LA TECNOLOGÍA DE BARBARA IOT

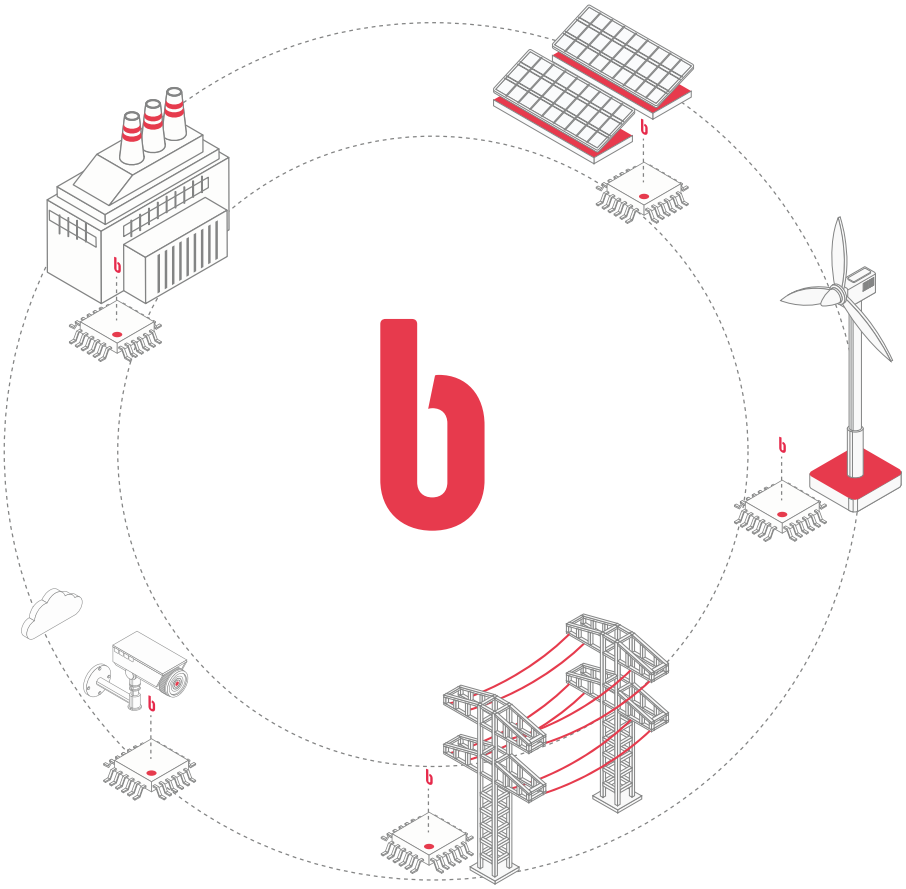
FICHA DE PRODUCTO

PRODUCIDO POR:
Barbara IoT
6 de mayo de 2021

ÍNDICE

01. INTRODUCCIÓN

Barbara es una tecnología IoT para el Edge que permite capturar datos de distintas fuentes de manera cibersegura, homogeneizarlos y procesarlos in situ y enviarlos a plataformas en la nube, públicas o privadas.

