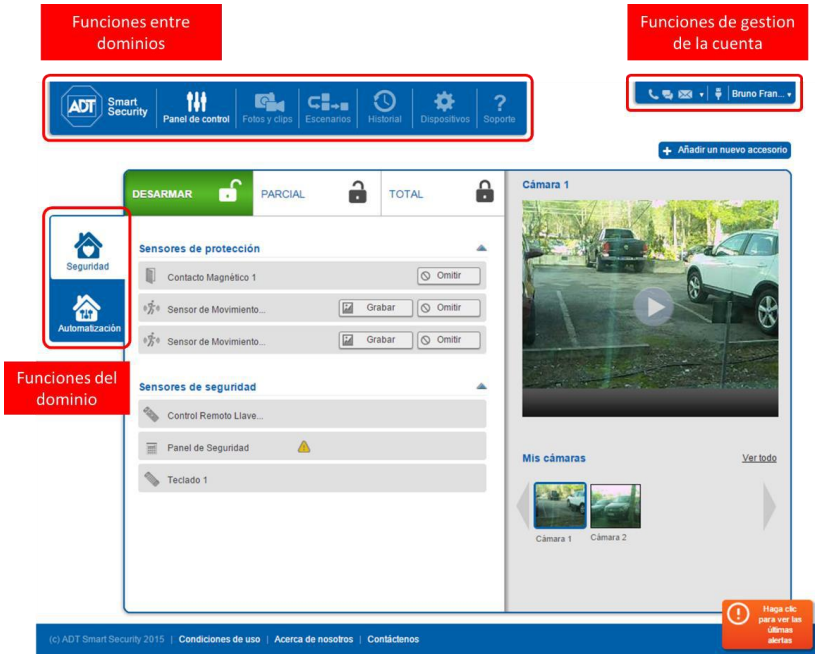
https://smartsecurity.adt.com.ar/selfcare



Se requiere del usuario que ingrese su nombre de login de la cuenta y su contraseña para acceder al sistema.

Como se describió en el capítulo anterior, cuando no se haya registrado un gateway con la cuenta, se requiere del usuario que ingrese el número de serie de un gateway. Cuando una cuenta ya está plenamente establecida, se muestra el tablero después de cada login.

Una vez efectuado el login, el usuario puede ver tres conjuntos diferentes de pestañas y botones para acceder a las diferentes funciones de su cuenta en línea. Estas pestañas o botones aparecen destacadas en rojo en la ilustración siguiente.

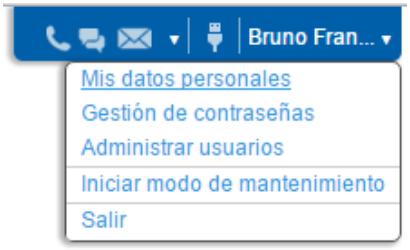


Funciones del dominio: Estas pestañas brindan acceso a los diferentes dominios de seguridad y dispositivos que son soportados por la suscripción del usuario. Por ejemplo, la pestaña Seguridad permite al usuario armar y desarmar el panel de alarmas, y ver la lista de sensores de seguridad registrados con ese panel de alarmas.

Funciones entre dominios: Estos botones proveen acceso general a las funciones del servicio de alarma y dispositivos, tales como ver videos grabados, configurar acciones automáticas (escenarios), ver una lista de las alertas (historia), y gestionar los dispositivos.

Funciones de gestión de la cuenta: Aquí el usuario puede definir cómo desea ser notificado acerca de los eventos, cuáles usuarios adicionales pueden acceder al sistema, y cómo ellos pueden modificar sus ajustes de la cuenta, tales como cambiar sus contraseñas de la cuenta o su información de contacto.

4.2. Gestión de la cuenta



El status de conexión en tiempo real del gateway y la información del servicio siempre aparecen en la esquina superior derecha. Específicamente, se indica el tipo de conexión Internet (Ethernet/Wi-Fi).

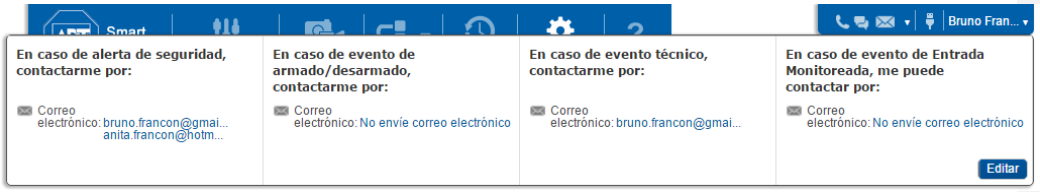
El tipo de conexión Internet aparece como sigue:

- Ya sea cableado: 
- o Wi-Fi: 

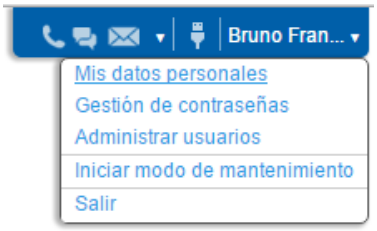
Nota: el gateway solamente soporta una red Wi-Fi. Esta red soporta la conexión a las cámaras IP de video. Como resultado, la conexión Internet a este gateway debe ser siempre cableada.

Además, también se puede acceder a varios menús desplegables desde la sección Gestión de Cuenta:

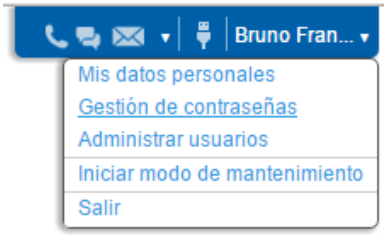
- **Configuración de alertas**: este menú se usa para configurar las direcciones electrónicas a las que se envían las alertas de notificación de eventos de seguridad, eventos de servicio o eventos técnicos. Se puede ser notificado acerca de problemas técnicos que involucran el panel de alarmas (p.ej., el panel está desconectado), uno de los sensores de seguridad (p.ej, el sensor se quedó sin batería), el gateway (p.ej., perdió su conexión a Internet), o uno de los dispositivos.



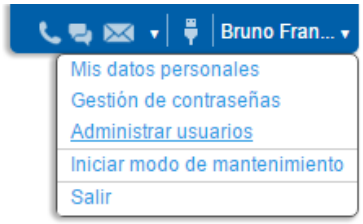
- **Nombre de usuario:** este menú provee acceso a los detalles personales del cliente, tales como su nombre y apellido y su dirección electrónica.



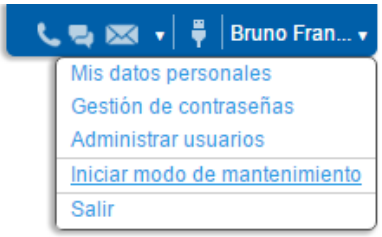
- Este menú también permite acceder a la página de **gestión de contraseña**, donde la contraseña del usuario puede ser modificada, así como también acceder a las preguntas de seguridad que puedan ser formuladas en caso de que el usuario haya olvidado su contraseña.



- Además, con la pagina **Administrar usuarios** es posible definir cuentas de sub-usuarios que son usuarios adicionales para la misma cuenta con permisos definidos establecidos por el usuario principal.



El usuario también puede pasar su cuenta al **Modo de Mantenimiento** durante el mantenimiento. En este modo los instaladores de ADT pueden acceder a la cuenta del usuario con sus propias credenciales privadas (no hay necesidad de compartir las credenciales del usuario principal con un instalador de ADT) y realizar cualquier tarea de instalación o mantenimiento que sea requerida. Cuando el modo de mantenimiento está habilitado, el usuario tiene acceso limitado a su cuenta. Sin embargo, el usuario siempre puede cancelar el modo de mantenimiento en todo momento, lo que a continuación bloquea al instalador impidiéndole el acceso a su cuenta y la realización de cualesquiera modificaciones adicionales. Será necesario volver a habilitar el modo de mantenimiento para volver a otorgar a acceso a un instalador.

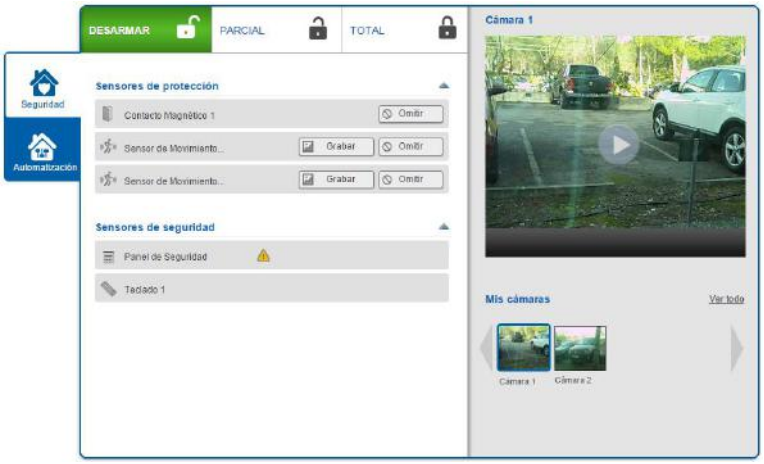


Estas funciones son descriptas en más detalles en la sección 12 de este documento.

4.3. Funciones del dominio

4.3.1. Pestaña Seguridad

La pestaña Seguridad permite al usuario armar y desarmar rápidamente el panel de alarmas, así como también monitorizar el estado actual de las zonas de seguridad.

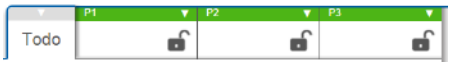


La visualización de la pestaña Seguridad se verá diferente, dependiendo de que si la característica de partición del panel ha sido activada o no.

La partición es una característica del panel que permite dividir el hogar en varias áreas independientes (p.ej., planta baja, piso de dormitorios, jardín, etc.), las cuales pueden ser armadas o desarmadas independientemente. Cada zona de seguridad (p.ej., sensor de movimiento, sensor de puerta, cámara PIR, etc.) puede ser asignada a una o más particiones.

Si el particionamiento no está activado en el panel de alarmas, los botones de armado en la parte superior del tablero están como así:

Si el particionamiento está activado en el panel de alarmas, los botones de armado en la parte superior del tablero están divididos según partición.



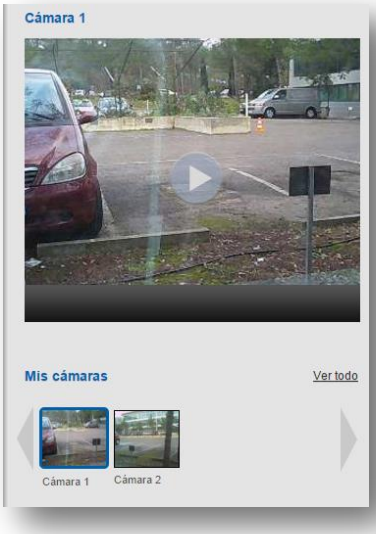
Al seleccionar los botones **PARCIAL** o **TOTAL** de una partición, el gateway instruye al panel de alarmas a ingresar el modo de seguridad correspondiente. Si en el panel de alarmas se ha configurado una cuenta regresiva para dar al usuario tiempo suficiente para salir de la casa sin activar una alerta, entonces esa cuenta regresiva es mostrada.

El indicador “Total” (mostrado en rojo) es para armar el sistema en su totalidad, y significa que todos los sensores de seguridad serán armados.

El modo “Parcial” (naranja) está destinado para proteger contra intrusiones mientras aún hay gente dentro de la casa. En este caso, solamente las zonas “perímetro” serán armadas, para monitorear las puertas y ventanas externas, mientras la gente puede aún vivir y moverse dentro de las zonas interiores de la casa.

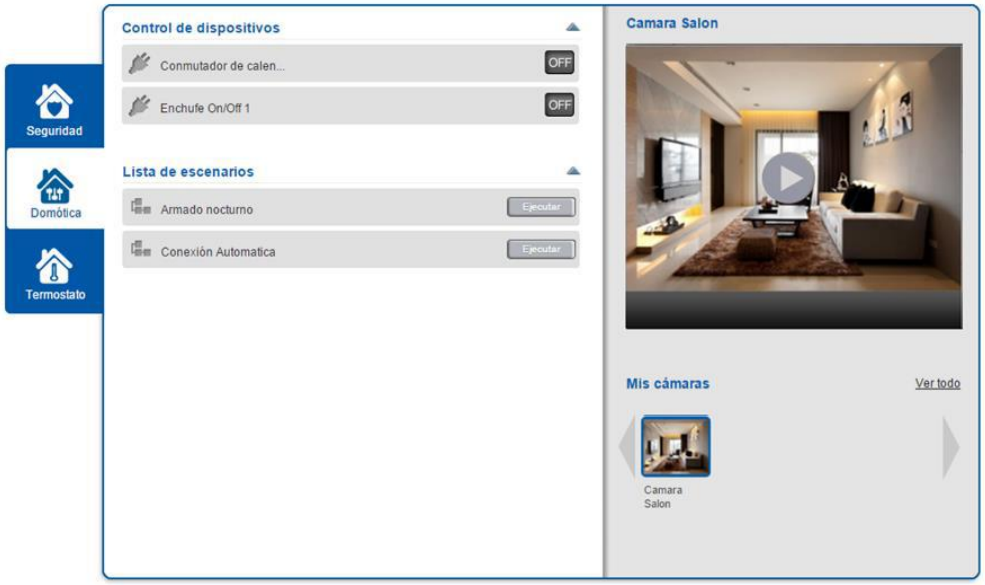
Ver las instrucciones del panel de alarmas por más detalles acerca de cómo configurar las particiones y cómo usar los modos de armado.

Al seleccionar la pestaña de seguridad, el usuario puede acceder a la sección de transmisión de video en vivo. Una de las cámaras de video registradas en el gateway puede ser seleccionada para poder ver su transmisión de video en vivo.



4.3.2. Domótica

Este servicio permite al usuario controlar en forma remota las luces y otros utensilios eléctricos.



Los dispositivos que controlan luces y otros dispositivos eléctricos, están representados por botones que reflejan sus capacidades.

- Los botones con ON y OFF permiten encender o apagar un dispositivo (y la lámpara o utensilio eléctrico conectado al mismo)

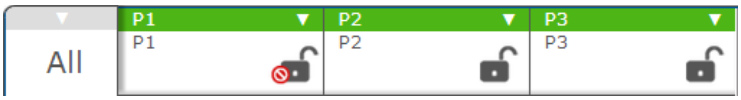
En la parte derecha del tablero, el panel de la cámara otorga al usuario acceso al streaming de video y grabación. El panel muestra todas las cámaras de IP asignadas a un gateway a manera de imágenes miniatura. Una vez seleccionada una cámara, el usuario puede pedir una secuencia de streaming en vivo y, si lo desea, pedir la grabación del stream de vídeo.

Refiérase a la sección 10 por más información sobre la característica de transmisión de video - streaming.

5. CONEXIÓN AL PANEL DE ALARMAS DEL POWERMASTER

5.1. Gestión del panel de alarmas desde la interfaz Web del gateway

Es posible armar y desarmar el panel con los botones de armado/desarmado. Se soportan hasta tres particiones. El número exacto de particiones se define cuando el panel de alarmas es configurado. Cada partición puede ser armada o desarmada independientemente una de la otra.

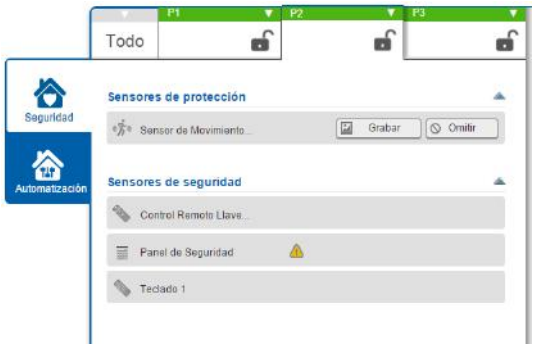


Un botón adicional rotulado **Todo** permite al usuario armar y desarmar todas las particiones configuradas con un único clic.

Note que el usuario final no solicita código PIN alguno cuando se arma o desarma el panel de alarmas a través del portal Web de autoservicio. En este caso, la aplicación del portal Web de autoservicio envía el código PIN automáticamente al panel de alarmas, en base al código de usuario que fue definido para el usuario de autoservicio actual en el menú "Gestionar usuarios" (ver Sección 12.4).

Al hacer clic en uno de los botones de armado, aparece una cuenta regresiva. En paralelo, el panel de alarmas podrá reproducir una serie de sonidos de pitidos (según cómo haya sido configurado). La duración del conteo regresivo es configurable en los ajustes del panel de alarmas.

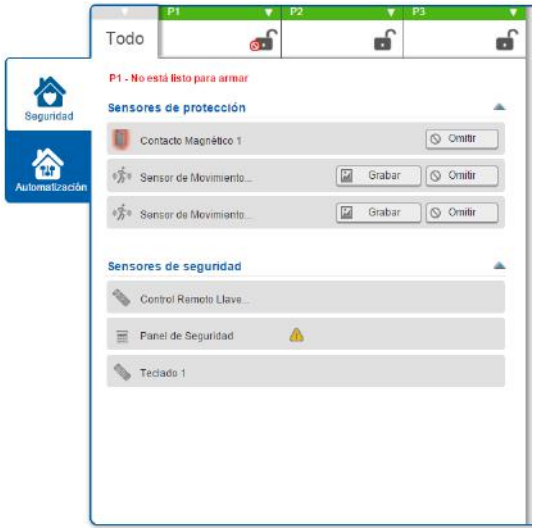
Es posible seleccionar una partición específica haciendo clic sobre la misma. Solamente se listan los dispositivos de seguridad registrados con la partición seleccionada.



Si se selecciona el botón Todo, entonces se listan todos los dispositivos de seguridad.

Si se activa un dispositivo del panel de alarmas (por ejemplo, se dejó una puerta entreabierta y se activa el sensor de la puerta), entonces el portal de ADT Smart Security destaca el sensor correspondiente y muestra un icono de candado con un signo de prohibido: .

Por ejemplo: en la imagen a continuación, la primera partición no está lista para ser armada porque fue activado un sensor de seguridad rotulado "Contacto Magnético 1".



Si el panel de alarmas está configurado con anulación manual de zonas de seguridad, entonces aparecen los botones **Omitir** junto a los dispositivos que pueden ser anulados:

Al hacer clic en el botón **Omitir**, el sensor correspondiente será anulado en el próximo armado.

En este caso, será posible armar el panel de alarmas a pesar de que el sensor aún esté activado. Sin embargo, mientras el panel de alarmas esté armado, el sensor anulado no puede informar ningún evento de intrusión. Esta es una violación de seguridad y el usuario debe comprender las consecuencias. Si alguien desea armar el panel de alarmas sin anular un sensor, antes deberá asegurarse de que no haya ningún dispositivo activado. Esto puede involucrar el cierre de todas las puertas y ventanas, y asegurarse de que los sensores de movimiento no detecten movimiento alguno.

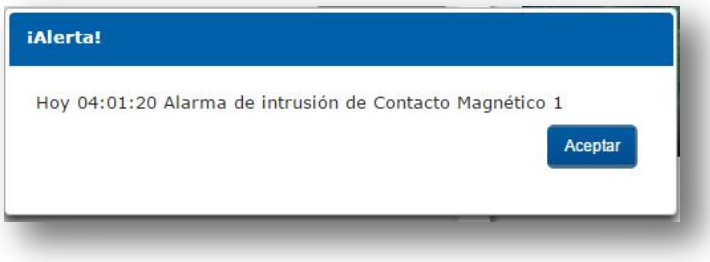
La anulación de un sensor es repuesta cuando el panel de alarmas es desarmado.

Si el panel de alarmas no está configurado para la anulación de sensores (algunos países tienen reglamentos que prohíben esta funcionalidad), entonces no aparecen los botones **Omitir**. Es necesario hacer esta configuración en el panel de alarmas propiamente dicho usando los ajustes del menú del instalador.

