Qué es Hellgrün Connect?

Hellgrün Connect es una plataforma web de vanguardia diseñada para simplificar y agilizar la gestión y monitorización de alarmas de manera segura y eficiente. Esta herramienta potente permite a los usuarios de la empresa supervisar y controlar los parámetros y el estado de las alarmas de forma remota y en tiempo real, facilitando una respuesta ágil tanto para la atención al cliente como para el personal técnico.

Su diseño intuitivo y sencillo convierte a Hellgrün Connect en una herramienta fácil de usar y comprender. Esta plataforma no solo sirve como una valiosa asistencia técnica de primera línea, sino que también puede ser empleada por el personal técnico y los operadores de monitoreo para ofrecer respuestas inmediatas y efectivas ante situaciones de emergencia. Al minimizar la necesidad de enviar personal técnico para atenciones simples, Hellgrün Connect optimiza la eficiencia operativa y mejora significativamente la experiencia del cliente.

Con Hellgrün Connect, la gestión de alarmas se transforma en un proceso fluido y seguro, brindando a las empresas una solución integral para el monitoreo remoto y la atención proactiva a las necesidades de sus clientes.

Portal de Acceso

Acceder a Hellgrün Connect es un proceso simple que requiere seguir ciertos pasos para garantizar una experiencia sin contratiempos. Antes que nada, es necesario contar con una Cuenta de Empresa habilitada, a la que denominaremos "Instancia", la cual se puede obtener a través de su agente de cuenta, distribuidor o canal de venta, desde donde adquirió el producto.

Pasos para Obtener su Cuenta Empresarial:

Contacte a su Agente de Cuenta, Distribuidor o Canal de Venta: Inicie el proceso comunicándose con el profesional o entidad a través de la cual adquirió los servicios de Hellgrün Connect. Solicite la creación de su cuenta empresarial, proporcionando la información necesaria.

Generación de la Cuenta: Una vez realizada la solicitud, se procederá a la generación de su Instancia. Este proceso puede variar en tiempo dependiendo de las políticas y procedimientos de su proveedor.

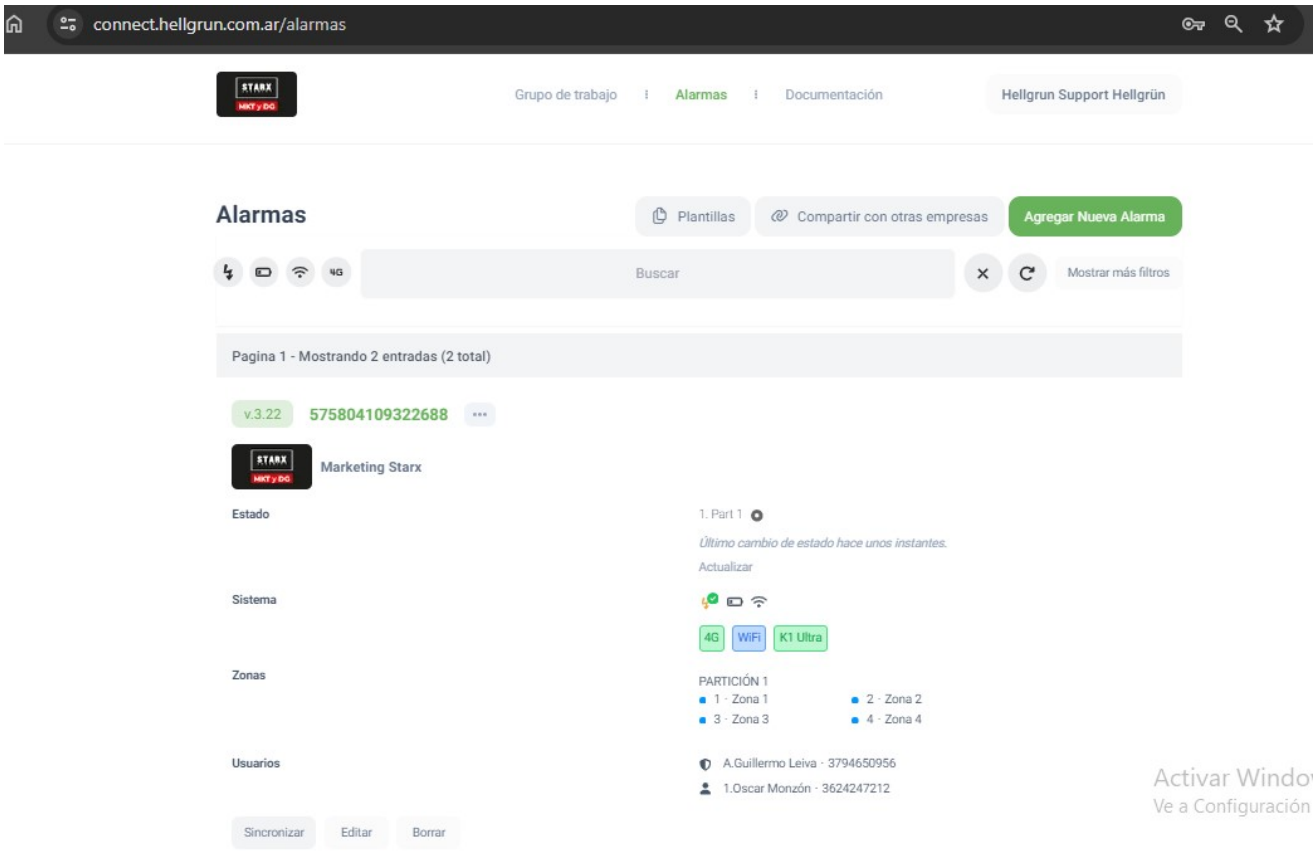
Recepción del Link de Registro: Una vez creada la cuenta, recibirá un correo electrónico en la dirección proporcionada durante el proceso de solicitud. Este correo contendrá un enlace que le permitirá completar su registro en Hellgrün Connect.

Acceso a Hellgrün Connect:

Ingrese al portal en el siguiente enlace: connect.hellgrun.com.ar

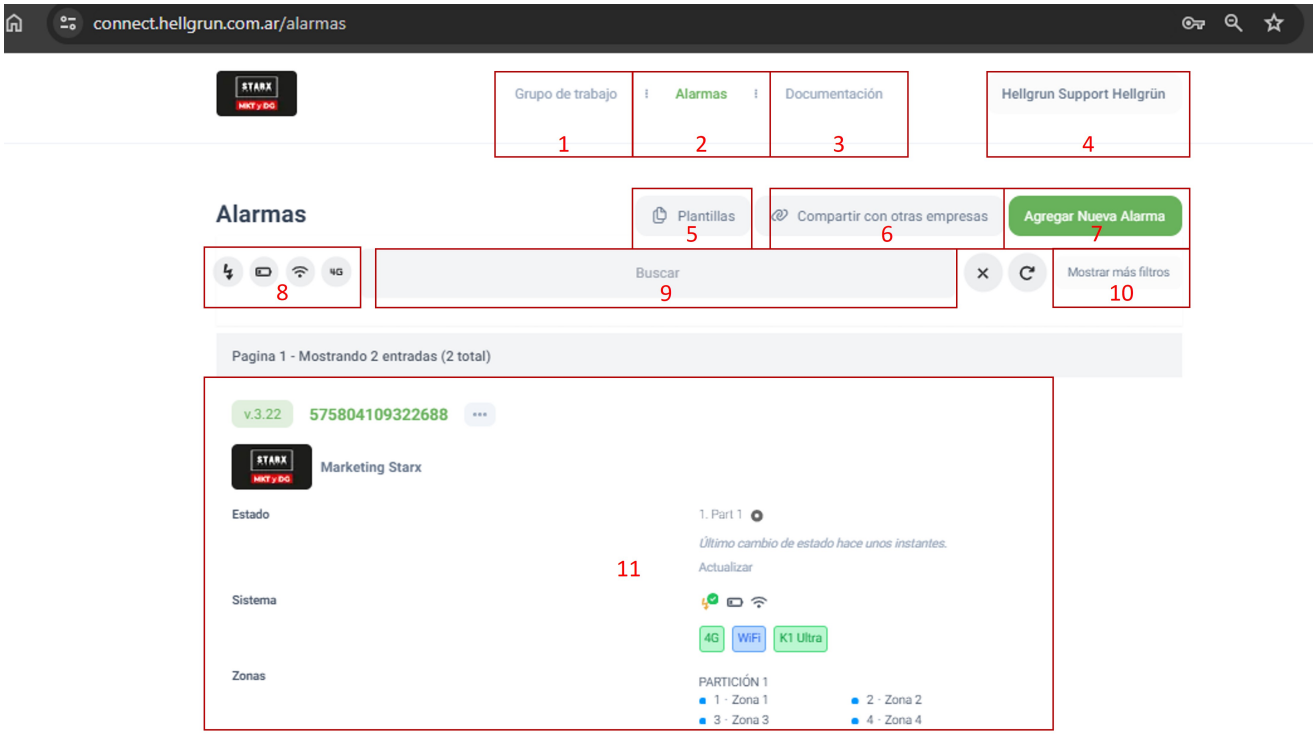
Vista principal: Alarmas

Al ingresar al portal, se mostrará un listado de alarmas, donde se puede ver el estado información relevante de cada una.



Funcionalidades

En la imagen de abajo se muestra los diferentes elementos de la vista principal del portal de Hellgrün Connect.



1- Grupo de Trabajo:

Permite gestionar los distintos usuarios que pueden acceder a la plataforma. Cada usuario tiene un rol asociado que determina el nivel de acceso. Al crearse una cuenta empresa, denominada "INSTANCIA", se asocia a un usuario administrador. Este usuario es el único que

puede gestionar los usuarios de la plataforma y los permisos de acceso de cada uno.

2- Alarmas:

Muestra el listado de alarmas asociadas a la cuenta empresa. Se presenta información sobre estado de la alarma, como por ejemplo, el estado de la comunicación, el estado de la batería, el estado de la conexión WiFi y el estado de la conexión 4G, entre otros.

3- Documentación:

Permite acceder a la documentación de los productos de Hellgrün. El contenido de esta sección es de acceso público y no requiere de un usuario registrado. Esta sección se encuentra en desarrollo y se actualiza periódicamente, dado que se encuentra en constante crecimiento.

4- Menú de Usuario:

Permite acceder a la configuración de la cuenta de usuario. Desde aquí se puede modificar la contraseña de acceso u otras configuraciones de la cuenta, según el rol del usuario.

5- Plantillas:

Permite acceder a la configuración de las plantillas de configuración de las alarmas. Las plantillas son configuraciones predefinidas que permiten agilizar la configuración de las alarmas. Por ejemplo, si se desea configurar una alarma con una configuración estándar, se puede crear una plantilla con dicha configuración y luego aplicarla a las alarmas que se desee. De este modo, se evita tener que configurar cada alarma de forma individual, disminuto los tiempo de configuración y minimiza los errores de configuración.

6- Compartir con otras empresas:

Esta opción permite compartir el acceso de sus alarmas con otra empresa. Esta opción es especialmente útil para empresas que contratan un servicio de monitoreo externo. De este modo, la empresa de monitoreo puede acceder a las alarmas de sus clientes si lo requiere. Además, una vez configurado el acceso, esta puede suspenderse o reactivarse en cualquier momento.

7- Agregar Nueva Alarma:

Permite agregar una nueva alarma a su cuenta. Para ello, se debe ingresar el número de serie de la alarma. El número de serie se encuentra en la etiqueta de la alarma y es único para cada alarma. El nombre de la alarma es un nombre que se le asigna a la alarma para identificarla, no es obligatorio. Los demas campos son atributos relacionados al cliente, como por ejemplo, el

nombre, el apellido, el número de teléfono, dirección, etc. Estos campos son opcionales y pueden ser completados en cualquier momento. Sirven para poder tener un registro de los clientes asociados a cada alarma.