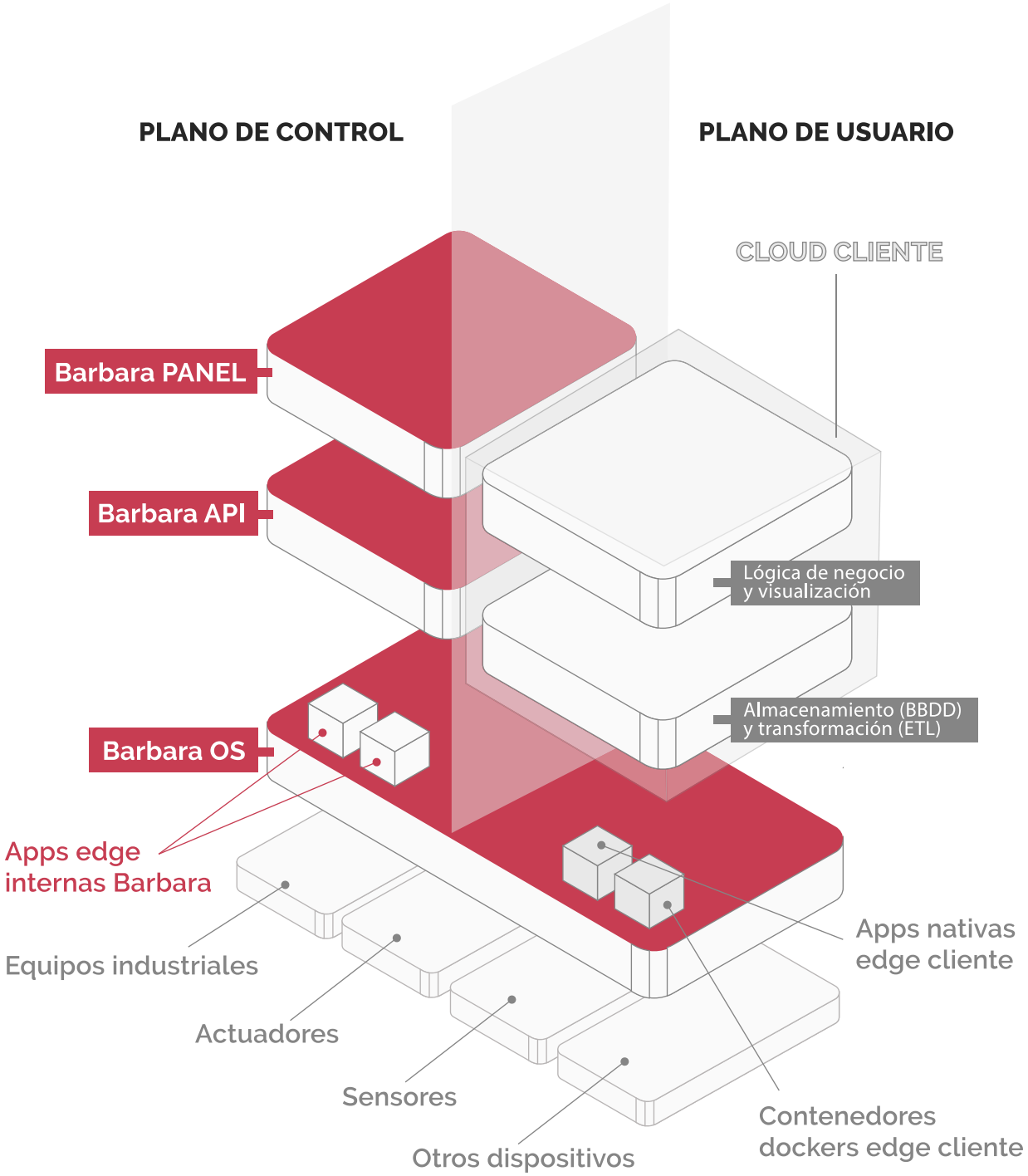


Como solución IoT para el Edge:

- Barbara **habilita la conectividad de cualquier equipo industrial**, utilizando sus protocolos industriales de comunicación, y los integra de manera cibersegura con sistemas cloud o remotos.
- Barbara **permite el procesado de los datos recogidos de manera local**, en el propio dispositivo, y ejecutar aplicaciones nativas o en Dockers
- Barbara **permite la gestión remota de todo el ciclo de vida de los dispositivos IoT** para mantener actualizados tanto su sistema como sus aplicaciones y algoritmos.
- Barbara **es una solución segura por diseño** que protege datos y equipos al conectarlos a la nube.

02. ARQUITECTURA

El stack tecnológico de Barbara tiene varios componentes que se reparten tanto en el Edge (en los nodos IoT) como en la nube.