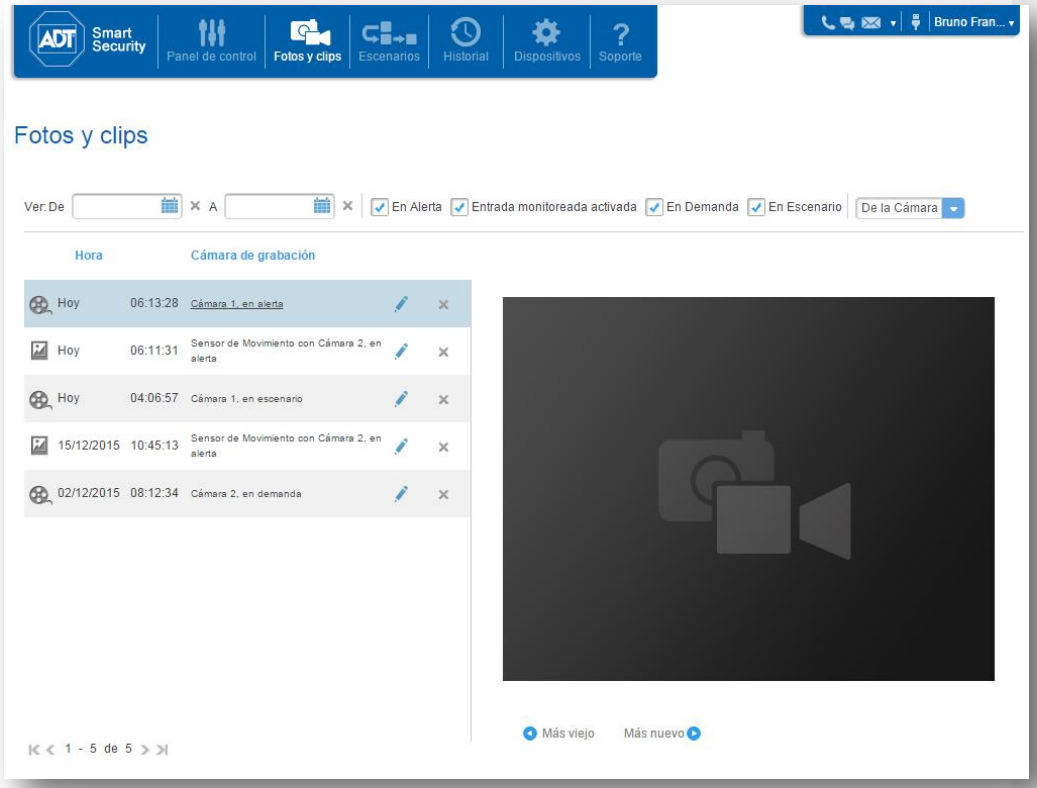
5.2. Detección de intrusiones

En caso de intrusión, el panel de alarmas se comporta como un panel de alarmas normal. Activa su(s) sirena(s) emparejada(s), notificando a un centro de monitorización a través sus propios medios de comunicación (por ejemplo, línea telefónica).

Además, se notifica a la plataforma ADT y se activan los mecanismos de notificación usuales. Por ejemplo, aparecerá una ventana emergente en las aplicaciones gráficas, se enviará un SMS y un email a las direcciones registradas, podrán activarse grabaciones de cámara, etc.

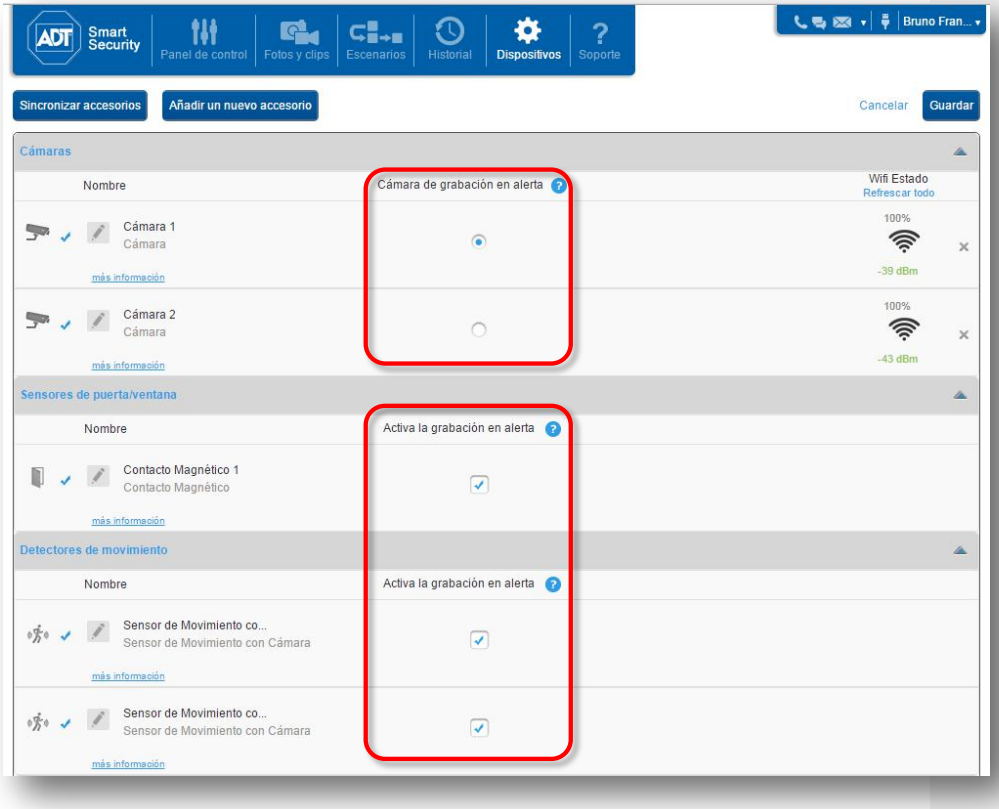


Si una de las cámaras de IP está configurada para efectuar una grabación de vídeo en una alerta, entonces se grabará automáticamente su transmisión de vídeo. Además, si el panel de alarmas tiene una cámara PIR que pueda tomar una serie de instantáneas, entonces se dispondrá de las mismas en cuanto se hayan transferido al gateway doméstico y serán cargadas a la sección Fotos y Clips del portal.



Para grabar un vídeo automáticamente usando una cámara IP, es necesario hacer lo siguiente:

- Seleccione la cámara que estará a cargo de la grabación; sólo se puede seleccionar una cámara.
- Seleccione los sensores de seguridad que pueden activar la grabación de vídeo. Si un sensor de seguridad está instalado demasiado lejos de la cámara, podría no tener sentido seleccionarlo para la grabación de vídeo. Por otra parte, probablemente los sensores ubicados cerca de la cámara o en una trayectoria que conduzca a la misma serían una mejor elección.



Note que aunque los sensores del panel de alarmas no sean gestionables directamente por el gateway (esto se realiza a través del panel de alarmas), el gateway es notificado por el panel de alarmas acerca de los cambios de status. Esto aporta beneficios tales como los siguientes:

- Las aplicaciones gráficas de ADT Smart Security muestran los status de los dispositivos en tiempo real, exactamente como con otros dispositivos.
- Es posible crear escenarios basados en los cambios de status de estos.

5.3. Grabar imágenes con los Videodetectores PIR

5.3.1. Descripción general

Esta característica permite al usuario solicitar a los videodetectores PIR (Visonic Next CAM PG2) obtener imágenes bajo demanda y ver el resultado en la sección Fotos & Clips.

El panel solicita las imágenes al videodetector. Puede llevar al Sistema uno o más minutos poner disponibles las imágenes para el usuario.

Esta función consume recursos de los videodetectores y del panel de seguridad por lo que el Sistema requiere de al menos de 15 segundos de tiempo entre dos peticiones de imágenes consecutivas. Durante este periodo otras peticiones de imágenes a los videodetectores serán rechazadas independientemente de si se realizan al mismo videodetector u otro o son solicitadas por otro usuario del sistema.

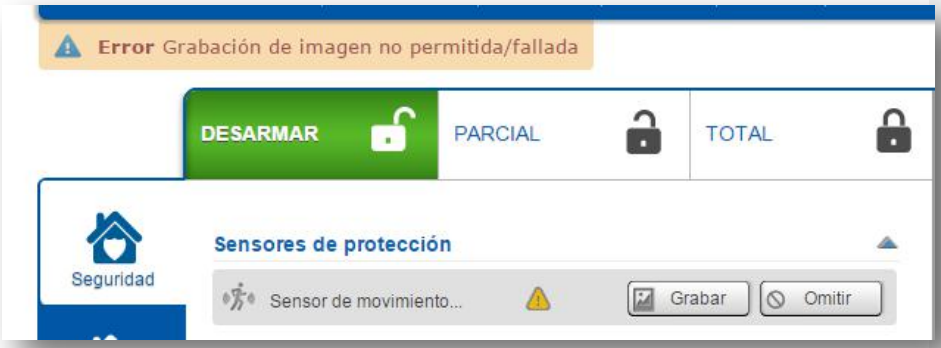
Una vez que las imágenes se han cargado en la nube los usuarios pueden acceder a ellas desde la sección de Fotos&Clips del portal web o de la aplicación ADT Smart Security.

5.3.2. Interfaz de usuario en el portal web.

La función de solicitar imágenes de los videodetectores está disponible en el panel de control de seguridad.

Un botón dedicado se muestra en cada línea de los videodetectores::

El resultado de la petición se muestra un mensaje que lo confirma.



Las imágenes se pueden ver en la sección Fotos&Clips:

En la sección de Fotos& Clips hay un filtro especial para seleccionar las imágenes provenientes de videodetectores bajo demanda.

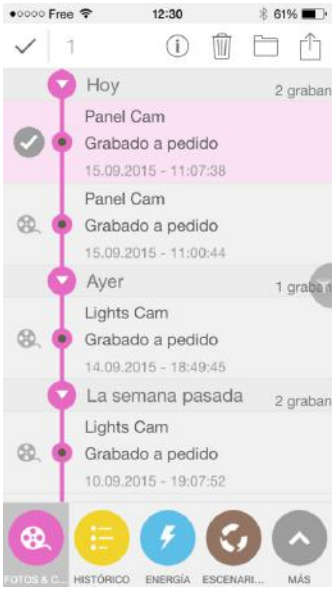
5.3.3. Interfaz de usuario de la aplicación móvil

En la aplicación móvil las peticiones de imágenes se pueden realizar desde el apartado de “ACCESORIOS”.

Pulsando en el botón de la cámara se lanza una petición de imágenes al videodetector PIR.

Un mensaje translúcido indica si la petición se ha realizado correctamente. En caso de que se haya realizado una petición reciente en el mismo panel un mensaje indicará que no se puede realizar la petición hasta pasar el periodo de 15 segundos.

Las imágenes serán visibles en la sección FOTOS&CLIPS.



En FOTOS&CLIPS hay un filtro adicional para seleccionar solo las imágenes solicitadas bajo demanda:

6. LA APLICACIÓN MÓVIL

6.1. Reseña

Es posible acceder a los servicios de ADT Smart Security con aplicaciones móviles ejecutadas en dispositivos iOS (iPhone, iPad, iPad Mini) o en smartphones y tabletas Android. Los interfaces de usuario suministrados para estos dispositivos son muy intuitivos y fáciles de usar. Estas aplicaciones móviles se pueden descargar de las tiendas de aplicaciones Apple AppStore y Google Play.

Para acceder a los servicios de ADT Smart Security en su smartphone, el usuario debe primero descargar e instalar la aplicación. Después de la instalación, el usuario puede ejecutar la aplicación desde su dispositivo móvil, seleccionando el icono de la aplicación. La aplicación se iniciará y solicitará del usuario ingresar sus detalles de login.

El usuario ingresará el mismo nombre de usuario y contraseña que se le pide para acceder a la cuenta en el portal Web.

La aplicación móvil se conectará entonces al servicio de la nube de ADT Smart Security, y proporcionará acceso a las características del gateway doméstico, según el conjunto de servicios a los que se suscribió este usuario.

En la parte inferior de la pantalla hay una barra de menú que contiene una lista de íconos:

Se dispone de más íconos haciendo clic en el botón "**Más**" o deslizando la barra de menú hacia arriba o hacia abajo.

Cada ícono representa una función a la que se puede ingresar. Para seleccionar una función, pulse con el dedo el icono correspondiente. La funcionalidad elegida es destacada, como se muestra en la figura anterior.

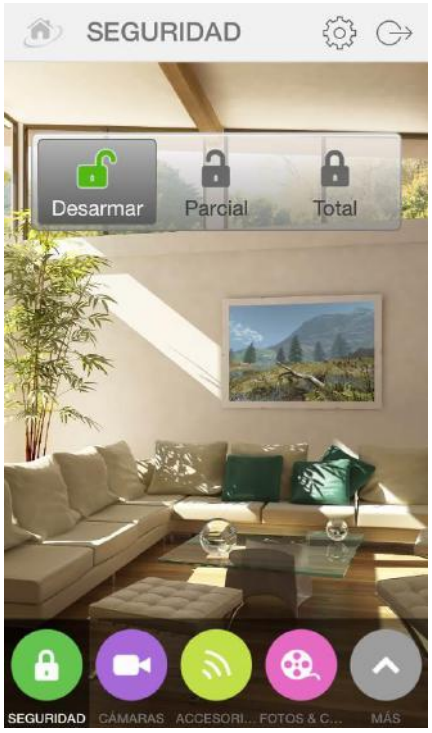
6.2. Seguridad

Por defecto, la primera pantalla que aparece es la pantalla Seguridad. Es posible acceder en cualquier momento al dominio Seguridad seleccionando el botón Seguridad en la parte inferior de la pantalla:

Se usa la pantalla Seguridad para armar o desarmar el panel de alarmas de seguridad.

En caso que el particionamiento no esté activado en el panel de alarmas de seguridad, la pantalla Seguridad muestra tres botones para:

- Desarmar el panel de alarmas
- Armar “parcial”
- Armar “total” (se arman todas las zonas de seguridad).



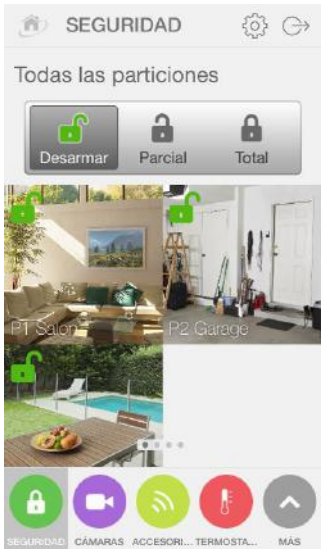
Cuando se pulsa uno de los botones de armado (Total o Parcial) aparece un conteo regresivo de salida antes de que se active el modo de configuración correspondiente. Esto coincide con el conteo regresivo de salida del panel de alarmas. Este conteo regresivo aparece solamente si el panel de alarmas fue configurado con un retardo de salida.

Si la gestión de las particiones está activada en el panel de alarmas de seguridad, la pantalla Seguridad permite armar o desarmar cualquier partición del panel de alarmas.

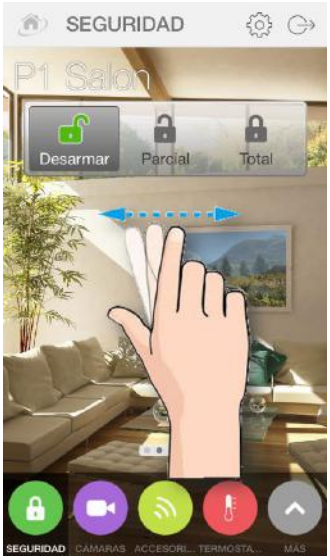
La primera pantalla muestra un mosaico de todas las particiones definidas en el sistema.

Los botones de armado/desarmado en este contexto son aplicables para todas las particiones juntas. Además, en los botones de armado y desarmado aparecen pequeños contadores que indican el número de particiones en cada estado de armado/desarmado.

Al hacer clic en una imagen de partición en esta pantalla, se mostrará la pantalla de seguridad de dicha partición.



También es posible acceder a cualquier partición deslizando el dedo hacia la derecha o la izquierda en la pantalla de partición.

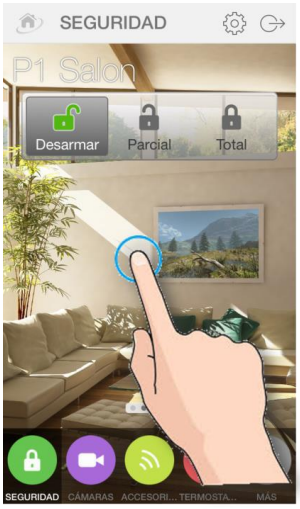


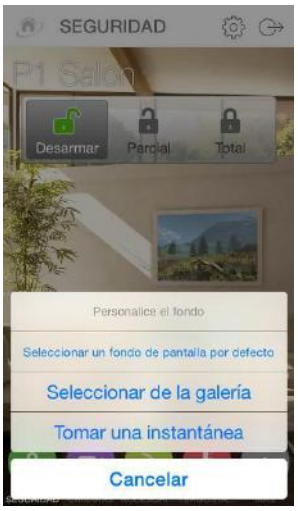
Se puede personalizar cada partición con un nombre y una imagen de fondo personalizadas.

Por defecto, las particiones son nombradas “P1”, “P2”, “P3” para partición 1, partición 2 y partición 3. Es posible dar un nombre más significativo y personal haciendo clic en el nombre de la partición, en la esquina superior izquierda de la pantalla.

Se puede también personalizar la imagen representando la partición, tanto descargarla como su foto tomada con la cámara de un Smartphone, o se puede seleccionarla dentro de las fotos pre-configuradas en la aplicación, o dentro de su galería personal.

Un pulso largo con el dedo en el medio donde está la imagen activa esta funcionalidad. Aparece un menú emergente, que indica cómo capturar una imagen para la partición (de las imágenes almacenadas en el teléfono, de la cámara integrada, etc.):





6.3. Accesorios

La pantalla Accesorios muestra la lista de accesorios instalados y permite enviarles los comandos de automatización.

Por defecto la pantalla lista todos los accesorios “actuadores”, es decir, los accesorios que aceptan comandos de automatización:

- Interruptor binario o toma binaria: Se muestra un botón que le permite poner dicha ficha/toma en ON y OFF.

Si deben poder ver todos los accesorios instalados, incluyendo los sensores, debe hacer clic en la pestaña filtro en el lado derecho de la pantalla y marcar la casilla de verificación “Mostrar todos”.

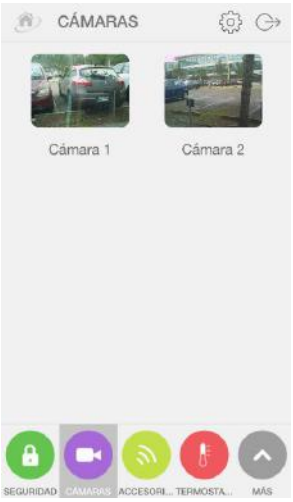
La lista de accesorios exhibidos puede ser refinada aún más con las siguientes opciones de filtrado:

- Filtrado por dominio: Muestra solamente accesorios de seguridad o accesorios;
- Filtrado por tipo de accesorio: Seleccione uno o más tipos de accesorio, tales como tomas, sensores de puertas, etc.
- Filtrado por sala: Seleccione una o más salas; los nombres de las salas propuestas en esta lista corresponden a los nombres de la ubicación asignados a los accesorios instalados durante el procedimiento del Asistente de emparejamiento.

En caso de que uno o más accesorios encuentren alertas técnicas tales como batería descargada o pérdida de conexión, dichos dispositivos serán listados en la primera sección de carpetas denominada “Necesita su atención”.

6.4. Cámaras

La pantalla Cámaras permite a los usuarios acceder a la transmisión en vivo de video de las cámaras IP emparejadas con sus gateways.



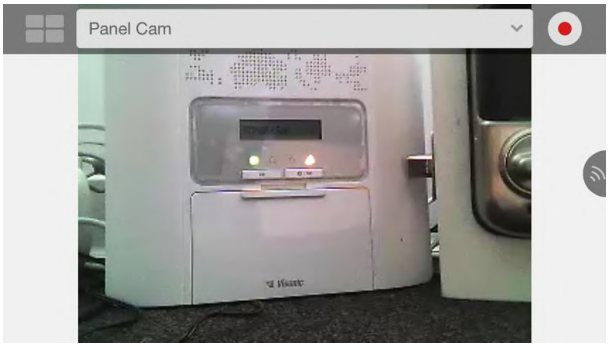
Elija una cámara de la lista de cámaras (primera pantalla), donde cada cámara es representada por una imagen recientemente capturada por esa cámara.

Una vez seleccionada la cámara, la segunda pantalla muestra un reproductor de video y la sesión de video comenzará inmediatamente. Inicialmente se muestran algunas imágenes instantáneas (foto por foto), permitiendo que el stream de video tenga tiempo de entrar a la memoria intermedia (“búfer”).

Cuando el stream de video esta disponible, un botón rojo aparece permitiendo la grabación del stream.