8- Filtro rápidos de Alarmas:

Permite filtrar las alarmas por estado suministro eléctrico, estado de la batería, estado de la conexión WiFi y estado de la conexión 4G.

9- Barrá de búsqueda:

Permite buscar alarmas por nombre, número de serie, número de teléfono, etc. También puede buscar a través del número de cuenta de monitoreo. Por ejemplo, suponiendo que la empresa de monitoreo asigne el número de cuenta 1234, puede realizar la búsqueda ingresando de la siguiente manera: C=1234.

10- Mostrar más filtros:

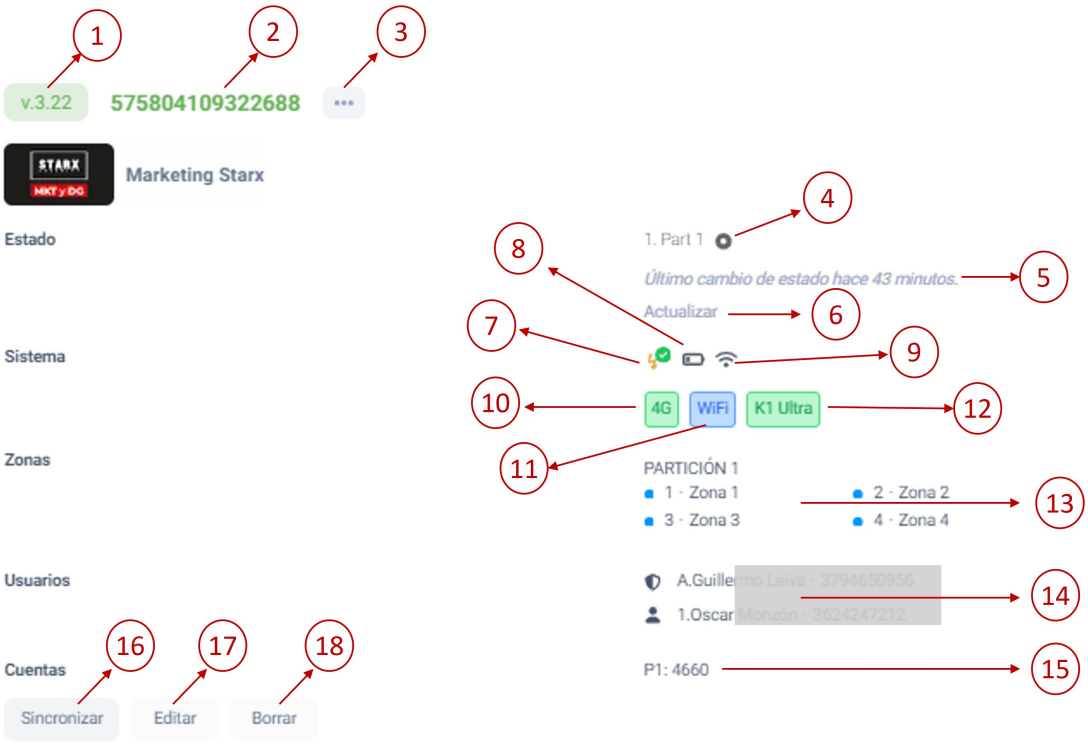
Permite realizar filtros más específicos, como por ejemplo, versión de firmware.

11- Estado de Alarmas:

Permite visualizar el estado de las alarmas. Se describe en detalle en la sección.

Estados de Alarma

El connect presenta un resumen de información relevante de cada alarma, mediante la cual, a simple vista, el personal técnico, operador u otro usuario puede identificar cualquier anomalía en el sistema.



1- Versión de firmware

Muestra la versión de firmware del panel.

2- Número de Identificación (Id)

Muestra el número de identificación del panel. Este número es único para cada panel. Puede seleccionarse haciendo click sobre él. También puede hacerse selección multiple para luego realizar una actualización masiva de firmware a uno o varios paneles. Esta opción sólo está disponible para usuarios de soporte de Hellgrün.

3- Menú de Opciones:

Es un menú que contiene algunas opciones, como sincronizar con el panel, cargar plantillas de configuración, editar información, generar un reporte de configuración, entre otras.

4- Partición:

Nombre de las particiones habilitadas. Puede haber hasta 4 particiones.

5- Último cambio de estado:

Muestra el tiempo transcurrido desde el último cambio de estado reportado por el panel. Estos estados pueden ser: armado, desarmado, disparo de alarma, falla de comunicación, etc.

6- Botón de "Actualizar":

Permite forzar una actualización de estado. Es similar a una PING. Sirve para verificar que el panel está comunicando correctamente con el servidor de Hellgrün Connect.

7- Estado de Suministro Eléctrico:

Muestra el estado del suministro eléctrico.

8- Estado de la Batería:

Si el panel posee batería baja, muestra el estado de la misma. Si la batería está óptima, no se muestra este ícono.

9- Vía de Comunicación utilizada:

Este indicador revela la vía de comunicación empleada por el panel. Puede ser WiFi o 4G. Es importante destacar que este ícono no guarda relación con el estado de los comunicadores detallados a continuación, sino que simplemente informa sobre la vía de comunicación que el panel está utilizando.

10- Estado del Comunicador 4G:

Muestra el estado actual del comunicador 4G, que puede ser: 4G, 2G/3G o Sin Servicio. Es crucial resaltar que el panel realiza pruebas periódicas para evaluar el estado del comunicador 4G, lo que garantiza la actualización casi en tiempo real de esta información. Para prevenir indicaciones incorrectas, lleva a cabo pruebas de comunicación con el servidor de Hellgrün Connect. Por ejemplo, una línea sin saldo podría reflejar un estado de 4G, pero sin servicio. En tal caso, este ícono mostrará "Sin Servicio" para indicar la falta de conectividad.

11- Estado del Comunicador WiFi:

Muestra el estado actual del comunicador WiFi, que puede ser: Conectado o Sin WiFi. Es importante entender que aquí el estado del comunicador refleja el estado de la conexión WiFi del panel, en la red LAN. Este indicador, junto al del Estado del Comunicador 4G y la Vía de Comunicación, sirven para determinar rápidamente el estado de la comunicación. Sin embargo, dentro de la configuración de la alarma, se puede acceder a información más detallada sobre el estado de la comunicación.

12- Modelo de Panel:

Muestra el modelo específico del panel. Puede ser K1, K1i o K1 Ultra.

13- Nombre y estado de las zonas:

Muestra el nombre y el estado de las zonas. El estado de las zonas puede ser: Abierta (celeste), cerrada (verder), disparada (roja), excluida (gris). El panel solo actualiza los estados de las zonas cuando se produce un cambio de estado. Si se desea actualizar el estado de las zonas, se debe hacer click en el botón de "Actualizar" (6), y el panel mantendrá actualizado los estados de las zonas durante 1 minuto.

14- Usuarios:

Muestra los usuarios que están registrados en el panel.

15- Número de cuenta de monitoreo:

En caso de que la alarma esté siendo monitoreada por una empresa de monitoreo, se muestra el número de cuenta de monitoreo. Puede haber un número de cuenta por partición.

16- Sincronizar:

Accede a la programación del panel.

17- Editar:

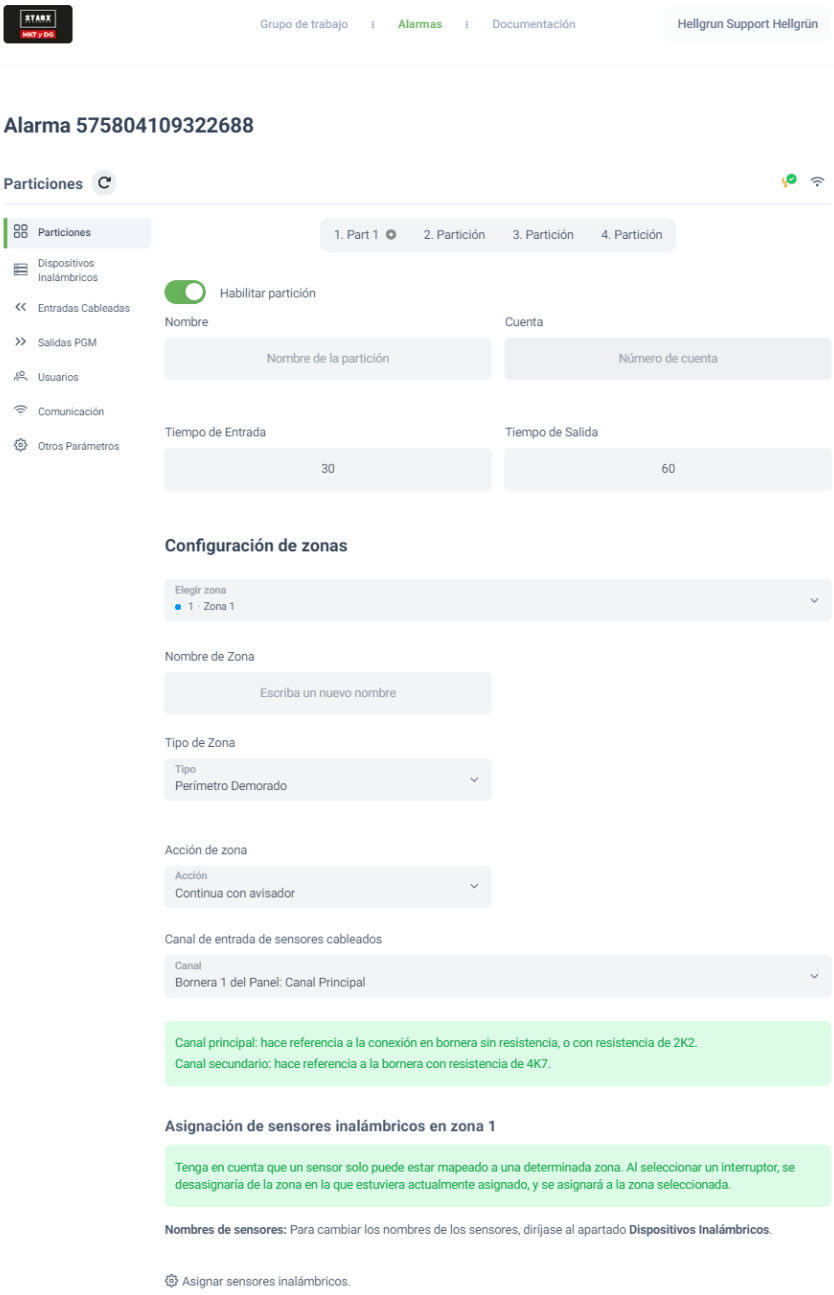
Permite editar la información asociada al panel.

18- Borrar:

Permite borrar el panel de la cuenta.

Configuración del Panel

Para acceder a la configuración del panel, se debe hacer click en el botón de Sincronizar. Se abrirá una nueva ventana con la configuración del panel.



En el menú de opciones a la izquierda, se puede acceder a las diferentes secciones de configuración del panel. Estas son:

- Particiones
- Dispositivos Inalámbricos
- Entradas cableadas
- Salidas PGM
- Usuarios
- Comunicación
- Otros Parámetros

Para realizar la programación de los campos, se debe hacer click en el campo a programar, ingresar el valor y luego presionar Enter. Un mensaje de confirmación indicará si la programación fue exitosa o no. Cada campo se edita y programa de forma independiente. No

puede realizarse una programación masiva de campos. Por ejemplo si se desea programar la dirección IP y el puerto de comunicación, se debe programar cada campo por separado.

