# LECCIONES DE DCIM A IOT

**Aunque IoT es un concepto relativamente nuevo, lo cierto es que en el data center llevan años proliferando los sensores que recogen todo tipo de información. ¿Qué le puede enseñar el DCIM al IoT para sacar el máximo partido a la experiencia?**

## JORGE JIMÉNEZ
**Schneider Electric Iberia**

Los centros de datos han sido las primeras soluciones IoT por su complejidad, por la cantidad de dispositivos, por la inteligencia de los mismos y por la aparición de herramientas superiores (DCIM) para aportar valor a toda la información.

Entre las lecciones aprendidas, me quedaría con una principalmente: el dispositivo conectado nos puede dar mucho, pero también nos lo puede quitar. Podemos tener muchos datos, pero si no contamos con un buen sistema por encima que los convierta en información, seguirán siendo datos que consuman recursos. DCIM nos ha ayudado a aprender a utilizar esos datos para mejorar.

## JOHN CURRAN
**Vertiv**

La gestión de DCIM y los centros de datos constituye una versión reducida del IoT moderno. Los operarios de los centros de datos deben afrontar la misma proliferación de dispositivos provistos de IP, con lo que tienen que gestionar un sistema de IoT interno.

Aquellos que deben pensar en el IoT deben aplicar las mismas reglas que las de un DCIM. Para aprovechar al máximo los datos es fundamental quedarse únicamente con aquellos que son importantes, normalizarlos y condensarlos para que puedan ser consultados o para ver cuáles de sus elementos pueden resultar de interés.

## ÁNGEL OTERMÍN
**Hewlett Packard Enterprise**

DCIM nos ha enseñado a administrar y configurar correctamente los sensores y dispositivos conectados para hacerlos más seguros dentro de los entornos industriales. Estos entornos son en general más críticos y exigentes en términos de disponibilidad, seguridad y rendimiento. El problema es que mientras que los sistemas DCIM son de monitorización, los sistemas IoT son de monitorización y también de control, lo que aumenta considerablemente el peligro de ser manipulados de forma incorrecta.

La mayor recomendación es implementar la seguridad por diseño y por defecto en todos los dispositivos/sensores para IoT, tanto dentro como fuera del data center.

## PABLO LEGARDA
**BMC Software**

Los sensores de temperatura, consumo energético o inundación son los primeros "smart-meters". La principal diferencia es la ubicación de los sensores y el uso que se hace de ellos. Por un lado, la solución de DCIM se creó orientada al DC, incluyendo unas premisas de confianza tanto en el acceso a la información de los distintos sensores como en las comunicaciones. Por otro lado, IoT ha incluido la seguridad en su "mindset" desde el principio. Los datos que se transmiten han demandado altos estándares de seguridad en la comunicación, en el almacenamiento y en los protocolos.

## MANEL OROBITG
**Systam Technology**

Los elementos ahora llamados IoT no son más que los tradicionales sensores que en la industria llevan años utilizándose y que ahora se han generalizado a nivel de usuario. Los mismos fabricantes los potencian y nos permiten acceder fácilmente a ellos a través de Internet.

En base a mi experiencia con DCIM, mi consejo es analizar con mucho detalle los dispositivos IoT, sus funcionalidades, verificar el origen (fabricante) y buscar en Internet información de hackeo sobre el mismo. Aun así, un equipo que hoy es seguro mañana puede no serlo.