

# Remote System Management

CBS-RM-DIPx





# Contenido

1	<b>Funciones principales</b>	<b>4</b>
2	<b>Requisitos del sistema</b>	<b>5</b>
3	<b>Aplicación web</b>	<b>6</b>
4	<b>Documentación</b>	<b>7</b>
5	<b>Componentes de software de código abierto</b>	<b>8</b>
6	<b>Alojamiento de servicio</b>	<b>9</b>
7	<b>Nivel de servicio y mantenimiento</b>	<b>10</b>
8	<b>Obligaciones del cliente y del usuario</b>	<b>11</b>
9	<b>Información relacionada con el RGPD</b>	<b>12</b>

# 1 Funciones principales

El servicio Remote System Management de Bosch le permite aprovechar la potencia del Internet de las cosas (IoT) a fin de ofrecer una gestión de activos segura, transparente y rentable durante el ciclo de vida de un sistema de vídeo. Este servicio permite a los usuarios finales, integradores de sistemas e instaladores realizar la gestión de inventario y actualizaciones, así como tareas de supervisión del estado de todo un sistema de vídeo de Bosch (DIVAR IP + BVMS + cámaras) desde una plataforma Remote Portal centralizada.

El servicio brinda tranquilidad a los clientes finales al permitir la supervisión del sistema las 24 horas del día, de forma segura. Esto permite al usuario actuar de forma proactiva cuando surgen problemas y solucionarlos, por ejemplo, antes de que se pierdan las grabaciones de vídeo por un fallo del disco duro. La conexión segura MQTTS también mantiene la privacidad de los datos, ya que nadie puede acceder a las grabaciones de vídeo a través de esta conexión, debido a que este protocolo no admite la transferencia de datos de vídeo e imágenes. Además, el servicio permite actualizaciones remotas de software y firmware, lo que mantiene el sistema actualizado y seguro. La conectividad en la nube se basa en una única conexión saliente desde DIVAR IP a Remote Portal, donde DIVAR IP consolida todas las comunicaciones entrantes y salientes de todo el sistema de vídeo.

El servicio está diseñado para grandes organizaciones de clientes finales que realizan su propio mantenimiento de sistemas en múltiples emplazamientos dispersos o para instaladores que ofrecen estos servicios a una gran variedad de clientes finales. Las ventajas de utilizar Remote System Management se centran en una mayor eficiencia a la hora de realizar las tareas de mantenimiento del sistema, evitando desplazamientos innecesarios in situ gracias a las funciones de mantenimiento remoto, como el despliegue de actualizaciones en caso de aviso de seguridad o a la información más reciente sobre el sistema, que permite preparar mejor los desplazamientos in situ. Efecto colateral positivo: servicio completo con emisiones de CO<sub>2</sub> mínimas. Además, los usuarios pueden mejorar la experiencia de servicio que ofrecen actuando de forma proactiva y teniendo la oportunidad de resolver los problemas sobre el terreno antes de que los clientes (internos) se den cuenta siquiera de que tienen un problema.

Para conocer los detalles funcionales, consulte las hojas de datos correspondientes del servicio.



## **Aviso!**

Encontrará las fichas técnicas en el catálogo de productos correspondiente a su región o país.

## 2 Requisitos del sistema

### Requisitos de software

La interfaz web Remote Portal se puede usar con modernos navegadores web compatibles con HTML5. Para disfrutar de la mejor experiencia, Bosch recomienda utilizar Google Chrome.

### Requisitos del dispositivo

Para usar Remote System Management al máximo, las cámaras IP de Bosch tienen que funcionar con la versión de firmware 6.50 o posterior.

Tal como se indica en la hoja de datos, solo se admiten modelos DIVAR IP concretos. Para estos modelos, el requisito mínimo de software es la compatibilidad con DIVAR IP System Manager 2.0 o una versión posterior. Consulte las hojas de datos correspondientes para obtener más información.

El ancho de banda requerido depende de las especificaciones del sistema de vídeo y de la estructura del emplazamiento, es decir, el número de cámaras y dispositivos DIVAR IP en el emplazamiento. Bosch recomienda un ancho de banda mínimo de 11 Mbps o 1,31 MBps por DIVAR IP, ya que el DIVAR IP consolida la comunicación de entrada y salida para sí mismo y las cámaras conectadas. Esta recomendación se basa en el caso de uso más exigente en términos de ancho de banda, a saber, la descarga de archivos de actualización de mayor tamaño que crean un pico de demanda de ancho de banda cada vez que dichas actualizaciones se activan desde Remote Portal. La mayor parte del tiempo de funcionamiento valle demandará anchos de banda de unos 10 Kbps, por ejemplo, para control de parámetros de estado y otros intercambios de datos telemétricos.