Configuración de Particiones y Zonas

Dentro del apartado de particiones se accede a la configuración de los parámetros asociados a una partición y a las zonas de esa partición. Es importante tener en cuenta que el panel soporta hasta 4 particiones. La configuración de cada partición es independiente de las demás. Por defecto, solo la partición 1 está habilitada. Para habilitar las demás particiones, se debe acceder a la configuración de cada una y habilitarlas.

Los 4 primeros campos de la configuración de la partición son los siguientes:

Nombre de la Partición

Permite asignar un alias o nombre a la partición para identificarla. Este nombre es opcional. Si no se asigna un nombre, se mostrará Part 1, para la partición 1 y así sucesivamente para las demás. Es de buena práctica asignar un nombre a cada partición para identificarla rápidamente. Además, al usuario final también le resultará más fácil identificar en la Aplicación móvil la partición que desea armar o desarmar.

Cuenta

Número de cuenta de monitoreo. Cada partición puede tener un número de cuenta diferente. Si la alarma no está siendo monitoreada, este campo puede dejarse en blanco. Este campo admite la carga de valores hexadecimales.

Tiempo de Entrada:

Tiempo en segundos de la demora de entrada.

Tiempo de Salida:

Tiempo en segundos de la demora de salida.

Configuración de zonas:

El panel admite hasta 16 zonas por partición. Cabe aclarar que el concepto de zonas no es lo mismo que sensor, sea este de tipo cableado o inalámbricos. El concepto zona refiere a un lugar, espacio, área o elemento que se desea proteger. A cada zona se le puede asignar uno o más sensores dependiendo del nivel de protección y/o requerimientos del lugar.

En este sentido, cuando hablamos de configuración de zonas, debemos tener en cuenta que no se está configurando un sensor.

Cada zona, posee una serie de atributos que deben ser configurados:

Nombre de la zona

Es una buena práctica asignar un nombre a cada zona para identificarla rápidamente. Además el usuario final, también podrá identificar la zona de forma más rápida en la aplicación móvil. En caso de no asignar un nombre, se mostrará Zona 1, para la zona 1 y así sucesivamente para las demás.

Tipo de zona

El valor programado en esta dirección determina el comportamiento de la zona en cuestión.

Los posibles valores son:

- **Nula:** Estas zonas no son supervisadas y no generarán alarmas.
- **Perimetral Instantánea:** Estas son zonas supervisadas que generan alarmas instantáneas. Es usado normalmente para supervisión de aberturas y cierres de puertas.
- **Perimetral Demorado:** Estas son zonas supervisadas que generan alarmas demoradas. Es usado normalmente para supervisión de puertas de acceso y/o salida. Esta zona no generará alarma hasta que se cumpla el tiempo de espera, tanto en el momento de la activación como en el momento de la desactivación. El circuito puede ser abierto y cerrado durante el período de demora de salida sin causar una alarma. Una vez que la demora de salida ha terminado, al abrir la zona empezará a correr el tiempo de entrada. Durante el período de demora de entrada, el zumbador del teclado sonará en forma intermitente para advertir al usuario que el sistema debe ser desarmado. Si el control es desarmado antes de que la demora de entrada culmine, ninguna alarma será generada.
- **Interior Instantánea:** Este tipo de zona es normalmente usado para detectores de movimiento interiores, tiene la demora de salida normal, pero es instantánea cuando se abre después de que la demora de salida haya expirado.
- **Interior Seguidora:** Este tipo de zona se usa para detectores ubicados en el camino entre la puerta de entrada y el teclado. Esta zona "sigue" en su activación al tiempo de demora de entrada. Si primero se abre una zona con demora, la Seguidora también tendrá demora. En cambio si se abre una zona seguidora, ésta será instantánea.
- **24 Horas:** Si esta zona es abierta, independientemente de que el sistema esté armado o desarmado, el panel inmediatamente activará la alarma y comunicará a la estación de monitoreo . La alarma sonará hasta que el tiempo de Corte de Campana culmine o hasta que un código sea introducido.
- **Fuego:** Cuando esta zona es activada, el control inmediatamente activa la sirena de modo pulsante y comunica a la estación de monitoreo. La alarma sonará hasta que el tiempo de Corte de Campana culmine o hasta que un código sea introducido. Se recomienda que las zonas programadas como fuego deben programarse siempre pulsantes y SIN EXCLUSIÓN.

  Ver también: Configuración de PGM: Reset de Humo.

- **Armado Ausente/Desarmado por Pulsos:** Esta zona se usa normalmente con controles remotos. Cada vez que se activa esta zona, conmutará el estado del panel, de armado a desarmado y viceversa siempre que el sistema esté listo para armar. Como alternativa para dar aviso de este tipo de operación, el panel generará 1 beep de sirena para el armado y 2 beeps para el desarmado. Las zonas programadas como llave on-off serán siempre invisible sin avisador, y deben ser programadas en forma concordante, Normal Cerrado o Normal Abierto, con el control remoto que se utilice, y éste debe ser monoestable, o sea apertura y cierre o viceversa en cada pulsado.
- **Asalto:** LA ZONA DEBE SER INVISIBLE, SILENCIOSA Y SIN AVISADOR. (Sólo reporta a la central)
- **Médico:** con esta programación LA ZONA PUEDE SER SILENCIOSA O CON SIRENA.
- **Perimetral seguidora:** Este tipo de zona se usa para detectores ubicados en el camino entre la puerta de entrada y el teclado. Esta zona "sigue" en su activación al tiempo de demora de entrada. Si primero se abre una zona con demora, la Seguidora también tendrá demora. En cambio si se abre una zona seguidora, ésta será instantánea.
- **Armado Presente/Desarmado por Pulsos:** Ídem opción 7, pero con la diferencia de que el panel se arma en modo presente.

Acción de Zona

El valor programado en esta dirección determina la acción que se ejecutará cuando la zona se active. Ésta puede ser:

- **Invisible**: Esta es una zona programada para no producir una alarma sonora, a la vez que en la pantalla del teclado y/o en la APP no habrá indicación alguna de que esta zona se ha violado. Pero generará un reporte a monitoreo.
- **Silenciosa:** Esta es una zona programada para activar la pantalla del teclado, pero no las sirenas.
- **Continua:** Cuando esta zona genera una alarma, la sirena sonará en forma continua. Se recomienda este tipo de acción para todas las zonas de ROBO y PÁNICO.
- **Pulsante:** Cuando esta zona genera una alarma, la sirena sonará en forma pulsante con un patrón de 1seg. encendida, y 1seg. apagada.

Si la acción seleccionada además incluye la opción "Con avisador" (chime), determinará que cuando una zona con avisador habilitado se abre, el buzzer de los teclados emita una señal rápida y corta. Dado que esta función es sólo funcional cuando el sistema incluye un teclado, el chime podrá desactivarse o activarse para todas las zonas con avisador, a través del teclado por medio del comando [*] [4].

Asignación de Sensores a las zonas

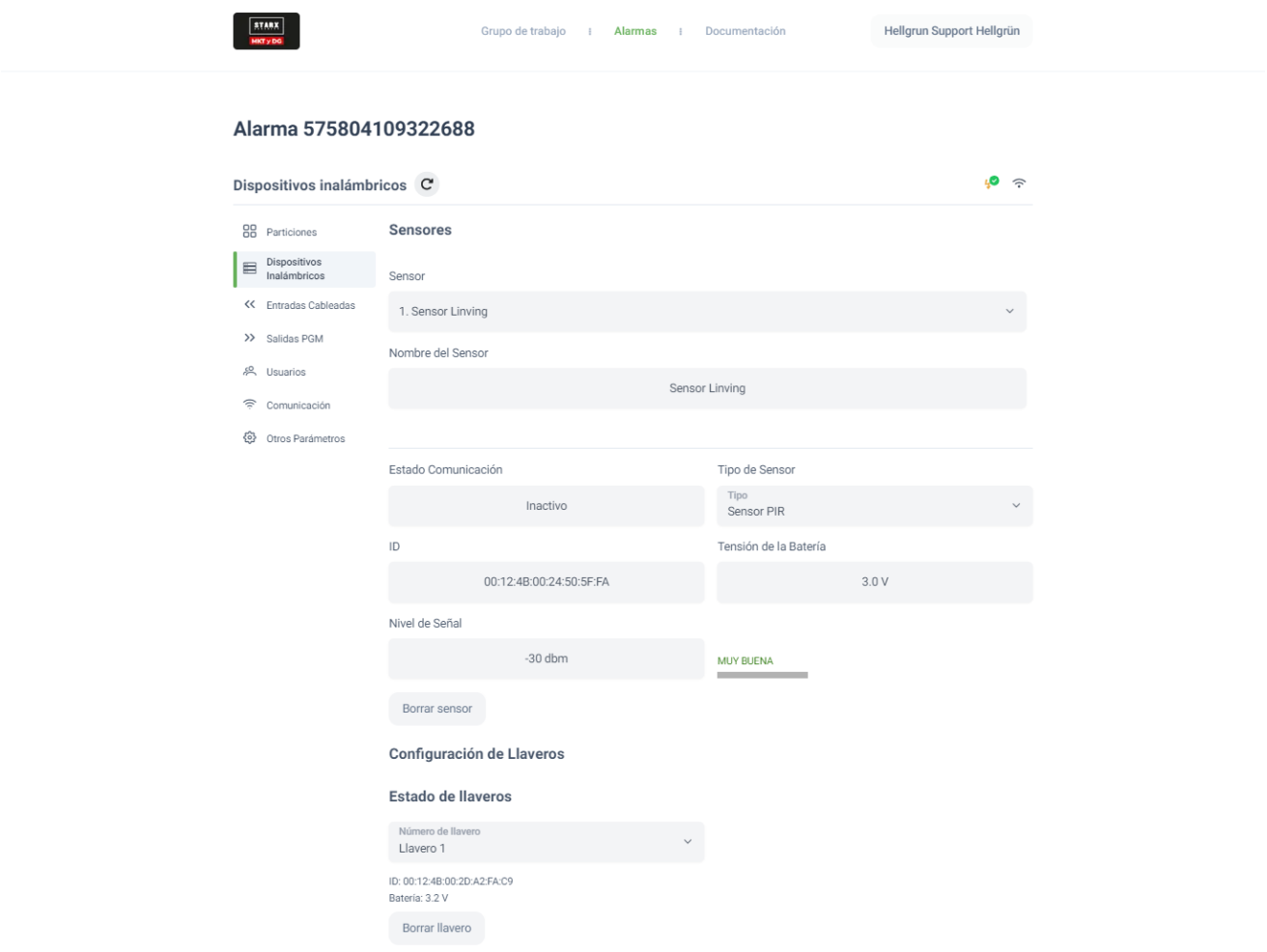
Hasta aquí hemos configurado el comportamiento de la zona en cuestión. Ahora debemos asignarle los sensores que deseamos que activen la zona. Recordemos que el panel es totalmente híbrido, lo que significa que puede tener sensores cableados e inalámbricos simultáneamente en una misma zona.

Para el caso de sensores cableados, debe entenderse que no existe ningún condicionamiento respecto a la bornera utilizada para conectar el o los sensores y el número de la zona. Así por ejemplo, la zona 1, podría ser activada por la bornera de un teclado. Solamente basta con seleccionar el canal de entrada correspondiente. En este punto, se recomienda leer el concepto de canal, desarrollado aquí.