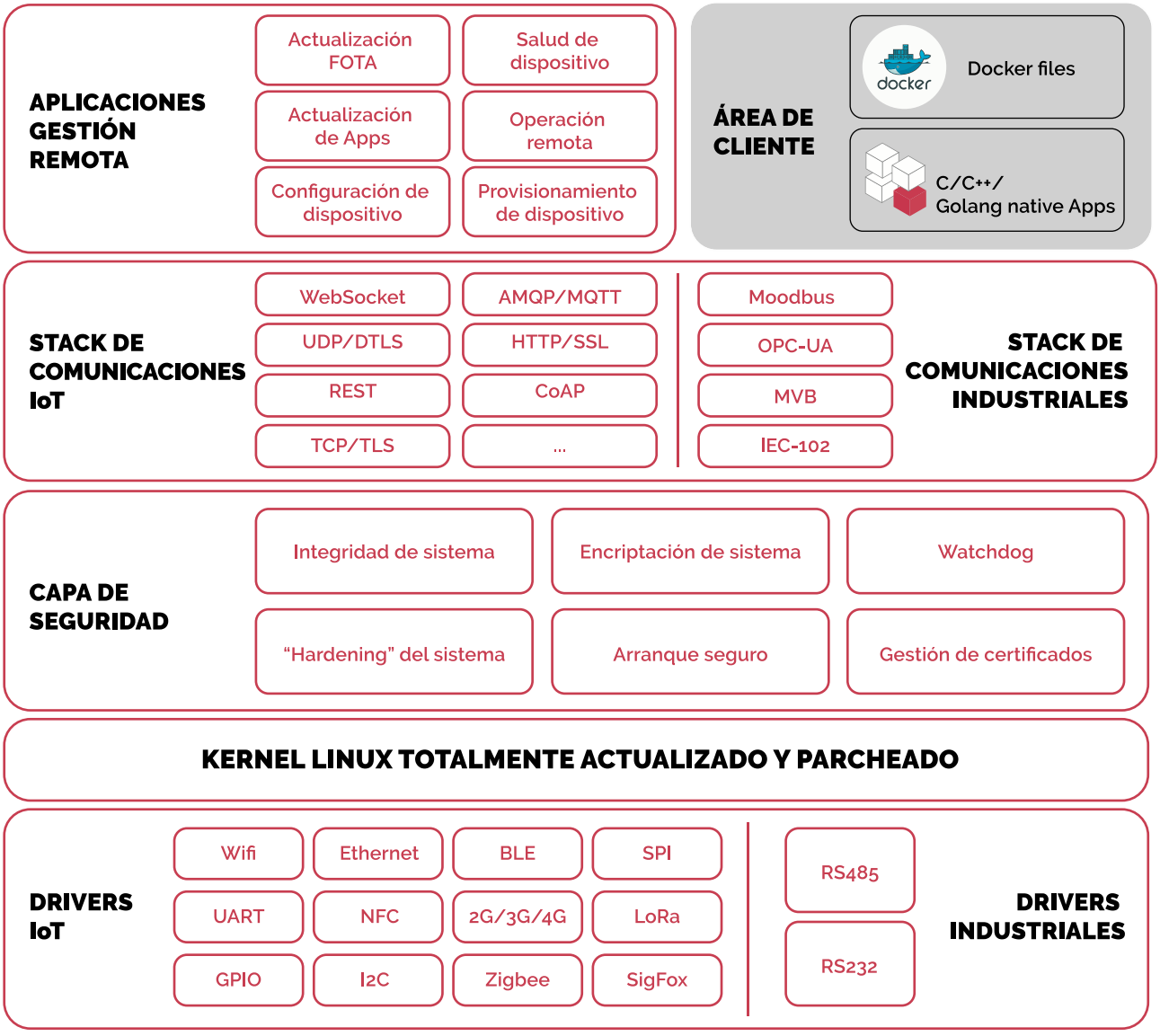


Los principales componentes son:

- **Barbara OS** - El Sistema Operativo Seguro por diseño para nodos IoT
- **Barbara API** - El interfaz para comunicarse con los nodos IoT
- **Barbara Panel** - La herramienta de gestión remota de los nodos IoT

03. BARBARA OS - EL SISTEMA OPERATIVO

El stack tecnológico de Barbara tiene varios componentes que se reparten tanto en el Edge (en los nodos IoT) como en la nube.



- **Drivers de IoT e Industriales:** Barbara OS incluye drivers para soportar los principales componentes hardware utilizados en IoT y aplicaciones industriales como Ethernet, Wifi, Bluetooth, LoRa, Rs485, RS232, I2C… y muchos otros. Además, el equipo de Barbara IoT y su comunidad y partners realiza una integración continua de nuevos drivers.
- **Kernel de Linux:** En el núcleo, Barbara OS contiene un kernel de Linux actualizado y totalmente parcheado. Para prevenir y protegerse contra vulnerabilidades que puedan ser aprovechadas por entidades maliciosas. El equipo de Barbara IoT parchea Barbara OS contra vulnerabilidades de día cero en tiempo récord, y genera una nueva versión de Barbara OS que pone a disposición de sus usuarios inmediatamente.
- **Capa de Seguridad:** Barbara OS viene equipado con un conjunto de funcionalidades que lo convierten en la elección perfecta para dispositivos en despliegues de IIoT (IoT Industrial) que tengan requisitos críticos de privacidad o resiliencia.

