

## Servidor ASTRA CSH (Complejo de hardware y software)



Plataforma para la recopilación de datos de telemetría y control remoto de sistemas de ingeniería.

### ¿Qué es Astra CSH?

Una plataforma en la nube para organizar un sistema de monitoreo unificado para objetos remotos a través de Internet.

### Nominación de Astra CSH

Comodidad adicional, seguridad y uso eficiente de la energía para los propietarios.

El hardware del servidor varía según la cantidad de objetos admitidos, así como otros factores.

### Características

El complejo está construido sobre la base de la "Plataforma de servidor multifuncional de alto rendimiento del sistema de monitoreo central", cuya base es el sistema operativo "Gentoo Linux", como el más productivo de toda la familia "Unix".

Su característica principal es que se suministra en códigos fuente, lo que permite, en primer lugar, usarlo en todas las plataformas de hardware existentes sin restricciones, desde supercomputadoras hasta dispositivos móviles, y en segundo lugar, tener un control total en términos de seguridad (en el sistema no es posible implementar marcadores con código fuente abierto, lo cual es especialmente importante a la luz de los últimos ataques de virus en computadoras de Windows, donde los atacantes usan marcadores establecidos por el fabricante).

La actualización del sistema operativo se lleva a cabo en forma de versión continua (Rolling-Release) sin una división clara en versiones, lo que le permite mantener todas las versiones en funcionamiento en el mismo estado actual.

Después de una larga prueba, el motor de base de datos InnoDB fue elegido como subsistema para almacenar información.

Para aislar los datos del acceso no autorizado, la plataforma del servidor proporciona acceso a ellos a través de interfaces estrictamente reguladas de los servicios correspondientes (y nunca directamente a través del DBMS o entre sí). Para esto, en el complejo como parte de la plataforma del servidor hay servicios correspondientes:

"Servicio de aplicaciones": está diseñado para intercambiar información con observadores (operadores de estaciones de trabajo, aplicaciones móviles y web de usuarios)

"Servicio de eventos", que proporciona el intercambio de información con los controladores de los sistemas de transferencia de información (STI) de dispositivos de objetos terminales

Los "controladores STI", que están aislados del DBMS a través del "Servicio de eventos" e implementan el intercambio de datos en los canales de comunicación del STI correspondiente y pueden implementarse tanto en hardware como en software, y en diferentes plataformas.

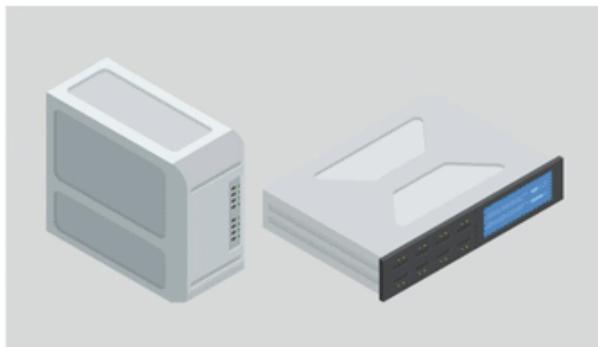
Astra CMS es un sistema multiusuario con delimitación estricta de los derechos de acceso por grupos de objetos y por roles de usuario.

Una plataforma de servidor puede proporcionar un funcionamiento independiente de varias organizaciones separadas o divisiones estructurales. Dentro de cada organización, se puede crear un número ilimitado de grupos separados: "dominios", que pueden ser centros de monitoreo y grupos de usuarios finales separados (por ejemplo, miembros de la familia que tienen acceso a un departamento compartido).

Se ha desarrollado un sistema único de transmisión de datos en un canal TCP constantemente abierto para CSH. Esto significa que el equipo Astra mantiene constantemente un canal de comunicación asíncrono abierto con el servidor y está listo para el intercambio en cualquier momento, independientemente de quién inicie el intercambio. Al mismo tiempo, esta funcionalidad se proporciona sin VPN adicionales, túneles, apertura de puertos IP en dispositivos terminales, así como sin el uso de direcciones IP "blancas".

Astra CSH está diseñado de tal manera que permite integrarse a cualquier STI existente lo antes posible, así como transmitir información a sistemas de procesamiento de información de terceros. Para estos fines, se han desarrollado interfaces estandarizadas y protocolos de intercambio de información: "Punto de interfaz con SPI" y "Punto de interfaz con AWP".

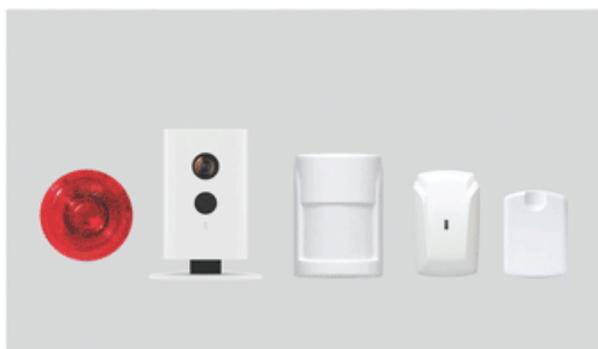
## Contenido de Astra CSH



4. Servidor de nube



3. Controlador inteligente Security Hub



2. Dispositivos inalámbricos



1. Servidores de cliente

### SERVIDOR DE LA NUBE

Parámetro	Medida
Sistema operativo	UNIX (Gentoo Linux)
Procesador	Intel Core i3
Memoria de acceso aleatorio	16 Gb
Unidad de estado sólido SSD	250 GB
Disco duro HDD	1 TB
Canales de conexión usados	LAN
Control de canales de conexión	constante
Cifrado de protocolo de interfaz	claves 128bit
Integración con otros servidores	iVideon, Firebase Cloud Messaging, Irbis, Surgard