Para asignar sensores inalámbricos, hacer click en la opción "Asignar Sensores Inalámbricos" y se desplegará una lista con los sensores inalámbricos disponibles. Es importante tener en cuenta que los sensores inalámbricos deben estar previamente vinculados al panel. En el apartado de dispositivos inalámbricos se explica este procedimiento. Luego, seleccionar el o los sensores que se desean asignar a la zona. Si un sensor determinado ya se encuentra asignado a otra zona, éste se moverá automáticamente a la nueva zona seleccionada. Un sensor no puede estar asignado a más de una zona.

Dispositivos Inalámbricos

En este apartado, se accede a la información de los dispositivos inalámbricos vinculados al panel. El panel soporta hasta 32 dispositivos inalámbricos, que pueden ser, sensores magnéticos y/o PIR, como también en breve habrán de otros tipos. Respecto a los llaveros, el panel soporta hasta 21 llaveros.
Este se divide en dos secciones: Sensores y Controles Remotos.



Sensores

En esta sección se visualiza toda la información de cada uno de los sensores inalámbricos vinculados al panel. Seleccionar el sensor que se desea visualizar.

Nombre

Es un atributo opcional, que puede ser utilizado por el instalador para identificar el sensor. Este nombre no se muestra en la aplicación móvil.

Estado de comunicación

Puede ser Activo o Inactivo. Indica si el sensor se encuentra en red o ha perdido comunicación.

Tipo de Sensor

Indica el tipo de sensor.

ID

Número de identificación del sensor. Este número es único para cada sensor.

Tensión de la bateria

Indica la tensión de la pila, en voltios. Cuando la batería alcanza un valor de 2.7V se genera un reporte de aviso de baja batería a la estación de monitoreo.

Nivel de señal

Indica el nivel de señal del sensor en dBm. Para identificar la calidad de la señal, puede utilizarse la siguiente tabla:

Nivel de señal	Calidad de señal
-30 a -70dBm	Excelente
-70 a -85dBm	Buena
-85 a -90dBm	Regular
-90 a -127dBm	Mala

Éste indicador es muy útil al momento de la instalación. Permite identificar la calidad de la señal del sensor en el lugar donde se encuentra instalado. Si el nivel de señal es bajo, se recomienda reubicar el sensor o el panel. También, es importante destacar que es un indicador dinámico, es decir, que su valor puede variar según las condiciones del ambiente,

como por ejemplo, la presencia de obstáculos, la distancia, etc., y/o la tensión de la batería. Un nivel de señal de calidad Mala, no necesariamente signfica que el sensor se encuentra fuera de comunicación.

Borrar sensor

Permite borrar el sensor del panel. Al borrar el sensor, se desvincula del panel y se elimina de la lista de sensores. Este proceso, no realiza un default sobre el sensor, por lo que el sensor no queda disponible para ser vinculado a otro panel hasta producirle un default. Para realizar un default al sensor, presione el pulsador que se encuentra en el interior del sensor, durante 10 segundos. Luego, el sensor quedará disponible para ser vinculado a otro panel.

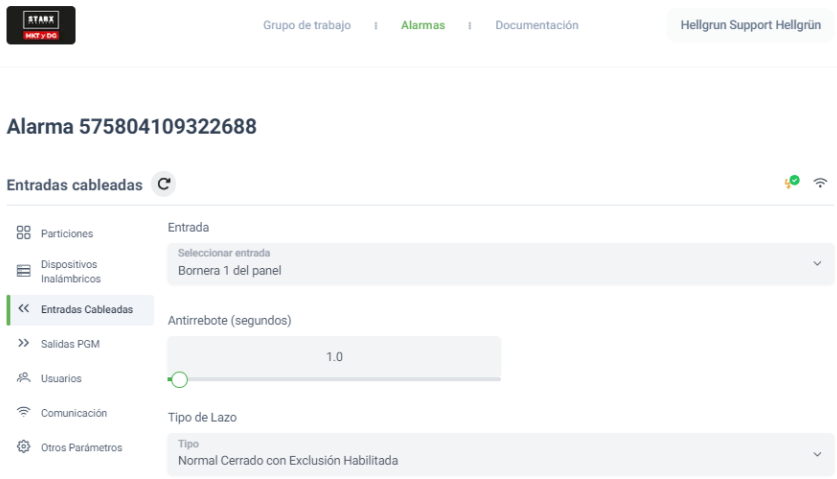
Controles Remotos

En esta sección se visualiza toda la información se cada uno de los controles remotos vinculados al panel.

La información que aquí se muestra, es el ID del llavero y la tensión de la batería, que es la que tiene registro el panel desde la última vez que se utilizó el llavero.

Entradas Cableadas

En este apartado, se accede a la información de las entradas cableadas del panel. El panel soporta hasta 8 entradas cableadas. 4 borneras se encuentran en la placa del panel y las otras 4 se encuentran en el teclado, 1 por cada teclado.



En el campo Entrada, se debe seleccionar la entrada que se desea visualizar. Puede ser la bornera 1, 2, 3 o 4 del panel, o la bornera del teclado 1, 2, 3 o 4.

Antirrebote

Es el tiempo mínimo, expresado en segundos, en el que una entrada, debe permanecer sin cambios luego de una transición de estado -abierto a cerrado y viceversa- para ser considerado válido. Esto permite filtrar, fluctuaciones transitorias de los sensores, ruido electríco, etcétera.

Tipo de Lazo

El tipo de lazo de entrada, hace referencia a la forma en que se encuentra conectado el sensor a la entrada.

La diferencia entre "Con Exclusión Habilitada" y "Sin Exclusión Habilitada", refiere a un mecanismo de seguridad, que permite o no al usuario, excluir una zona vinculada a dicha entrada. Si la exclusión está habilitada, el usuario podrá excluir la zona vinculada a la entrada. Si la exclusión está deshabilitada, el usuario no podrá excluir la zona vinculada a la entrada. Es útil para evitar que el usuario pueda excluir una zona que no debe ser excluida, como por ejemplo, una zona de incendio.

Es oportuno aquí, repasar los conceptos Guía de Instalación -> Sensores Cableados y de Programación por Teclado -> Dirección 003: Tipo de Lazo, para comprender mejor estas configuraciones.

Salidas PGM

Los paneles Kümmert soportan hasta 2 salidas PGM. Cada PGM puede ser configurada entre las diferentes opciones:

- **Listo para armar:** Una partición está lista para armar, cuando todas las zonas de la misma se encuentran cerradas, excepto las de tipo interior, que pueden estar abiertas y permite al panel armarse en modo presente.
- **Sistema armado:** Se activa cuando la/s particion/es está/n armada/s.
- **Sistema armado con memoria de disparo:** Se activa cuando la/s particion/es está/n armada/s y se produjo un disparo de alarma.
- **Sirena:** Esta salida sigue al estado de la sirena. Se activa cuando la sirena está activa. Dado que puede vincularse con las diferentes particiones de forma independiente, permite extender la salida de la sirena para cada partición por separado.
- **Alerta de Asalto:** Se activa cuando se produce un disparo de alarma por asalto.
- **Luz de cortesia:** Se activa durante el tiempo de entrada y salida.
- **Reset de Humo:** La mayoría de los sensores de humo, una vez disparados, no se reestablecen automáticamente. Es necesario apagarlo y volverlo a encender para que vuelvan a estar operativos. Esta salida permite realizar esta acción de forma automática. La salida PGM se encuentra activada siempre. Cuando se produce un disparo en una zona configurada como de tipo Fuego, y el usuario desactiva la alarma, el PGM se desactiva por un lapso de 10 segundos y luego se vuelve a activar. Mediante este proceso, conectando el negativo del sensor a la salida PGM, se logra controlar el reseteo del sensor de humo.

`Es importante destacar, que cuando esta función es utilizada, la entrada cableada donde se encuentra conectado el sensor de humo, debe tener un tiempo de antirrebote mayor a 10 segundos para evitar que el sistema entre en un bucle de disparo y reseteo.`

- **Falla de comunicación:** Se activa cuando se produce una falla de comunicación.
- **Asignado a control remoto:** Responde a la configuración asignada al control remoto. Puede ser de tipo ON/OFF o de tipo Pulso.
- **Luz de emergencia en todos los estados:** Se activa ante el corte de suministro eléctrico.
- **Luz de emergencia en estado armado ausente:** Se activa ante el corte de suministro eléctrico y el sistema está armado ausente.
- **Luz de emergencia en estado armado presente:** Se activa ante el corte de suministro eléctrico y el sistema está armado presente.
- **Luz de emergencia en estado desarmado:** Se activa ante el corte de suministro eléctrico y el sistema está desarmado.
- **Desactiva:** Desactiva la salida PGM.

Además, cada función puede vincularse a una o más particiones, lo que permite tener un mayor control sobre las salidas PGM.

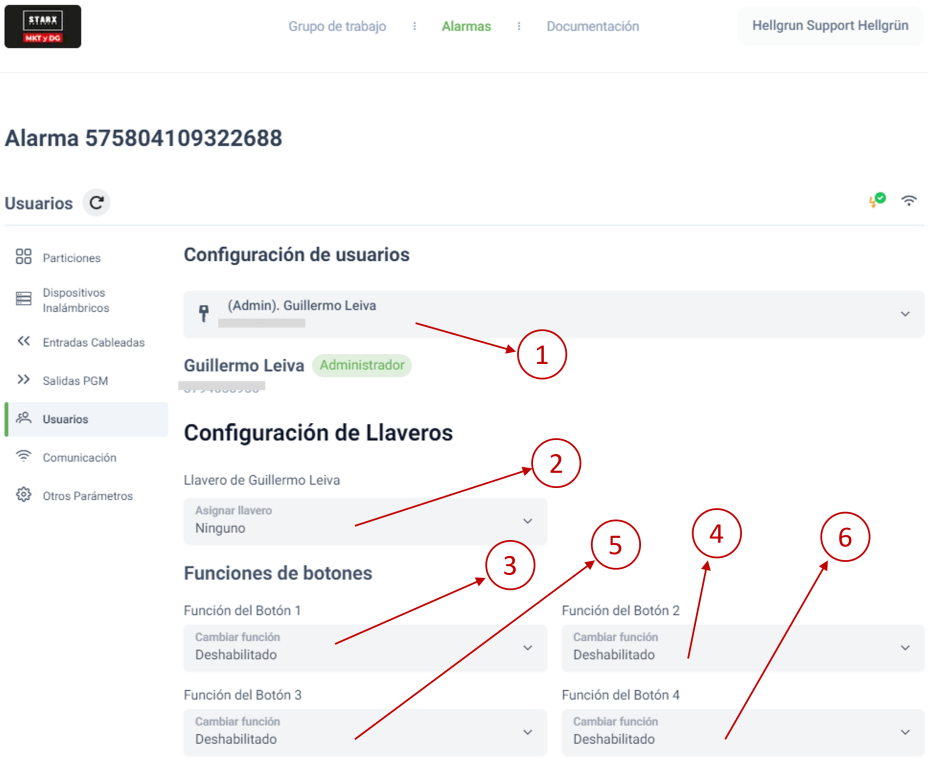
Para entender mejor, como funciona una salida PGM, se recomienda leer el siguiente artículo: Salidas PGM.

Usuarios

Usuario Administrador

El panel admite hasta 20 usuarios, además de un administrador, análogo al comunmente conocido como "usuario maestro". La creación del usuario administrador se realiza a través de la aplicación Hellgrün Check mediante el escaneo del código QR en la etiqueta del panel. No es posible generar otro usuario administrador si ya existe uno. En caso de necesitar uno nuevo, es necesario eliminar el usuario administrador existente. Debido a políticas de seguridad, la eliminación del usuario administrador no puede llevarse a cabo desde el portal Hellgrün Connect; debe realizarse desde la aplicación Hellgrün Check por el administrador actual o solicitarse al departamento de soporte de Hellgrün, que analizará y realizará la eliminación según corresponda.

