"Working for a RiskLess environment"

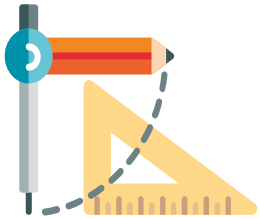
Cyber Security Posture: Industria 4.0 #ICS OT

Marzo 2019

Somos una Consultoría e Ingeniería independiente, con vocación innovadora, enfocada a la transformación de la Seguridad Integral

Líneas

Diagnóstico
Auditoría
Test de Penetración

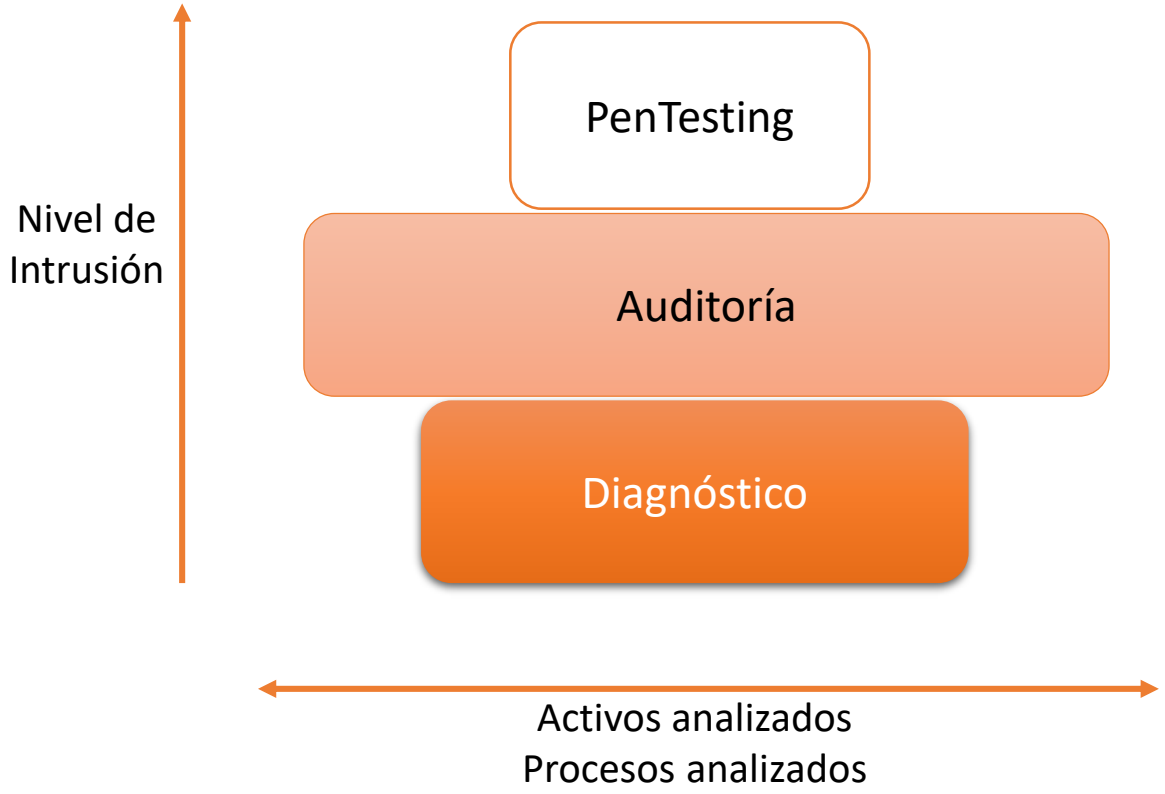


Convergencia IT/OT:
Diseño Arquitecturas seguras
Gestión de proveedores y accesos remotos
Zonas y conducto