## Datos técnicos

### Requisitos técnicos para los parámetros del servidor:

sistema operativo	UNIX (Gentoo Linux) que admite el mecanismo de ramificación POSIX.1c, extensiones de subprocesos (IEEE Std 1003.1c-1995)
la capacidad del procesador	es de 32 o 64 bits (compatible con x86 o ARM), para una implementación específica se recomienda utilizar la plataforma Intel x64 (familia de procesadores Core iX y Xeon de la cuarta generación de microarquitectura Haswell)
rendimiento del procesador	2 gigaflops
volumen de memoria de acceso aleatorio	1 GB
volumen de HDD / RAID	250x2 GB / software RAID por sistema operativo
velocidad de Ethernet	100 Mb / s

### Requisitos técnicos para los parámetros de PC para instalar ETA (Estación de trabajo automatizado):

sistema operativo	Windows 7 o posterior
otro software	.NET Framework 4.5 y superior
Procesador	Intel Core i3 de 1.4 GHz o superior o equivalente AMD
Memoria de acceso aleatorio	al menos 2 GB
Espacio en el disco duro al menos	50 MB
monitor (configuración recomendada): - diagonal - proporción de aspecto - permiso	20 pulgadas 16: 9 1920x1080

## Capacidad de Astra CSH:

controladores de abonado (de objeto), no menos de	1,000,000
aplicaciones de suscriptores, no menos de	300,000
sesiones simultáneas de interfaces web, no menos de	10000

## Soluciones:

### AVISO A TIEMPO:

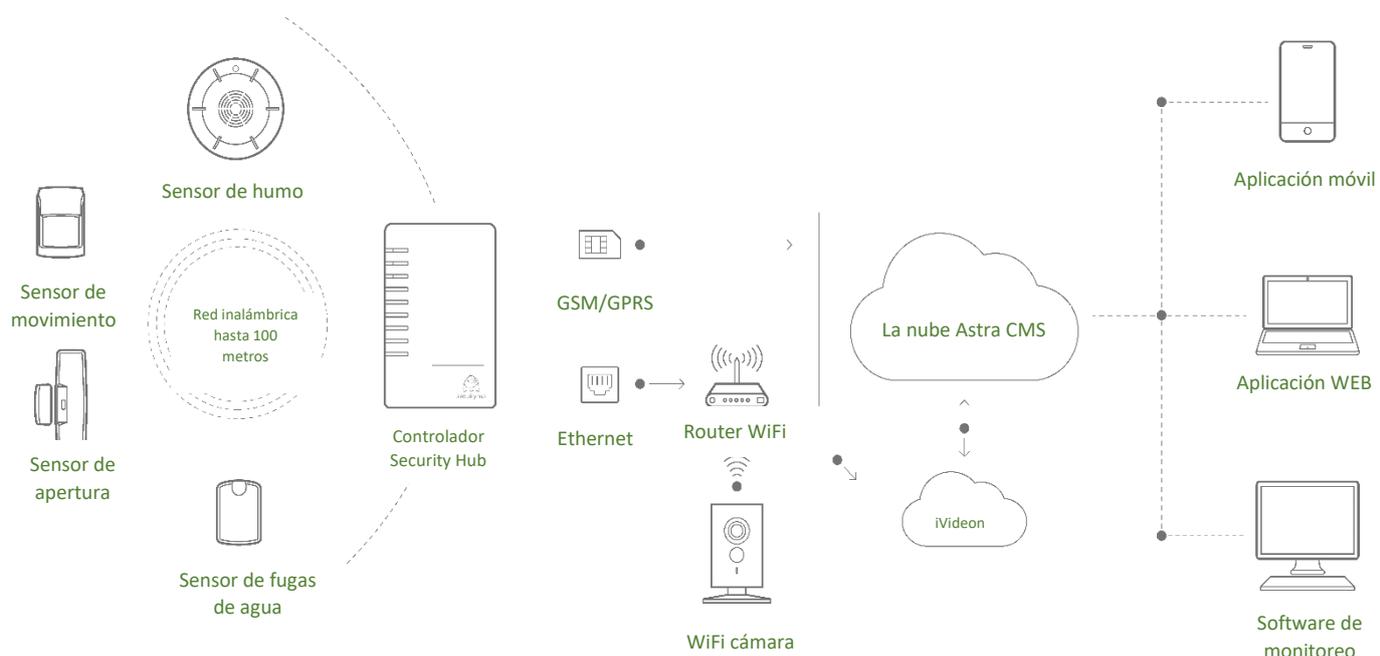
- sobre la intrusión y el fuego;
- sobre accidentes en el suministro de agua y cortes de energía;
- sobre cambios de temperatura y problemas en el sistema de calefacción.

### CENTRO DE MONITOREO UNIFICADO PARA:

- empresas de gestión y organizaciones de servicios;
- empresas policiales y de seguridad privada;
- Ministerio de Situaciones de Emergencia y departamentos de bomberos.

### VIDA SEGURA Y CÓMODA DE LOS PROPIETARIOS:

- control de iluminación, persianas y / o cortinas;
- climatización en apartamento



## Hospedaje en el servidor público SECURITY-HUB

Servicio	Integrador
Costo de suscripción	no
Cantidad de conexiones	hasta 1000
Aplicación móvil	gratis
Aplicación web	gratis
Software local de configuración, administración, rendición y gestión	gratis
Soporte técnico	24/7
Actualizaciones	si
Base de socios y anuncios en interfaz de software	si

Servicios	Más de 1000 conexiones	Al comprar 300 y más dispositivos de Security Hub
Precio de software	1000 \$	gratis
Instalación y activación de software	gratis	gratis
Aplicación móvil propia	gratis	gratis
Aplicación WEB	gratis	gratis
Software local de configuración, administración, rendición y gestión	gratis	gratis

Soporte técnico del servidor	<b>8/5</b>	<b>8/5</b>
Integración con software tercero (SurGuard)	<b>si</b>	<b>si</b>
Marca propia del controlador	<b>acordado</b>	<b>gratis</b>
Marca propia total, integración al procesos de negocio	<b>acordado</b>	<b>acordado</b>
Integración con plataformas programáticas de terceros	<b>gratis sin cambiar la estructura de plataforma</b>	<b>gratis sin cambiar la estructura de plataforma</b>
Acceso a las actualizaciones (anual)	-	-

## Descargar Astra CSH Client

El programa de cliente Astra CSH se puede descargar aquí: <https://dl.security-hub.ru/Test/public/install-1.4.0.1.exe>

## Sistema de monitoreo

Para comenzar, deberá introducir el nombre de usuario y la contraseña del administrador de la organización recibida del administrador del servidor público.