En la figura siguiente se presenta la configuración de un usuario administrador.

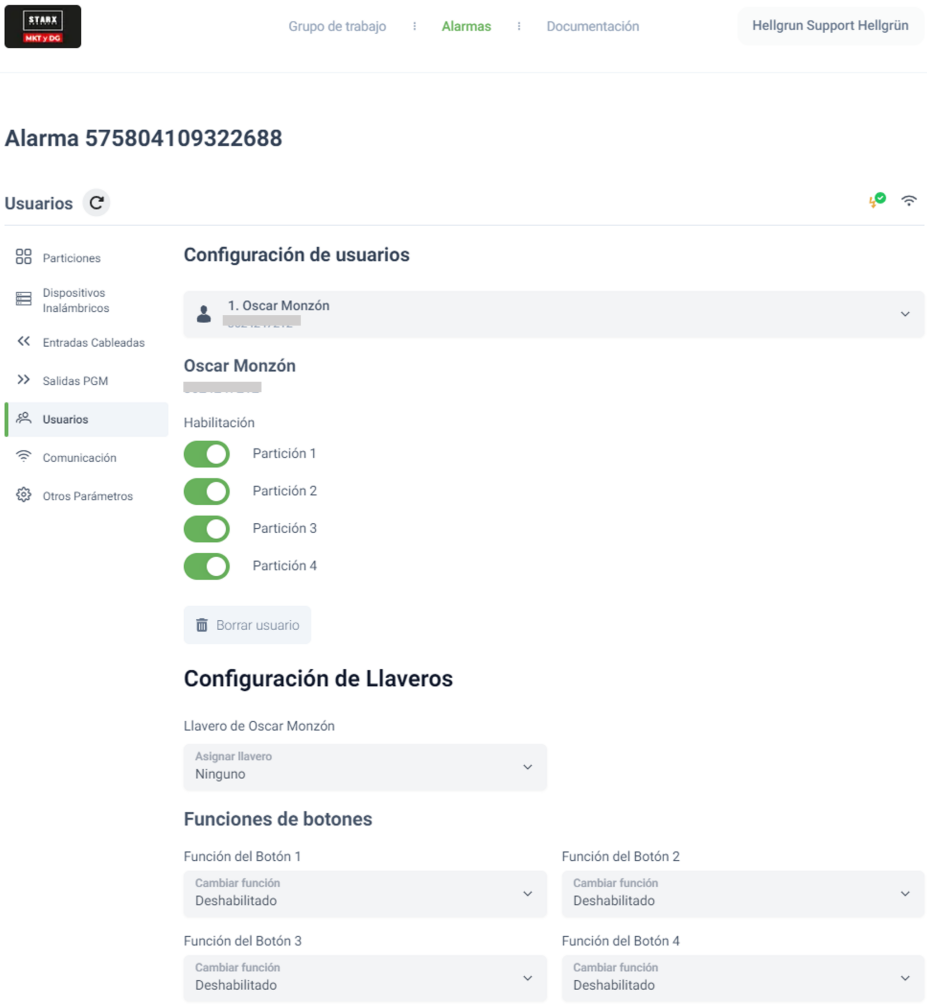


- **1- Usuarios:** Lista desplegable de selección de usuarios. Permite seleccionar el usuario que se desea visualizar.
- **2- Asignación de Llaveros:** Asigna un llavero al usuario. El llavero debe estar vinculado al panel. Si el llevaro seleccionado se encontraba asignado a otro usuario, se cambiará a éste nuevo. Un llavero no puede estar asignado a más de un usuario.
- **3- Configuración de la función del botón 1:** Permite configurar la función del botón 1 del llavero.
- **4- Configuración de la función del botón 2:** Permite configurar la función del botón 2 del llavero.
- **5- Configuración de la función del botón 3:** Permite configurar la función del botón 3 del llavero.
- **6- Configuración de la función del botón 4:** Permite configurar la función del botón 4 del llavero.

Usuario Normal

El usuario normal, o simplemente usuario, es el aquel que puede tener asignado diferentes roles y/o restricción de acceso a las distintas particiones. Éste tipo de usuarios puede ser totalmente administrado por el usuario administrador. El usuario administrador puede crear, editar y borrar usuarios normales. Además, puede asignarle diferentes roles y/o restricciones de acceso a particiones desde la APP Hellgrün Check.

En la figura de abajo se muestra la configuración de un usuario normal. La única diferencia con respecto al usuario administrador, es que este puede puede tener restricciones de acceso a particiones y puede ser borrado desde el portal de Hellgrün Connect.



Gestión de Usuarios

El panel permite administrar los usuarios de diferentes formas:

- **A través de la aplicación móvil Hellgrün Check:** Es la forma más segura y eficiente de gestionar usuarios, ya que permite identificar a cada uno mediante nombre, apellido, número de celular y clave de usuario única. Mediante la aplicación, el administrador puede administrar otros permisos y/o funcionalidades sobre los demás usuarios, por ejemplo, si un usuario puede o no armar o desarmar el sistema, si puede o no recibir notificaciones, etc. Además un usuario de la aplicación móvil, puede sin problemas acceder a través del teclado mediante su clave de usuario o bien tener también asignado un control remoto.
- **Usuarios que pueden acceder sólo por teclado:** Los usuarios que sólo pueden acceder por teclado, son dados de alta a través de la programación por teclado, y sú única credencial de acceso es la clave de usuario. No pueden acceder a través de la aplicación móvil aunque sí pueden tener asignado un control remoto.
- **Usuarios con Control Remoto:** Los controles remotos de Hellgrün, una vez vinculados al panel, por sí solos no realizan acción alguna. Es necesario vincularlo a un usuario para que pueda realizar alguna acción. Además, cada control remoto puede tener acciones

diferentes para cada usuario. Hay casi 40 acciones posibles que pueden asignarse a cada uno de los 4 pulsadores de cada control remoto de manera independiente para cada usuario.

Funciones de los botones de los controles remotos

Las funciones que pueden asignarse a cada botón son las siguientes:

- Deshabilitado: Ninguna acción será ejecutada cuando se presione el botón.
- Armar Presente Partición 1: Arma la partición 1 en modo presente. Debe tener permiso habilitado sobre la partición 1.
- Armar Presente Partición 2: Arma la partición 2 en modo presente. Debe tener permiso habilitado sobre la partición 2.
- Armar Presente Partición 3: Arma la partición 3 en modo presente. Debe tener permiso habilitado sobre la partición 3.
- Armar Presente Partición 4: Arma la partición 4 en modo presente. Debe tener permiso habilitado sobre la partición 4.
- Armar Ausente Partición 1: Arma la partición 1 en modo ausente. Debe tener permiso habilitado sobre la partición 1.
- Armar Ausente Partición 2: Arma la partición 2 en modo ausente. Debe tener permiso habilitado sobre la partición 2.
- Armar Ausente Partición 3: Arma la partición 3 en modo ausente. Debe tener permiso habilitado sobre la partición 3.
- Armar Ausente Partición 4: Arma la partición 4 en modo ausente. Debe tener permiso habilitado sobre la partición 4.
- Desarmar Partición 1: Desarma la partición 1. Debe tener permiso habilitado sobre la partición 1.
- Desarmar Partición 2: Desarma la partición 2. Debe tener permiso habilitado sobre la partición 2.
- Desarmar Partición 3: Desarma la partición 3. Debe tener permiso habilitado sobre la partición 3.
- Desarmar Partición 4: Desarma la partición 4. Debe tener permiso habilitado sobre la partición 4.
- Armar Ausente/Desarmar Partición 1: Arma la partición 1 en modo ausente o desarma la partición 1. Debe tener permiso habilitado sobre la partición 1.
- Armar Ausente/Desarmar Partición 2: Arma la partición 2 en modo ausente o desarma la partición 2. Debe tener permiso habilitado sobre la partición 2.
- Armar Ausente/Desarmar Partición 3: Arma la partición 3 en modo ausente o desarma la partición 3. Debe tener permiso habilitado sobre la partición 3.
- Armar Ausente/Desarmar Partición 4: Arma la partición 4 en modo ausente o desarma la partición 4. Debe tener permiso habilitado sobre la partición 4.
- Armar con Asalto Partición 1: Arma la partición 1 en modo ausente con asalto. Debe tener permiso habilitado sobre la partición 1.
- Armar con Asalto Partición 2: Arma la partición 2 en modo ausente con asalto. Debe tener permiso habilitado sobre la partición 2.

- Armar con Asalto Partición 3: Arma la partición 3 en modo ausente con asalto. Debe tener permiso habilitado sobre la partición 3.
- Armar con Asalto Partición 4: Arma la partición 4 en modo ausente con asalto. Debe tener permiso habilitado sobre la partición 4.
- Desarmar con Asalto Partición 1: Desarma la partición 1 con asalto. Debe tener permiso habilitado sobre la partición 1.
- Desarmar con Asalto Partición 2: Desarma la partición 2 con asalto. Debe tener permiso habilitado sobre la partición 2.
- Desarmar con Asalto Partición 3: Desarma la partición 3 con asalto. Debe tener permiso habilitado sobre la partición 3.
- Desarmar con Asalto Partición 4: Desarma la partición 4 con asalto. Debe tener permiso habilitado sobre la partición 4.
- PGM 1 ON/OFF: Activa o desactiva la salida PGM 1. La salida PGM 1 se configurará automáticamente como tipo "Asignado a control remoto".
- PGM2 ON/OFF: Activa o desactiva la salida PGM 2. La salida PGM 2 se configurará automáticamente como tipo "Asignado a control remoto".
- PGM1 PULSO: Activa la salida PGM 1 por un tiempo de 2 segundo. La salida PGM 1 se configurará automáticamente como tipo "Asignado a control remoto".
- PGM 2 PULSO: Activa la salida PGM 2 por un tiempo de 2 segundo. La salida PGM 2 se configurará automáticamente como tipo "Asignado a control remoto".
- Pánico: Se envía un reporte de pánico a la estación de monitoreo y a las aplicaciones móviles de los usuarios. La sirena sonará o no según la configuración establecida en la Tecla Pánido en el teclado.
- Emergencia: Se envía un reporte de emergencia a la estación de monitoreo y a las aplicaciones móviles de los usuarios. La sirena sonará o no según la configuración establecida en la Tecla Emergencia en el teclado.
- Armado Demorado Particion 1: Arma la partición 1 en modo ausente con demora. Debe tener permiso habilitado sobre la partición 1. Permite armar la partición desde el interior de la propiedad. Asi también, si durante la demora, la zona demorada se abre, el panel cambiará el estado de la partición a armado ausente automáticamente.
- Armado Demorado Particion 2: Arma la partición 2 en modo ausente con demora. Debe tener permiso habilitado sobre la partición 2. Permite armar la partición desde el interior de la propiedad. Asi también, si durante la demora, la zona demorada se abre, el panel cambiará el estado de la partición a armado ausente automáticamente.
- Armado Demorado Particion 3: Arma la partición 3 en modo ausente con demora. Debe tener permiso habilitado sobre la partición 3. Permite armar la partición desde el interior de la propiedad. Asi también, si durante la demora, la zona demorada se abre, el panel cambiará el estado de la partición a armado ausente automáticamente.
- Armado Demorado Particion 4: Arma la partición 4 en modo ausente con demora. Debe tener permiso habilitado sobre la partición 4. Permite armar la partición desde el interior de la propiedad. Asi también, si durante la demora, la zona demorada se abre, el panel cambiará el estado de la partición a armado ausente automáticamente.
- Armado Presente Demorado c/Asalto Particion 1: Ídem a la opción "Armado Presente Demorado", pero con la diferencia de que se genera adicionalmente un reporte de asalto a la estación de monitoreo. El asalto en este caso, será siempre silencioso.