Para ver la imagen video en modo “full screen”, torna el teléfono en modo paisaje:

Tocar la pantalla para hacer apareciendo las comandas de la cámara:

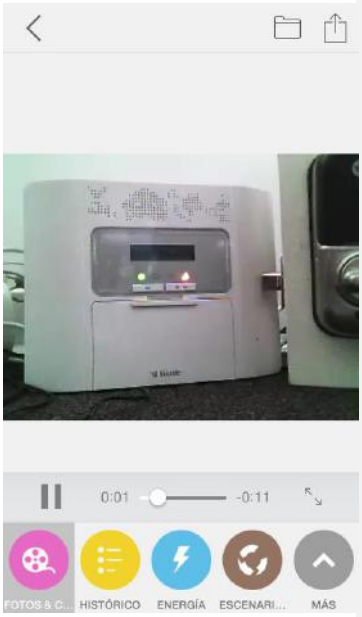


Tocar la pestaña al lado derecho de la pantalla para acceder a los accesorios de automatización.

6.5. Fotos y Clips

Es posible acceder a los archivos de video grabados mediante la pantalla **Fotos & Clips**. Esta pantalla presenta una lista vertical, con las grabaciones de video ordenadas por fechas. Es posible desplazarla hacia arriba y hacia abajo para poder ver toda la lista.

Al seleccionar uno de los clips (presionar con el dedo), el archivo correspondiente es descargado y comienza a mostrarse automáticamente:



Al girar el teléfono móvil a la posición apaisada, el reproductor de video muestra el clip de video en el modo de pantalla completa.

Mediante filtros se puede reducir la cantidad de fotos o clips de video que aparecen en la lista. Se pueden activar los filtros haciendo clic en la pestaña filtro en el lado derecho de la pantalla.

Se dispone de tres filtros:

- Filtro por período: muestra fotos y clips de las últimas 24 horas, la última semana, el último mes, o todas las fechas.
- Filtro por cámara: muestra fotos y clips de las cámaras IP o PIR cámaras seleccionadas.
- Filtro por tipo de evento: muestra fotos y clips que fueran grabado con los métodos seleccionados.

6.6. Histórico

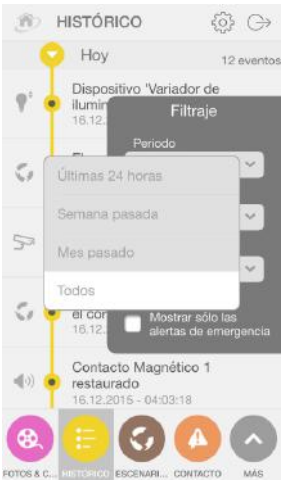
La pantalla Histórico provee los últimos registros de eventos para el gateway y sus accesorios así como también otra información de eventos tal como cuando fue iniciada una sesión de video desde la Web o una aplicación móvil. La lista está ordenada por fecha, la que puede ser plegada o desplegada haciendo clic en la flecha a la izquierda de la fecha.

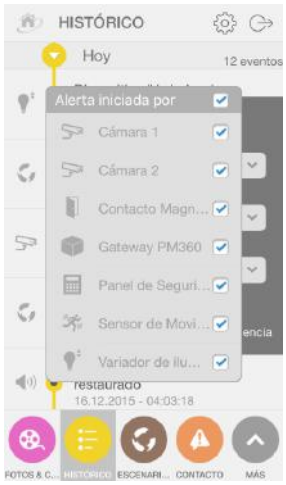
La cantidad de eventos de histórico mostrados puede ser reducida o ampliada también haciendo clic en la pestaña filtro a la derecha de la pantalla.

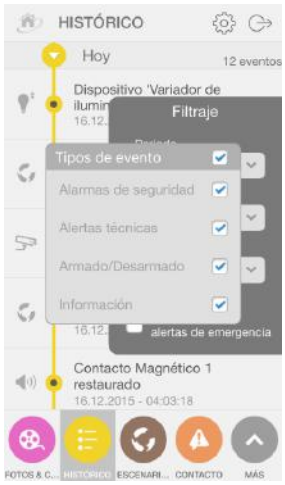
Se dispone de tres niveles de filtrado que pueden ser combinados entre sí:

- Filtrado por período: muestra eventos de las últimas 24 horas, la última semana, el último mes, o todos los eventos.
- Filtrado por accesorio: muestra los eventos que han sido iniciados por uno o más tipos específicos de accesorios.
- Filtrado por tipo de evento: muestra los eventos que fueron notificados por SMS, email, MMS o alertas de voz.
- Filtrado por prioridad: muestra solamente los eventos de alertas de emergencia o muestra todos los tipos de prioridad de eventos.


HISTÓRICO
Hoy
12 eventos
Filtraje
Periodo
Todos
Alerta iniciada por
Todos
Tipos de evento
Todos
Mostrar sólo las alertas de emergencia
Contacto Magnético 1 restaurado
16.12.2015 - 04:03:18
FOTOS & C...
HISTÓRICO
ESCENARI...
CONTACTO
MÁS

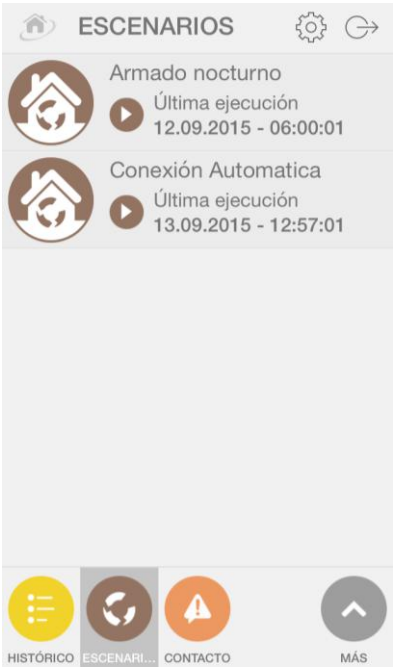

HISTÓRICO
Hoy
12 eventos
Filtraje
Periodo
Últimas 24 horas
Semana pasada
Mes pasado
Todos
Mostrar sólo las alertas de emergencia
Contacto Magnético 1 restaurado
16.12.2015 - 04:03:18
FOTOS & C...
HISTÓRICO
ESCENARI...
CONTACTO
MÁS


HISTÓRICO
Hoy
12 eventos
Alerta iniciada por
Cámara 1
Cámara 2
Contacto Magn...
Gateway PM360
Panel de Seguri...
Sensor de Movi...
Variador de ilu...
16.12.2015 - 04:03:18
FOTOS & C...
HISTÓRICO
ESCENARI...
CONTACTO
MÁS


HISTÓRICO
Hoy
12 eventos
Filtraje
Tipos de evento
Alarmas de seguridad
Alertas técnicas
Armado/Desarmado
Información
alertas de emergencia
Contacto Magnético 1 restaurado
16.12.2015 - 04:03:18
FOTOS & C...
HISTÓRICO
ESCENARI...
CONTACTO
MÁS

6.7. Escenarios

Los escenarios definidos por usuario pueden ser vistos haciendo clic en el botón escenarios.



Un escenario puede ser creado solamente usando la interfaz Web de autoservicio. Sin embargo, una vez que un escenario es creado, aparecerá en la lista de escenarios mostrados por la aplicación del smartphone.

No obstante, es posible borrar un escenario usando la aplicación del smartphone.

Para cada escenario definido es posible cambiar el status del escenario o ejecutar el escenario manualmente usando la aplicación del smartphone. Estas características son accesibles haciendo clic con el dedo en el ícono del escenario y visualizando la barra del menú de edición que aparece en el tope de la pantalla:

Una vez que este menú es accedido, sobre el ícono del escenario seleccionado aparece una marca de verificación para indicar a cuál escenario se le aplicarán las acciones.

La barra del menú permite diversas acciones en el escenario:

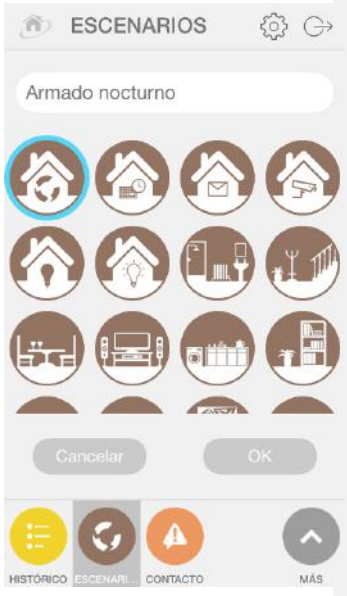
	Deseleccionar el escenario (y abandonar el modo de edición).
	Forzar la ejecución del escenario: el escenario es ejecutado inmediatamente, aún si el evento causante está ausente.
	Desactivar el escenario: el escenario no será ejecutado, aún si el evento causante está presente. Esto está disponible solamente si el escenario está activo.
	Activar el escenario: si el escenario había sido desactivado, es reactivado. Esto está disponible solamente si el escenario estaba inactivo.
	Editar el ícono del escenario: es posible seleccionar un ícono específico de una lista de íconos propuestos. Actualmente no hay una opción para expandir esa lista con íconos personalizados.

Al hacer clic en el ícono del triángulo  , es posible ver la configuración de un escenario:

Los diferentes componentes de un escenario (evento activador, acciones, duración) son listados verticalmente, desde arriba hacia abajo. Las versiones existentes de la aplicación del smartphone no permiten al usuario modificar ninguno de los componentes del escenario.

Sin embargo, haciendo un clic sobre el icono “Editar” se puede cambiar:

- El nombre del escenario
- El icono del escenario



7. GESTIÓN DE ACCESORIOS

7.1. ¿Qué es emparejamiento y porqué es importante?

Los accesorios son dispositivos que pueden ser configurados para intercambiar información con el gateway de ADT Smart Security. Los accesorios están conectados al gateway de la misma manera en que los sensores de seguridad están conectados al panel de alarmas para comunicar alertas y status.

Algunos accesorios operan con baterías portátiles mientras que otros deben ser enchufados a un tomacorrientes eléctrico. Los siguientes son los tipos de dispositivo que se conectan al panel de alarmas y al gateway:

- Sensores: Pueden medir/detectar condiciones en el entorno (temperatura, movimiento, humo, líquido, etc.) e informarlas al panel de alarmas.
- Actuadores: pueden recibir comandos y realizar ciertas acciones, como por ejemplo, encender o apagar una lámpara. están conectados al gateway doméstico y son controlados por el mismo.

El emparejamiento consiste en vincular un accesorio y el gateway para que puedan intercambiar información. El propósito de esta actividad es habilitar al accesorio a enviar información al - y aceptar datos del - gateway objetivo en una manera confiable y unificada. Este emparejamiento asegura que un vecino con un sistema similar no podrá controlar los accesorios de otra persona usando su propio gateway. Los accesorios no se comunican con un gateway hasta que hayan sido emparejados y no pueden ser controlados a distancia hasta que este proceso haya sido completado. Una vez emparejados, los accesorios interactúan con su gateway y no con otros. El accesorio también puede interactuar con otros accesorios emparejados con el mismo gateway.

7.2. Cómo emparejar un accesorio nuevo

El emparejamiento consta de dos pasos principales:

- Primero, el gateway doméstico es configurado al modo de emparejamiento, o sea que ya sabe que un dispositivo nuevo le solicitará unirse al ecosistema y puede prepararse para la comunicación inicial. Esto se hace típicamente sobre la interfaz de la Web, pero puede involucrar el pulsar un botón en el alojamiento del gateway para activar el modo de emparejamiento. Esto depende del modelo de gateway en uso.
- Segundo, el accesorio es activado para buscar un gateway doméstico que esté en el modo de emparejamiento y que esté registrado con el ecosistema. Esto se hace pulsando un botón en el accesorio propiamente dicho que permite que el proceso de emparejamiento sea ejecutado automáticamente.

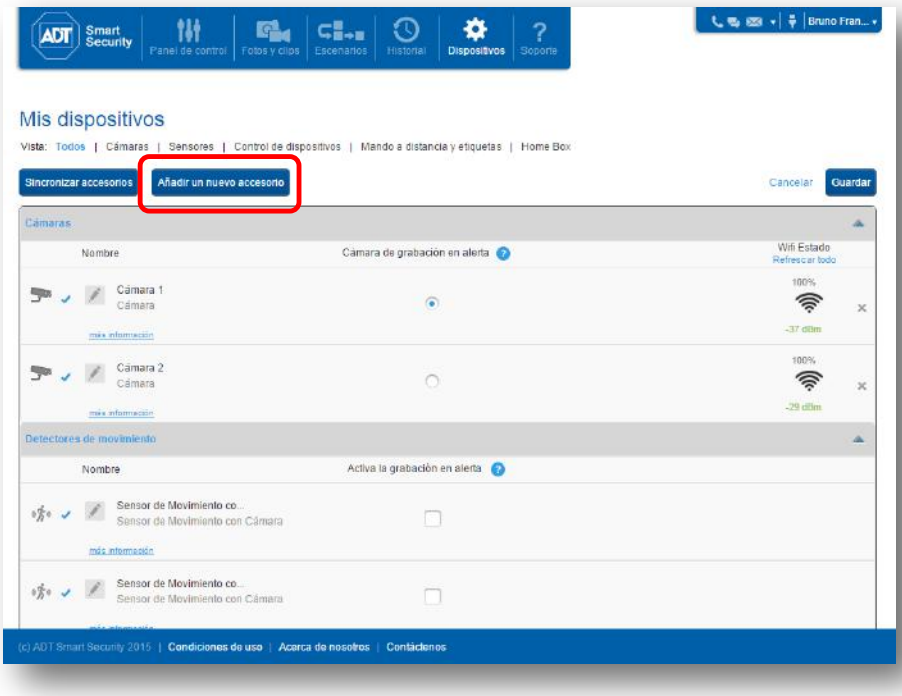
Dependiendo del accesorio, puede ser necesario pulsar una vez, dos veces e incluso hasta tres veces en el botón pulsador del dispositivo para iniciar el proceso de emparejamiento. Esto depende del dispositivo y en las decisiones de diseño efectuadas por cada fabricante del accesorio. La plataforma ADT Smart Security provee instrucciones en su interfaz Web para guiar al usuario a través de los diferentes pasos de emparejar un accesorio nuevo. Si el accesorio nuevo es soportado por la plataforma ADT Smart Security, las instrucciones del Asistente toman en cuenta las particularidades de dicho accesorio y permite al usuario seguir un conjunto simple de pasos para emparejarlo sin tener que consultar la guía del usuario del dispositivo.

7.3. Emparejar un accesorio con la interfaz Web de ADT Smart Security

(Nota: El emparejamiento de un accesorio está actualmente soportado solamente desde el autoservicio Web, pero no desde las aplicaciones móviles iOS y Android)

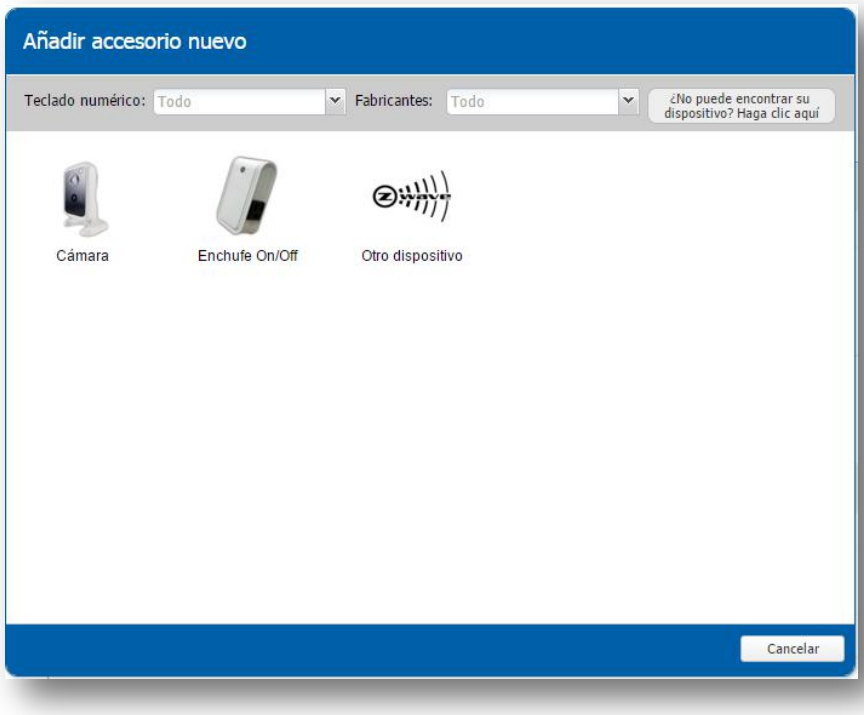
El emparejamiento de accesorios nuevos es extremadamente sencillo e intuitivo. Puede ser logrado en segundos usando unos pocos pasos simples. Sin embargo, esta actividad de emparejamiento forma parte de los servicios de instalación realizados por un instalador ADT autorizado. Esto incluye actividades de verificación adicional y también la colocación y el cableado del accesorio en el hogar.

Para añadir un accesorio, haga clic en el menú **Dispositivos** y luego en el botón **Añadir un accesorio nuevo** a la izquierda.



También hay un botón de acceso rápido en la esquina superior derecha del tablero:

La interfaz Web provee una lista de accesorios soportados, como se ilustra a continuación (esta lista se expande cuando hay accesorios nuevos que son soportados).



Dependiendo del accesorio seleccionado, un Asistente específico guía al usuario final a través de los pasos de emparejamiento del accesorio.

Los dos ejemplos en las secciones siguientes ilustran cuán sencillo es emparejar accesorios nuevos.

7.4. Ejemplo 1 – Aparear un enchufe de alimentación con un gateway

7.4.1. Instalación de un enchufe de alimentación

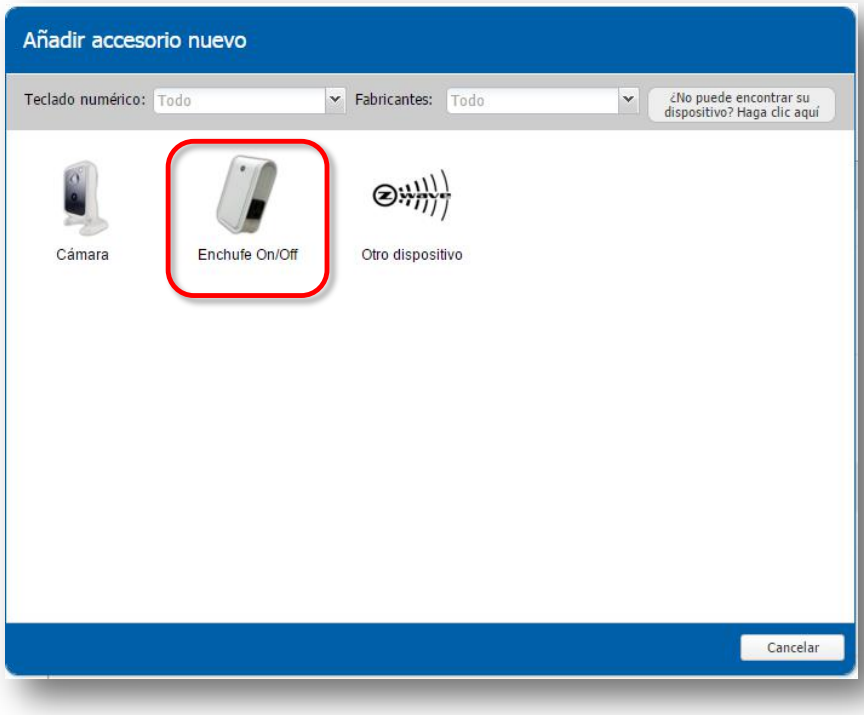
El enchufe de alimentación es conectado a un tomacorrientes y controla un utensilio de iluminación que esté conectado al mismo. Tiene un botón ON/OFF manual para control directo, pero también puede ejecutar comandos ON/OFF enviados a él por el gateway domiciliario.

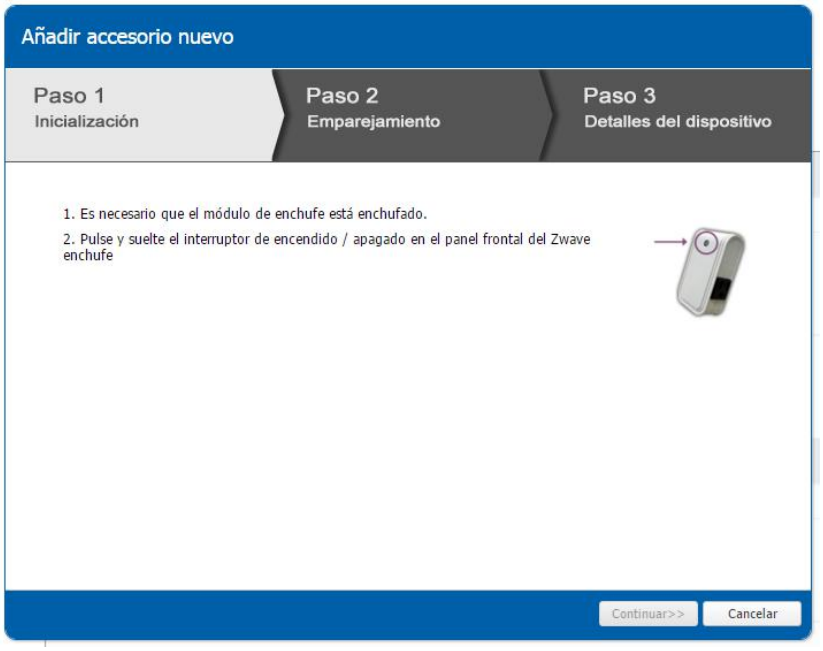
Para operar y emparejar este dispositivo, el enchufe de alimentación debe primero estar enchufado a un tomacorrientes eléctrico. Esto provee al módulo del enchufe la energía para que su circuito pueda operar.