Autorización
✕



Login:

Contraseña:

Recordarme

Versión: 1.4.0.1

### **¡ATENCIÓN!**

¡Con la misma cuenta no se puede iniciar sesión desde diferentes dispositivos al mismo tiempo!

## Configurador

La estación de monitoreo Configurador Astra es una utilidad que permite configurar Astra CSH. Por ejemplo, configurar/cambiar las direcciones IP del servidor.

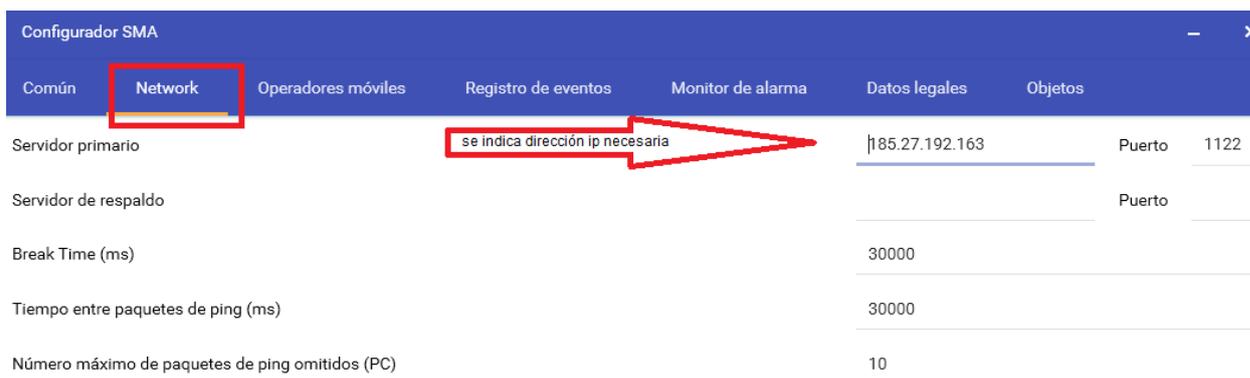
Al instalar la estación de trabajo Astra CSH, el acceso directo del configurador se instala en el escritorio de su computador.



Todas las configuraciones son predeterminadas, puede cambiarlas si es necesario.

Después de cambiar la configuración en el Configurador, haga clic en el botón "Guardar" y vuelva a ingresar a la estación de trabajo.

En la pestaña **Network**, puede cambiar la dirección del servidor. La configuración restante, con una buena conexión a Internet ( $\leq 10\text{Mb}$ ), recomendamos no modificarla.



En la pestaña **Registro de eventos**, active  en los campos que deben mostrarse.

Los eventos en objetos sin contratos: si lo opuesto es , los efectos sobre estos objetos no se producirán si no tienen un contrato válido.

Configurador SMA

Común Network Operadores móviles **Registro de eventos** Monitor de alarma Datos legales Objetos

Clave del evento  Mostrar

Ocurrencia  Mostrar

Origen del evento  Mostrar

Eventos en objetos sin contrato  Hide

El período de tiempo para el cual solicitar eventos 1

Informatividad Máximo Personalizar

Abrir

Save

En la pestaña **Datos legales**, es posible incluir campos como TIN, PSRN y CAT. Estos campos se muestran al crear organizaciones, contratos, contratistas.

Configurador SMA

Común Network Operadores móviles Registro de eventos Monitor de alarma **Datos legales** Objetos

Campo TIN  Habilitado

Campo OGRN  Habilitado

Campo PPC  Habilitado

Abrir

Save

## Creación de organizaciones

El administrador del servidor crea la organización en la estación de trabajo del administrador del servidor.

### Administrador del servidor

Administrador del servidor: es el usuario responsable de crear organizaciones de seguridad (Vigilante de seguridad, seguridad privada) que trabajan en un servidor público. Nombra administradores de organizaciones de seguridad.

### Estación de trabajo del administrador del servidor público

La estación de trabajo del administrador de un servidor público está diseñada para crear organizaciones que planean organizar la protección de objetos en un servidor público. Después de activar la función de administrador del servidor, el usuario tiene la oportunidad de llevar a cabo la creación de organizaciones, así como designar a sus administradores.

\*Al comprar el servidor propio, tiene posibilidad de crear organizaciones como un administrador general (super administrador)

### Crear usuarios de la organización

Los usuarios de la organización son creados por el administrador de la organización.

El ADMINISTRADOR DE ORGANIZACIÓN puede crear usuarios que no sean de dominio y usuarios de dominio.

#### Roles del servidor:

Administrador del servidor

Administrador del servidor: el usuario responsable de la creación de organizaciones de seguridad que trabajan en el servidor Astra CMS. Nombra administradores de organizaciones de seguridad.

*Derechos:*

- Crear y eliminar organizaciones.
- Gestión (creación / eliminación / edición) de usuarios de organizaciones y su visualización.
- Importar dispositivos al servidor.

*Roles Organizacionales:*

Administrador (organización)

Administrador de la organización: un usuario responsable de crear dominios y determinar su espacio de direcciones. Asigna administradores de dominio y crea usuarios entre dominios:

"Abogado", "Ingeniero" y "Operador". Es posible una combinación diferente de roles para un usuario. Todos los roles se pueden agregar al Administrador de la organización.

*Derechos:*

- Gestión de dominios
- Administrar usuarios de dominio.
- Organización de gestión local. La configuración regional en este contexto significa la elección del idioma.
- Asistente de creación de objetos: creación y delegación de objetos al dominio PTO.

Operador BCS (organización)

Operador BCS: un usuario que tiene la capacidad de ver dispositivos, eventos, delegaciones de objetos, en dominios que pertenecen a esta organización

*Derechos:*

Ver dispositivos, objetos, usuarios, delegaciones, eventos, etc.