- **Capa de comunicaciones:** Para poder interactuar con otros dispositivos, la pila de comunicaciones segura de Barbara OS incluye tanto protocolos IoT como industriales, y está en continua expansión. Tanto si es un protocolo de IT (p.ej. HTTPS), de IoT (p.ej. MQTT) o de OT (p.ej. Modbus/TCP), la pila se implementa en Barbara OS y se deja accesible a las aplicaciones de usuario.
- **Sandbox de Cliente:** Barbara OS contiene un Sandbox (implementado con chroot) que puede correr tanto contenedores Docker como aplicaciones "cross-compiladas" C/C++ o Golang. Este sandbox está totalmente aislado del Sistema Operativo de manera que si una de estas aplicaciones es comprometida o falla, el núcleo del dispositivo permanece seguro y estable. Las aplicaciones y contenedores Docker del sandbox pueden ser gestionadas y actualizadas remotamente de manera independiente a través del API de Barbara, accesible desde el Panel de Gestión de Barbara OS.
- **Apps Internas de Barbara:** Barbara OS incluye unas pocas aplicaciones que permiten la interacción con el API de Barbara y, en última instancia, con el Panel de Gestión de Barbara para una gestión completa de todos los dispositivos:
  - **Sistema seguro de actualizaciones OTA:** Permite el despliegue de parches y otras actualizaciones de Barbara OS a través de un canal encriptado y verificado. Los paquetes de actualización están optimizados desde el punto de vista del ancho de banda, con tamaños cercanos a 1MB.
  - **Sistema de actualización de aplicaciones:** Este servicio permite la gestión independiente de las Apps nativas y los contenedores Docker que corren en el sandbox de cliente
  - **Salud del Dispositivos:** Recoge periódicamente datos sobre el rendimiento del dispositivo, como el nivel de uso de CPU, porcentaje de ocupación de memoria y mensajes de log, entre otros y los envía periódicamente al Panel de Gestión de Barbara, a través del API
  - **Sistema de configuración seguro:** En los dispositivos con Barbara OS se pueden gestionar remotamente cambios en la configuración de usuario y aplicación que van más allá de las puras actualizaciones de firmware. Para ello, Barbara OS incluye un sistema de configuración seguro. Con este sistema de configuración, los usuarios pueden actualizar remotamente y de manera segura cosas como paquetes binarios de aplicación, variables de entorno y de aplicación, configuraciones de red y muchos otros parámetros del software.
  - **Sistema de provisionado:** Barbara OS incluye una secuencia de primer arranque donde la configuración inicial del dispositivo, así como los certificados de comunicaciones de ese dispositivo son configurados. Esto permite que los dispositivos puedan salir de fábrica con una versión estándar común ("vanilla") y terminar su configuración particular una vez arranquen.

CAPACIDADES DE SEGURIDAD

Barbara OS ha sido ideado y creado con la filosofía de "Seguridad desde el diseño". Viene equipado con un conjunto de funcionalidades de seguridad que lo convierten en la elección perfecta para dispositivos en despliegues de IIoT que tengan requisitos críticos de privacidad o resiliencia. Estas funcionalidades, implementan las recomendaciones de organismos como la GSMA, OWASP o el Industrial Internet Consortium (IIC).

1. Integridad de sistema

Mediante la ejecución de algoritmos criptográficos de chequeo durante el arranque, Barbara OS es capaz de determinar si un software a ejecutar ha sido correctamente firmado con las claves criptográficas adecuadas. De esta manera, se garantiza que el origen de esta porción de software es conocido, confiable y no ha sido alterado.

2. Arranque seguro por hardware

En casos en los que la plataforma hardware donde esté corriendo el sistema operativo Barbara OS soporte Trusted Platform Modules (TPM), las firmas de archivos binarios de firmware que se comprueban durante el arranque son verificados contra los certificados almacenados en dicho TPM

3. Encriptación completa de todos los datos

Tanto los datos de sistema como los de usuario en Barbara OS están encriptados en reposo (es decir, incluso cuando el dispositivo no está en uso). De esta forma, se previene la extracción de datos sensibles del dispositivo por parte de una entidad no autorizada o un atacante malicioso.

Securizar datos durante su transmisión es tan importante como securizar los datos almacenados en el dispositivo. Barbara OS implementa protocolos de seguridad estándar para la capa de transporte, como TLS y DTLS en sus versiones más restrictivas. Por otro lado, para aquellos despliegues que no permitan encriptación en la capa de transporte, se crean librerías cliente/huésped que permiten la encriptación y verificación de los datos enviados por la capa de aplicación (payload o carga útil), creando así un canal de comunicaciones seguro.

4. Endurecimiento (hardening) del dispositivo

El sistema operativo Barbara OS está "endurecido" de fábrica: no hay servicios de red abiertos por defecto, no hay una combinación de usuario-contraseña, ni ninguna otra forma para acceder al dispositivo más allá del canal seguro de comunicación establecido con el Panel de Gestión Remota de dispositivos (a través del API de Barbara), que no es nunca una comunicación entrante.

5. Gestión de permisos de usuario

Barbara OS segmenta de manera muy clara el acceso a los datos de aplicaciones de usuario que corran en el dispositivo, y previene el riesgo producido por un escalado en los privilegios.

6. Gestión de errores

Barbara OS implementa un completo sistema de traceo que permite detectar potenciales eventos relacionados con la seguridad o problemas funcionales. El sistema de traceo puede integrarse fácilmente con soluciones SIEM.

7. Sistema de monitorización y autocorrección

A través de su sistema activo de monitorización, Barbara OS permite reducir el tiempo de parada de un dispositivo por fallo, permitiendo corregir de forma autónoma y automática los problemas del sistema.

8. Gestión de certificados

Barbara OS utiliza un control de identidad y de acceso al servicio cloud basado en certificados criptográficos, que son únicos para cada dispositivo. Esto se hace de manera transparente al usuario final y es gestionable remotamente a través del Panel de Gestión Remota o directamente a través del API de Barbara.

