IoT MAD LAB
UNA CIUDAD CONECTADA

REQUISITOS TÉCNICOS

I. El dispositivo debe contar con identidades únicas, de manera genérica y dentro del entorno IoT donde se despliega.

II. Debe ser posible identificar el modelo del dispositivo.

III. El acceso a la configuración debe estar protegido con mecanismos de autorización y autenticación seguros y simples.

IV. Los parámetros de seguridad deben ser únicos y no debe ser posible devolverlos a valores genéricos.

V. No se deben poder obtener los parámetros de seguridad por mecanismos automáticos o mediante información pública. Se deben almacenar de forma segura y deben resistir ataques de fuerza bruta.

VI. Los algoritmos y primitivas criptográficas se deben poder actualizar.

VII. El dispositivo debe contar con mecanismos de gestión segura y automatizada de actualizaciones.

VIII. Los datos sensibles se deben almacenar y borrar de forma segura.

IX. La información disponible en el dispositivo debe ser la mínima posible.

X. Todas las interfaces del dispositivo, así como la información contenida en él y el acceso a los servicios de intercambio de datos deberían contar con mecanismos de autenticación, autorización y confidencialidad, que usen sistemas criptográficos fuertes, para el acceso a la información sensible.

XI. Los datos introducidos a través de interfaces, o intercambiados en los servicios de intercambio de datos deben estar validados.

XII. El dispositivo debería contar con funciones para detectar anomalías en el flujo normal de funcionamiento de sus interfaces, unidades de proceso, software/firmware y servicios de intercambio de datos

XIII. Todas las funciones, software o interfaces no utilizadas deberían estar deshabilitadas o eliminarse.

XIV. El software ejecutado debería tener el mínimo nivel de privilegio necesario para su funcionamiento.

XV. El dispositivo debe contar con mecanismos de arranque seguro, incluyendo la verificación de firmas del bootloader.

XVI. El software debe estar protegido ante uso no autorizado de funciones de prueba o debugging.

XVII. El software debe almacenar logs de forma segura y permitir su auditoría.

XVIII. El dispositivo debe ofrecer información de su estado de seguridad y de posibles cambios no autorizados.

XIX. Las unidades de proceso deben contar con sistemas de autorización y los procesos deben ejecutarse de manera aislada.

FORO DE EMPRESAS POR MADRID
Capital Digital | MADRID
UNIVERSIDAD POLITÉCNICA MADRID