Abogado (organización)

Abogado de la organización: trabajo precontractual y contractual con contratistas. Creación de un contrato para la protección de la instalación. Proporcionar un procedimiento para terminar objetos. La base de datos creada por este rol es utilizada por todos los dominios de la organización.

*Derechos:*

- Gestión de objetos (agregar / eliminar / editar).
- Gestión de contraparte.
- Gestión de contratos.
- Revocación de delegación de objetos.

Ingeniero (organizaciones)

Ingeniero de organización: un usuario que tiene los siguientes derechos: agregar, editar y eliminar dispositivos de objetos relacionados con esta organización; para vincular un dispositivo a un dominio, enviar comandos a un dispositivo, etc.

*Derechos:*

- Gestión de dispositivos (enlace al dominio, al objeto, desvinculación) y visualización.

- Envío de comandos al dispositivo.
- Renombrar / borrar zonas.
- Ver delegaciones.

### **Roles de dominio:**

#### Administrador (dominio)

Administrador de dominio - usuario - curador de dominio. Crea usuarios con los derechos de "estación de monitoreo de servicio", "operador", "ingeniero";

#### *Derechos:*

- Administrar usuarios de dominio.
- Ver y recordar delegaciones.

#### Operador (dominio)

Un operador de dominio es un usuario que organiza el trabajo con los clientes para garantizar que los objetos sean tomados bajo protección, procesamiento primario de mensajes de alarma y servicio, para su posterior transferencia al oficial de turno y al grupo de detención.

#### *Derechos:*

- Ver objetos, sus esquemas, programas de protección, dispositivos, eventos, etc.
- Gestión de alarmas:
- Tomando alarma para el procesamiento.
- Transferencia de una alarma al lugar de destino.
- Cerrando la alarma.
- Ver usuarios (organismos económicos) de un objeto delegado.

#### *Roles de dominio:*

#### Administrador (dominio)

Administrador de dominio - usuario - curador de dominio. Crea usuarios con los derechos de "estación de monitoreo de servicio", "operador", "ingeniero";

#### *Derechos:*

- Administrar usuarios de dominio.
- Ver y recordar delegaciones.

#### Operador (dominio)

Un operador de dominio es un usuario que organiza el trabajo con los clientes para garantizar que los objetos sean tomados bajo protección, procesamiento primario

de mensajes de alarma y servicio, para su posterior transferencia al oficial de turno y al grupo de detención.

*Derechos:*

- Ver objetos, sus esquemas, programas de protección, dispositivos, eventos, etc.
- Gestión de alarmas:
- Tomando alarma para el procesamiento.
- Transferencia de una alarma al lugar de destino.
- Cerrando la alarma.
- Ver usuarios (organismos económicos) de un objeto delegado.

Abogado (dominio)

Abogado de dominio: la funcionalidad del rol es similar a la del "abogado de la organización", limitada por el dominio.

*Derechos:*

- Gestión de objetos y visualización.
- Ver contrapartes.
- Ver contratos.
- Administre la delegación de objetos utilizando un motor de código.

Ingeniero (dominio)

Ingeniero de dominio: el usuario que fija la composición del equipo utilizado en el objeto protegido. Realiza análisis sobre falsos positivos y mantenimiento de rutina.

*Derechos:*

- Gestión de objetos, sus esquemas y visualización.
- Gestión de dispositivos (enlace al dominio, al objeto, desvinculación) y visualización.
- Renombrar / borrar particiones / zonas.
- Ver delegaciones.
- Gestión y visualización del cronograma de seguridad.
- Ver usuarios (organismos económicos) de un objeto delegado.

PTsO en servicio (dominio)

La estación de monitoreo en servicio: un usuario que tiene este rol puede administrar alarmas, es decir, tomar alarmas para su procesamiento, enviarlas al despertador, cerrar alarmas, etc.

*Derechos:*

- Gestión de alarmas

- Tomando alarma para el procesamiento.
- Aceptar una alarma del operador.
- Transmisión de alarma GZ.
- Cerrando la alarma.
- Ver objetos, dispositivos, eventos, horarios de seguridad, etc.

Hogar Autoridad (dominio)

Organismo económico: un usuario que tiene este rol puede enviar comandos a dispositivos, por ejemplo, tomar / quitar un objeto, etc.

*Derechos:*

Envío de comandos al dispositivo.

Grupo de detención (dominio)

Grupo de detención: el usuario que verifica el objeto protegido después del mensaje de alarma.

*Derechos:*

- Ver objetos, sus esquemas, programas de protección, dispositivos, eventos, etc.
- Gestión de alarmas
- Aceptación de una alerta para su procesamiento.
- Transmisión de alarma y apagado.

Despachador GZ (dominio)

GZ Manager: un usuario que recibe y procesa alarmas, transmite información sobre alarmas y también puede cerrar una alarma en nombre de GZ que están en el mismo dominio. Este rol funciona simultáneamente con el rol de Duty CCO.

*Derechos:*

- Ver objetos, sus esquemas, programas de protección, dispositivos, eventos, etc.
- Gestión de alarmas
- Aceptación de una alerta para su procesamiento.
- Transmisión de alarma y apagado.

**Crear un usuario de dominio y usuario de aplicación móvil**

**Creación de dominio**

La creación de un dominio se realiza el administrador de la organización.

Panel de vigilancia centralizada del Sistema de Protección Inalámbrica Astra -diliwoo5@gmail.co

Sesión Administrador Asesor Operador Oficial de guardia Ingeniero Informes Ivideon

Instalación(es) x Usuarios x



	NOMBRE	LOGIN	DATOS DE CONTACTO
>	diliwoo5@gmail.com	diliwoo5@gmail.com	
	Dilyara	dh	
	Stand	Stand	

Crear un nuevo usuario x

Nombre:

Login:

Contraseña:

Datos de contacto:

Teléfono:

Activo:

Roles

- Operador del Punto de Vigilancia Remota:
- Operador de guardia de la consola de seguridad centralizada:
- Ingeniero:
- Responsable administrativo:
- Asesor del dominio:
- Grupo de Intervención:
- Gestor del Grupo de Intervención:

## Añadir un objeto

El usuario añade una instalación con los roles de Abogado de la organización o Abogado del dominio.