7.4.2. Emparejar un enchufe de alimentación

Para emparejar el enchufe de alimentación, primero debe hacer login al portal Web de autoservicio y hacer clic en el botón “Añadir un accesorio nuevo”. Aparecerá la ventana del Asistente de emparejamiento y suministrará una lista de los dispositivos que pueden ser emparejados por el sistema. Seleccione el enchufe de alimentación de la lista, identificando la foto que coincida y el número del modelo. Además, la lista de accesorios puede ser filtrada para hallar el dispositivo con más facilidad. Los filtros incluyen grupos (por ejemplo, “Enchufes”) y fabricantes (por ejemplo, “Everspring”).

El primer paso de emparejamiento del accesorio suministra instrucciones para preparar el accesorio para emparejarlo.





Suponiendo que el dispositivo aún no esté emparejado, el usuario puede seguir las instrucciones de preparación para el dispositivo y luego hacer clic en el botón Continuar para proceder con el emparejamiento.

Sírvase notar que un dispositivo Z-Wave nunca se emparejará al gateway si ya fueron emparejados, ya sea al gateway doméstico actual o a otro. En esta situación, el Asistente sugiere que el usuario primero cancele el emparejamiento del dispositivo (desemparejarlo) y mostrará las instrucciones sobre cómo hacerlo. No hay ningún riesgo en realizar el procedimiento de desemparejar, independientemente del status de emparejamiento del dispositivo. Si está en la duda, de todas maneras es más seguro ejecutar el proceso de desemparejar.

Además, note que dado que el proceso de emparejamiento comienza poniendo el gateway en el modo de exclusión, cualquier accesorio Z-Wave que sea activado para entrar en su propio modo de emparejamiento /desemparejamiento (denominado modo de inclusión/exclusión en Z-Wave) será desemparejado (excluido) del gateway. Se requiere que el usuario trabaje con solamente un gateway y un accesorio durante el emparejamiento.

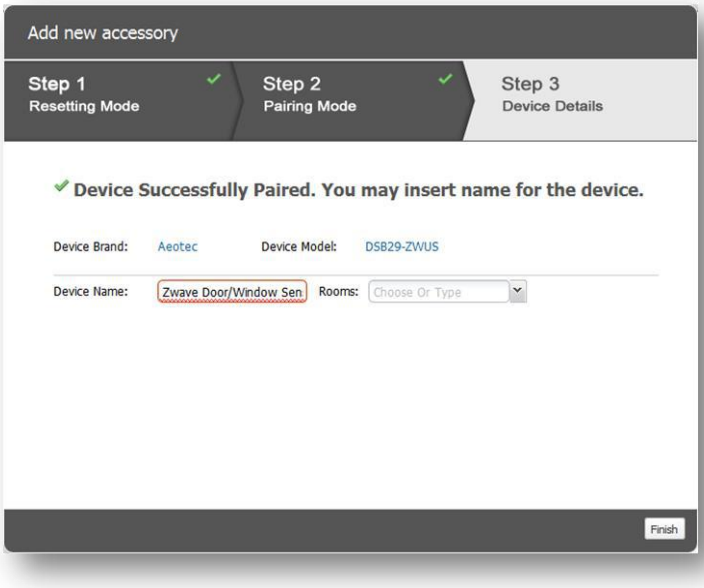
Una vez completado el desemparejamiento y que el dispositivo esté listo para ser emparejado nuevamente, haga clic en el botón Continuar para llegar a la segunda etapa del proceso de emparejamiento.

El gateway está ahora puesto en el modo de inclusión, y uno de sus LEDs destellará indicando que el emparejamiento puede ser realizado.

Pulse brevemente el botón de emparejamiento en el enchufe de alimentación, como lo instruye el Asistente. En el caso del enchufe de alimentación ADT son tres pulsaciones rápidas en sucesión. El proceso de emparejamiento comenzará automáticamente.

Durante este proceso hay un intercambio de datos entre el dispositivo y el gateway. El Asistente mostrará el status del proceso de emparejamiento en la barra de progreso en la parte inferior de la pantalla. El gateway finalizará el proceso de emparejamiento e indicará el éxito una vez que el proceso haya sido completado.

El Asistente solicitará del usuario que provea un nombre para el nuevo dispositivo.



Comment [BF1]: To be updated for TIFS Spain

Ingrese un nombre apto, y haga clic en el botón **Finalizar**. El dispositivo está ahora emparejado con el gateway.

El gateway domiciliario saldrá automáticamente de su modo de inclusión/ emparejamiento cuando el Asistente finalice.

El enchufe de alimentación puede ahora ser controlado por el gateway.

7.5. Ejemplo 2 – Emparejar una cámara nueva

Las cámaras permiten a los usuarios efectuar comprobaciones visuales de lo que está sucediendo en el hogar.

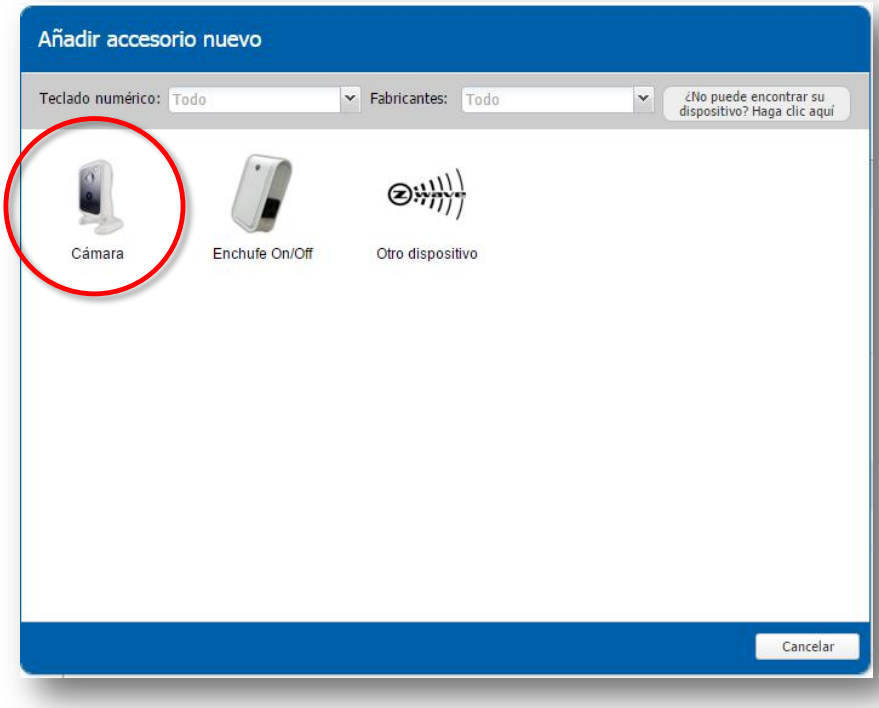
Se soportan dos tipos de cámaras:

- Cámaras Visonic PIR: estas cámaras son emparejadas con el panel de alarmas; pueden detectar movimientos usando sus módulos PIR. Si el panel de alarmas está armado, puede activarse una alerta de intrusión y la cámara PIR puede capturar varias instantáneas. Estas instantáneas son transmitidas automáticamente por el gateway domiciliario al almacenamiento personal de video de la plataforma de ADT Smart Security. Sin embargo, el emparejamiento de la cámara PIR no es realizado mediante el sitio Web de ADT Smart Security. Esto debe ser hecho directamente con el panel de alarmas. Refiérase a la guía del panel de alarmas por este procedimiento.
- Cámara IP: esta cámara de video es manejada por el gateway de ADT Smart Security. Su emparejamiento es hecho mediante la interfaz Web del gateway domiciliario, y se describe a continuación.

Para emparejar una cámara nueva:

1. Conecte la unidad de la fuente de alimentación de la cámara a un tomacorrientes (y la cámara a su fuente de alimentación).
2. Conecte la cámara al puerto LAN Ethernet del gateway de ADT Smart Security usando un cable Ethernet. Si el panel de alarmas ya está enchufado en el puerto LAN, desconéctelo y reconéctelo cuando haya finalizado el emparejamiento de la cámara.
3. Haga login en el portal de autoservicio de la cuenta (de no haber hecho ya login) y haga clic en la opción “Añadir un nuevo accesorio” en el menú Dispositivos para iniciar el Asistente de emparejamiento.

   Seleccione la imagen que coincida con la cámara a ser emparejada.

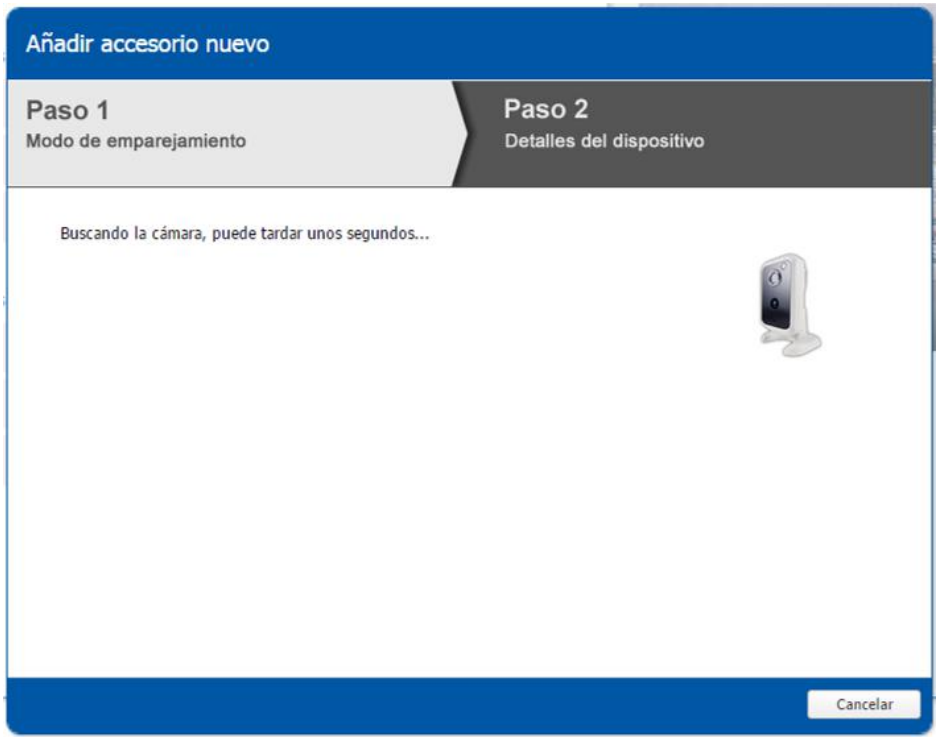


4. Aparecerán las instrucciones para el proceso de emparejamiento. Note que el protocolo de emparejamiento de la cámara es diferente que el protocolo de emparejamiento del enchufe de alimentación. El propósito del Asistente de Emparejamiento es ocultar las diferencias entre los diferentes protocolos y mantener el proceso tan simple como sea posible. Además, y a diferencia de lo que pasa en el procedimiento del enchufe de alimentación, no hay un botón para pulsar en la cámara para iniciar el emparejamiento. El emparejamiento puede ocurrir automáticamente si la cámara está en la misma red que el gateway domiciliario.

Para emparejarse apropiadamente, la cámara solamente debe estar encendida y conectada al gateway mediante un cable Ethernet. Si la cámara no es detectada, repita la operación desde el inicio. Si al inicio la cámara estaba apagada (su cable de alimentación eléctrica estaba desconectado), asegúrese que la cámara esté encendida y espere hasta que la cámara se haya inicializado completamente (para la cámara RC8221 ambos LEDs verdes en la parte posterior de la cámara deben estar iluminados).

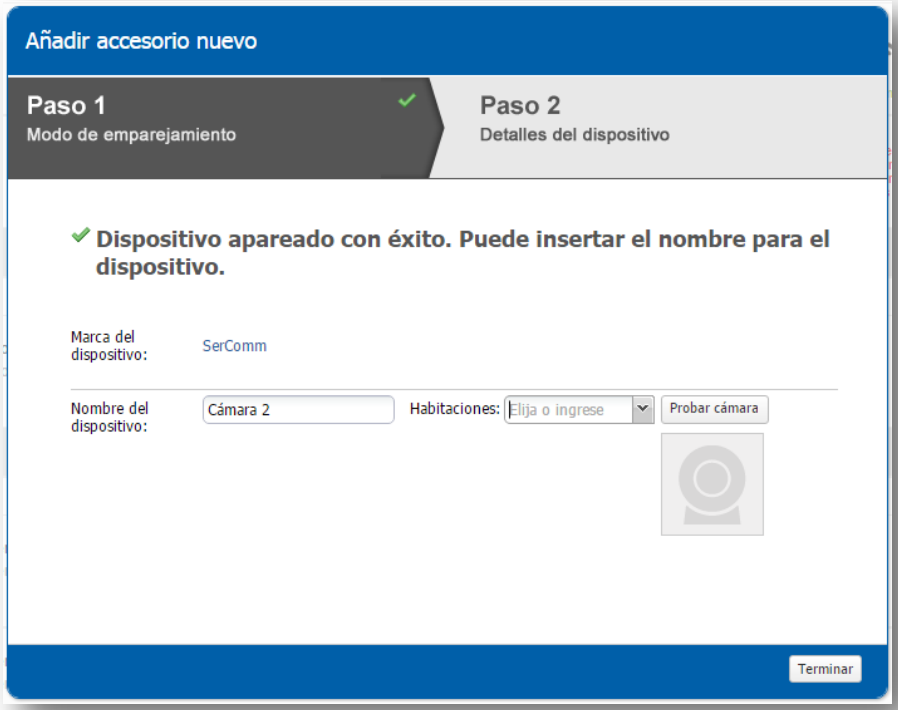
Nota: el dispositivo con dos antenas mostrado en la ilustración anterior, y que se encuentra entre el gateway domiciliario y la cámara, representa su enrutador de red domiciliaria. Ésta es únicamente una ilustración representativa, y el enrutador no es provisto con la plataforma ADT Smart Security. Si bien es posible emparejar la cámara al disponer tanto del gateway como de la cámara conectados a un enrutador, se recomienda conectar la cámara directamente al puerto LAN del gateway. Esta actividad de emparejamiento también forma parte de los servicios de instalación realizados por un instalador de ADT autorizado. Esto incluye actividades de verificación adicional, y también la colocación y el cableado del accesorio en el hogar.

5. Haga clic en el botón **Continuar**.



El gateway ahora intenta hallar la cámara en la red.

6. Cuando la cámara es hallada, el Asistente requiere dar un nombre a la nueva cámara (propone un nombre por defecto)



Ingrese un nombre que le ayude a identificar fácilmente la cámara. En el campo "Habitaciones", elija una ubicación en la lista de habitaciones, o ingrese su propio nombre de ubicación (por ejemplo: “Dormitorio de Pablo”).

7. Al hacer clic en el botón “Probar Cámara”, es posible capturar una imagen instantánea desde la cámara recientemente emparejada. Este instantánea aparece debajo del botón. Si la imagen no aparece, podría haber un problema con la cámara. Compruebe que nada esté obstruyendo la visibilidad de la lente. Si no halló ninguna obstrucción, entonces intente reiniciar el proceso desde el comienzo o contacte al Servicio de Asistencia por soporte.
8. A continuación el Asistente configura la cámara automáticamente para conectarla al gateway de manera inalámbrica. El punto de acceso a la red inalámbrica ("hotspot") del Wi-Fi es ocultado intencionalmente: su SSID no es difundido y no aparece en la interfaz de autoservicio. Además, la señal de Wi-Fi es encriptada y no se muestra la contraseña. Esto es por propósitos de seguridad y confiabilidad, ya que la señal de Wi-Fi del gateway domiciliario debe ser reservada exclusivamente para las cámaras.
9. Haga clic en el botón **Finalizar.** El Asistente de emparejamiento se cierra.

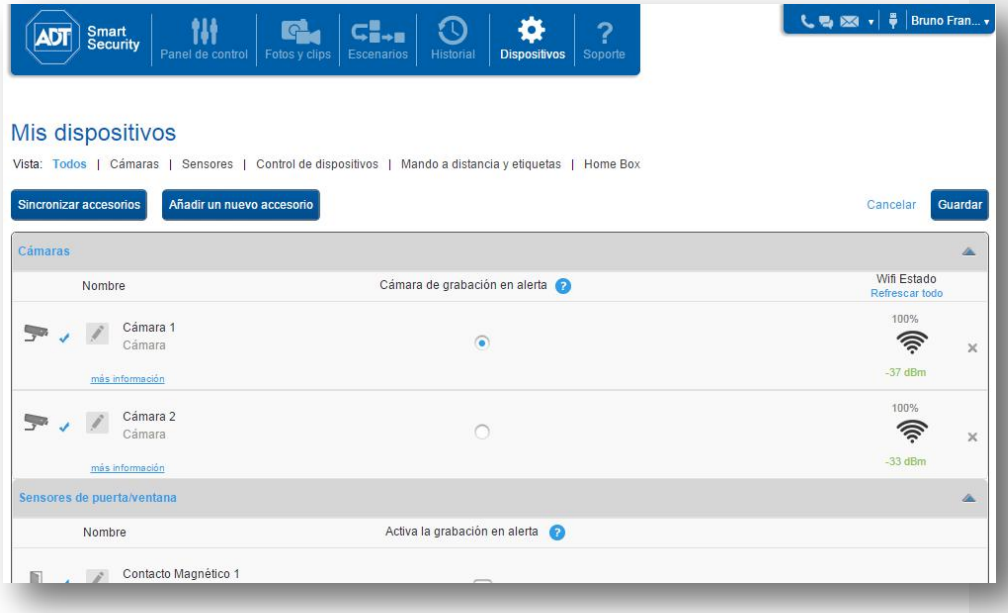
   La cámara está ahora emparejada con el gateway. Desconecte el cable Ethernet y conéctelo de nuevo al panel de alarmas. Para tener mejores resultados se recomienda apagar y encender la cámara, desconectando y reconectando su cable de electricidad.

Ésta también es una buena oportunidad para mover la cámara a su ubicación final deseada. La cámara se conectará automáticamente a la LAN privada y asegurada de la gateway en modo WiFi.

7.6. Gestión de accesorios emparejados

Es posible eliminar un accesorio o cambiar algunos de los ajustes de configuración del dispositivo después que el accesorio haya sido emparejado.

Para modificar los ajustes de configuración de un accesorio, haga clic en el menú **Dispositivos**:

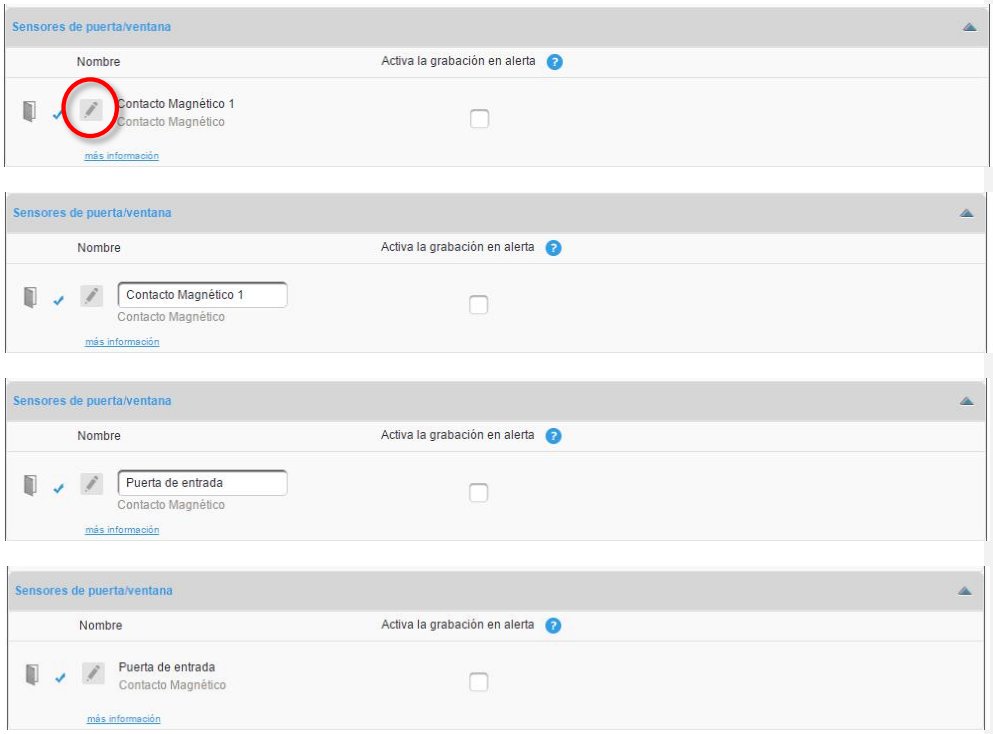


7.6.1. Sincronización de accesorios

Si alguno de los accesorios que fueron agregados (emparejados) o eliminados no fueron actualizados correctamente en la interfaz Web, es posible forzar una sincronización de su status haciendo clic en el botón "**Sincronizar accesorios**". Esto fuerza una actualización de la lista de accesorios emparejados almacenados en el gateway. Este procedimiento impactará solamente dispositivos que están emparejados con el gateway, usando el protocolo Z-Wave, tales como enchufes de alimentación. Los dispositivos emparejados con el panel de alarmas no se ven impactados.