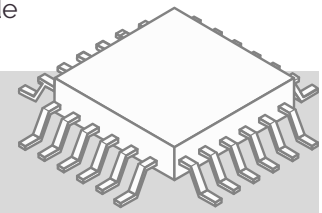
CONSTRUCTOR DE VERSIONES SOFTWARE

Barbara OS ha sido específicamente diseñado para dispositivos IoT y se acomoda a las necesidades de los desarrolladores, permitiéndoles crear su propia versión del sistema operativo totalmente adaptada a sus dispositivos. Todo esto se hace a través de la sección de construcción de versiones software que Barbara Panel incluye, o directamente a través del API de Barbara. Una vez generada la versión, puede descargarse e instalarse.

COMPATIBILIDAD DE HARDWARE

Partiendo de una perspectiva de arquitectura de hardware, Barbara OS está soportado actualmente por las siguientes plataformas: x86_64, armv6, armv7 y aarch64 (arm64)

Algunos ejemplos de plataformas para las que actualmente hay versiones de Barbara OS ya preparadas son:



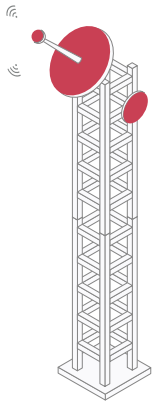
- **Advantech ARK-1220L**
- **Advantech EPC-R3220**
- **Advantech UNO-220**
- **Beelink BT3 Pro**

- Raspberry Pi Zero
- Raspberry Pi 3b/+ (32/64 bits)
- Raspberry Pi 4 (32/64 bits)

El equipo de Barbara IoT y sus partners continúan progresivamente añadiendo nuevas plataformas y productos a la lista de dispositivos y hardware compatible.

COMPATIBILIDAD DE PROTOCOLOS

A día de hoy, Barbara OS es compatible con los siguientes protocolos y tecnologías de comunicación:

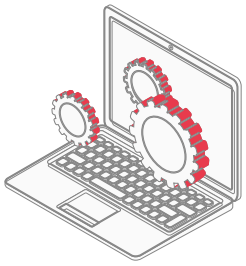


Tecnologías de red de largo alcance:

- Cellular (2G/3G/4G)
- 5G (en pruebas)
- LTE-M
- NB-IoT
- Lora / LoraWAN
- Ethernet
- Serie (RS-232/RS-485)

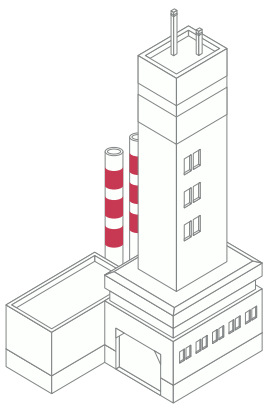
Tecnologías de redes de corto alcance:

- Zigbee
- Bluetooth
- Wi-Fi
- Wireless M-BUS



Protocolos IT/IoT:

- HTTP/S
- MQTT
- AMQP
- CoAP



Protocolos Industriales

- Modbus
- OCP-UA
- IEC-102/104
- DNP3
- MVB
- Siemens S7 (soporte parcial)
- Profibus (en pruebas)
- Profinet (en pruebas)

04. BARBARA API - EL INTERFAZ DE COMUNICACIONES

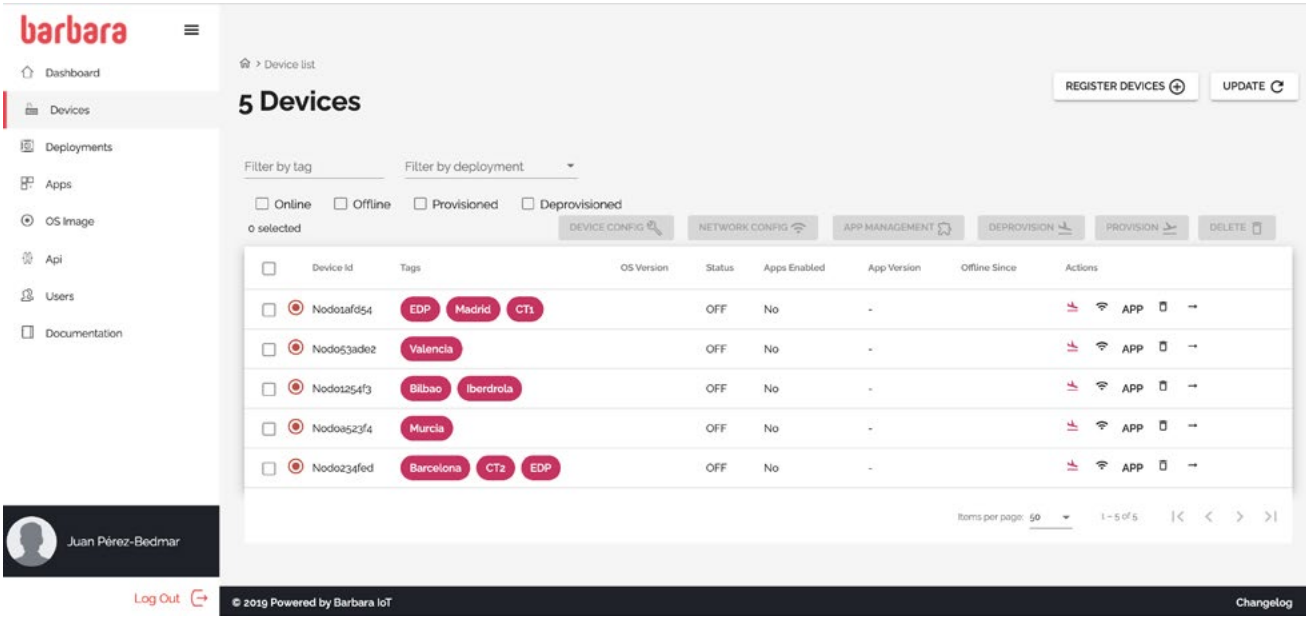
Barbara cuenta con un Interfaz de Programación de Aplicaciones (API) web de tipo REST que permite el acceso a todas las funcionalidades del Panel de Gestión, que se explica en la siguiente sección.