En la pestaña "Instalaciones", seleccione el icono de añadir la instalación.



Introducimos el nombre de instalación bajo el contrato, determinamos su tipo, categoría e ingresamos su dirección.

Para ingresar la dirección, se utiliza el clasificador ruso KLADR, debe ingresar de 4 a 5 letras del nombre de la ciudad y SELECCIONAR el nombre propuesto de la lista. Sin ESPACIOS, ingrese el nombre de la calle. Introducimos el número de la casa y el apartamento en orden habitual. A continuación se muestra un cuadro para comentarios, si es necesario, puede escribir información adicional sobre la instalación.

Haga clic en el botón "Guardar".

Crear instalación

Denominación:

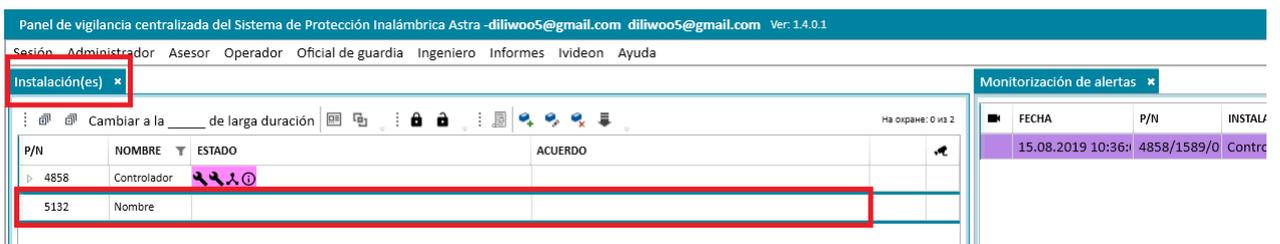
Tipo:

Categoría:

Dirección:

Comentario:

Nueva instalación creada con éxito. Aparecerá en la pestaña "Objetos".



## Añadir un dispositivo (Security Hub)

La adición de un dispositivo se realiza en el Astra CMS por un usuario con el rol de Ingeniero de Dominio.

En la pestaña "**Dispositivos**", seleccione el icono Añadir dispositivo al dominio.

Sesión Administrador Asesor Operador Oficial de guardia Ingeniero Informes Ivideon Ayuda

Dispositivos x

Monitorización de alertas x

P/N	NOMBRE	DOMINIO	RETRASO	TIPO	ESTADO
1589	SecurityHub.1.83	Controlador	dilivoo5@gmail.com		<ul style="list-style-type: none"><li>🔴 Pérdida de conexión (1589, Todo el dispositivo (0), 0)</li><li>🔴 Pérdida de conexión (1589, General door (2), cso (6))</li><li>🔴 Avería del canal de comunicación GSM (1589, Kit (0))</li><li>🟡 Actualización lista para su utilización (1589, Kit (0), S</li></ul>

FECHA	P/N	INSTALACIÓN
15.08.2019 10:36:	4858/1589/0	Controlador

La base del identificador al agregar el dispositivo terminal "Security Hub" es el código de barras ubicado en la placa del dispositivo.

Hay dos tipos de códigos de barras en un dispositivo:

1. El código de barras de un dispositivo lanzado antes de enero de 2019 se ve así:



Complete: dirección del dispositivo - número de serie del dispositivo, código PIN - últimos 4 dígitos en el código de barras del dispositivo. Y seleccione el clúster ("Security Hub o Astra Pro 4.0"). Haga clic en el botón "Añadir".

Asociar el dispositivo al dominio
✕

Dirección (cuenta) del dispositivo:

Código PIN:

Cluster:

2. El código de barras de un dispositivo lanzado desde enero de 2019 se ve así:



Complete: dirección del dispositivo - número de serie del dispositivo, código PIN - últimos 4 dígitos en el código de barras del dispositivo. Y seleccione el clúster ("Security Hub o Astra Pro 4.0"). Haga clic en el botón "Agregar".

Asociar el dispositivo al dominio
✕

Dirección (cuenta) del dispositivo:

Código PIN:

Cluster:

### Vinculación del dispositivo al objeto

En la pestaña "**Dispositivos**", haga clic con el botón derecho para vincular el dispositivo al objeto.

Sesión Administrador Asesor Operador Oficial de guardia Ingeniero Informes Ivideon Ayuda							
Dispositivos *							
P/N	NOMBRE	TIPO	Asociar el dispositivo a la instalación	DOMINIO	RETRASO	TIPO	ESTADO
1589		SecurityHub.1.83	Controlador	diliwoo5@gmail.com			<ul style="list-style-type: none"> <li>Pérdida de conexión (1589, To</li> <li>Pérdida de conexión (1589, G</li> <li>Avería del canal de comunicac</li> </ul>

Aparece una ventana en la que en nuestro dispositivo seleccionamos instalación deseada de la lista. Haga clic en "Asociar el dispositivo".

**Asociación del dispositivo a la instalación** ✕

Dispositivo:  Instalación:

Desvincular dispositivo del dominio

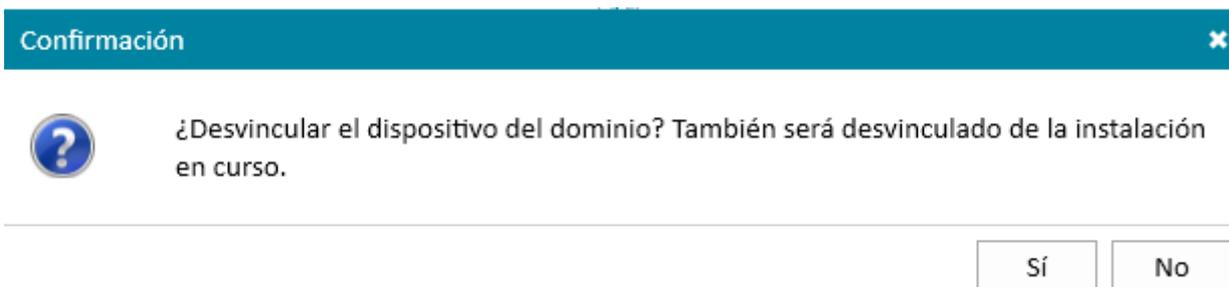
**ATENCIÓN!**  
 ¡Al desvincular el dispositivo del dominio, también se desvinculará de instalación actual!