7.6.2. Renombrar un accesorio

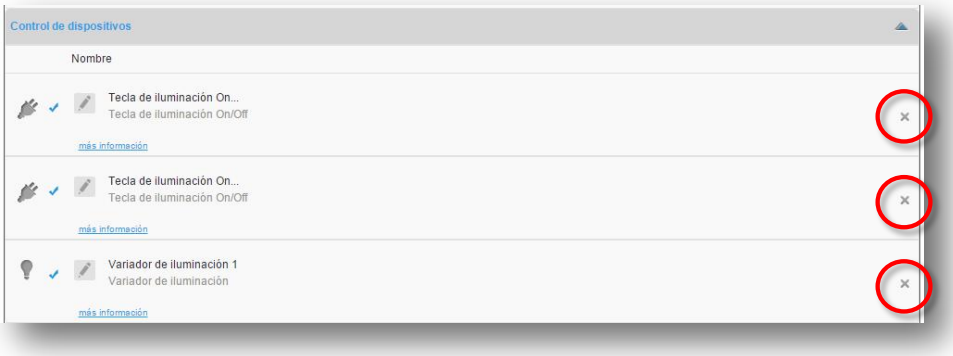
Para renombrar un accesorio haga clic en el icono del lápiz  y actualice el nombre del accesorio en la zona de edición.



Luego haga clic en el botón **Guardar** para guardar los cambios efectuados.

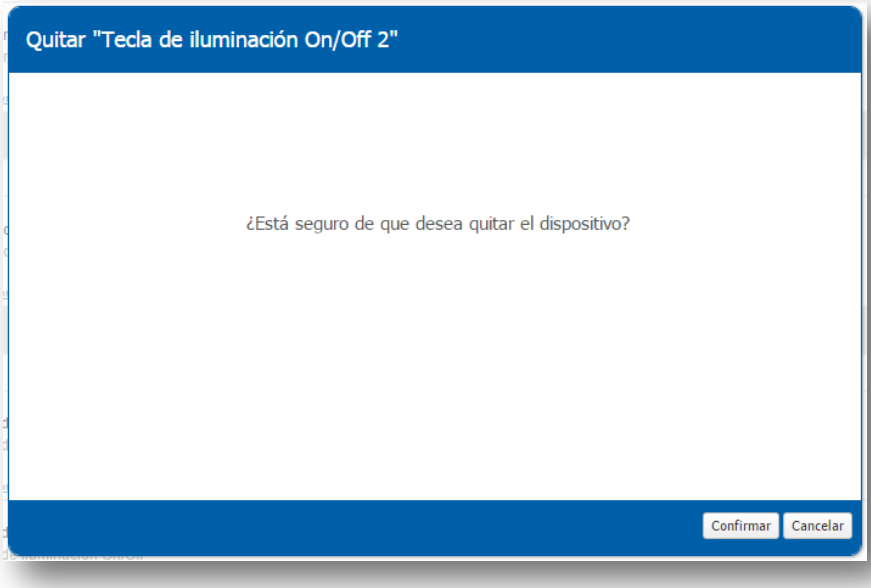
7.6.3. Eliminar (desemparejar) un accesorio no Z-Wave: cámaras de IP y dispositivos del panel de alarmas

Para eliminar un accesorio de la lista de dispositivos que usted haya previamente emparejado,



haga clic en la marca de la cruz a la derecha.

Aparecerá la pantalla Eliminar dispositivo y se solicitará confirmación de la acción. Haga clic en el botón **Aceptar** para confirmar la eliminación del dispositivo.

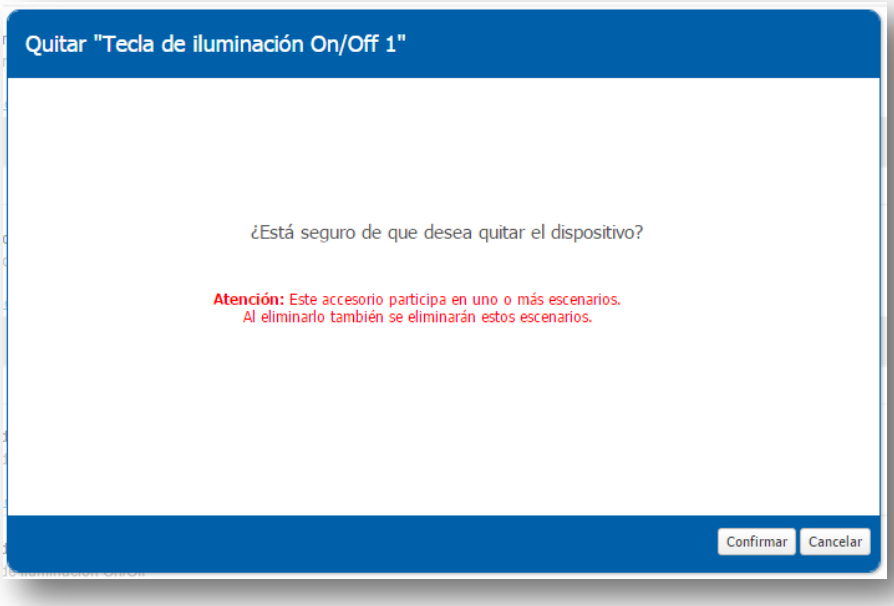


Si se elimina algún accesorio por error, entonces será necesario volver a emparejarlo mediante un procedimiento de emparejamiento de accesorio nuevo.

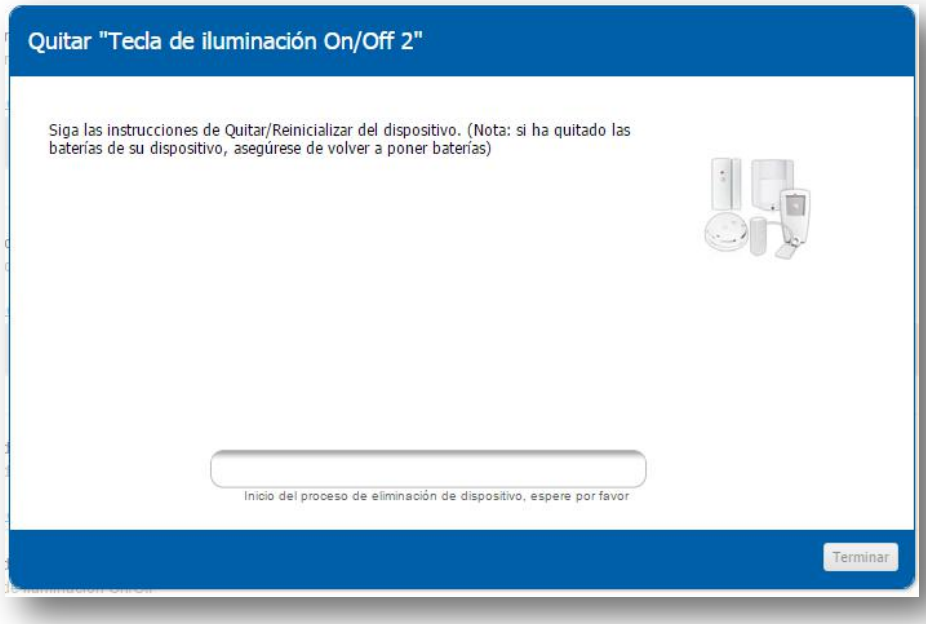
También es posible eliminar un dispositivo emparejado con el panel de alarmas. Sin embargo, si es necesario volver a emparejar un dispositivo eliminado, entonces será necesario ejecutar el procedimiento de emparejamiento en el panel de alarmas para restaurarlo. Esto requiere conocer el código PIN del instalador del panel de alarmas y los procedimientos apropiados.

El procedimiento para eliminar un accesorio Z-Wave es levemente diferente que con un dispositivo no Z-Wave. Esta acción debe ser llevada a cabo en el dispositivo mismo, para iniciar el procedimiento de desemparejar. El proceso es similar al procedimiento de emparejar. Es necesario establecer el gateway doméstico en modo de exclusión, y se requiere una acción en el dispositivo (pulsar un botón) para notificar de que debe ser desemparejado. Esto permite que el dispositivo y el gateway doméstico intercambien datos para que ambos sepan que no deberán seguir comunicándose. Una vez completado este proceso, el dispositivo deja de intercambiar datos con el gateway doméstico y está listo para ser emparejado con otro gateway (o restaurado al mismo gateway si se desea). Note que no es necesario que un dispositivo Z-Wave sea desemparejado por el mismo gateway al que se encuentra emparejado. Si un dispositivo está emparejado con un gateway que ya no está presente, entonces el gateway existente lo puede desemparejar sin problemas. Sin embargo, el gateway no puede emparejar un accesorio con otro gateway que no sea él mismo.

Nota: Si el accesorio es utilizado por un escenario, mientras que la eliminación del accesorio también eliminará el escenario.



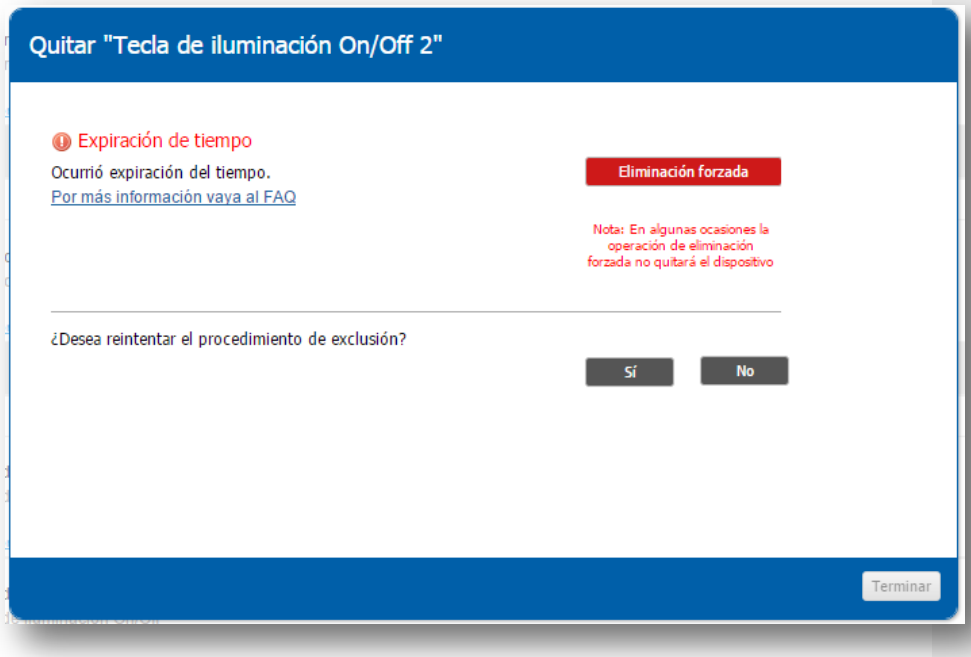
Una vez iniciado el proceso de eliminación de un dispositivo (desemparejamiento), aparece automáticamente un Asistente en el portal de autoservicio. Él guía al usuario a través de los pasos de desemparejamiento del dispositivo. El ejemplo a continuación muestra al Asistente para el desemparejamiento de un dispositivo Z-Wave. Después de solicitar confirmación ("¿Está seguro de que desea eliminar este dispositivo?") el Asistente pone al gateway en modo de exclusión:



El proceso tarda unos pocos segundos e involucra la interrogación del gateway por el dispositivo, detectando que está en modo de exclusión y luego borrando su información de registro del gateway. Otros dispositivos Z-Wave no son eliminados mientras sus botones de emparejamiento/desemparejamiento no estén pulsados mientras el gateway aún se encuentre operando en modo de exclusión.

Una vez finalizado el desemparejamiento, el Asistente termina deteniendo el modo de exclusión del gateway.

Cuando el gateway ingresa al modo de exclusión se activa un temporizador. Si después de algún tiempo ningún dispositivo solicitó la exclusión, entonces el Asistente termina el modo de exclusión del gateway.



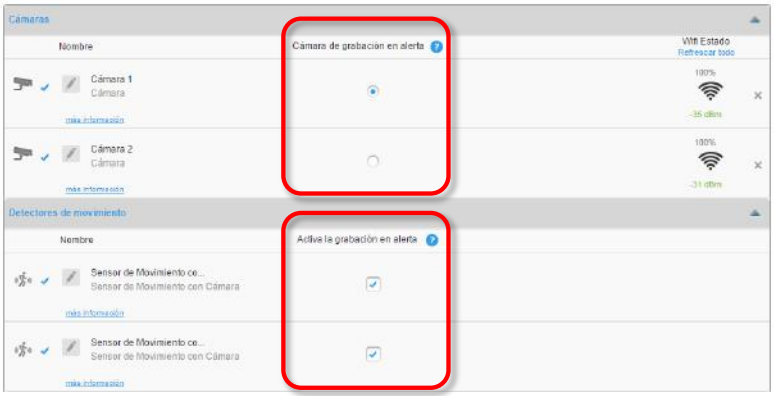
Haga clic en el botón **Sí** para reintentar el procedimiento de exclusión o en el botón **No** para salir del Asistente.

7.6.4. Grabación automática de la cámara

Es posible grabar vídeos automáticamente desde una cámara de IP cuando el sistema de seguridad detecta una alarma de intrusión, alarma de manipuleo, alerta de pánico o alerta de seguridad. Solamente se puede seleccionar una cámara de IP para grabaciones automáticas de entre las cámaras emparejadas disponibles. Si hay múltiples cámaras emparejadas con el gateway de ADT Smart Security, entonces es posible especificar cuál cámara graba vídeos en forma automática y los carga en tiempo real a la plataforma de ADT Smart Security basada en nube. Se debe elegir muy cuidadosamente la cámara seleccionada para esta característica, para asegurar que las grabaciones en caso de alerta sean significativas.

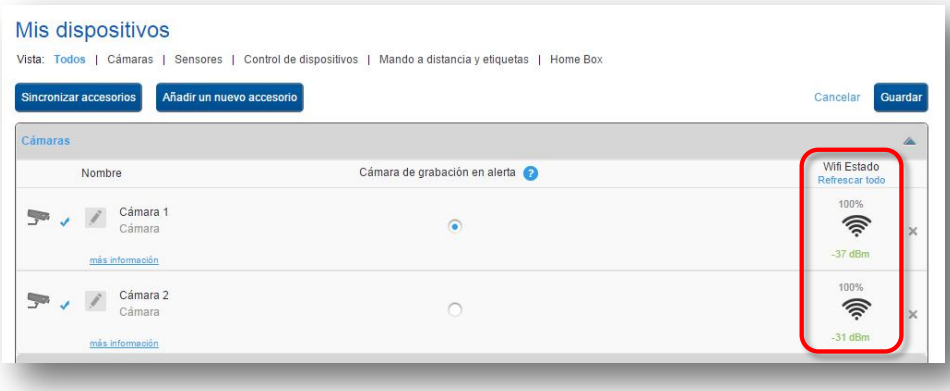
Haga clic en el botón Dispositivos en la barra de botones de funciones entre dominios y haga clic en el botón de radio “Cámara de grabación en alerta”.

Nota: También debe seleccionar los sensores de seguridad que deben activar la grabación de vídeo desde la cámara de IP seleccionada. Puede seleccionar uno o más sensores.



7.6.5. Verificación de la intensidad de la señal de WiFi de las cámaras IP

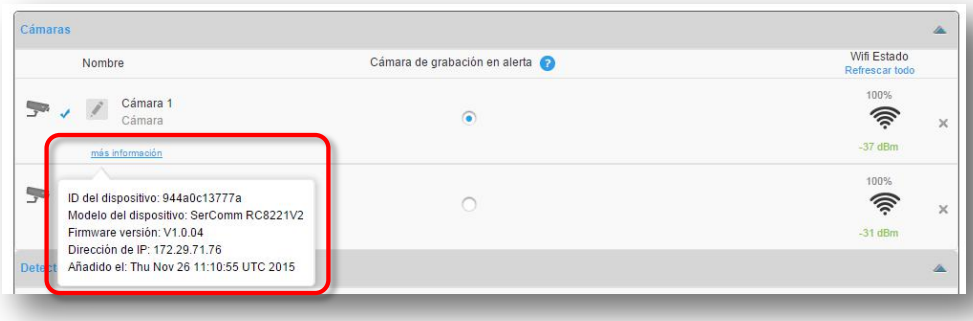
Durante la instalación de la cámara, es importante verificar que las cámaras IP estén instaladas en una ubicación que esté dentro del alcance de la red privada de WiFi del gateway. Puede verificar la calidad de la red WiFi del gateway recibida por la cámara de IP, observando el icono de WiFi en el extremo derecho del dispositivo.



El icono del WiFi muestra la calidad del porcentaje de la señal de WiFi y el valor de RSSI en unidades de dBm. Los valores son actualizados con cada carga de la página Web Dispositivos. Puede renovar los valores de la intensidad de la señal de WiFi haciendo clic en el enlace “Renovar todos”, lo que renovará los valores medidos para todas las cámaras de IP registradas.

7.6.6. Verificación de la dirección de IP de las cámaras IP

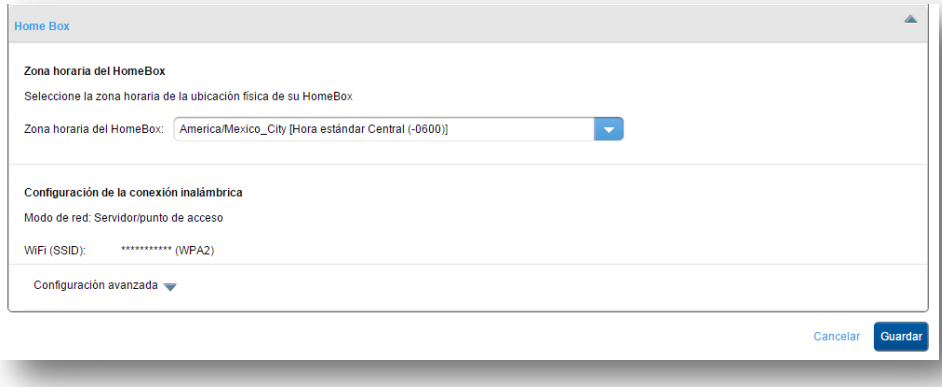
Puede verificar la dirección de IP asignada a una cámara IP haciendo clic en el enlace “más información”, debajo del nombre del dispositivo.