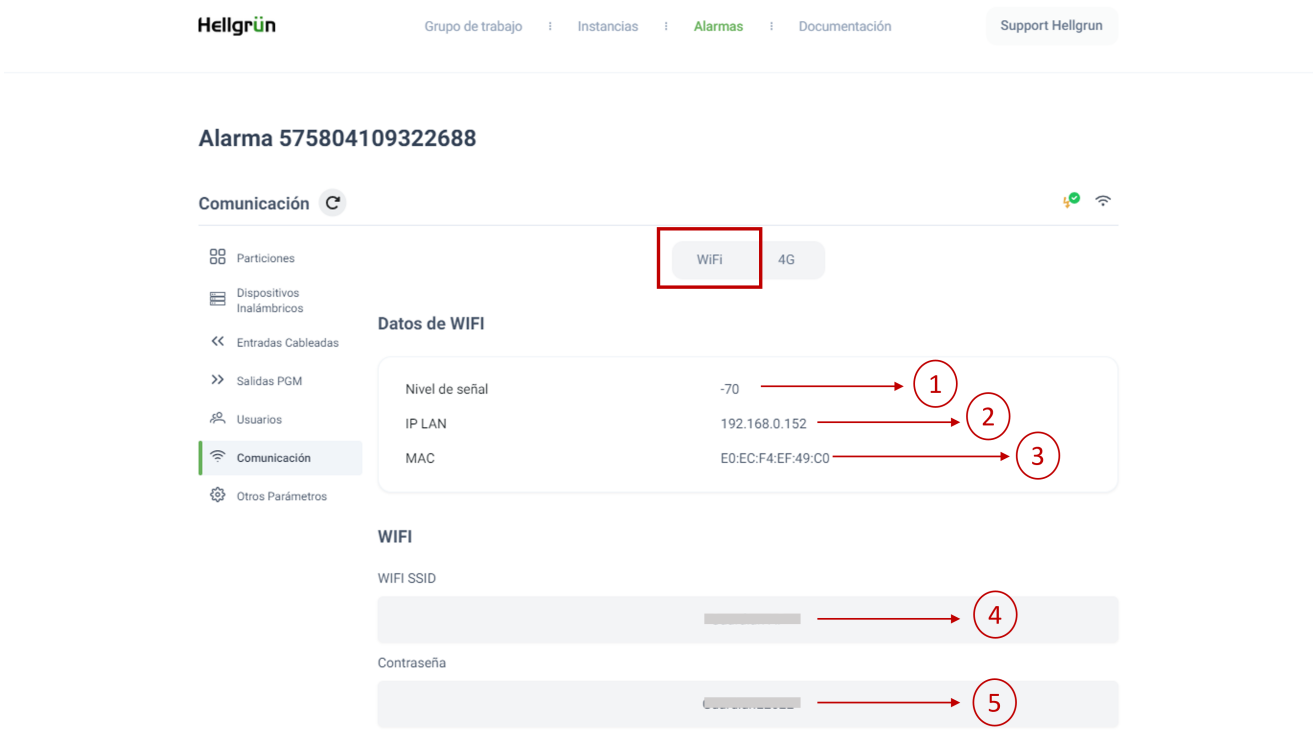
- Armado Presente Demorado c/Asalto Particion 2: Ídem a la opción "Armado Presente Demorado", pero con la diferencia de que se genera adicionalmente un reporte de asalto a la estación de monitoreo. El asalto en este caso, será siempre silencioso.
- Armado Presente Demorado c/Asalto Particion 3: Ídem a la opción "Armado Presente Demorado", pero con la diferencia de que se genera adicionalmente un reporte de asalto a la estación de monitoreo. El asalto en este caso, será siempre silencioso.
- Armado Presente Demorado c/Asalto Particion 4: Ídem a la opción "Armado Presente Demorado", pero con la diferencia de que se genera adicionalmente un reporte de asalto a la estación de monitoreo. El asalto en este caso, será siempre silencioso.

Comunicación

En esta sección se pueden leer y programar parámetros específicos relacionados a los comunicadores del panel, tanto WiFi como 4G en los paneles K1 Ultra y K1 4G.

Comunicador WiFi

En la imagen siguiente se muestra la configuración del comunicador WiFi.



- **1- Nivel de señal:** Es el valor de RSSI en dBm del comunicador WiFi. Los valores de RSSI son valores negativos, por lo que cuanto más cercano a 0, mejor es la calidad de la señal. Un nivel de señal a partir menor a -85dBm, se considera de baja calidad.
- **2- IP LAN:** Es la dirección IP que tiene asignada el panel en la red local. Esta dirección IP es asignada por el router de la red local. Si el panel no tiene asignada una dirección IP, entonce la conexión WiFi no se ha establecido correctamente. Esto puede deberse a

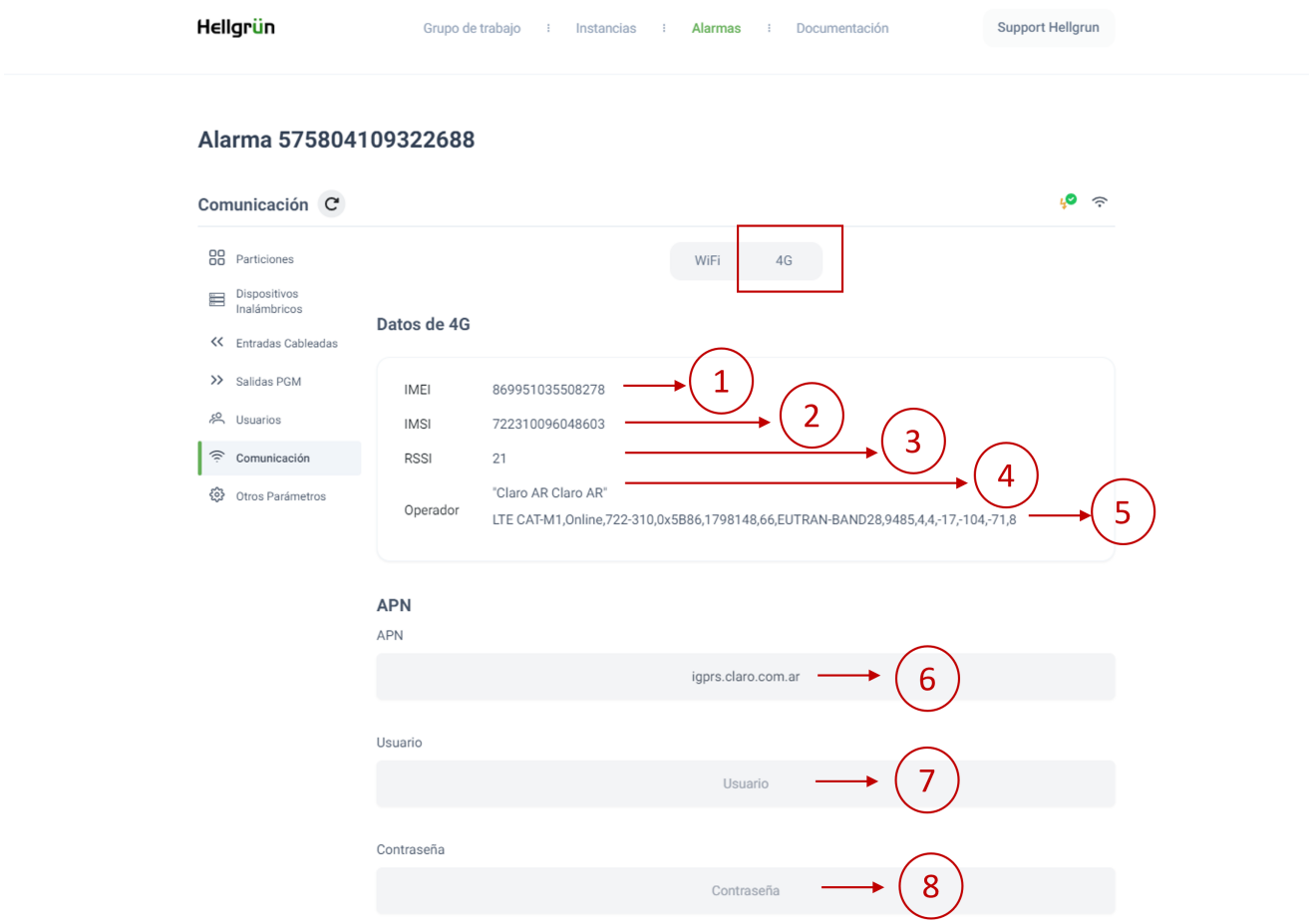
alguna configuración del router, como por ejemplo, que el router no tenga habilitado el DHCP o simplemente que la contraseña de la red WiFi sea incorrecta.

- **3- MAC:** Es la dirección MAC del comunicador WiFi. Esta dirección es única para cada dispositivo y no puede ser modificada. Puede ser utilizada para identificar el panel en la red local y asignarle una dirección IP fija u otros parámetros de red específicos.
- **4- SSID:** Es el nombre de la red WiFi a la que está conectado el panel. Este parámetro puede ser modificado si se desea. Para ello, hacer click en el campo, ingresar el nuevo nombre y presionar Enter.
- **5- Contraseña:** Es la contraseña de la red WiFi a la que está conectado el panel. Este parámetro puede ser modificado si se desea. Para ello, hacer click en el campo, ingresar la nueva contraseña y presionar Enter.

`Los cambios realizados en los parámetros SSID y Contraseña, se aplicarán una vez que el panel se reinicie.`

Comunicador 4G

En la imagen siguiente se muestra la configuración del comunicador 4G.



- **1- IMEI:** El IMEI (International Mobile Equipment Identity) es un número de serie único que se asigna a cada módulo 4G. Es un identificador de 15 dígitos que se utiliza para identificar de manera exclusiva a un dispositivo móvil en una red de telefonía móvil.

- **2- IMSI:** EEl IMSI (International Mobile Subscriber Identity) es un número de serie único que se asigna a cada tarjeta SIM en una red de telefonía móvil. Es un identificador de 15 dígitos que se utiliza para identificar de manera exclusiva a un abonado en la red.

El IMSI se utiliza para vincular el panel de alarma con los portales de gestión que ofrecen las compañías de telefonía celular. Proporciona información sobre el operador de red y el país al que pertenece la tarjeta SIM. También se utiliza para autenticar y autorizar al usuario en la red. Estas son funcionalidades asociadas a la línea móvil, y depende del tipo de herramienta utilizado para su gestión.

Es importante destacar que el IMSI no se puede modificar, ya que está grabado en la tarjeta SIM durante su fabricación.

- **3- RSSI:** Es un indicador numérico que va desde 0 a 31, que indica la calidad de la señal 4G. Cuanto más cercano a 31, mejor es la calidad de la señal. Un valor menor a 15, se considera de baja calidad.
- **4- Operador:** Es el nombre de la compañía de telefonía celular a la que está conectado el panel. En una segunda línea se encuentra información técnica relevante sobre la conexión la red, como por ejemplo, el tipo de red, la banda de frecuencia, tipo de servicio, etc. En esta sección, puede identificarse si el panel se encuentra conectado a una red 4G (LTE CAT-M1), GSM/GPRS (GSM) o sin servicio (No Service).
- **5- APN:** Es el nombre del punto de acceso a la red de datos de la compañía de telefonía celular. Los APN públicos de las compañias Personal, Claro y Movistar se encuentran precargados en el panel. Si se desea utilizar un APN privado, se debe ingresar el nombre del APN en el campo y presionar Enter.
- **6- Usuario:** Es el nombre de usuario del APN. Este parámetro puede ser modificado si se desea. Para ello, hacer click en el campo, ingresar el nuevo nombre y presionar Enter.
- **7- Contraseña:** Es la contraseña del APN. Este parámetro puede ser modificado si se desea. Para ello, hacer click en el campo, ingresar la nueva contraseña y presionar Enter.