---

### Aviso!



Este requisito de ancho de banda puede variar y el usuario debe verificar que el ancho de banda disponible cumple los requisitos de la aplicación. Bosch facilita varias herramientas para calcular el ancho de banda necesario, pero no se hace responsable de la disponibilidad real del ancho de banda ni de su correcta configuración.

---

## 3 Aplicación web

Remote System Management se integra con Remote Portal, que sirve de plataforma web central para la activación del servicio y otras funciones generales, independientes de la oferta de servicios, como se describe a continuación.

### Gestión del sistema y de dispositivos con una vista de panel de control

Los sistemas y dispositivos individuales pueden agruparse por orden jerárquico para adaptarse a la ubicación del cliente o de la instalación, limitar el acceso de un conjunto de dispositivos o agregar el estado de varios dispositivos.

### Descripción del servicio

La sección "Servicios" en Remote Portal ofrece una descripción de todos los servicios disponibles en los distintos tipos de dispositivos. Cada servicio mostrará una lista consolidada de todos los dispositivos y sistemas en los que se utiliza activamente.

### Gestión de licencias de servicio

Los servicios se pueden activar visitando Remote Portal después de la puesta en servicio inicial del DIVAR IP a Remote Portal.

El servicio Remote System Management requiere licencias para su activación. En función del modelo DIVAR IP y del modo de funcionamiento, se aplican distintas licencias. Compruebe las hojas de datos para obtener información. Las licencias se gestionan y activan en Remote Portal en la sección "Licencia de servicio".

### Gestión de usuarios

Remote Portal permite un control preciso del acceso a los dispositivos y servicios. Mediante la gestión de roles, los *administradores*, *técnicos* y *usuarios finales* pueden asociarse individualmente a sistemas, grupos y servicios.

---

### Aviso!



Para obtener más información sobre Remote Portal visite la página de productos correspondiente disponible en: <https://commerce.boschsecurity.com/gb/en/Remote-Portal/p/86180387339/>

---

## 4 Documentación

La documentación de usuario y las hojas de datos de todos los sistemas individuales basados en DIVAR IP se puede encontrar y acceder a la misma desde aquí:

Formaciones técnicas: <https://academy.boschsecurity.com/>

**NOTA:** estará disponible una formación de introducción de Remote System Management independiente. Esta formación se integrará posteriormente en la formación para certificación de DIVAR IP all-in-one.

Notas de instrucciones/  
configuración: [https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt\\_community-tkb-video/label-name/remote\\_system\\_mgmt?labels=remote\\_system\\_mgmt](https://community.boschsecurity.com/t5/Security-Video/tkb-p/bt_community-tkb-video/label-name/remote_system_mgmt?labels=remote_system_mgmt)

Notas de hojas de datos/  
aplicación: <https://commerce.boschsecurity.com/gb/en/bt/search/?text=cbs-rm-dip>

## 5 Componentes de software de código abierto

Los componentes de software de código abierto incluido en la plataforma de Remote Portal pueden encontrarse aquí: [https://remote.boschsecurity.com/open\\_source/open\\_source\\_licenses.txt](https://remote.boschsecurity.com/open_source/open_source_licenses.txt)

## 6 Alojamiento de servicio

Los servicios que figuran en esta lista están alojados en la infraestructura como servicio de AWS.

La aplicación Remote Portal es una plataforma global multiinquilino. Esta plataforma, su base de datos, backend y frontend están alojados en la región de AWS de Fráncfort, Alemania.

## 7 Nivel de servicio y mantenimiento

Bosch ofrece un contrato de nivel de servicio (SLA) específico para los distribuidores autorizados de Remote System Management de Bosch. Este SLA describe detalladamente la disponibilidad garantizada, el mantenimiento y el proceso de soporte técnico Remote System Management de Bosch e incluye datos de contacto para líneas directas de emergencia, cláusulas de penalización, etc.

Póngase en contacto con su representante de ventas local para obtener más información.

## 8 Obligaciones del cliente y del usuario

Para los clientes directos de Bosch se requiere la aceptación de los Términos y Condiciones para Revendedores de Software como Servicio para poder obtener licencias o suscripciones de Remote System Management. Para la activación de licencias de servicio o suscripciones, los usuarios deben aceptar los términos y condiciones de Remote Portal. Entre otras obligaciones se incluyen:

- 8.1. La conexión a Internet entre los clientes, su centro de monitorización/sala de control y el lugar de instalación de los dispositivos compatibles (incluidas las cámaras de vídeo, en lo sucesivo denominadas "Dispositivos") hasta la interfaz de Internet del centro de datos utilizada por Bosch, así como la relación final entre el cliente y sus socios contractuales son responsabilidad exclusiva de los clientes.
- 8.2. La instalación, el funcionamiento, el mantenimiento y, en caso necesario, la reparación de los dispositivos son responsabilidad exclusiva de los clientes.
- 8.3. La aplicación no se ha diseñado ni se garantiza para su uso en aplicaciones de alto riesgo que requieran un rendimiento especial a prueba de fallos, como el funcionamiento de instalaciones nucleares, el control del tráfico aéreo, el soporte vital u otras aplicaciones, dispositivos o sistemas en los que el fallo de un dispositivo o aplicación pudiera ocasionar directamente la muerte, lesiones personales o graves daños físicos o medioambientales ("actividades de alto riesgo"). Sin perjuicio de cualquier otra disposición, los clientes no utilizarán ni permitirán que terceros empleen la Aplicación en ninguna actividad de alto riesgo.
- 8.4. Obtener el consentimiento necesario de las personas afectadas de acuerdo con las normas de seguridad y protección de datos, ya que los datos personales se recopilan, tratan o utilizan en el curso del uso de la aplicación por parte de dichas personas y no se aplica al caso en cuestión ninguna legislación que permita dicha recopilación, tratamiento o uso sin necesidad de obtener el consentimiento.
- 8.5. Comprobar los datos y la información en busca de virus u otros programas dañinos antes de enviar los datos y la información a Bosch, y asegurarse de que los programas antivirus cumplan los requisitos más recientes.
- 8.6. Notificar los defectos en los servicios contractuales a Bosch tan pronto como tenga conocimiento del defecto. Si se produce un retraso en el envío de la notificación o si no se realiza la notificación a pesar de que el cliente tenga conocimiento del defecto, se excluye una reducción unilateral de la tarifa o la suspensión por parte del cliente, así como la rescisión extraordinaria.
- 8.7. Las siguientes funciones y tareas son responsabilidad exclusiva del cliente:
  - 8.7.1. Asignación de roles y autorizaciones a las personas o unidades correspondientes para los roles de usuario disponibles en Remote Portal y gestión de dichos roles y autorizaciones.
  - 8.7.2. Asignación de dispositivos a los socios contractuales del cliente y a los sitios de los socios contractuales.
  - 8.7.3. Adquisición, instalación y conexión de dispositivos adecuados para el funcionamiento de acuerdo con los requisitos del sistema. La Aplicación permite el uso de dispositivos por parte del cliente mediante las funciones descritas.

## 9 Información relacionada con el RGPD

### Finalidad del tratamiento de datos

Bosch realiza el tratamiento de datos personales solo en la medida y de la manera necesarias:

1. para cumplir las obligaciones de Bosch en virtud del acuerdo/condiciones de uso de la oferta de servicios de Remote System Management; y
2. para cumplir con las instrucciones del cliente de vez en cuando (que pueden ser instrucciones específicas o instrucciones de carácter general tal como se establece en el presente acuerdo o de otra manera notificada por el cliente a Bosch),
3. y no tratará los datos personales para ningún otro fin.

### Categorías de datos

- Datos del dispositivo: datos introducidos por el Responsable del tratamiento o transferidos por el dispositivo del Responsable del tratamiento: datos maestros del dispositivo, datos de telemetría de estado del dispositivo y metadatos de versiones de software. Ubicación y persona de contacto de un dispositivo. Se usa para habilitar el servicio Remote System Management facilitado al controlador de datos.
- Registros relacionados con el dispositivo: las actividades del dispositivo se registran para permitir la resolución de problemas del sistema.
- Datos de configuración del usuario: datos introducidos por el Controlador de datos durante el uso de la solución, como la información de acceso del usuario, incluida la dirección IP, la empresa, el nombre, los apellidos y la dirección de correo electrónico necesarios para proporcionar acceso a la aplicación del usuario.
- Registros de acciones de los usuarios: documentación del uso del sistema por parte de los usuarios, incluidas las acciones realizadas y las marcas de tiempo asociadas. Se utiliza para ayudar a resolver casos de mantenimiento y mejorar la experiencia del usuario.
- Datos que no son de carácter personal, como datos de configuración de sitios, cuentas de clientes y servicios, incluidos tipos y flujos.

### Interesados

- Empleados del cliente
- Usuarios finales o socios contractuales del cliente ("cliente del cliente")

### Subcontratistas

Todos los subcontratistas se incluyen en la lista de la **Tabla 1**.

