**Agregar a la comparativa**

**5.5.1 Plataforma IoT**

Por otra parte, también debemos considerar la plataforma dedicada específicamente para Internet en las Cosas (IoT) que las prestadoras de servicios de IBM, Azure y AWS ofrecen. Se deben considerar ciertas cuestiones para poder elegir correctamente la indicada que se adapte al sistema de Estacionamiento, se ha elegido un conjunto de características importantes, entre ellas rescatamos

**5.5.1.1 Robustez**

Una buena plataforma debe ofrecer un máximo de funcionalidad, la plataforma debe permitir la comunicación entre los dispositivos y los protocolos de conexión de maquina a máquina necesarios.

**5.5.1.2. Compatibilidad del proveedor**

La plataforma debe integrarse fácilmente a su sistema de backend (administrador del sitio con sus respectivos sistemas) Y, además de la interoperabilidad entre dispositivos, debe haber una fuerte comunicación entre aparatos y sistemas externos. también debe permitir que utilice API (Interfaces de Programa de Aplicación) para interactuar y compartir datos con otras empresas.

**5.5.1.3 Realice una comprobación de seguridad**

La seguridad es una preocupación principal al elegir una plataforma cada componente de la plataforma debe tener sus propias opciones de seguridad, tales como SSL (Secure socket Layer).

**5.5.1.4. Empaquetado**

Existen otros factores con una consideración importante, se pueden remarcar por ejemplo cuales son los protocolos de IoT que la plataforma sea compatible, compatibilidad con el proveedor de Hardware (en la próxima sección se verá en detalle).

A continuación, se ve a grandes rasgos que ofrece cada una. Para luego hacer hincapié en las características principales mencionadas en la sección 5.5.1

**5.5.2 Comparativas de plataformas**

**5.5.2.1 IBM Watson IoT Platform** [IoT Watson – IBM 2018]

A través de IBM Watson se podrá conectar y controlar sensores, aparatos, viviendas e industrias IoT. proporciona un conjunto de herramientas integradas y de complementos. En pocas palabras, es una herramienta que facilita la conexión de Dispositivos con la nube, osea internet. Se pueden hacer uso de herramientas integradas y externas para la limpieza y transformación de datos, el resumen y el aprendizaje automático, entre otros. Puede utilizar Watson IoT Platform Analytics (complemento) para permitir a los usuarios de negocio interactuar fácilmente con los datos de métrica en bruto procedentes de entidades IoT utilizando funciones de análisis configurables incorporadas.  A su vez a lo que se refiere a seguridad Los dispositivos, las pasarelas y las aplicaciones se conectan a Watson IoT Platform utilizando el protocolo MQTT o HTTP. Las conexiones pueden ser seguras o no seguras.

| **Tipo de conexión** | **Protocolo** | **Número de puerto** |
| --- | --- | --- |
| No segura\* | MQTT y HTTP | 1883 u 80 |
| Secura (TLS) | MQTT y HTTPS | 8883 o 443 |

Tabla 3. Puertos de IBM Watson

Si bien es una de las mejores prestadoras de plataformas IoT, pero tiene una gran desventaja, que este producto no está disponible para Argentina, lo que hace imposible elegirla como opción, pero es importante tenerla en cuenta, ya que en un futuro seguramente sea aprobada en el país en cuestión, o puede ser tomada en cuenta para otros países.

* + - 1. **Azure IoT Hub** [Azure hub – Microsoft 2018]

IoT Hub es un servicio administrado, hospedado en la nube, que actúa como centro de mensajes para comunicaciones bidireccionales entre la aplicación de IoT y los dispositivos que administra. Puede usar Azure IoT Hub para compilar soluciones de IoT. y un back-end de solución hospedado en la nube. Puede conectar virtualmente cualquier dispositivo a IoT Hub.

* + - * 1. **Seguridad**

Proteger las soluciones IoT requiere garantizar el aprovisionamiento seguro de los dispositivos, proteger la conectividad entre estos dispositivos y la nube y garantizar la protección de los datos en la nube durante su procesamiento y almacenamiento. Azure IoT Suite protege los dispositivos proporcionando una clave de identidad única a cada uno, para establecer una comunicación única, con esto se gana que los dispositivos no acepten conexiones de red no solicitadas. Los dispositivos solo se conectan a servicios conocidos con los que están emparejados, o con los que tienen rutas establecidas, como un centro de IoT de Azure. La eficacia es un factor importante para garantizar la conservación de recursos y el funcionamiento en un entorno con recursos limitados. HTTPS (HTTP seguro), la versión segura estándar del sector del conocido protocolo HTTP, se admite en Azure IoT Hub, lo que permite una comunicación eficaz. Advanced Message Queuing Protocol (AMQP) y Message Queuing Telemetry Transport (MQTT), admitidos en Azure IoT Hub, están diseñados no solo para la eficacia en términos del uso de recursos, sino también para la entrega confiable de mensajes.

* + - 1. **AWS IoT** [AWS IoT – AWS 2019]

AWS IoT proporciona comunicación bidireccional entre dispositivos conectados a Internet, como sensores, actuadores, microcontroladores integrados o dispositivos inteligentes y la nube de AWS.  Proporciona un mecanismo de publicación y suscripción de mensajes, que están manejados con el protocolo MQTT, a su vez proporciona integración con otros servicios de AWS, Se puede apreciar que AWS IoT dispone de funciones de seguridad para el envío de mensajes, este debe estar cifrado sobre el protocolo Transport Layer Security (TLS), que garantiza la confidencialidad de los protocoles de aplicación (MQTT, HTTP) que se detallaran en el punto 6, además los dispositivos deben estar conectados utilizando certificado X.509 sobre una conexión segura para autenticar y autorizar las acciones de la cuenta. En simples palabras, se debe cumplir reglas que impone AWS donde el centro de la atención es la seguridad y confidencialidad de los datos y dispositivos.