Para desvincular el dispositivo del dominio:

1. Va a la pestaña "Dispositivos".
2. Seleccione el dispositivo necesario pulsando clic derecho y seleccione Desvincular dispositivo del dominio.

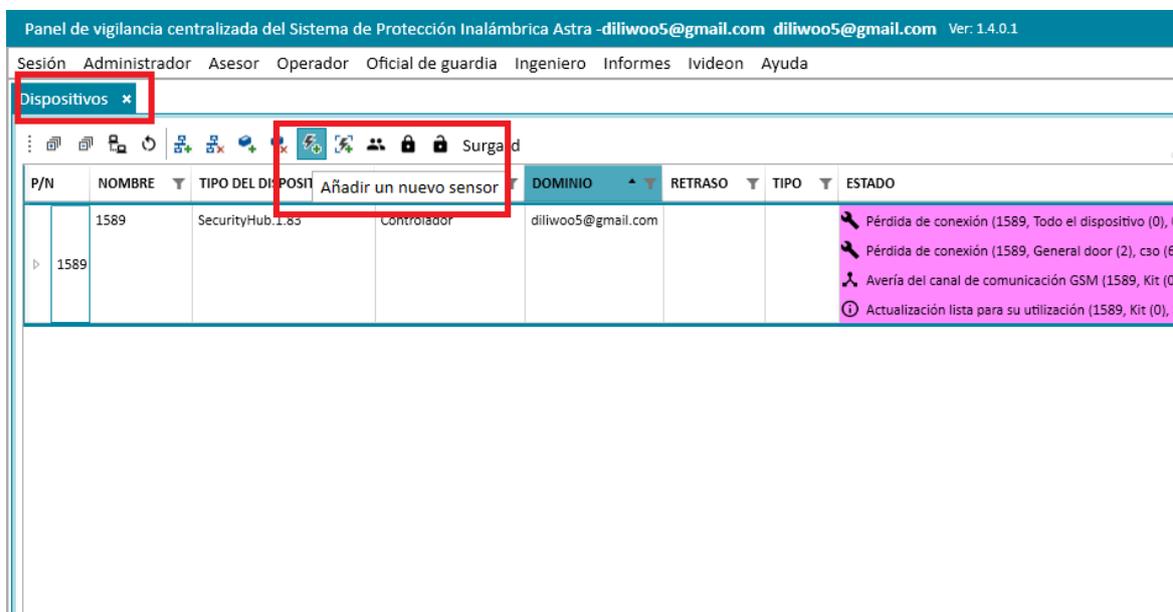
Panel de vigilancia centralizada del Sistema de Protección Inalámbrica Astra -diliwoo5@gmail.com diliwoo5@gmail.com Ver: 1.4.0.1						
Sesión Administrador Asesor Operador Oficial de guardia Ingeniero Informes Ivideon Ayuda						
Dispositivos *						
P/N	NOMBRE	TIPO	Desvincular dispositivo de la instalación	RETRASO	TIPO	ESTADO
1589		SecurityHub.1.83	Controlador	diliwoo5@gmail.com		<ul style="list-style-type: none"> <li>Pérdida de conexión (1589, Todo el dispositivo (0), 0</li> <li>Pérdida de conexión (1589, General door (2), cso (6)</li> <li>Avería del canal de comunicación GSM (1589, Kit (0), S</li> <li>Actualización lista para su utilización (1589, Kit (0), S</li> </ul>

3. A continuación, aparecerá una ventana de confirmación. Haz clic en el botón Sí.



## Conexión del sensor inalámbrico

En la pestaña "Dispositivos", haga clic con el botón derecho para vincular el sensor.



Aparece una ventana donde elegimos que sensor conectamos con cable o inalámbrico.

Haga clic en el botón "Añadir usuario / zona inalámbrica".

Modo interactivo

Entrada en el modo interactivo

Seleccione la acción necesaria

Espera

Añadir la zona conectada con cable    **Añadir zona inalámbrica**    Cancelar

El programa ofrece salir del dispositivo en modo interactivo. Haga clic en el botón "Confirmar".

El dispositivo está intentando interactivamente detectar el sensor.

Modo interactivo

Entrada en el modo interactivo

Para entrar en el modo interactivo presione el botón CONFIRMAR

Espera

**Aplicar**    Cancelar

## Modo interactivo

Entrada en el modo interactivo

Enviado e comando de entrada en el modo interactivo, se espera la respuesta del dispositivo...

Espera

Aplicar

Cancelar

Insertamos la batería al sensor. Cuando el sensor esté detectado. Lo nombramos y seleccionamos una sección para ello. Para la sección de seguridad, es posible seleccionar un retraso\* para armado/ desarmado.

---

\*El retraso de entrada es el tiempo después del cual el sensor se enciende después de armarlo. En el Centro de seguridad: a la entrada de 45 segundos y a la salida de 60 segundos. (Permite, por ejemplo, activar el armado en el panel y salir de la habitación antes de que suene la alarma).

Presione el botón "Asociar". Aparece un mensaje de que el sensor se agregó correctamente.

El sensor conectado se muestra en la pestaña "Dispositivos" en su zona.