	<b>Nombre y dirección del subcontratista y nombre del responsable de la protección de datos / persona de contacto para cuestiones relacionadas con la protección de datos</b>	<b>Ámbito del servicio (ámbito del pedido realizado por el contratista)</b>	<b>Lugar de tratamiento de los datos</b>	<b>Transferencia/ acceso a datos personales del cliente (tipo de datos y grupo de interesados)</b>
1	Amazon Web Services (AWS)	Infraestructura/ proveedor de alojamiento (como se indica en el concepto de seguridad) y proveedor de servicios administrados para el almacenamiento, la manipulación y la recuperación de datos, así como la conectividad a la nube	Regiones de infraestructura de AWS (véase la sección 6)	Todas las categorías e interesados enumerados en los datos 9
2	Robert Bosch India Responsable de protección de datos de Bosch India (RBEI/ DSO) DPO.India@in.bosch.com	Restricted group of Technical Operations Support	No.123, Industrial Layout, Hosur Road, KoramangalaBengaluru-560 095 Karnataka, India	Todas las categorías e interesados enumerados en los datos 9 El equipo de operaciones solo tiene acceso a la aplicación y al almacenamiento a nivel de sistema operativo, no a nivel de cuenta o de sitio.
3	Bosch.IO GmbH <a href="https://www.bosch-digital.com/imprint/">https://www.bosch-digital.com/imprint/</a>	Funcionamiento y mantenimiento de la base de datos de dispositivos gemelos digitales ( <a href="https://eclipse.dev/ditto/">https://eclipse.dev/ditto/</a> ) para el almacenamiento, la manipulación y la recuperación de datos del dispositivo	Regiones de infraestructura de AWS (véase la sección 6)	Categoría de datos Datos del dispositivo

**Tabla 1**

### Medidas técnicas y organizativas

Las siguientes MTO se han acordado entre el Responsable del tratamiento y el Encargado del tratamiento y se especifican en el presente caso concreto. Véase la lista de ejemplares.

- I. Medidas para garantizar la confidencialidad (art. 32 par. 1 let. b del RGPD)
  - I. Control de acceso físico: Ningún acceso no autorizado a los sistemas de tratamiento de datos.
  - II. Control de acceso lógico: impedir el uso no autorizado del sistema mediante contraseñas (seguras), mecanismos de bloqueo automático, autenticación de dos factores y codificación de datos.
  - III. Control de acceso a los datos: prohibición de lectura, copia, modificación o eliminación no autorizadas dentro del sistema mediante conceptos de autorización y derechos de acceso específicos para cada usuario, y registro de los accesos.
  - IV. Control de separación: tratamiento por separado de los datos recopilados para diversos fines.
  
- II. Medidas para garantizar la integridad (art. 32 par. 1 let. b del RGPD)
  - I. Control de las transferencias: imposibilidad de leer, copiar, modificar o eliminar sin autorización durante la transmisión o el transporte electrónicos mediante codificación, redes privadas virtuales (VPN) y firma electrónica.
  - II. Control de las entradas: determinación de si se han introducido, modificado o eliminado datos personales en los sistemas de tratamiento de datos y quién lo ha hecho, mediante el registro y la gestión de documentos.
  
- III. Medidas para garantizar la disponibilidad y la resistencia (Art. 32 par. 1 let. b del RGPD), p. ej.:
  - I. Control de disponibilidad: protección contra daños accidentales o destrucción o pérdida mediante estrategia de copias de seguridad.
  - II. Control de pedidos: no hay tratamiento de datos bajo encargo según el Art. 28 del RGPD sin las correspondientes instrucciones del responsable del tratamiento mediante el diseño explícito del contrato, la gestión formalizada del pedido, la selección rigurosa del proveedor de servicios, la obligación de convencer por adelantado y las inspecciones de seguimiento.
  - III. Resiliencia: los sistemas y servicios (por ejemplo, almacenamiento, acceso, capacidad de las líneas, etc.) se diseñan de forma que puedan garantizarse incluso altas tensiones intermitentes o altas cargas constantes de procesamientos.
  
- IV. Medidas para la seudonimización de datos personales a través de:
  - I. Separación de los datos maestros del controlador de datos del cliente y los datos del cliente
  - II. Uso de identificadores de personal, clientes y proveedores en lugar de nombres
  
- V. Medidas para la codificación de datos personales a través de:
  - I. Codificación simétrica
  - II. Codificación asimétrica
  - III. Hashing

- VI. Medidas para restablecer rápidamente la disponibilidad de los datos personales tras un incidente físico o técnico mediante el concepto de copia de seguridad.
- VII. Procedimientos de revisión, valoración y evaluación periódicas (Art. 32 par. 1 let. d del RGPD; Art. 25 par. 1 del RGPD) via:
  - I. Gestión de la privacidad
  - II. Gestión de respuesta a incidentes
  - III. Protección de datos de forma predeterminada (Art. 25 par. 2 del RGPD)
  - IV. Evaluación por DSO, auditorías de IT
  - V. Evaluación externa, auditorías, certificaciones









**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2023

**Building solutions for a better life.**

202309141013