AWS IoT proporciona tres formas de aprovisionar dispositivos:

* Aprovisionamiento de un solo objeto con una plantilla de aprovisionamiento.

Esta es una buena opción si solo necesita aprovisionar los dispositivos de uno en uno.

* Aprovisionamiento "just-in-time" (JITP) con una plantilla que registra y aprovisiona un dispositivo cuando se conecta por primera vez a AWS IoT.

Esta es una buena opción si necesita registrar un gran número de dispositivos, pero no dispone de información sobre ellos que se pueda incluir en una lista de aprovisionamiento por lotes.

* Aprovisionamiento por lotes.

Esta opción le permite especificar una lista de valores de aprovisionamiento de un solo objeto que se almacenan en un archivo en un bucket de S3(Servicio de almacenamiento de AWS). Este enfoque funciona bien si tiene un gran número de dispositivos conocidos cuyas características puede incluir en una lista.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Peso | IBM Watson IoT | | Azure IoT Hub | | AWS IoT | |
| Características |  | Nota | Puntaje | Nota | Puntaje | Nota | Puntaje |
| Robustez | 30% | 8 | 2.4 | 9 | 2.7 | 7 | 2.1 |
| Compatibilidad del proveedor | 20% | 3\* | 0.6 | 7 | 1.4 | 8 | 1.6 |
| Seguridad | 40% | 9 | 3.6 | 7 | 2.8 | 7 | 2.8 |
| Empaquetado | 10% | 7 | 0.7 | 8 | 0.8 | 7 | 0.7 |
| TOTAL | 100% | 27 | 7.3 | 31 | 7.7 | 29 | 7.2 |

Tabla comparativa ponderada

Con la tabla ponderada, estableciendo las características marcadas en el comienzo del punto 6 se puede llegar a la conclusión del resultado obtenido que obtiene como ganadora a

Tanto IBM, Azure y AWS IoT publican mensajes de eventos cuando se producen determinados eventos. Por ejemplo, el registro genera eventos cuando se añaden, actualizan o eliminan objetos. Cada evento provoca que se envíe un único mensaje de evento. Los mensajes de evento se publican a través de MQTT con una carga JSON. El contenido de la carga depende del tipo de evento.

Para recibir mensajes de eventos, el dispositivo debe usar una política adecuada que le permita conectarse a la Gateway de dispositivos de IoT y suscribirse a los temas de eventos de MQTT. También debe suscribirse a los filtros de temas adecuados.

¿Qué necesito para poder conectarme a la nube de IBM?

Antes de empezar a recibir datos desde los dispositivos de IoT, debe conectarlos a Watson IoT Platform. La conexión de un dispositivo a Watson IoT Platform implica el registro del dispositivo con Watson IoT Platform y, a continuación, el uso de la información de registro para configurar el dispositivo para conectarlo a Watson IoT Platform.

Los requisitos para poder utilizar IBM Watson son los siguientes:

* Una cuenta de IBM Cloud.
* Una instancia de Watson IoT Platform.
* Un dispositivo que cumple los requisitos siguientes:
  + El dispositivo debe poder comunicarse mediante protocolos HTTP o MQTT.
  + Los mensajes del dispositivo deben ajustarse a los requisitos de carga útil de mensajes de Watson IoT Platform.

**5.5.1** los requerimientos que tiene que cumplir el dispositivo (se cual sea), y lo que tiene que hacer, independiente del hardware.

5.5**.2** la comunicación puede ser realizada por MQT, pero también por HTTP (y ahí comentas muy, pero muy brevemente que es cada cosa, poniéndolo entre paréntesis o algo así). Habla más de las alternativas de autentificación (¡esto es muy importante!!!!! cuales hay y que implican cada una de ellas)

hacer referencia a SSL

se conectará un dispositivo IoT a Watson IoT Platform.

Antes de empezar a recibir datos desde los dispositivos de IoT, debe conectarlos a Watson IoT Platform. La conexión de un dispositivo a Watson IoT Platform implica el registro del dispositivo con Watson IoT Platform y, a continuación, el uso de la información de registro para configurar el dispositivo para conectarlo a Watson IoT Platform.

Antes de empezar

Antes de empezar a utilizar Watson IoT Platform, debe tener los elementos siguientes:

* Una cuenta de IBM Cloud.
* Una instancia de Watson IoT Platform.  
  Puede crear una instancia de Watson IoT Platform directamente desde la [página de Watson IoT Platform del Catálogo de servicios de IBM Cloud](https://cloud.ibm.com/catalog/services/internet-of-things-platform/).
* Un dispositivo que cumple los requisitos siguientes:
  + El dispositivo debe poder comunicarse mediante protocolos HTTP o MQTT.
  + Los mensajes del dispositivo deben ajustarse a los requisitos de carga útil de mensajes de Watson IoT Platform.  
    Para obtener más información, consulte [Desarrollo de dispositivos en Watson IoT Platform](https://www.ibm.com/support/knowledgecenter/SSQP8H/iot/platform/devices/device_dev_index.html).

Explore las opciones siguientes en función de su situación:

|  | **El servicio se despliega** | **El servicio no se despliega** |
| --- | --- | --- |
| **Tengo ningún dispositivo que conectar** | Siga el proceso que se describe en este tema. | Explore la conexión de dispositivos en el apartado sobre Practicar con Watson IoT Platform . |
| **No tengo un dispositivo para conectar** | Simule datos de dispositivo o Conecte su teléfono inteligente . | Iníciese en Watson IoT Platform Starter. |

* <https://www.semantix.com.br/es/blog/7-consejos-para-seleccionar-la-mejor-plataforma-de-iot>