La documentación de uso de este API se encuentra publicada en el siguiente enlace: https://prod.bap.barbaraiot.com/documentation/

05. BARBARA PANEL - LA HERRAMIENTA DE GESTIÓN REMOTA

La gestión remota de dispositivos es una funcionalidad crítica para poder desplegar y gestionar de manera escalable una infraestructura totalmente distribuida. De no poder realizarse esta gestión remota y centralizada, los costes de despliegue, operación y mantenimiento del sistema podrían hacer inviable una implantación real del proyecto. Barbara cuenta con un Panel que permite la gestión del ciclo de vida completo de los dispositivos IoT. Permite

- **Monitorizar:** Muestra información en tiempo real sobre el estado de todos los nodos IoT y asegura su correcto funcionamiento. Emite alarmas que avisan de comportamientos anómalos en el parque de nodos IoT
- **Adaptar:** Puede reajustar la configuración de los nodos IoT o de sus aplicaciones de manera remota. Adapta el comportamiento de los dispositivos sin necesidad de actualizar las aplicaciones de manera completa
- **Actualiza:** Mantiene los nodos IoT actualizados en todo momento con las actualizaciones OTA (Over the Air) de firmware, software y aplicaciones del dispositivo. Estas actualizaciones pueden incluir funcionalidades mejoradas y parches de seguridad



Esta plataforma, basada en microservicios e instalable en cualquier nube pública o privada, permite tareas de control y configuración de dispositivos en remoto por protocolos **MQTT, LWM2M, OMA-DM o TR-69**.

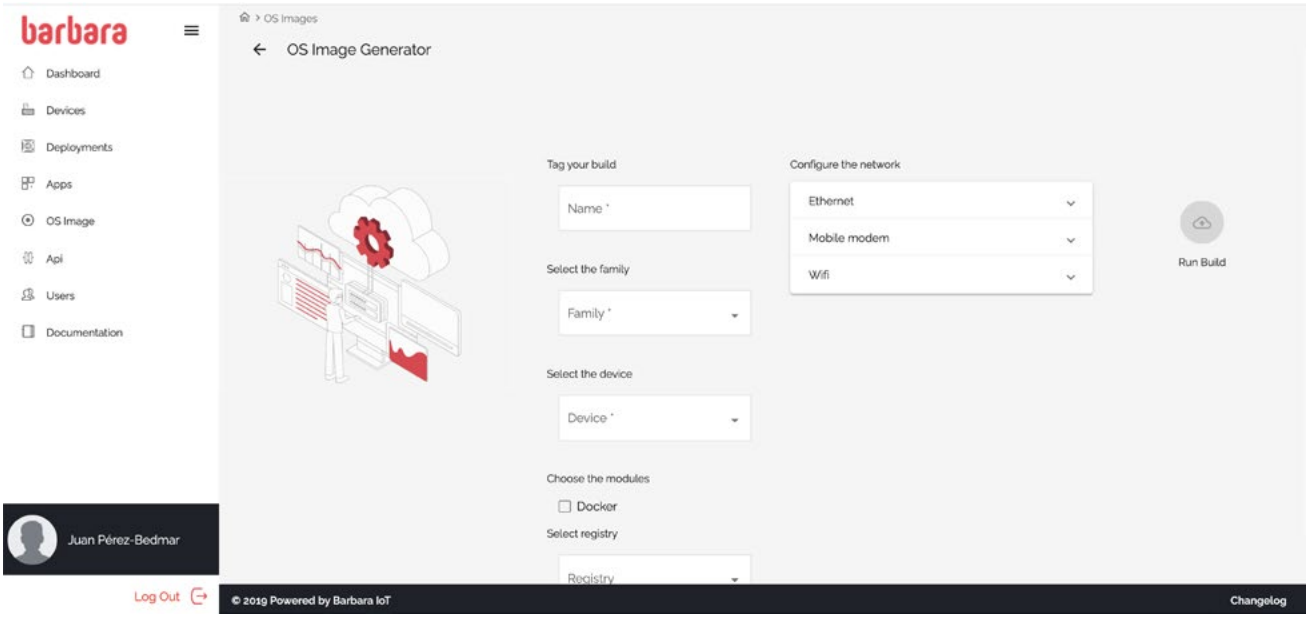
La gestión de los dispositivos se puede hacer unitariamente o en batch a través de la agrupación flexible por tags/zonas o filtros avanzados, y permite: el alta/baja de dispositivos, la monitorización y generación de alarmas y la actualización de los dispositivos