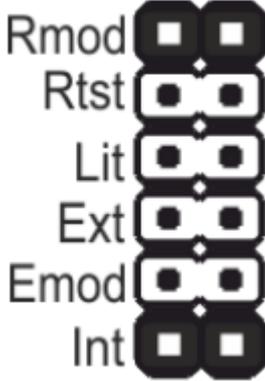
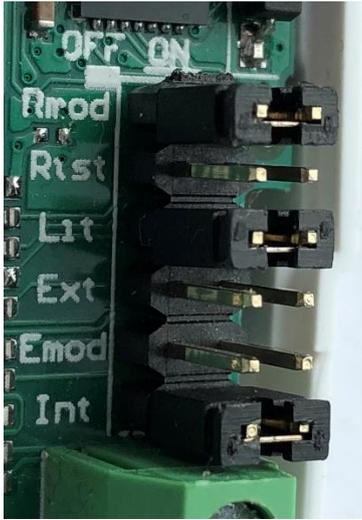
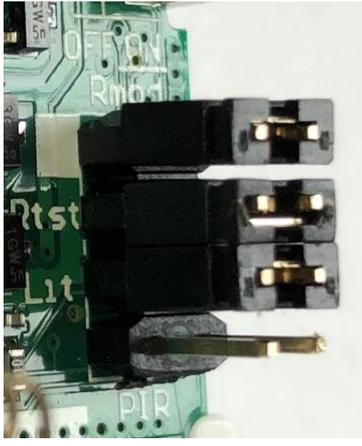
### ATENCIÓN!

Asegúrese de que los puentes y los caracteres de los sensores estén en la posición correcta.

### La posición de los puentes en los detectores para conectarse al Security Hub

Security Hub puede operar en 2 frecuencias 433.42 MHz y 434.42 MHz. La frecuencia de funcionamiento del DOE depende de la fecha de lanzamiento de Security Hub. Además, la frecuencia de funcionamiento del DOE se puede cambiar a través de la utilidad Localconfig.

Al agregar un sensor al sistema, debe asegurarse de que la ubicación de los puentes del sensor corresponda a la frecuencia de funcionamiento del Security Hub.

Nombre del sensor	Letra 1 (433,42 MHz)	Letra 3 (434,42 MHz)
<p data-bbox="347 241 529 286"><b>Astra-3321</b></p> 	 <p data-bbox="746 313 1011 694">Diagram showing terminal connections for Astra-3321: Rmod, Rtst, Lit, Ext, Emod, Int.</p>	 <p data-bbox="1107 237 1469 757">Photo of the terminal block for Astra-3321, showing connections for Rmod, Rtst, Lit, Ext, Emod, Int.</p>
<p data-bbox="347 810 529 855"><b>Astra-5121</b></p> 	 <p data-bbox="663 891 1088 1422">Photo of the terminal block for Astra-5121, showing connections for Rtst, Lit, and PIR.</p>	 <p data-bbox="1107 976 1469 1422">Photo of the terminal block for Astra-5121, showing connections for Rtst, Lit, and PIR.</p>

## Características funcionales

Registro en memoria no volátil de hasta 30 números de serie de sensores del sistema Astra-RI-M;

Proporciona intercambio de información con aplicaciones móviles y web a través del servidor:

1. A través de un canal cableado, a través de un conector RJ45 (Ethernet 10 BASE-T) y la red del proveedor,
2. A través de un canal inalámbrico, a través de dos tarjetas SIM (GPRS / EDGE) de un operador móvil GSM;

## Parámetros técnicos del canal de radio.

Security Hub (2.0) lanzado desde marzo de 2019:

Frecuencia de operación, MHz..... 433.42 MHz (letra “1”)

Radio del canal de radio, m, no menos de ..... .100 (en visibilidad directa)

Potencia de radiación, mW, no más de ..... 10

Security Hub (2.0) lanzado hasta marzo de 2019:

Frecuencia de operación, MHz ..... 434.42 MHz  
(letra “3”)

Radio del canal de radio, m, no menos de .....100 (en visibilidad directa)

Potencia de radiación, mW, no más de ..... 10

Para el trabajo conjunto de los detectores del sistema de canales de radio Astra RI-M y el Security Hub (2.0) UOO (emitido desde marzo de 2019) como parte de Astra CMS, es necesario establecer el modo de operación en "2" y la letra de frecuencia "1" para los detectores. El cambio del modo de funcionamiento y la letra de frecuencia se realiza de acuerdo con el manual de funcionamiento de los detectores del sistema de canales de radio Astra RI-M.

## Fuente de alimentación

El suministro de energía eléctrica del dispositivo terminal se lleva a cabo:

Desde la entrada USB 2.0 tipo V con un voltaje nominal de 5 V y una corriente de 1 A (adaptador de red), cable USB 2.0 AM-BM marcado 28 AWG / 2C + 24 AWG / 2C, longitud de hasta 1,5 m.

Desde fuentes de alimentación externas con voltaje de 12 V (a través de terminales “+ 12V” y “+ 12VR”).

En ausencia de una fuente de alimentación externa de la fuente de alimentación redundante incorporada, una batería de iones de litio de tamaño estándar 2 / 3A con un voltaje nominal de 3.7 V, una capacidad de 600 o 700 mA / h (suministrada).

La batería se usa solo como fuente de alimentación de respaldo (hasta 8 horas), para encender el dispositivo que necesita para conectar la alimentación externa.

Corriente nominal de consumo del dispositivo durante la fuente de alimentación:

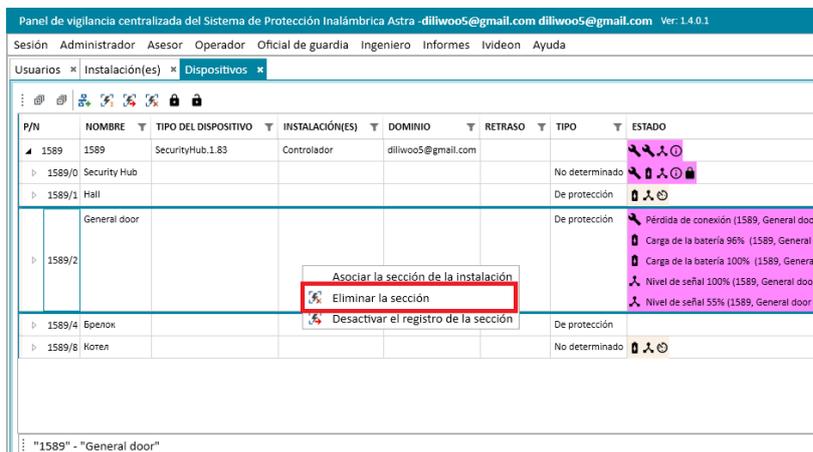
- desde el puerto USB - 200 mA (máximo 500 mA);
- de la batería: no más de 50 mA;
- a través de los terminales "+ 12V" y "+ 12VR" - 150 mA (máximo 300 mA).