  `Los cambios realizados en los parámetros APN, Usuario y Contraseña, se aplicarán una vez que el panel se reinicie.`

Otros Parámetros

En este apartado, se tiene la posibilidad de programar otros parámetros relacionados con el panel de control.

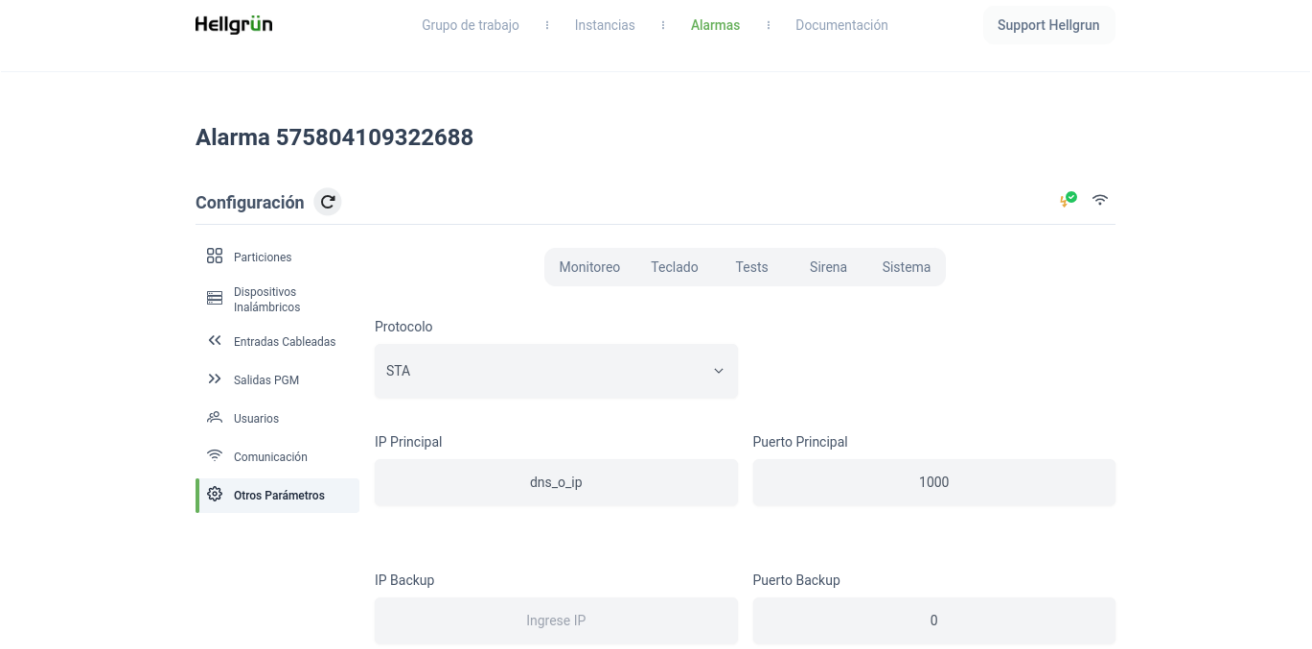
Estos parámetros se dividen en 5 grupos:

- **Monitoreo:** Se configuran los parámetros del servidor de la estación de monitoreo.
- **Teclado:** Configuraciones relativas al funcionamiento del teclado. Aunque específicamente se relaciona al uso del teclado, su configuración impacta en el comportamiento de otros periféricos.
- **Tests:** Se configuran los parámetros de envíos de tests a la estación de monitoreo.

- **Sirena:** Se establecen parámetros de funcionamiento de la sirena.
- **Sistema:**

Parámetros de Monitoreo

En la imagen de abajo se muestra la configuración de los parámetros de monitoreo:



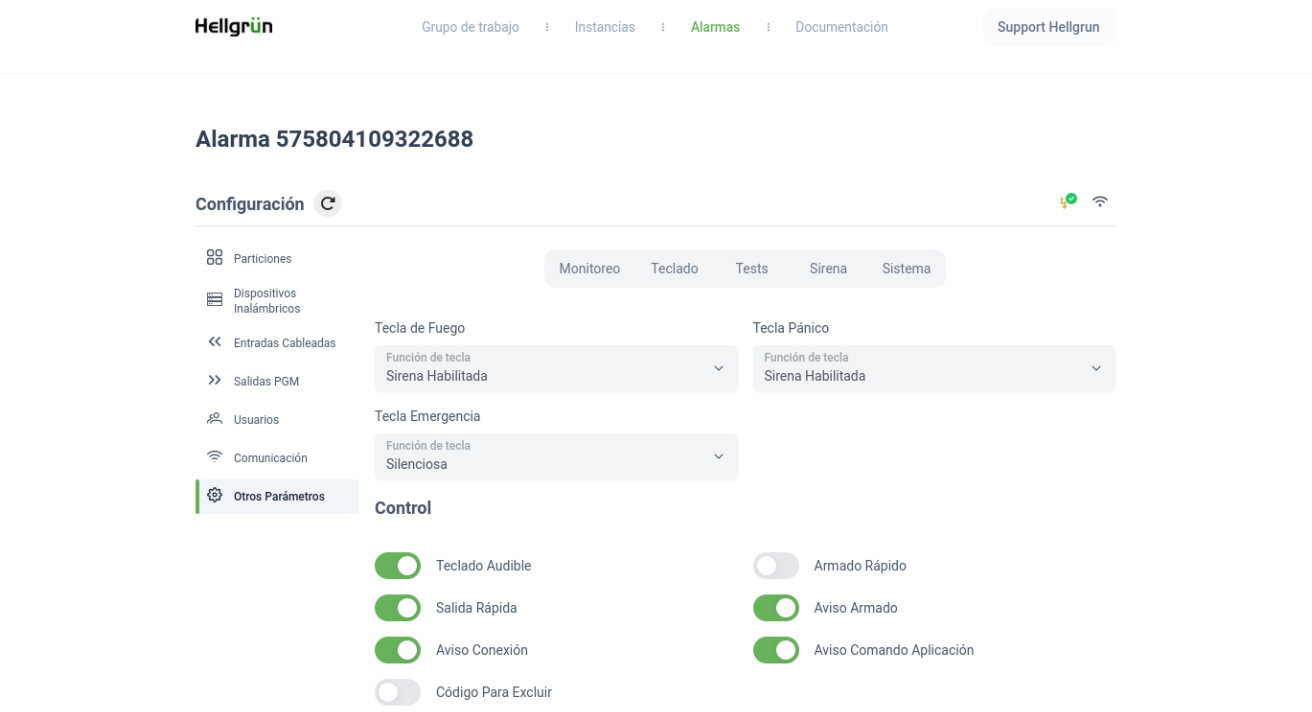
Los parámetros de configuración son:

- **Protocolo:** Selecciona el protocolo entre SIA-DC09 o STA.
  - El protocolo SIA-DC09 es un estándar definido para la comunicación entre sistemas de seguridad y centrales de monitoreo. SIA significa "Security Industry Association" (Asociación de la Industria de la Seguridad) y DC09 se refiere a la versión del protocolo. Este protocolo establece un conjunto de reglas y formatos para transmitir información de eventos a una central de monitoreo. Este procolo es un estándar ampliamente utilizado por las mayoría de los softwares de monitoreo. Al ser una conexión IP no requiere de una receptora física ni ninguna otra interfaz de software para la recepción de los eventos. Puede profundizar más sobre el funcionamiento del protocolo en el apartado Protocolo SIA-DC09
  - El protocolo STA, es un protocolo propietario cerrado, utilizado por un software de monitoreo en particular. Si se tiene interés profundizar sobre este tema, pónganse en contacto con el área de soporte de Hellgrün.
- **IP Principal:** Es la dirección IP o dirección DNS del servidor de monitoreo al que el panel se conecta. Asegúrese de ingresar la dirección correcta del servidor de monitoreo, sin caracteres adicionales ni espacios.

- **Puerto Principal:** El número de puerto se representa como un valor numérico y puede variar entre 1 y 65535. La IP Principal y el número de puerto determinan la dirección de destino para establecer la conexión con el servidor de monitoreo.
- **IP Backup:** Es la dirección IP o dirección DNS del servidor de monitoreo de backup al que el panel se conecta luego de no poder concretar satisfactoriamente el envío del evento a la dirección principal. Si no se cuenta con servidor de backup, este campo debe quedar vacío.
- **Puerto Backup:** Es número de puerto se representa como un valor numérico y puede variar entre 1 y 65535. La IP de backp y el número de puerto de backup determinan la dirección de destino para establecer la conexión con el servidor de backup. Si no se cuenta con servidor de backup, este campo debe quedar vacío.

Parámetros de Teclado

En la imagen de abajo se muestra la configuración relacionada a las funcionalidades del teclado.



- **Tecla Fuego:** Selecciona la acción que tendrá lugar ante una alarma de Fuego
- **Tecla Pánico:** Selecciona la acción que tendrá lugar ante una alarma de Pánico.
- **Tecla Médica:** Seleccina la acción que tendrá lugar ante una situación de emergencia médica.

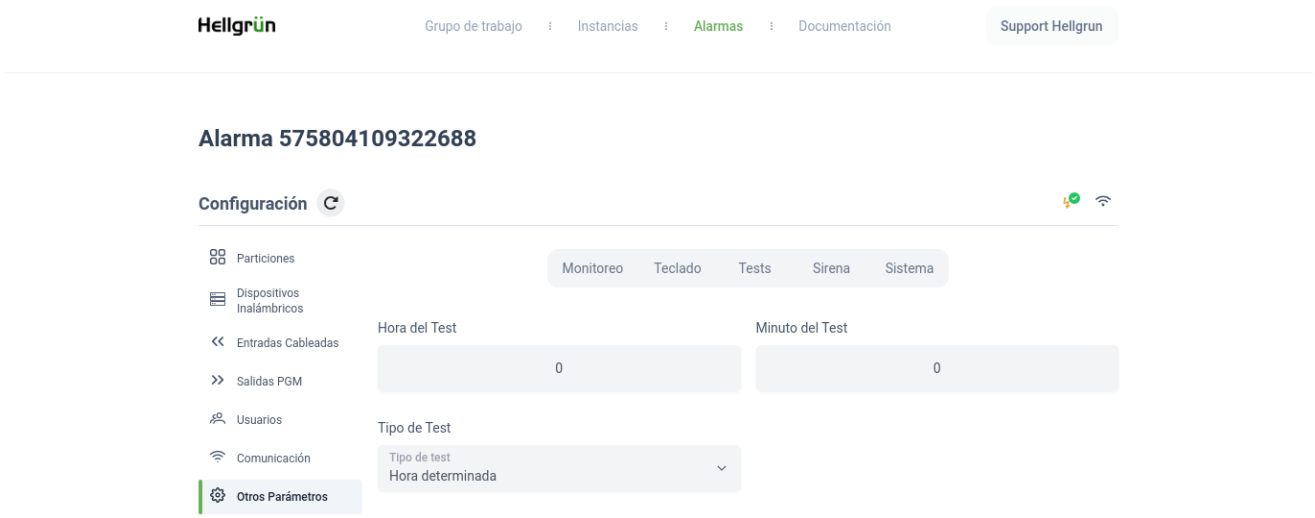
  `Las opciones "Silenciosa" o "Sirena Habilitada", se extiende al comportamiento de los llaveros.`

- **Teclado Audible:** Habilita a realizar un beep por segundo durante el tiempo de demora, de entrada o salida.