Desde un punto de vista técnico, se trata de una interfaz gráfica (frontend) propia de Barbara que el API explicado en la sección anterior. El uso de esta interfaz es opcional, ya que los clientes pueden integrar sus propias interfaces y plataformas con el API de Barbara directamente.

Las principales funcionalidades se recogen a continuación

CONSTRUCCIÓN DE VERSIONES DE BARBARA OS

Tal y como se explica anteriormente, Barbara OS ha sido específicamente diseñado para dispositivos IoT y se acomoda a las necesidades de los desarrolladores, permitiéndoles crear su propia versión del sistema operativo totalmente adaptada a sus dispositivos. Una vez generada la versión, puede descargarse e instalarse.



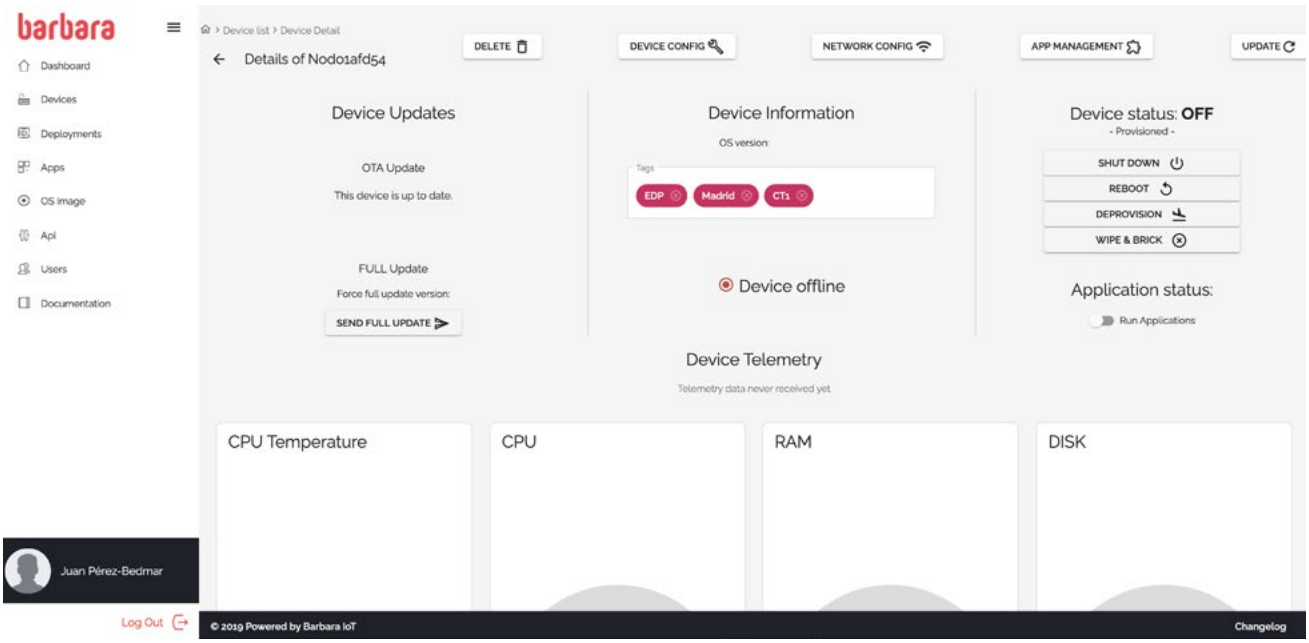
ALTA DE NUEVOS DISPOSITIVOS

En esta sección se puede tanto dar de alta nuevos dispositivos IoT / Edge como provisionarlos con su configuración de arranque, tales como conectividad de red, mapas de adquisición de datos (p.ej. mapas Modbus), frecuencias de captura, etc.