## Eliminación del sensor

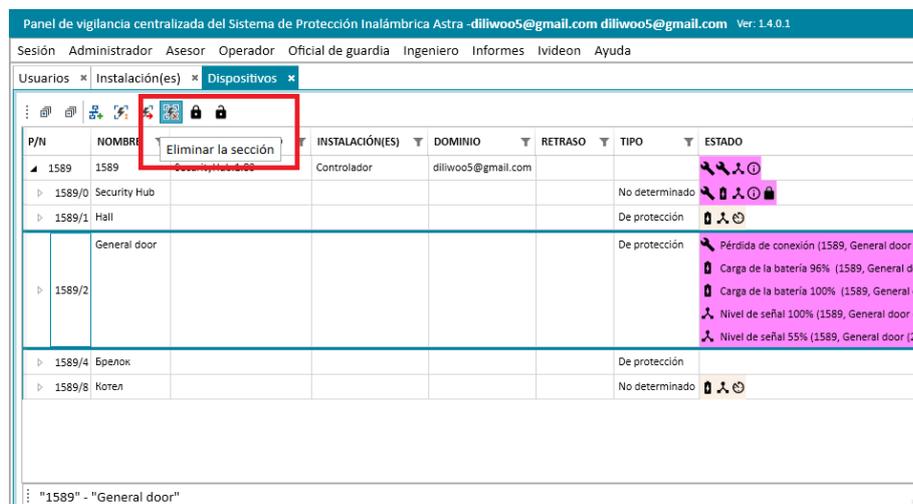
1. Debe asegurarse de que el objeto esté desarmado.
2. Primero, el sensor debe ser desatado de la sección. Para hacer esto, vaya a la pestaña "Dispositivos" y seleccione el sensor que necesita ser desatado.

### Hay dos maneras de eliminar el sensor:

- Elige el sensor que desea eliminar y haga clic con botón secundario, seleccione "desatar el sensor".



- Elige el sensor y en la parte superior, seleccione el icono "Desvincular sensor".



## Preguntas frecuentes del programa

*No puedo cambiar el nombre de la sección en la aplicación.*

Para garantizar que se realicen cambios, el sistema debe desarmarse y mantenerse en contacto.

*Cuando la batería está instalada, el indicador del sensor no responde*

Compruebe que la batería suministrada o que coincida con el pasaporte del dispositivo.

Verifique que la batería esté instalada con la polaridad correcta.

Intente usar una instancia diferente de la batería.

*¿Por qué, cuando apago la alimentación principal con la alimentación de respaldo instalada (batería), el controlador pierde la conexión con la nube?*

Al desconectar el adaptador de corriente, el canal Ethernet no funciona. Toda la comunicación con la nube se realiza a través del canal GPRS. La batería está diseñada para respaldar la potencia del controlador solo cuando se trabaja con tarjetas SIM. Se recomienda instalar una tarjeta SIM.

Es posible que la batería esté descargada o que no haya tenido tiempo de cargarse.

*¿Por qué al desconectar Internet y GSM no hay señal de pérdida de comunicación con el objeto?*

Para excluir mensajes sobre la pérdida de canales de comunicación asociados con una calidad de comunicación variable, se emite un mensaje sobre la pérdida de comunicación con el objeto después de 10 minutos de la ausencia de respuestas del objeto. La pérdida de comunicación en uno de los canales se emite instantáneamente.

*Conéctese a un enrutador con un módem Yota.*

En la configuración del enrutador, habilite DHCP y abra el puerto 2222. El controlador verifica constantemente los canales de comunicación con el servidor; si la conexión no es estable en el área donde se encuentra el objeto, recomendamos cambiar el operador.pac

*El controlador (objeto) no se agrega*

La base del identificador al agregar el dispositivo terminal Security Hub es el número de serie ubicado en la placa del dispositivo.

Asegúrese de que la dirección del dispositivo y el PIN se ingresen correctamente, así como en la selección del clúster. La dirección del dispositivo consta de los primeros 4 dígitos, después de ceros, el número

del dispositivo. Código PIN: los últimos 4 dígitos del dispositivo. Grupo seleccione "Security Hub o Astra Pro 4.0".

## **Especificaciones del sistema**

*¿Cuál es el rango de sensores?*

El alcance de los sensores en la línea de visión no es inferior a 100 metros.

*¿Cuál es el número máximo de sensores que se pueden conectar a un controlador?*

El número máximo de sensores que se pueden conectar al sistema no puede exceder de 30 a 16 llaveros.

*¿Qué sensores son compatibles con el controlador?*

El captador de la apertura de la puerta Astra-3321

El sensor de movimiento que no responde a los animales (hasta 20 kg.) Astra-5121

El sensor de movimiento "cortina" para bloquear las aberturas de puertas / ventanas Astra-5131 A

El sensor de movimiento para la instalación en el techo Astra-7 ver. RC

Sensor combinado de movimiento y rotura de cristales para instalación en techo Astra-8 ver. RC

Sensor de humo Astra-421 RC

Sensor de rotura de cristales Astra-6131

Sensor de fugas de agua Astra-361 ver. RC

Sensor de temperatura Astra-3731

Sirena Astra-2331

Bloque de relé Astra-8231

Botón de pánico Astra-3221

Mando a distancia con la función del botón de pánico Astra-RC

*¿Cuántas particiones puedo crear?*

Hasta 8 secciones en el rango de 1 a 8.

*¿Con qué operadores trabaja el controlador?*

El controlador funciona con todos los proveedores de operadores de comunicaciones por Internet y GSM por cable, y las velocidades de Internet GPRS (2G) son suficientes para establecer comunicación con el servidor.