RESUMEN EJECUTIVO
Proyecto A023. Ciberseguridad Industrial (TO)

DESCRIPCIÓN DEL PROYECTO

El proyecto **"Ciberseguridad Industrial (TO)"**, se ha desarrollado para dar cumplimiento a los trabajos asociados a la A023 de la propuesta de PERTE "Mejora Digitalización del Ciclo Integral del Agua en el área de Málaga. Fase I" de EMASA.

Como consecuencia del desarrollo del Plan Director de Ciberseguridad Industrial para los sistemas y las tecnologías de la operación, se realizó una evaluación de la situación en ese momento, identificando puntualmente las brechas de seguridad y proponiendo un conjunto de acciones en el corto, medio y largo plazo para reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables.

Las actuaciones que se describen a continuación corresponden a las más prioritarias y cuyo desarrollo se han finalizado.

LOGROS Y ENTREGABLES PRINCIPALES

Durante la ejecución del proyecto se han alcanzado los siguientes hitos determinantes:

- **Implantación de PyStation** como plataforma de gestión e integridad de datos para garantizar la disponibilidad de la información de proceso
- **Despliegue de la Segmentación de la red OT:** incorporando nueva electrónica de comunicaciones y reorganizando la arquitectura de red.
- **Modernización de la red de radio de Banda Ancha Inalámbrica (BAI):** mediante el mallado de red, la incorporación de nuevos enlaces y el aumento de la redundancia de las comunicaciones.
- **Ampliación y puesta en marcha del nuevo CPD,** con infraestructura redundante y centro de respaldo para garantizar la continuidad del servicio.
- **Implantación de nuevos sistemas de ciberseguridad industrial**, incluyendo protección endpoint, prevención de intrusiones y monitorización avanzada de amenazas.

ALCANCE TÉCNICO Y ARQUITECTURA

- **Implantación de una estrategia integral de ciberseguridad industrial,** basada en las actuaciones prioritarias definidas en el Plan Director para reforzar la protección de los sistemas de Tecnología de la Operación (OT).
- **Modernización de la arquitectura de comunicaciones,** mediante la segmentación de la red industrial y la reorganización del direccionamiento IP para mejorar la seguridad, disponibilidad y mantenimiento.

- **Refuerzo de la infraestructura de comunicaciones inalámbricas (BAI),** evolucionando a una arquitectura mallada y redundante que garantiza la continuidad del servicio y la resiliencia frente a fallos.
- **Ampliación y modernización del Centro de Proceso de Datos (CPD),** con una infraestructura hiperconvergente redundante y un centro de respaldo que asegura la continuidad de la operación.
- **Implantación de un sistema avanzado de gestión de datos (PyStation)** para garantizar la integridad de la información y la disponibilidad de los datos de proceso.
- **Despliegue de una arquitectura de ciberseguridad multicapa,** incorporando protección endpoint, sistemas de prevención de intrusiones (IPS), monitorización avanzada del tráfico y detección de amenazas para proteger los sistemas industriales frente a ciberataques.

CONCLUSIÓN

Se han cumplido los objetivos:

- **Refuerzo de la ciberseguridad industrial,** mediante una arquitectura de protección multicapa adaptada a los entornos de Tecnología de la Operación (OT).
- **Incremento de la resiliencia y continuidad del servicio,** gracias a la implantación de infraestructuras redundantes y sistemas de respaldo para las comunicaciones y el procesamiento de datos.
- **Modernización de la arquitectura tecnológica, mejorando la disponibilidad, escalabilidad y capacidad de gestión de los sistemas industriales**.
- **Mayor fiabilidad de las comunicaciones y de la información de proceso,** garantizando la integridad y disponibilidad de los datos para la operación.
- **Preparación de la infraestructura para futuros procesos de digitalización,** facilitando la incorporación de nuevas herramientas de supervisión, análisis avanzado de datos y optimización de la explotación.