Capacitación:
Concienciación,
Formación y
Entrenamiento

Monetización de
la ciberseguridad
industrial

Servicios de Ciberseguridad: Diagnóstico, Auditoría, Pentesting



Diagnóstico

Problemática

La industria no posee visibilidad de las vulnerabilidades ni las amenazas existentes en su planta industrial en relación con los aspectos de ciberseguridad. No sabe si:

- Existe una política siguiendo normativas y buenas prácticas ni si se implementa esa política
- Existe una arquitectura segmentada para proteger la parte OT
- Se realiza un buen uso de las infraestructuras OT en consonancia con las buenas prácticas
- Si existen activos vulnerados que ya ralentizan el rendimiento y producción (↓OEE)

Objetivo

Se desarrolla un diagnóstico basado en estándares pero adecuando a las necesidades de la industria. Estos estándares son universales (NIST Framework, IEC 62443 y ISO27001) así como un análisis de vulnerabilidades

Duración estimada del servicio	Precio estimado
5 días	2.500-3500 €

Beneficios

La industria obtendrá una mayor visibilidad y un PLAN DE ACCIÓN detallado que puede servir al CISO a definir presupuestos (Plan de Inversión) en la mitigación de los riesgos detectados en el DIAGNÓSTICO

Auditoría

Problemática

Se realiza una auditoría ante una normativa o ley:

- Esta normativa puede ser externa (ISO-UNE) o una normativa interna.
- Se establecen los planes de prueba para realizar la auditoría en ciberseguridad
- Una normativa en la industria puede ser el IEC62443, NIST Framework o el 27019.

Objetivo

1) Se audita para conocer si el sistema en sí cumple con los requisitos
2) Se audita los componentes más importantes del sistema para conocer su estado así como sus interfaces entre sí.

Duración estimada del servicio	Precio estimado
10 días	3.500-5.000€

Beneficios

La industria obtiene un sello o la certificación o precertificación de que la auditoría con respecto a la norma ha sido correcta así como los puntos de mejora tanto si ha pasado la auditoría como sí no.

Test de penetración

Problemática

Estos test en zonas de sistemas de control hay que hacerlos con sumo cuidado para que la producción siga su curso. Normalmente se pide este servicio si la infraestructura ya ha tenido algún altercado o incidente en ciberseguridad. Se pide a la empresa, bajo acuerdos de confidencialidad y horarios de prueba, una test de penetración para capturar un activo concreto

Objetivo

1) El objetivo no es auditar ni diagnosticar todo el sistema
2) El objetivo es ir directo hacia el activo concreto que han acordado ambas entidades: por ejemplo el control de la sala de control, el control sobre el sistema de PLCs en el nivel 1 o los sistemas SIS.

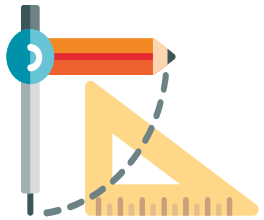
Duración estimada del servicio | | Precio estimado

10-12 días 5.000-8000

Beneficios

Conocer si ciertos activos que se consideran esenciales están bastionados o si por lo contrario son suscecptibles a ser vulnerados.

Convergencia IT/OT y arquitecturas



Convergencia y arquitecturas

Problemática

La planta industrial posee usualmente una arquitectura desorganizada, uniendo varios puntos de la parte corporativa con la industrial sin securizar. No se establecen la definición de zonas y conductos y existe una gran problemática a la hora de acceder por parte de los proveedores a esta arquitectura.

Objetivo

1) Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT.
2) Diseño y ejecución de arquitecturas seguras así como la segmentación de redes
3) Securización de accesos remotos y gestión de los procesos de proveedores
4) Definición de zonas y conductos según un modelo PURDUE evolucionado

Duración estimada del servicio | | Precio estimado

Dependiendo del tamaño y complejidad de la industria

Beneficios

Minimizar la superficie de ataque estableciendo una arquitectura expecífica para la parte industrial, con bajo coste y una monetización real sobre la inversión realizada

Concienciación, formación y entrenamiento.