7.7. Zona horaria

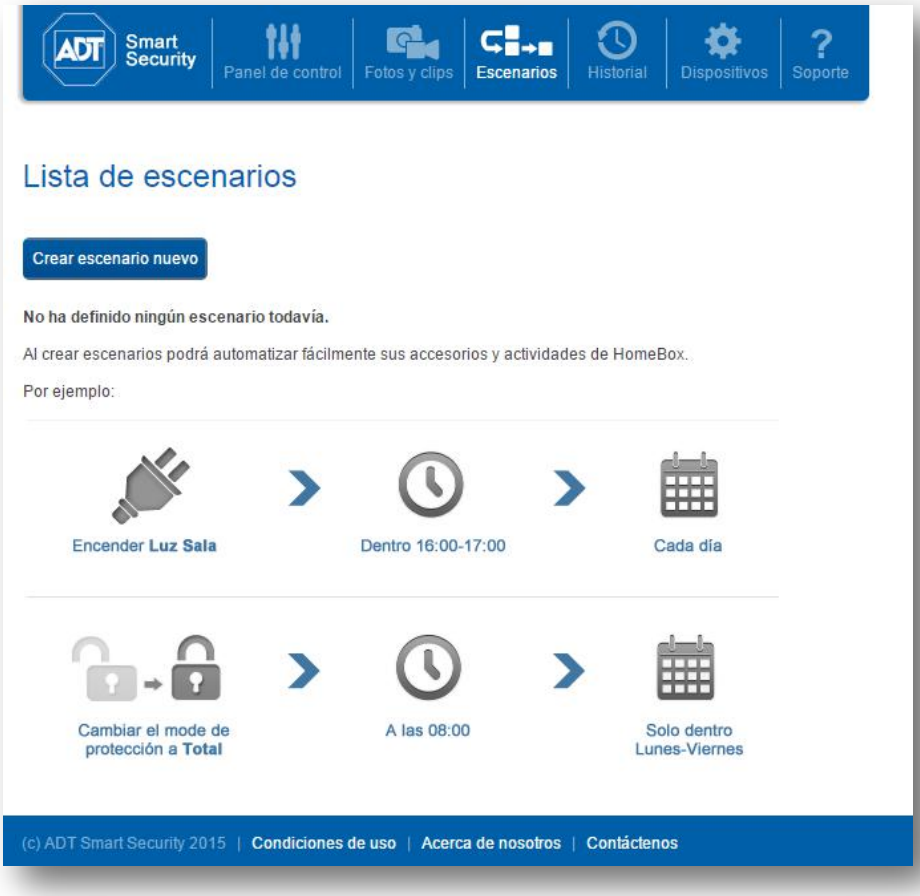
Se recomienda especialmente seleccionar la zona horaria apropiada para el gateway. De lo contrario, es posible que el sello de fecha y hora colocado para los eventos en el Registro histórico no sea preciso.

Para establecer la zona horaria del gateway, vaya a la página DISPOSITIVOS y a la sección HomeBox.



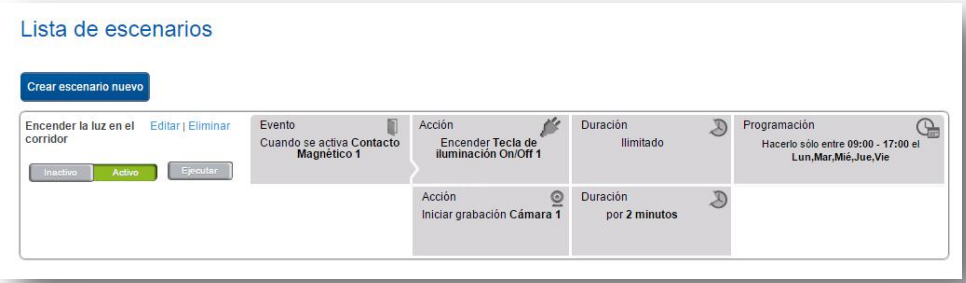
8. ESCENARIOS

Los escenarios permiten al usuario configurar acciones automáticas realizadas por el gateway a horas determinadas del día o si los sensores detectan eventos específicos. Esto proporciona la capacidad de personalizar el comportamiento del sistema ADT Smart Security para que cumpla con las necesidades exactas del usuario.
Los Escenarios pueden ser gestionados haciendo clic en el botón **Escenarios**.



La creación de un escenario nuevo es sencilla e intuitiva, y puede accederse desde la página **Escenarios** haciendo clic en el botón **Crear escenario nuevo**.

Es posible crear tantos escenarios como se desee. Es posible establecer cada escenario como activo o inactivo, haciendo clic en el botón de conmutación Inactivo/Activo junto al detalle de cada escenario. Si un escenario está “Inactivo” no se ejecutará, sin importar si el evento es recibido por el gateway.



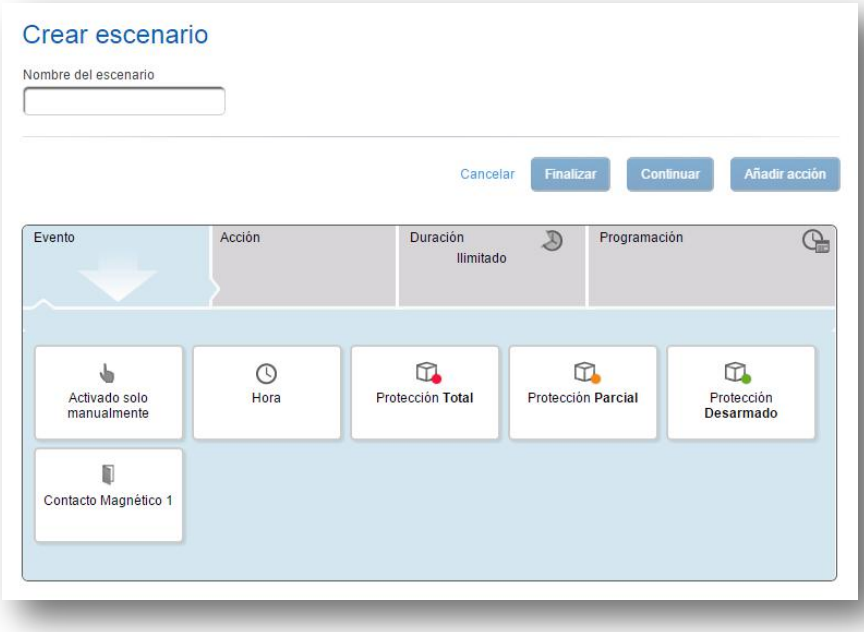
A manera de ejemplo, es posible crear un escenario que active un dispositivo durante 10 segundos si alguien abre el armario de medicamentos. Esto implica que hay un sensor de puerta instalado en la puerta del armario, para que el gateway pueda ser notificado cuando el armario es abierto.

Haciendo clic en el botón **Crear escenario nuevo** abre una página para construir un escenario. Esta página proporciona los siguientes parámetros para que el usuario defina las condiciones operativas del escenario:

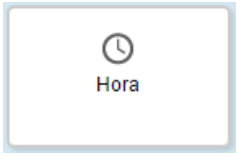
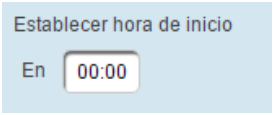
- Un nombre para el escenario: elija un nombre que recuerde a los usuarios fácilmente lo que realiza el escenario;
- Una causa para activar el escenario: puede ser un evento temporal (como todos los lunes a las 14:00; el 31 de enero a las 18:00, etc.) o una notificación activada por uno de los dispositivos emparejados (ya sea con el gateway o con el panel de alarmas);
- La acción que debe ejecutar el escenario al ser activado: esto puede ser enviar un comando a uno de los dispositivos emparejados (con el gateway) o enviar un mensaje de texto (email);
- Rangos de tiempo posibles durante los cuales se puede ejecutar el escenario; esto permite al usuario refinar la temporización del escenario.

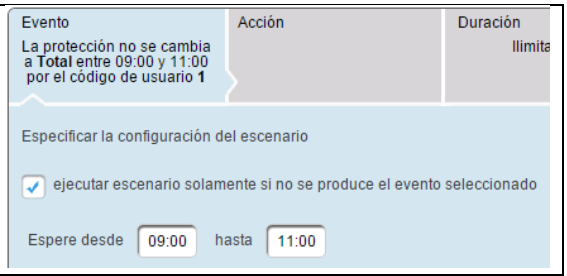
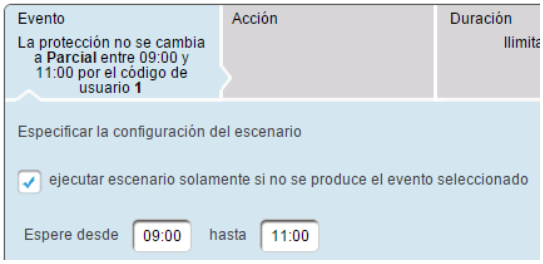
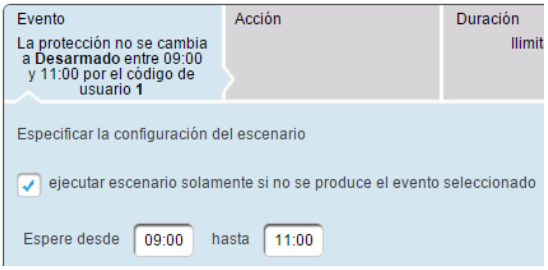
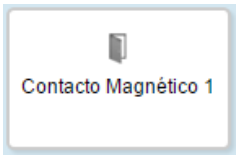
Por defecto, un escenario nuevo aparece con las secciones de los parámetros vacías. El usuario es responsable por rellenar cada sección, una después de la otra, para definir por completo las condiciones operativas del escenario.

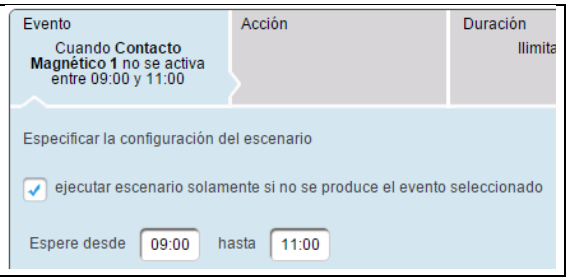
La primera sección de un escenario es la categoría Evento, que permite al usuario definir el evento que debe activar la ejecución del escenario. Debajo de la definición del escenario aparece automáticamente una lista de eventos posibles, permitiendo al usuario hacer clic en alguno para seleccionarlo como evento que debe activar el escenario.



Como se muestra arriba, la lista contiene algunos de los dispositivos disponibles para el gateway, es decir, dispositivos emparejados ya sea con el panel de alarmas o con el mismo gateway. Estos dispositivos son accesorios que pueden enviar eventos o notificaciones al gateway. Ítems adicionales incluyen eventos de tiempo y el status de armado/desarmado de protección del panel de alarmas.

Lista de ítems	Iconos	Parámetro adicional
Evento temporal		Horario (hora:minuto) en que ocurrirá el evento. Aparece un campo para capturar la hora: 
Protección Total		Seleccione si el evento a ser procesado debe o no estar basado sobre la falta de un evento específico que ocurre. Por ejemplo, es posible activar el escenario si la protección no se arma entre las 09:00 y las 11:00:

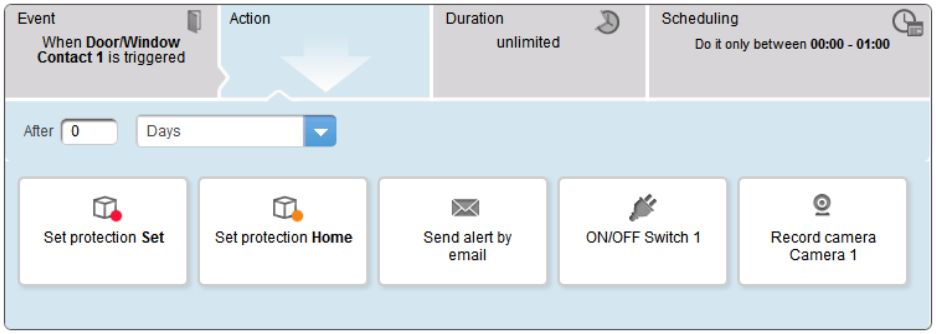
		
Protección Parcial		Seleccione si el evento a ser procesado debe o no estar basado sobre la falta de un evento específico que ocurre. Por ejemplo, es posible activar el escenario si la protección no se arma (modo personalizado) entre las 09:00 y las 11:00. 
Protección desarmada		Seleccione si el evento a ser procesado debe o no estar basado sobre la falta de un evento específico que ocurre. Por ejemplo, es posible activar el escenario si la protección no se desarma entre las 09:00 y las 11:00. 
Cualquier dispositivo que pueda enviar una notificación		Seleccione si el evento a ser procesado debe o no estar basado sobre la falta de un evento específico que debería ocurrir. Por ejemplo, es posible activar el escenario si un sensor de puerta no detecta la apertura/cierre de una puerta entre las 09:00 y las 11:00.

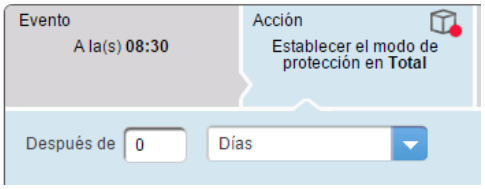
Es posible completar el campo “Nombre” en cualquier momento mientras se construye un escenario.

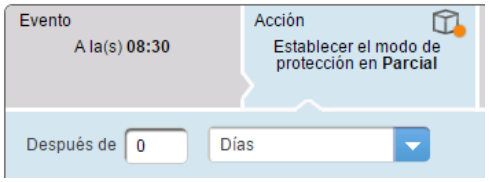
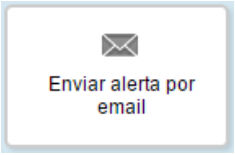
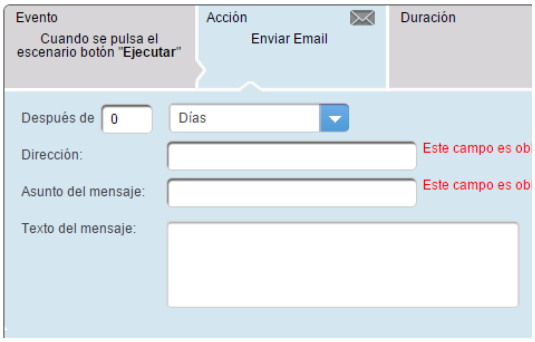
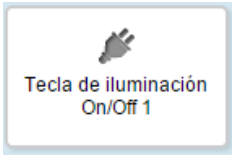
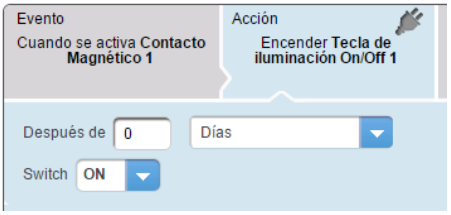
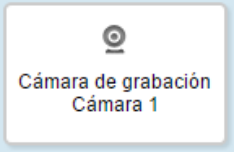
Una vez seleccionado el evento de activación, haga clic en el botón **Continuar**.

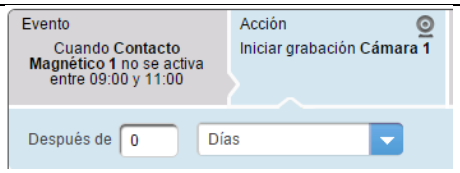
La sección siguiente es la categoría **Acción**. Esta sección permite al usuario definir la acción que se debe ejecutar cuando el escenario es activado. Aparece una lista de todas las acciones posibles como un conjunto de íconos sobre los que podrá hacer clic.



Las siguientes alternativas se encuentran disponibles en la categoría **Acción**:

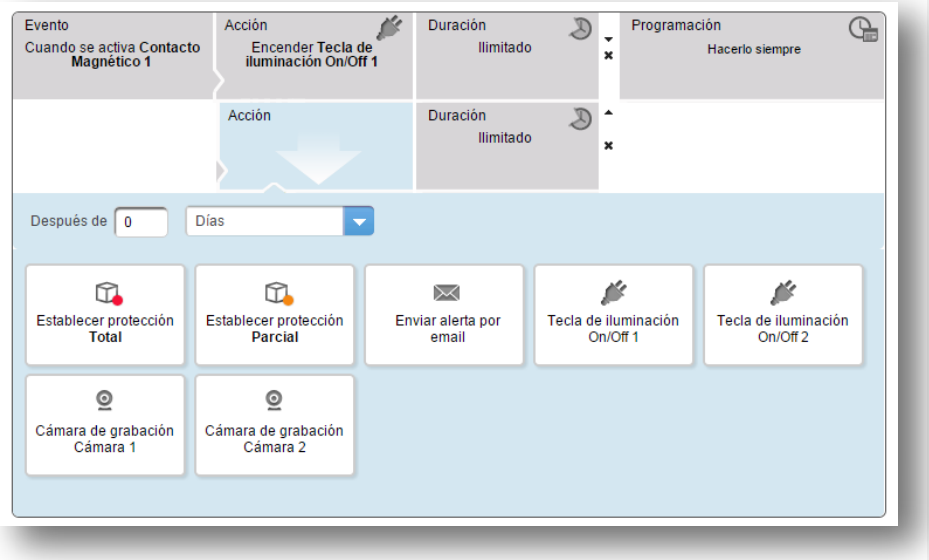
Ítems de la lista	Iconos	Explicación/Parámetros adicionales
Establecer protección TOTAL		Esta acción arma el sistema Smart Security en protección total. Es posible establecer un retardo entre el escenario que activa el evento y la acción de armar el sistema. 

Establecer protección PARCIAL		Esta acción arma el sistema Smart Security en protección parcial. Es posible establecer un retardo entre el escenario que activa el evento y la acción de armar el sistema. 
Enviar un email		La plataforma de Hogar Conectado envía un mensaje a una dirección de email determinada. Aparecen campos de texto para capturar la dirección del objetivo, un tema y el cuerpo de su email. 
Poner un enchufe ON/OFF		Es posible poner un enchufe ON/OFF en ON o en OFF. Es posible establecer un retardo entre el escenario que activa el evento y la acción ON/OFF. 
Grabar vídeo de una cámara de IP		La cámara de IP seleccionada comenzará una sesión de grabación de vídeo automática de 2 minutos de duración. Es posible establecer un retardo entre el escenario que activa el evento y la acción de grabación de vídeo.



Una vez seleccionada la acción, es posible hacer clic sobre el botón **Añadir Acción** si se requiere más de una acción de escenario, o hacer clic sobre el botón **Continuar** si no se requiere otra acción de escenario.

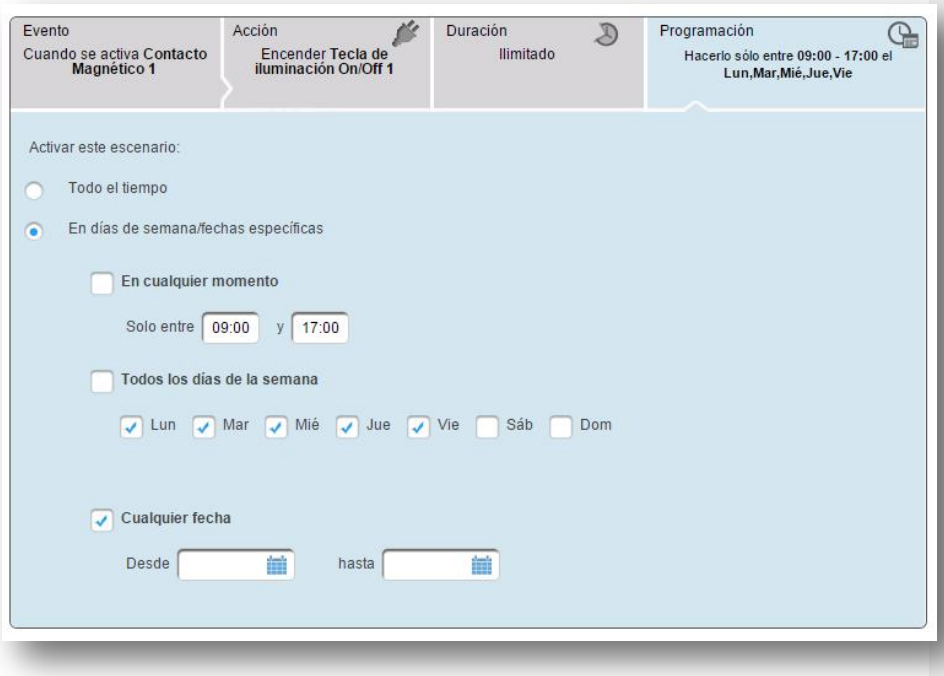
Si se hace clic sobre Añadir Acción, se agregará una línea en el marco de definición del escenario y deberá seguir el mismo proceso para definir sus parámetros de acción.



Después de hacer clic en **Continuar**, la sección siguiente es la categoría **Duración**. Consiste en especificar el tiempo durante el cual persiste la acción anterior. Note que algunas acciones (como armar o desarmar el modo de protección) no requieren establecer una duración. En este caso, no hay una duración para especificar, ya que la acción es discreta. Sin embargo, para acciones que tienen comandos inversos, como poner un enchufe de alimentación en ON u OFF, la duración especifica el tiempo de espera antes de ejecutar el comando inverso. Por ejemplo, si la acción consiste en enviar un comando ON a un enchufe de alimentación, entonces la duración es el tiempo de espera antes de que el gateway envíe un comando OFF (opuesto) al mismo enchufe.