- **Salida Rápida:** Esta función permite a los usuarios salir de una propiedad sin desarmar la alarma. Ver más aquí
- **Aviso de conexión:** El teclado emite un beep cada vez que ocurre una falla en la conexión con el servidor cloud.
- **Código para excluir:** Define si para excluir una zona desde el teclado, es necesario o no ingresar la clave.
- **Armado Rápido:** Habilita a usar la opción de armado rápido sin contraseña, presionando la tecla asterisco y luego el cero. [*][0].
- **Aviso de armado:** La sirena sonará una vez al armar y dos veces al desarmar, cuando la acción es realizada desde el control remoto.
- **Aviso Comando App:** El teclado emite un beep cada vez que ejecuta un comando remoto desde la aplicación.

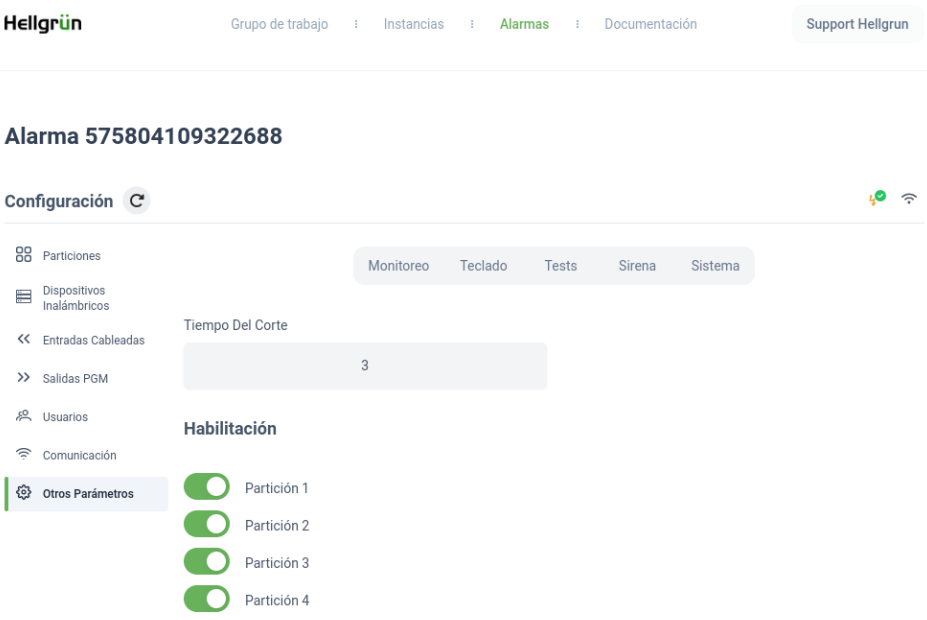
Configuración de Test Periódicos

En la imagen de abajo se muestra la configuración relacionado al envío de test periódicos a la estación de monitoreo.



- **Hora del Test:** Especifica el valor de la hora del reporte.
- **Minuto del Test:** Especifica el valor de los minutos.
- **Tipo de Test:** Permite seleccionar la forma en la que se generarán los test entre las diferentes opciones:
    - A la hora determinada: enviará un test diario, a la hora y minuto especificados.
    - Selectivo: igual que el anterior, pero sólo si el panel está armado.
    - Intervalo: enviará test periódicamente en intervalos de tiempo especificados en hora y minuto de test.
    - Intervalo selectivo: Igual que a Intervalo, pero sólo cuando el panel está armado.
    - Deshabilitado: No envía test.

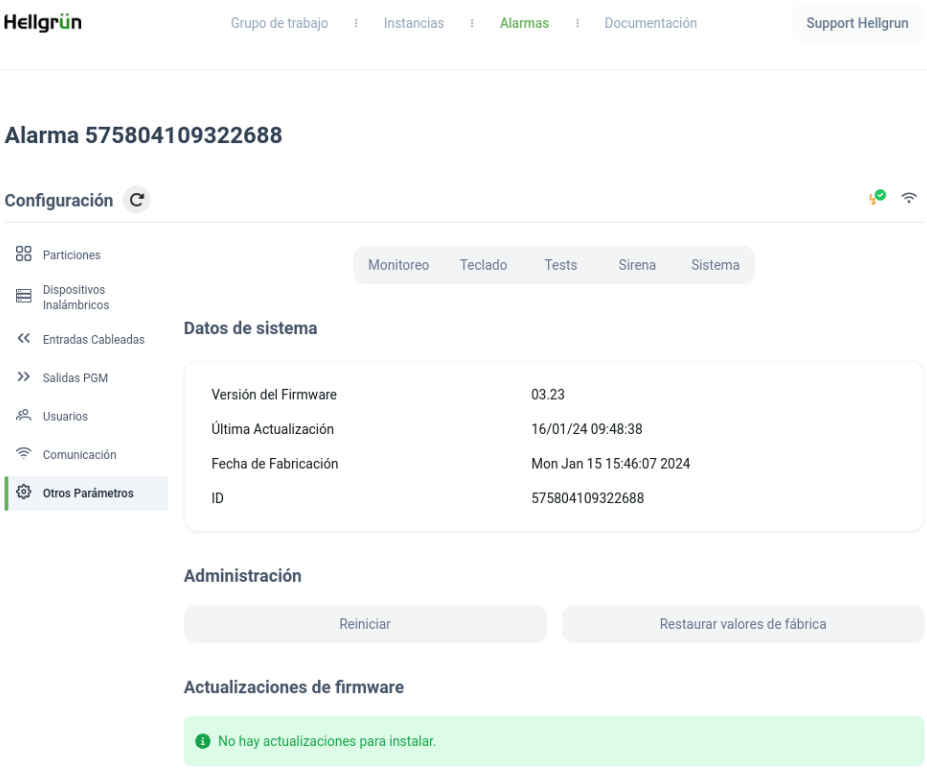
Configuración de la sirena



- **Tiempo del corte:** Estable el tiempo, en minutos, de activación de la sirena.
- **Habiltiación:** Permite especificar qué particiones podrá activar la sirena.

```
Es importante notar que si bien en el panel Kümmert posee una única salida de sirena, es
```

Parámetros de Sistema



- **Versión del Firmware:** Versión de firmware del panel.

- **Última actualización:** Fecha de publicación de la versión del firmware vigente.
- **Fecha de Fabricación:** Fecha en la que se fabricó el equipo
- **ID:** Número de serie del panel.
- **Reiniciar**: Reinicia el panel. Luego del reinicio, el panel continúa en el mismo estado que estaba previamente.
- **Restaurar valores de fábrica:** Aplica al borrado de la configuración total del equipo, pero no borra los datos de la red WiFi ni de los dispositivos inalámbricos vinculados. Esto es debido a que es un comando remoto, y el borrado de estos campos, sólo podría ser recuperado accediendo al panel.

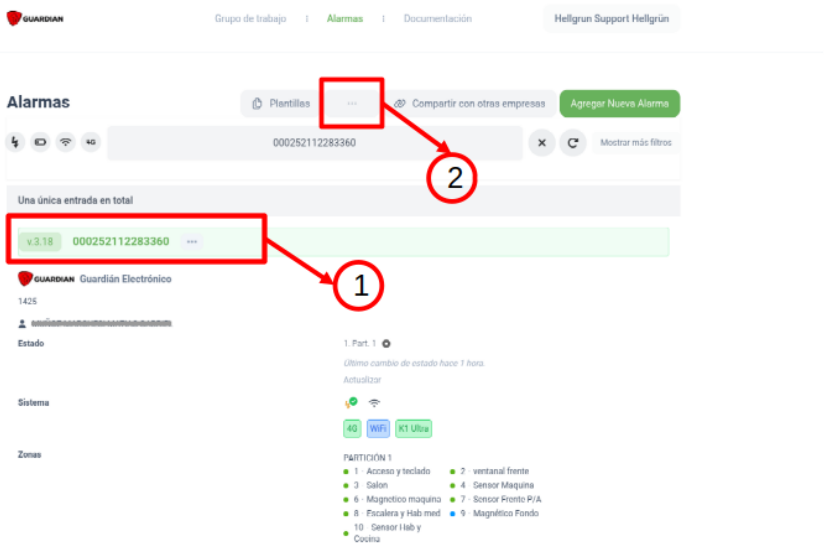
Actualización de Firmware de Paneles Kümmert

Procedimiento

Sólo usuarios con cierto nivel de acceso pueden realizar esta operación. El proceso de actualización es totalmente administrado por el panel y lo que aquí se hace se resume en sólamente dar una orden al panel para que inicie un proceso de auto-programación de su software con la versión que se encuentra en el sernvicor. De esta manera, se puede hacer un upgrade que implique el agregado de mejoras en la seguridad, nuevas funcionalidades, correcciones, etcétera.

Para que el panel pueda realizar esta acción, es necesario que se encuentre con conexión a internet vía WiFi. Esta operación no puede realizarse por vía 4G.

A continuación, se describe la secuencia de pasos para realizar la actualización:



En la parte izquierda de la imagen, bajo la referencia número 1, se muestra la versión actual del firmware del panel, junto al ID del mismo. Para iniciar la actualización, debe seleccionar el panel o paneles deseados haciendo clic sobre el ID correspondiente.

Al seleccionar un panel, se activará el botón señalado en la referencia número 2. Al hacer clic en este botón, aparecerá una opción denominada "Act. Firmware". Seleccione esta opción, y a continuación, se abrirá una ventana con un mensaje de advertencia sobre el proceso de actualización que está a punto de iniciar. Si está seguro de proceder, haga clic en "Actualizar Firmware". En ese momento, el panel comenzará a descargar el nuevo firmware desde el servidor y, una vez completada la descarga, procederá a auto-programarse con la nueva versión.

Este proceso asegura que su panel esté siempre actualizado con las últimas mejoras disponibles, garantizando así una mayor seguridad y rendimiento del sistema.

Consideraciones

El proceso de actualización del firmware es completamente autónomo y cuenta con diversos mecanismos de seguridad para garantizar su correcta ejecución. En caso de detectar cualquier problema, el sistema está programado para abortar automáticamente la operación como medida de precaución. Sin embargo, existe un margen de riesgo de que un error inesperado durante el proceso pueda causar una falla irreparable en el equipo.

Es importante tener en cuenta que la duración del proceso de actualización puede variar entre 5 y 10 minutos, dependiendo de la calidad de la conexión WiFi. Esta variabilidad se debe a las fluctuaciones en la velocidad de internet que pueden afectar el tiempo de descarga y la posterior instalación del nuevo firmware.

Se recomienda a los usuarios realizar estas actualizaciones en momentos en los que el dispositivo no sea crítico para sus operaciones diarias, y asegurarse de contar con una conexión WiFi estable y confiable para minimizar cualquier riesgo de interrupción.

Si la actualización no se completa con éxito, es posible que esto se deba a problemas de conectividad o a un uso intensivo del equipo durante el procedimiento. En tales casos, se recomienda intentar nuevamente la actualización en un momento posterior, asegurándose de que el dispositivo cuente con una conexión WiFi estable y que no esté siendo sometido a tareas que demanden un alto uso de sus recursos. Esta precaución ayuda a evitar conflictos que puedan interferir con el proceso de actualización y asegura una mayor probabilidad de éxito en la instalación del nuevo firmware.

Descarga Resumen PDF

Obtenga aquí el resumen de este apartado en PDF.

Descargar