Problemática

La planta industrial se ha erigido como una planta funcional para producir y no ha tenido en cuenta los aspectos no funcionales (ciberseguridad) en su crecimiento. El proceso de digitalización hace que existan mayores riesgos al encontrarnos con protocolos ethernet y TCP/IP dentro de la planta. Los operarios e ingenieros no son conscientes de posibles paradas que puedan ocurrir por el mal uso del correo, navegador, USB-s o la propia gestión con proveedores.

Objetivo

1) Realizar cursos de concienciación sobre amenazas y vulnerabilidades para CONCIENCIAR a los operarios, ingenieros y demás empleados de la planta industrial. **Todo ello mediante plataformas colaborativas**.
2) Realizar curso especializado sobre ciberseguridad industrial a responsables de sistemas en la parte OT convergiendo con la parte IT.

Beneficios

Reducir la superficie de ataque más vulnerable de todo el sistema: el ser humano. El 60% de las incidencias por ciberseguridad en la industria son por incidencias (negligencias, omisiones, insider threats. Fuente: Gartner)

Formación específica del IEC-62443

Problemática

El estándar IEC-62443 (antigua ISA99) es de facto el más usado en la industria, tanto a nivel de sistema como a nivel de componentes para su certificación. RKL imparte y ha impartido cursos de dos días para entender los diferentes elementos de este estándar para poder adaptarlo

Objetivo

1) Adaptación a estándares de Ciberseguridad industrial
2) Formar a ingenieros de producción sobre la problemática y formalización de dicha problemática de la ciberseguridad en el campo industrial

Duración estimada del servicio | | Precio estimado

2 días (5 horas por la mañana) 1.500€

Beneficios

Avanzar en las mejores prácticas, dando a conocer sobre ellas a la parte más vulnerable en ciberseguridad: las personas

Monetización de la ciberseguridad industrial

Problemática

Las máquinas (por ejemplo en el sector de máquina herramienta) recogen a través del sistema MES los fallos originados por fallos de producción, falta de abastecimiento, fallos de safety funcional y por ello se puede saber cuantas horas se pierden por estos fallos. Sin embargo no recogen aquellas paradas originadas por incidentes de ciberseguridad. RKL con este servicio permite definir el mecanismo de conocer cuántos horas se han perdido por los incidentes de ciberseguridad.

Objetivo

1) Conocer el impacto de la ciberseguridad en la producción
2) Especificar los mecanismos reales y necesarios para minimizar el riesgo con la inversión adecuado optimizando su ROI (Retorno de inversión)

Duración estimada del servicio | | Precio estimado

Dependiendo del tamaño y complejidad de la industria

Beneficios

Conocer el retorno de inversión de la ciberseguridad. Visualizar la ciberseguridad como un habilitador de negocio y no como un mero gasto

Iñaki Eguia Elejabarrieta

CTIO

Experto Ciberseguridad ICS / OT

Responsable de la concepción, diseño y desarrollo de las soluciones y productos innovadores.

inaki@rklintegral.com

+34 664 103 934

linkedin.com/in/inakieguia

Experiencia Profesional

2001	2003	2006	2016	2018	Actualidad
Investigador	Analista y desarrollador software	Investigador Principal Ciberseguridad	Desarrollo Negocio UNIT71 – Director de Innovación	Socio Responsable Ciberseguridad	

Competencias

- Ciberseguridad Industrial ●●●●●
- Desarrollo equipos ●●●●○
- Investigación ●●●●○
- Desarrollo producto ●●●●●

Publicaciones y Eventos

Patente Whitezone. Panelista en foros en Ciberseguridad OT. Artículos escritos en revistas de ciberseguridad SIC.