Después de definir la duración, hacer clic en el botón **Continuar** para acceder a la última sección del Asistente de definición de escenarios. La sección contiene la definición de la **Programación** y le permite especificar cuando el escenario puede ser ejecutado. Esta sección proporciona una

lista de opciones que le permiten al usuario definir las fechas y horas durante los cuales el escenario está activo.



Como se muestra arriba, podrá seleccionar:

- Todo el tiempo: es posible ejecutar el escenario en cualquier momento
- En horarios y fechas específicos: podrá especificar un rango de tiempo (por ejemplo, entre las 09:00 y las 10:00); también podrá especificar que el escenario se ejecute solamente en determinados días de la semana, o entre dos fechas.

Después de completar todas las secciones de definición de escenarios, haga clic en el botón **Terminar** para guardar el escenario en el sistema y cargarlo al gateway. Por defecto, el escenario es activado. Es posible agregar escenarios adicionales sin restricciones, y siempre es posible modificar un escenario más adelante. También es posible eliminar un escenario cuando ya no se lo necesita. Note que si se elimina un accesorio del sistema también se eliminan los escenarios asociados con ese dispositivo, dado que la definición del escenario ya no sería válida.

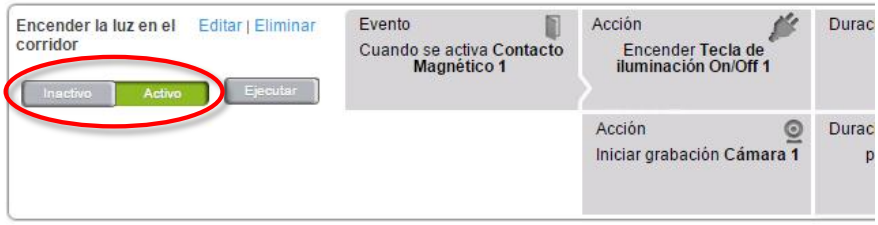
Es posible ejecutar las acciones de un escenario sin esperar que ocurra el evento que lo active. Cuando se despliega la lista de escenarios, cada escenario tiene un botón Ejecutar, como se muestra a continuación:

Si se hace clic en este botón se activa la ejecución de una acción (o acciones) que fueron definidas para ese escenario.

En caso que no se ejecute algún escenario durante algún tiempo, hay dos opciones:

- Eliminar el escenario haciendo clic en su enlace “Eliminar”: Pero deberá ser recreado si alguna vez se vuelve a necesitar.

- Desactivar el escenario: Haga clic en su botón “Inactivo” y el escenario no será ejecutado cuando ocurra el evento de activación... Es posible rehabilitar el escenario en cualquier momento, haciendo clic en el botón “Activo”.



9. MODO DE INSTALADOR

9.1. ¿Qué es el modo de instalador?

Los instaladores ADT tienen un sitio Web dedicado al que pueden ingresar con sus propias credenciales (login y contraseña). El sitio Web les permite tomar control de un gateway de usuario específico, pero con limitaciones estrictas:

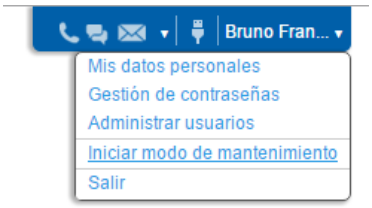
- El usuario siempre tiene conocimiento de cuando es posible que un instalador podrá tener acceso a su gateway y cuando un instalador no lo puede acceder.
- Un instalador ADT no puede tener acceso a un gateway si un usuario no se lo permite.
- Un usuario no comparte la contraseña de su cuenta con un instalador ADT.

Estas limitaciones son la razón por la cual existe el Modo de Instalador. Siempre que un usuario active el Modo de Instalador, un instalador puede tener acceso al gateway y gestionarlo, pero sin usar las credenciales de la cuenta en línea del usuario. En cuanto el usuario salga del Modo de Instalador, los instaladores ADT dejarán de tener acceso a su gateway.

9.2. Activación del Modo de Instalador

Es necesario que el usuario haga login en su cuenta para activar el Modo de Instalador. Nota: ésto está disponible solamente para la interfaz gráfica de autoservicio de la Web. Esta característica no está disponible en las aplicaciones móviles.

Después de hacer login, vaya a la barra de botones de usuario (arriba a la derecha) y haga clic en el nombre del usuario. Esto despliega un menú. Seleccione el ítem **Iniciar modo de mantenimiento**.



A partir de este momento, la interfaz gráfica aparecerá en gris para el usuario y los instaladores ADT podrán acceder al gateway. Esto evita que el usuario interfiera con algunas de las tareas que está efectuando el instalador.

Existe un pequeño riesgo de que el usuario olvide que el Modo de Instalador está activo, ya que hay muy pocas cosas que pueden hacer cuando su cuenta está en el Modo de mantenimiento. Más aún, la barra de botones de usuario es modificada y muestra un botón rojo “Finalizar modo” para salir del Modo de mantenimiento.

9.3. Salir del Modo de Instalador

Dos categorías de usuarios pueden salir del Modo de Instalador de un gateway:

- El usuario principal de la cuenta
- Un instalador ADT, después de haber completado la instalación del gateway.

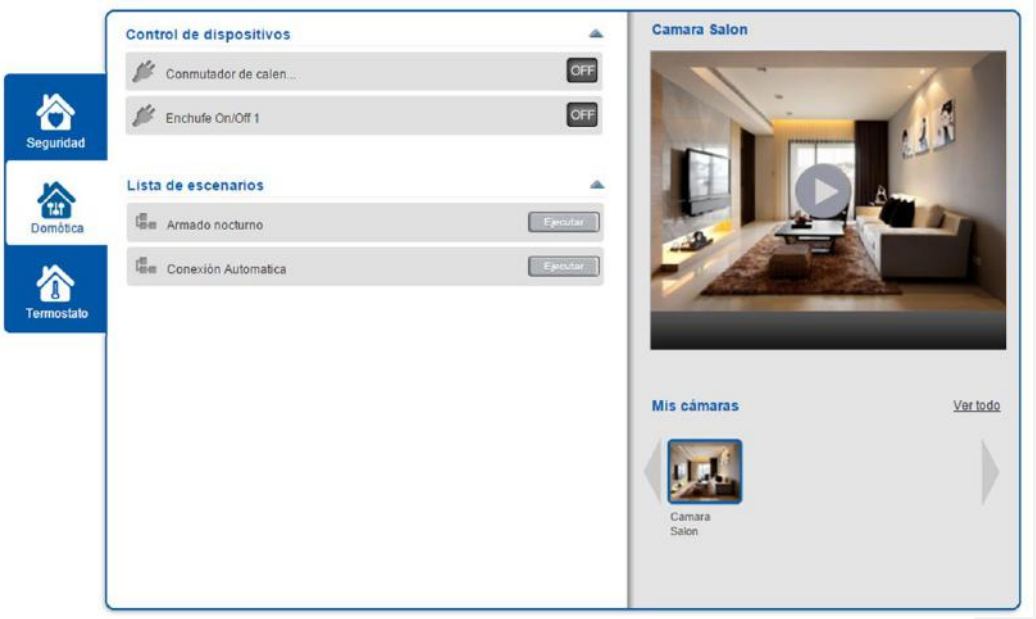
Cuando el Modo de Instalador está activo, aparece un botón Finalizar Modo en la parte superior izquierda de la página Web de autoservicio. Un botón similar aparece en la aplicación móvil. Si se hace clic en este botón se desactiva el Modo de Instalador, evitando que los instaladores sigan teniendo acceso a la cuenta.

10. GESTIÓN DE VÍDEO

El sistema ADT Smart Security permite a los usuarios cuidar sus hogares. Si un usuario está en casa y desea verificar si su bebé está durmiendo en otra habitación, o si están afuera de la casa y desea ver lo que está sucediendo después de recibir una alerta (SMS, email), siempre se podrá conectar a sus sistema a través del portal de autoservicio de la Web o del smartphone, y verificar el status de los eventos.

El sistema puede grabar vídeos automáticamente en caso de alerta o a pedido del usuario.

10.1. Primer vistazo al vídeo

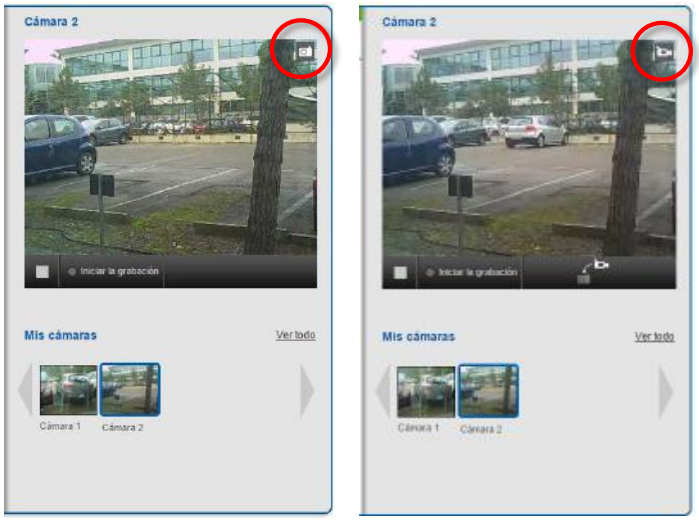


Para acceder a las cámaras, explore la pantalla panel de control. Todas las cámaras emparejadas están disponibles en el panel derecho de la vista.

Si hay múltiples cámaras, es posible ver una cámara específica haciendo clic en una de las imágenes en la parte inferior (debajo del área de visualización de las cámaras). Estas imágenes son instantáneas tomadas por cada cámara. Una vez seleccionada la cámara, haga clic en el botón de reproducir para iniciar la visualización del vídeo.

10.2. Transmisión de vídeo en vivo

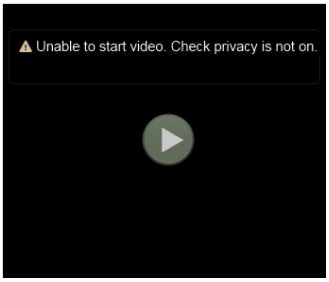
Para ver el vídeo en tiempo real de una cámara en particular emparejada con el gateway, haga clic en la cámara para ver la transmisión en la zona **Mis cámaras**. Cuando mira un vídeo, el usuario no está directamente conectado a su cámara, sino a un servidor de vídeo en la nube. Todas las transmisiones de vídeo son recolectadas por el gateway, cifradas, y transmitidas en forma segura a la plataforma de la nube del ADT Smart Security. Esto asegura máxima seguridad y protección de datos privados. Es posible que haya una leve demora antes de que comience el vídeo (5 a 20 segundos), pero esto es necesario para asegurar la correcta protección de los datos. Para minimizar el período de espera para que comience el vídeo, el sistema comienza con una transmisión de vídeo de imagen por imagen (es decir, imágenes mostradas y en paralelo, renovadas cada segundo). El vídeo en tiempo real comienza a poner la memoria intermedia búfer en segundo plano durante este proceso, y una vez que esté lista la transmisión de vídeo en tiempo real (el búfer llegó al 100%), el modo de imagen por imagen pasa automáticamente al modo de vídeo en tiempo real.



Mientras se ve un vídeo, es posible:

- Mostrar el vídeo en pantalla completa
- Comenzar a grabar lo que se muestra

Para respetar la protección de la privacidad, algunos modelos de cámaras tienen un botón de privacidad física. Esto activa un modo de privacidad local, y ya no es posible recolectar imágenes o vídeo de la cámara. Estando en este modo, el área de stream de vídeo en el portal de autoservicio proporciona una advertencia (ver a continuación).

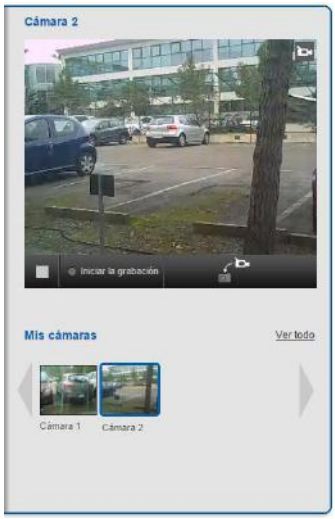


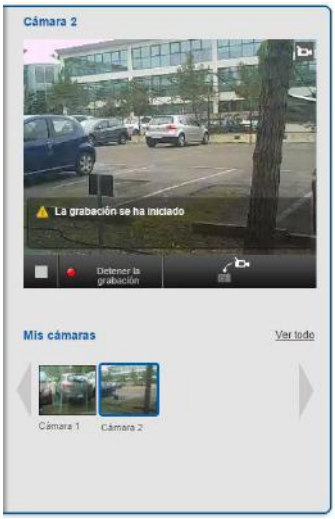
La única manera de volver a acceder al vídeo y a las imágenes de la cámara es pulsando nuevamente el botón de privacidad e inhabilitando el modo de privacidad local. No es posible inhabilitar el modo de privacidad local desde el portal Web. Esto asegura de que si alguien en casa no desea que se vea la transmisión de la cámara, entonces nadie podrá sobrepasar el establecimiento de la privacidad local.

La imagen a continuación muestra la parte posterior de la cámara ADT RC8221. El botón Privacidad se encuentra en el lado izquierdo.

10.3. Grabación de vídeo

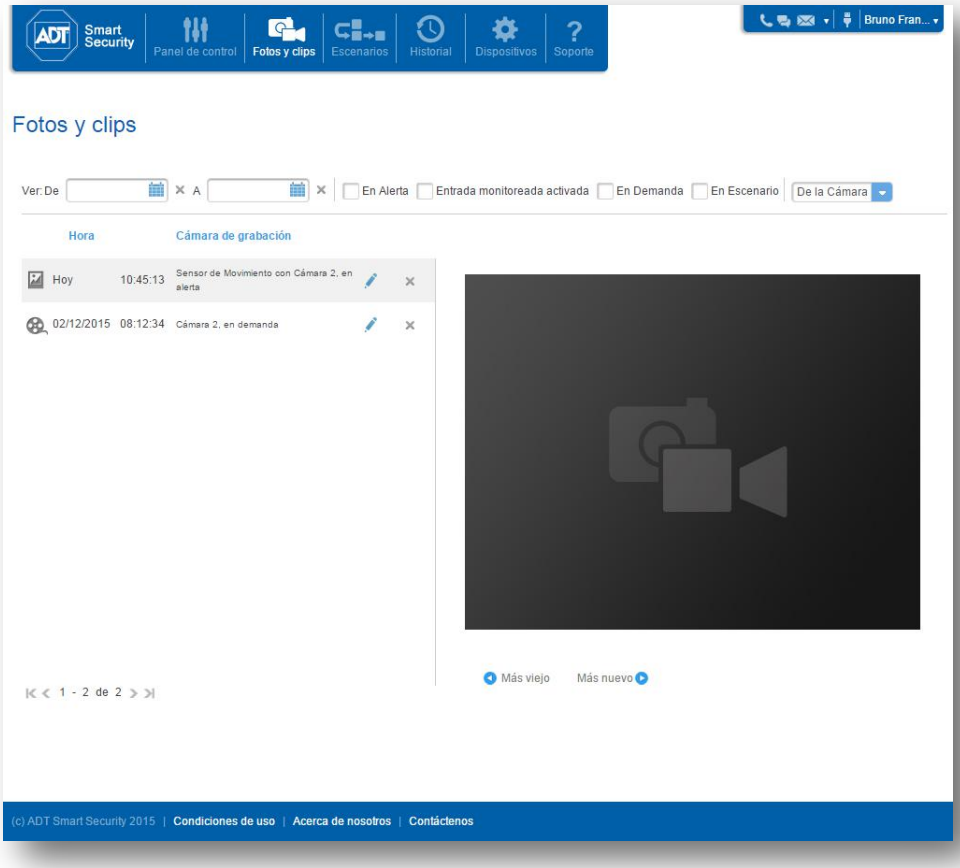
Cuando se mira un stream de vídeo en el portal Web o aplicación móvil, el usuario puede decidir, en cualquier momento, comenzar a grabar lo que se muestra. Para iniciar la grabación de un vídeo, haga clic en el botón **Iniciar grabación**. Aparecerá una indicación de que comenzó la grabación de vídeo, como se muestra a continuación. Todo el vídeo es grabado en la nube segura de ADT Smart Security.





Para detener la grabación, pulse el botón **Detener grabación** (que aparece solamente cuando una grabación está en progreso). Además, también es posible grabar vídeos automáticamente ante alarmas.

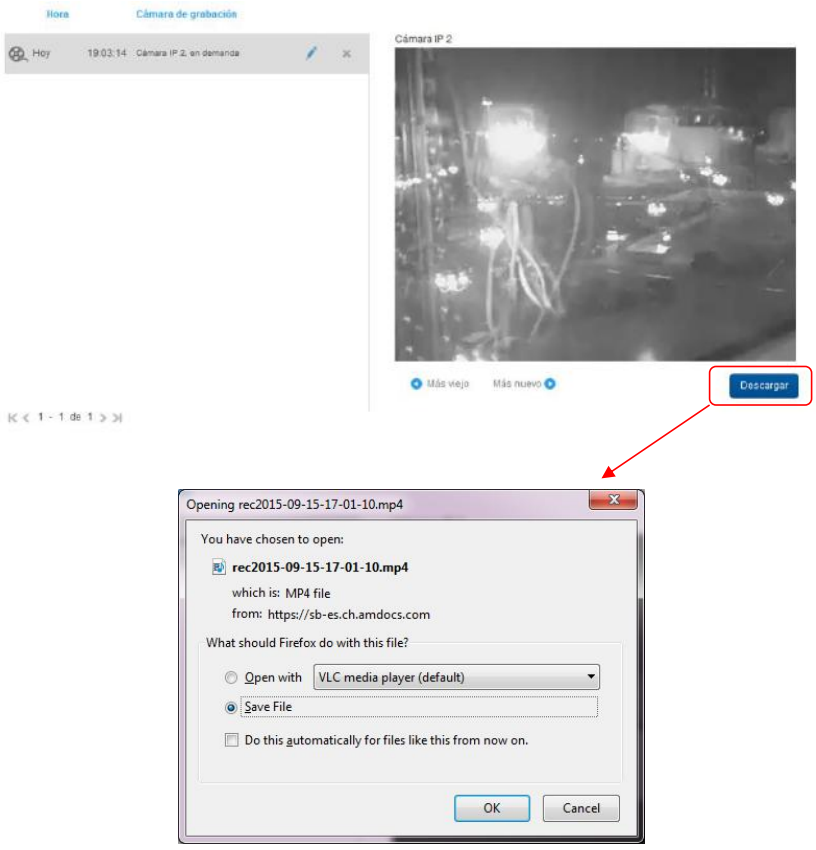
Para acceder a vídeos grabados, haga clic en el botón **Fotos y Clips** en la barra de funciones entre dominios:



Es posible reproducir un vídeo grabado en cualquier momento, haciendo clic en la imagen de vídeo en la lista de vídeos grabados. Es posible pausarlo o reproducirlo en pantalla completa, como se desee.

Para descargar uno de los vídeos grabados a un ordenador local, haga clic en el botón **Descargar** (ángulo derecho inferior) en la ventana de visualización del vídeo.

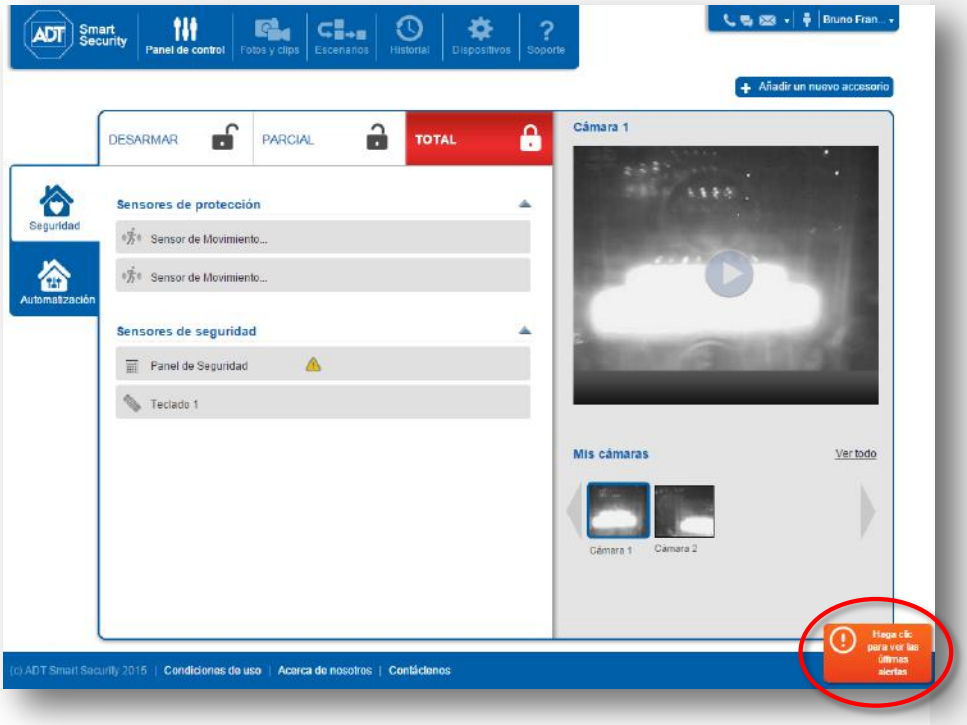
Aparecerá una ventana emergente que pregunta si es necesario guardar el vídeo (en formato mp4). Note que, dependiendo de la configuración del producto de exploración de Web utilizado, es posible descargar el archivo del vídeo en forma automática, guardándolo en un directorio de Descarga.


