

Implantación de un ciclo de vida ciberseguro alineado con la CRA y la IEC 62443

Reto

La regulación europea de ciber resiliencia (CRA) ha traccionado la cultura de la ciberseguridad de producto en las distintas industrias. Esta obligación impone el reto de adaptar tanto los productos como los procesos de diseño, desarrollo, producción y mantenimiento. Para ello, es necesario realizar un análisis exhaustivo en términos funcionales del producto así como de distintas prácticas de ciberseguridad a lo largo de todo el ciclo de vida.

Solución

Se ha definido un Ciclo de Vida Ciberseguro de producto y se han implantado distintos marcos de trabajo para aplicarlo. Especialmente, pero no solo, se ha establecido una metodología de Análisis de Riesgos, un sistema de validación de ciberseguridad de producto y un Sistema de Gestión de Vulnerabilidades. Todas ellas se han implantado ya trabajando un primer piloto que permite al primer producto de Fagor AOTEK cumplir íntegramente con la CRA.

Beneficio

El cumplimiento de la Ciber Resilience Act a través del estándar de referencia en ciberseguridad, la IEC 62443, posicionando ante el mercado y para todos sus clientes a FAGOR AOTEK como un proveedor de confianza en cuanto a ciberseguridad de producto, un atributo, sin duda, que cada día obtiene mayor relevancia en procesos comerciales.

Tecnología utilizada



Ciberseguridad