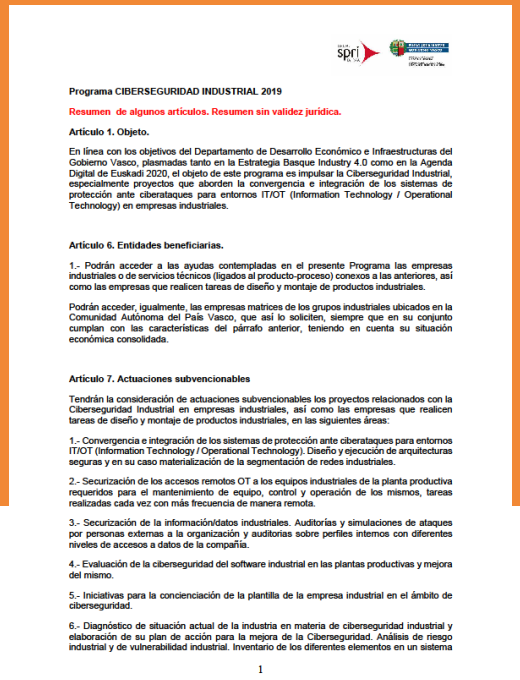
Formación/Idiomas

- Ingeniero Informático y en Organización Industrial
- Ingeniero en Org. Industrial GICSP
- Suficiencia Investigatoria UPV
- IEC-62443
- Lead Auditor ISO 27001

Alineación con SPRI

Servicios

Todos estos servicios son susceptibles a ser subvencionados por la SPRI. Más información en:



Programa CIBERSEGURIDAD INDUSTRIAL 2019

Resumen de algunos artículos. Resumen sin validez jurídica.

Artículo 1. Objeto.

En línea con los objetivos del Departamento de Desarrollo Económico e Infraestructuras del Gobierno Vasco, plasmadas tanto en la Estrategia Basque Industry 4.0 como en la Agenda Digital de Euskadi 2020, el objeto de este programa es impulsar la Ciberseguridad Industrial, especialmente proyectos que aborden la convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology / Operational Technology) en empresas industriales.

Artículo 6. Entidades beneficiarias.

1.- Podrán acceder a las ayudas contempladas en el presente Programa las empresas industriales o de servicios técnicos (ligados al producto-proceso) conexos a las anteriores, así como las empresas que realicen tareas de diseño y montaje de productos industriales.

Podrán acceder, igualmente, las empresas matrices de los grupos industriales ubicados en la Comunidad Autónoma del País Vasco, que así lo soliciten, siempre que en su conjunto cumplan con las características del párrafo anterior, teniendo en cuenta su situación económica consolidada.

Artículo 7. Actuaciones subvencionables

Tendrán la consideración de actuaciones subvencionables los proyectos relacionados con la Ciberseguridad Industrial en empresas industriales, así como las empresas que realicen tareas de diseño y montaje de productos industriales, en las siguientes áreas:

1.- Convergencia e integración de los sistemas de protección ante ciberataques para entornos IT/OT (Information Technology / Operational Technology). Diseño y ejecución de arquitecturas seguras y en su caso materialización de la segmentación de redes industriales.

2.- Securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos, tareas realizadas cada vez con más frecuencia de manera remota.

3.- Securización de la información/datos industriales. Auditorías y simulaciones de ataques por personas externas a la organización y auditorías sobre perfiles internos con diferentes niveles de accesos a datos de la compañía.

4.- Evaluación de la ciberseguridad del software industrial en las plantas productivas y mejora del mismo.

5.- Iniciativas para la concienciación de la plantilla de la empresa industrial en el ámbito de ciberseguridad.

6.- Diagnóstico de situación actual de la industria en materia de ciberseguridad industrial y elaboración de su plan de acción para la mejora de la Ciberseguridad. Análisis de riesgo industrial y de vulnerabilidad industrial. Inventario de los diferentes elementos en un sistema

1

integral

"Working for a RiskLess environment"

Consultoría e Ingeniería
Safety & Security

contacta@RKLintegral.com

+34 946 401 011
RKLintegral.com