Hora
Cámara de grabación
Hoy
19:03:14
Cámara IP 2, on demanda
Cámara IP 2
Más viejo
Más nuevo
Descargar
1 - 1 de 1
Opening rec2015-09-15-17-01-10.mp4
You have chosen to open:
rec2015-09-15-17-01-10.mp4
which is: MP4 file
from: https://sb-es.ch.amdocs.com
What should Firefox do with this file?
Open with
VLC media player (default)
Save File
Do this automatically for files like this from now on.
OK
Cancel

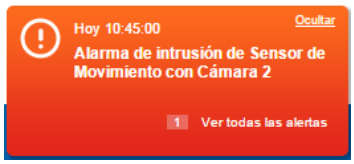
11. ACCESO A REGISTROS HISTÓRICOS

El servicio de ADT Smart Security registra todas las actividades que suceden en un gateway o alguno de sus accesorios. El sistema proporciona dos maneras para acceder y revisar estos registros.

La primera opción es observar el indicador de alertas del registro. Este indicador aparece en el ángulo inferior derecho del tablero, como se representa a continuación:



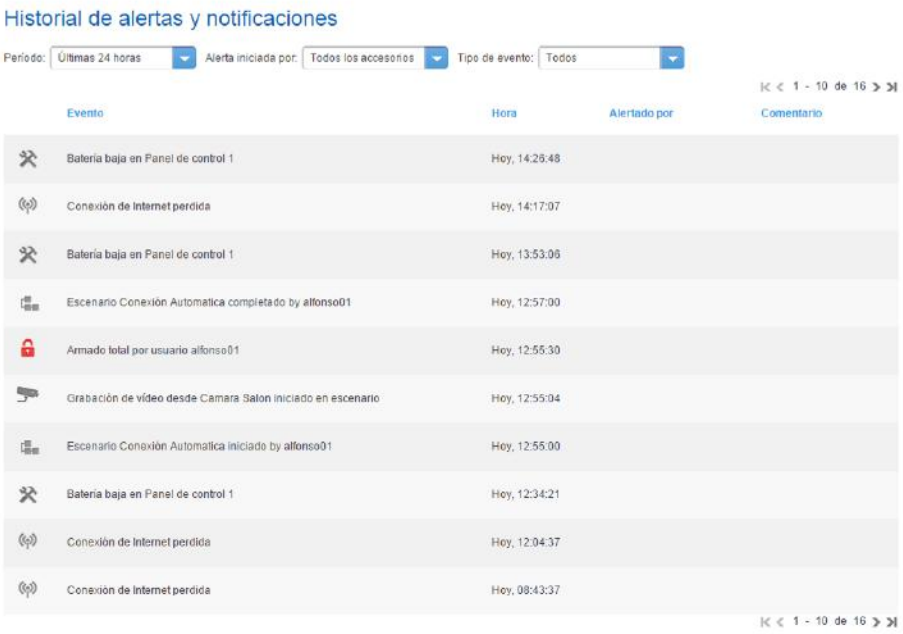
Al hacer clic en el indicador, el mismo se expande a una casilla de alerta de registro más grande, como se muestra a continuación:



Esta casilla muestra la(s) última(s) alertas grabadas por el gateway. El hipervínculo **Ver todas las alertas** proporciona acceso a la página histórica que muestra la lista completa de registros. Esta es la misma página a la que se puede acceder haciendo clic en la opción del menú **Historial**.

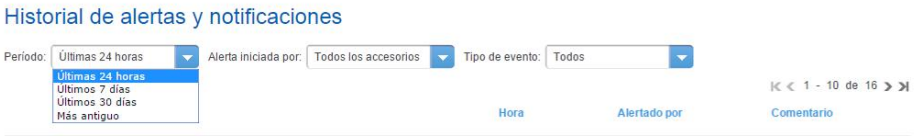
La segunda manera de acceder a los registros históricos es directamente a través del botón del menú **Historial**.

La página **Historial** muestra los registros clasificados por horario, con los eventos más recientes en la parte superior.



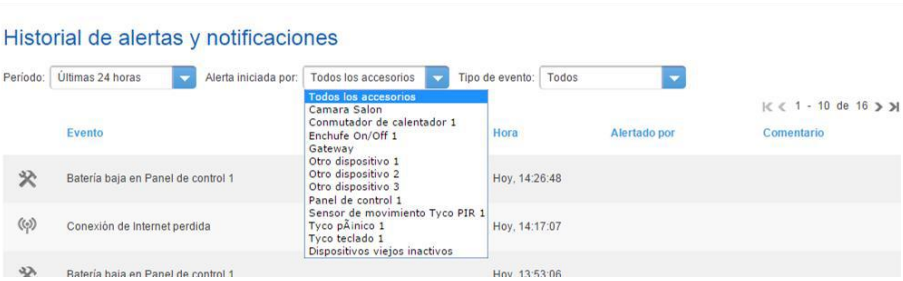
Es posible filtrar los eventos por período de tiempo, accesorio, partición o tipo de evento, como se indica a continuación:

Filtrado de eventos por períodos de tiempo:



Es posible mostrar los eventos que ocurrieron durante las últimas 24 horas, o los últimos 7 días o los últimos 30 días. Si selecciona Previos se muestran todos los eventos.

Filtrado de eventos por accesorios:



Es posible ver todos los eventos asociados a un sensor dado, independientemente de si este sensor está emparejado con el panel de alarmas o con el gateway. También es posible encontrar eventos de un dispositivo emparejado con el panel de alarmas en los registros históricos del mismo panel de alarmas.

Filtrado de eventos por particiones:

Esta funcionalidad existe solo por los paneles de alarmas que están configurados con particiones. Es posible mostrar solamente los eventos generados por los sensores que están registrados con una partición dada en el panel de alarmas o con todas las particiones.

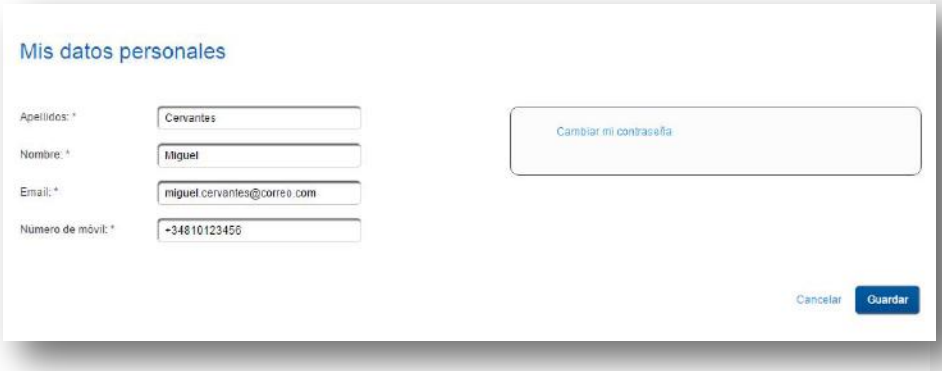
Filtrado de eventos por tipo de evento:

Hay muchos tipos de eventos, y no necesariamente todos los eventos están relacionados con una intrusión. Un evento puede corresponder al armado o desarmado de una partición, inicio de una sesión de vídeo, pasar al Modo de Instalador, etc.

12. ACCESO A LA INFORMACIÓN DE LA CUENTA

El usuario puede acceder a los datos de la cuenta personal mediante el menú emergente en la esquina superior derecha de la página Web del portal de autoservicio:

12.1. Mis datos personales



Esta página permite al usuario verificar y modificar la información personal.

12.2. Gestión de seguridad

Este menú brinda acceso a dos páginas relacionadas a la gestión de la contraseña del usuario principal:

- Modificar la contraseña del usuario principal
- Modificar las preguntas y respuestas de seguridad personal

12.2.1. Cambiar mi contraseña

El enlace de Cambiar mi contraseña brinda acceso a la página donde puede modificarse la cuenta en línea de ADT Smart Security.

Dado que la contraseña que es ingresada está enmascarada, el usuario debe ingresarla dos veces para asegurarse de que no se haya cometido un error. La contraseña debe ser ingresada manualmente, sin posibilidad de copiar y pegar el valor enmascarado.

También debe ser suministrada la contraseña anterior, para asegurarse de que la persona que efectúa el cambio de contraseña es un usuario legítimo.

Si un usuario olvida su contraseña, puede activar un procedimiento automático que le permitirá ingresar una contraseña nueva, sin saber cuál era la contraseña previa. Sin embargo, el sistema debe asegurarse de que solamente el titular real de la cuenta esté autorizado para hacerlo. Esta es la base de las preguntas de seguridad requeridas. Los titulares de las cuentas principales deben asegurarse de que sus preguntas de seguridad sean definidas apropiadamente para su fácil recuperación, y también para que las respuestas puedan ser proporcionadas solamente por ellos mismos.

12.2.2. Preguntas de seguridad

Haga clic en el enlace de Preguntas de Seguridad en la página Cambiar Contraseña.

Aparece un formulario con cuatro líneas, donde cada línea muestra una pregunta de seguridad y la respuesta personal del usuario.

Si no está completado, es necesario seleccionar cuatro preguntas y proveer cuatro respuestas.

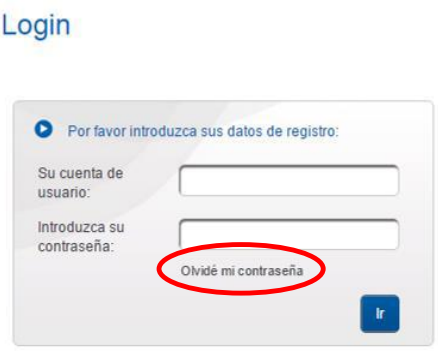
Cada línea comienza con una lista desplegable de preguntas. Seleccione una de las preguntas para la cual su respuesta es bien conocida por el usuario final. Luego ingrese la respuesta en el campo de edición a la izquierda. Repita el procedimiento para las cuatro líneas. El sistema asegura que ninguna pregunta pueda ser seleccionada más de una vez.

Las respuestas no son mostradas. De modo que es importante asegurarse de que no se cometan errores de escritura al ingresar las respuestas.

Las respuestas son almacenadas por el sistema en formato no legible, de modo que nadie podrá decirle a un usuario cuáles son ninguna de las respuestas.

12.3. Contraseña olvidada: cómo recuperarla

En caso de olvidar la contraseña de una cuenta, el usuario puede hacer clic en el enlace *Olvidé mi contraseña* en la página de login:



Aparece una primera página, la que comprueba cuál cuenta necesita el usuario para reinicializar la contraseña.

Esta página no se limita a simplemente preguntar cuál es el nombre de la cuenta. También pregunta los detalles que pueden ser encontrados en la página Mis Detalles Personales:

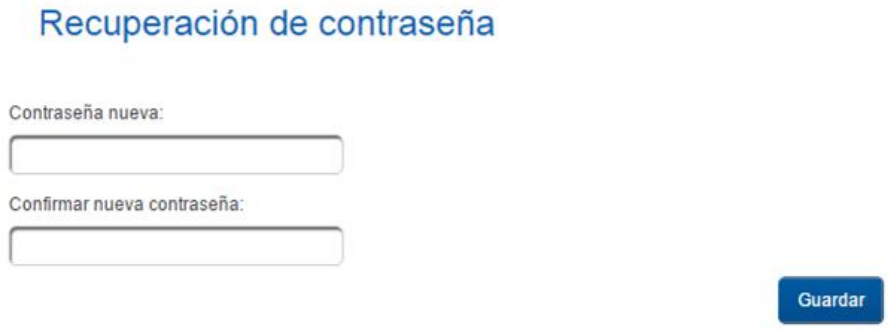
dirección de email tal como fue guardada por el usuario, nombres de pila y apellidos. Y por supuesto el sistema pregunta el nombre de la cuenta (nombre del usuario).

Esta página también requiere el ingreso de una serie de dígitos y/o letras que aparecen en una imagen. Esto es para asegurar que la solicitud de contraseña no sea accedida por un ordenador que esté ejecutando un programa de robo de contraseñas.

Una vez completados todos los campos, haga clic en el botón Recuperar contraseña.

La siguiente página presenta dos preguntas, seleccionadas aleatoriamente de entre las cuatro preguntas de seguridad. El usuario debe suministrar respuestas a ambas preguntas, que deben coincidir exactamente con las respuestas dadas previamente.

Si ambas respuestas son correctas, entonces se le permite al usuario forzar una nueva contraseña en la siguiente pantalla.



El usuario ingresará la nueva contraseña. Por razones de seguridad, los caracteres ingresados están enmascarados. Para asegurar que la contraseña sea ingresada sin errores, esta contraseña debe ser ingresada dos veces.

Si ambas contraseñas son idénticas, entonces la contraseña vieja es borrada y es reemplazada por la contraseña nueva.

12.4. Gestión de usuarios

12.4.1. Reseña

En el caso de varios miembros de la familia que usen las funcionalidades del servicio de ADT Smart Security, es posible definir múltiples logins y contraseñas para acceder a la misma cuenta. Cada conjunto de login/contraseña de usuario puede ser considerado como una subcuenta de la cuenta principal. En el resto de este documento, denominamos “usuario principal” al usuario de la cuenta principal, y “sub-usuario” al usuario de la subcuenta.

El propósito de esta funcionalidad consiste en brindar acceso al servicio a los miembros de la familia, pero sin compartir las mismas credenciales (login y contraseña) del usuario principal: Además, el usuario principal puede personalizar el conjunto de funcionalidades propuestas para cada subcuenta en la interfaz de usuario. Por ejemplo, un usuario puede crear una subcuenta para sus hijos, de modo que ellos puedan jugar con la iluminación pero no con armar/desarmar el sistema de seguridad. El conjunto de funcionalidades que la interfaz de usuario expone a cada sub-usuario se llama "permisos de usuario".

Siempre es posible cancelar cualquiera de las subcuentas si un usuario principal decide que un sub-usuario no debe tener más acceso al sistema.

Si nunca fue creada una subcuenta, la página **Gestión de Usuarios** muestra una lista de usuarios que contiene una sola entrada: la cuenta del usuario principal. Dado que ésta es la cuenta principal, no puede ser borrada o restringida (sus detalles aparecen en color gris) ya que todos los permisos de usuario han sido otorgados. Algunos de los detalles (nombre de pila y apellido, dirección de email, contraseña) pueden ser modificados, pero solamente mediante las páginas Web de gestión de cuenta dedicadas, como se describe previamente en este documento. La única parte de la información que puede ser actualizada con respecto al usuario principal es el "código de usuario" del panel de alarmas, el que será asociado al usuario principal. Los códigos de usuario son valores de índice (1, 2,… hasta un valor máximo que depende del modelo del panel de alarmas) que identifican el código PIN del panel de alarmas que usa el gateway al enviar comandos al panel de alarmas en nombre del usuario principal (por ejemplo, comandos de armar y desarmar). La asociación entre un índice de código de usuario y un código PIN de 4 dígitos es configurada directamente en el panel de alarmas. En el portal Web, el usuario principal seleccionará solamente cuál índice de código utilizará para sus propios comandos del panel de alarmas.

Al gestionar directamente el panel de alarmas mediante su interfaz de usuario dedicada (teclado y pantalla), un usuario debe ingresar un código PIN para realizar acciones sensitivas, tales como armar o desarmar una partición.. Es posible definir varios usuarios con sus propios códigos PIN dedicados. De esta manera, el panel de alarmas puede saber quién está realizando una acción basada en el código PIN ingresado y verificar que el usuario correspondiente disponga del nivel de permiso apropiado.

Cuando un usuario ejecuta una acción vía el portal Web o la aplicación móvil, el panel de alarmas debe verificar que este usuario esté autorizado a realizar dicha acción. El gateway añade el código PIN del usuario en el comando que envía al panel de alarmas. Por lo tanto, se efectúan dos verificaciones simultáneamente: el gateway verifica que un usuario esté autorizado a realizar una acción, y el panel de alarmas hace lo mismo. Por lo tanto, debe ponerse mucho cuidado al establecer los permisos de los códigos PIN durante la configuración del panel de alarmas, para que dichos permisos correspondan a los dados a una subcuenta.

Nota: en caso de usuarios múltiples en la misma cuenta, no hay obligación de definir un índice de código de usuario diferente para cada usuario. Varios usuarios de la aplicación pueden compartir el mismo código de usuario del panel de alarmas.

El índice del código de usuario del usuario principal debe ser ingresado en el campo **Código de usuario** (ver más abajo).

12.4.2. Subcuentas

Puede añadirse un nuevo usuario haciendo clic en el botón **Añadir nuevo usuario**… También es posible crear una cuenta nueva con los mismos permisos que una existente, haciendo clic en el botón **Duplicar usuario…**

Para crear un sub-usuario nuevo, es necesario ingresar los siguientes detalles de la cuenta:

Detalle del usuario	Tipo	Explicación
Código de usuario	Valor de índice, desde 1 hasta el valor máximo que depende del modelo del panel de alarmas.	Lista de los valores del código de usuario del panel de alarmas de seguridad que han sido previamente creados en el panel de alarmas y configurados con un código PIN.. Este código de usuario es requerido solamente si el derecho de permiso “Seguridad” está marcado.
Nombre de usuario	Nombre de login para el sub-usuario	Nombre de login utilizado por el sub-usuario para acceder a la interfaz de usuario de ADT Smart Security.
Nombre de pila	Cadena de texto libre	Nombre de pila del sub-usuario; esto es básicamente para recordar quién es dicho sub-usuario, en caso de que sean creadas subcuentas diferentes para personas diferentes con el mismo apellido.
Apellido	Cadena de texto libre	Apellido del sub-usuario; al igual que con el nombre de pila, el propósito es ayudar al usuario principal a recordar quién es dicho sub-usuario.
Contraseña de usuario	Contraseña de sub-usuario	Contraseña que el sub-usuario debe ingresar para acceder a la interfaz de ADT Smart Security. Al igual que con cualquier otra contraseña de ADT Smart Security, esta contraseña debe seguir ciertas reglas para hacerla lo suficientemente segura: no puede ser idéntica al nombre de login, y debe contener al menos una letra mayúscula y también una letra minúscula y un dígito.
Confirmar contraseña	Ingrese de nuevo la contraseña de sub-usuario	Dado que la contraseña está enmascarada, es necesario ingresarla dos veces.
Email	Dirección de email del sub-usuario	Dirección de email del sub-usuario

Junto con los detalles de la cuenta, es necesario definir los permisos que son otorgados al sub-usuario haciendo clic en las casillas de verificación correspondientes:

Permisos de usuario	Explicación
Seguridad	Otorga al sub-usuario acceso a la pestaña Seguridad de la cuenta y a sus modos de armado/desarmado
Domótica	Otorga al sub-usuario acceso a la pestaña de dispositivos de la cuenta, a ver el status de los dispositivos en tiempo real, y a encender y apagar las luces
Vídeo	Permite al sub-usuario la opción de ver en vivo la transmisión de la(s) cámara(s), grabar el stream de video o reproducir los videos grabados.
Operar escenario	Permite al sub-usuario habilitar e inhabilitar escenarios, así como también ver y ejecutar escenarios existentes.
Modificar escenario	Permite al sub-usuario crear, modificar y eliminar escenarios

Permisos de usuario	Explicación
Operar dispositivo	Permite al sub-usuario enviar comandos (mediante clics en los botones) a un dispositivo; por ejemplo, encender y apagar un enchufe de alimentación.
Modificar dispositivo	Permite al sub-usuario emparejar y desemparejar cámaras y dispositivos con el gateway, renombrar los dispositivos o modificar sus ajustes de configuración (de haberlos).
Notificación	

13. OBTENCIÓN DE SOPORTE – LOCALIZACIÓN DE FALLAS

En caso de preguntas o problemas con el sistema, es posible obtener asistencia haciendo clic en el botón **Soporte**.

La página **Soporte** brinda acceso a esta Guía del Usuario, e indica cómo contactar el soporte de línea directa.