Checklist de ciberseguridad en equipos conectados

Usa este checklist para revisar si los equipos conectados de una tienda o un edificio están protegidos. Marca cada punto que se cumple y anota lo que veas.

Tienda / Edificio:	Fecha:
Responsable de la instalación:	Revisado por:

Conoce y aísla tus equipos (empieza por aquí)

OK	Punto a revisar	Observaciones
☐	Hay un inventario actualizado de equipos conectados Marca, modelo, red y soporte de cada equipo.	
☐	Ningún equipo de control es accesible desde internet	
☐	Los equipos de control están en una red separada Aparte de la red de oficina, del punto de venta y de la wifi de clientes.	
☐	Las órdenes remotas pasan por una capa local que las filtra Una capa edge que valida, limita o bloquea las órdenes.	

Reduce la superficie de ataque

OK	Punto a revisar	Observaciones
☐	Se sabe qué equipos de la tienda tienen conexión propia Frío, clima, hornos, iluminación, PCI, contadores...	
☐	No quedan contraseñas de fábrica ni compartidas	
☐	Todos los equipos conectados tienen soporte del fabricante O están aislados y detrás de una capa edge.	
☐	Toda la instalación se gestiona desde una sola plataforma de telegestión	

Controla los accesos

OK	Punto a revisar	Observaciones
☐	El acceso remoto de mantenedores usa doble factor y queda registrado	
☐	No hay programas de escritorio remoto abiertos de forma permanente	

Prepárate para un incidente

OK	Punto a revisar	Observaciones
☐	Hay alarmas de temperatura o consumo independientes del	

OK	Punto a revisar	Observaciones
	controlador	
☐	Hay copia actualizada de las configuraciones	
☐	Hay un plan escrito de respuesta ante incidentes	
☐	Si se corta internet, la instalación sigue funcionando en local	

Cómo leer el resultado: cada punto sin marcar es algo que conviene revisar, empezando por el primer bloque. Más información en el artículo «Ciberseguridad en equipos conectados» del blog de EcoMT. ¿Quieres revisarlo con nosotros? [enlace de contacto]