El objetivo es que las tareas requeridas en campo para el despliegue de un nuevo Dispositivo IoT/ Edge se limiten a la instalación física, pero que toda la configuración y comisionado se pueda hacer en remoto. En su arranque inicial (bootstrap) el dispositivo conecta al panel utilizando certificados PKI de identificación, y tras un proceso de autenticación mutua satisfactorio, descarga la configuración establecida por el operador.

MONITORIZACIÓN Y GENERACIÓN DE ALARMAS

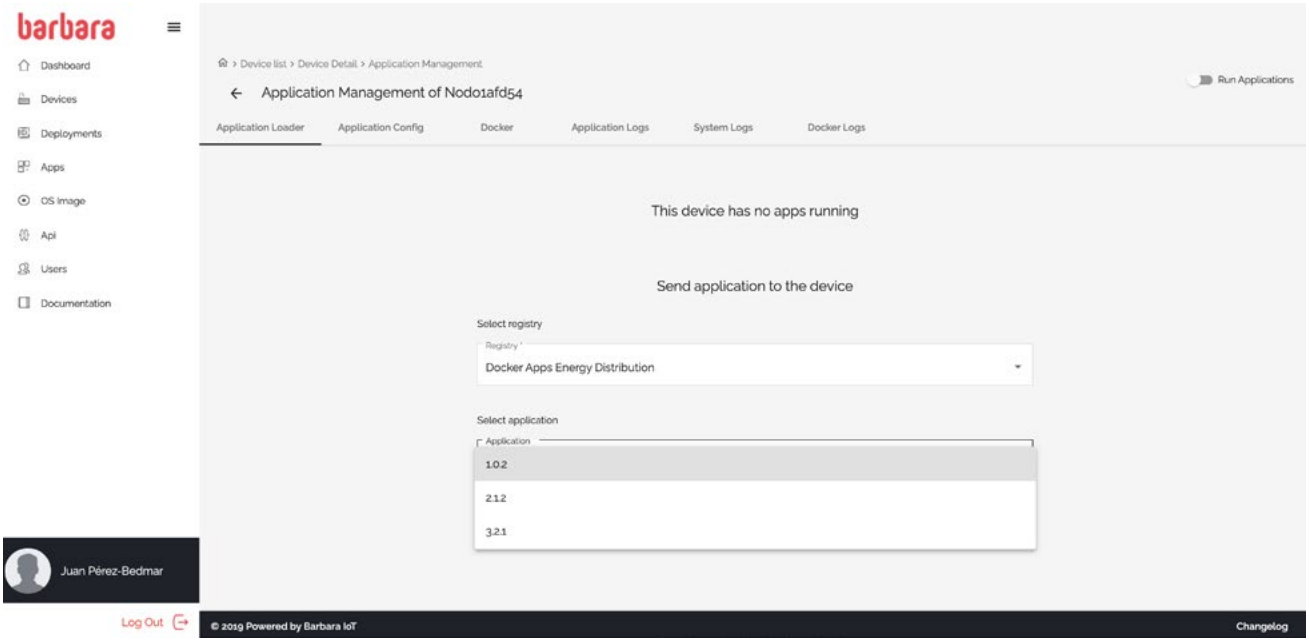
Incluye la monitorización y generación de alarmas relativas al funcionamiento del dispositivo IoT de campo, tratando parámetros relativos a la salud del dispositivo como conectividad, procesos arrancados, uso de recursos (CPU, Memoria, otros), accesos, etc.



ACTUALIZACIÓN DE LOS DISPOSITIVOS

La actualización de los equipos se realiza en dos planos:

- **Actualización de firmware:** Poder actualizar el firmware permite la posibilidad de solucionar vulnerabilidades de seguridad publicadas sobre cualquiera de los sub-módulos de terceros integrados en el firmware de los dispositivos (por ejemplo, librerías para la gestión de certificados SSL), o mejorar el rendimiento del sistema (por ejemplo, optimizar el consumo de energía).
- **Actualización del software del dispositivo:** es decir las aplicaciones concretas o librerías con la lógica de uso final.



BAJA O DECOMISIONADO DE LOS DISPOSITIVOS

La baja o decomisionado de cualquier dispositivo IoT se puede realizar en tres modalidades, de menor a mayor severidad:

- **Parada:** el dispositivo simplemente deja de ejecutar la lógica programada.
- **Apagado remoto:** el dispositivo se apaga, y necesitaría una acción manual física para su reinicio.
- **Borrado:** el dispositivo se apaga, pero previamente borra todo el software y firmware contenido, de manera que no vuelve a arrancar ni dispone de información sensible en su interior. Para su restablecimiento, sería necesario una acción manual de re-instalación de todo el software y re-provisión de su configuración.

barbara

Para estar informado sobre IoT industrial y ciberseguridad, suscríbete a nuestra newsletter

2021 | hola@barbaraiot.com | www.barbaraiot.com