Industrial Cybersecurity by LOGITEK

iberquimia
Congreso de Industria Química
MADRID - 27 y 28 abril 2016

La Ley PIC en la Industria Química

¿A qué me obligan los PSO y los PPE?
¿Cómo puede ayudarme Logitek?

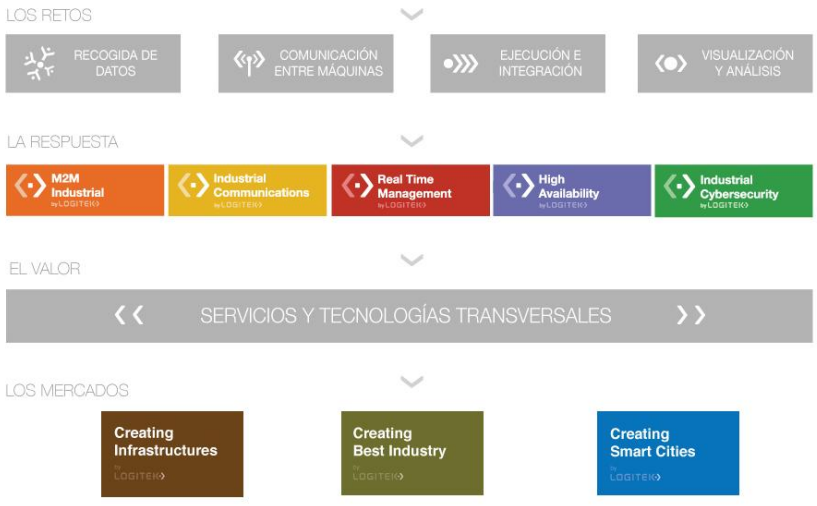
Dr. Fernando Sevillano
Solution Managers Director
fernando.sevillano@logitek.es

1

Logitek Ciberseguridad Industrial

Industrial Cybersecurity by LOGITEK

1. Logitek Ciberseguridad Industrial

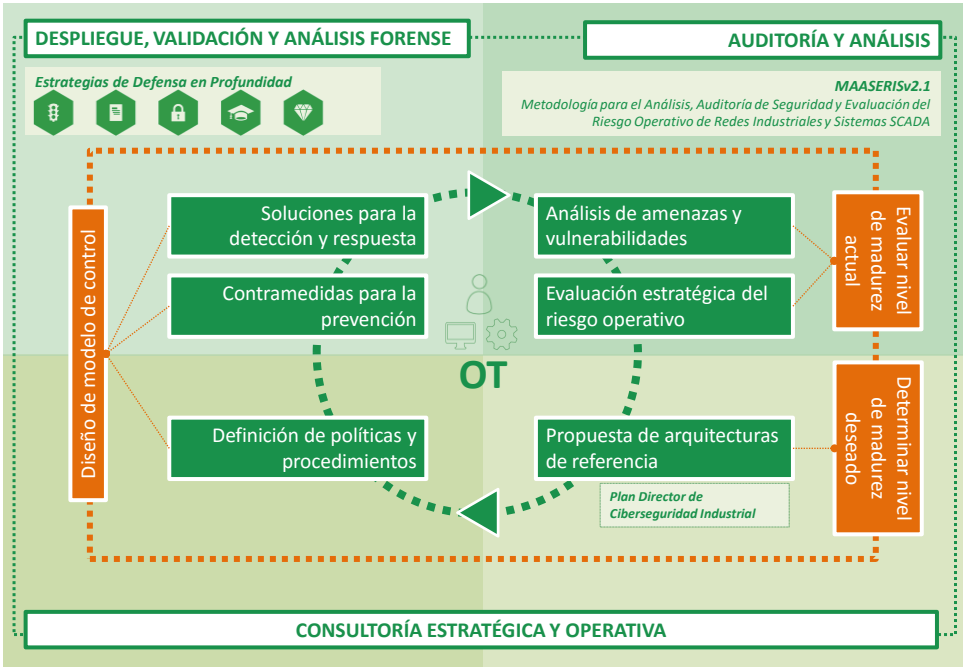


Industrial Cybersecurity by LOGITEK

1. Logitek Ciberseguridad Industrial

Industrial Cybersecurity by Logitek surge como una **nueva división de consultoría** dentro de Logitek con la vocación de ayudar a sus clientes **a mejorar los niveles de seguridad** de sus procesos, sistemas e infraestructuras asociados a entornos OT/críticos

Industrial Cybersecurity by LOGITEK


DESPLIEGUE, VALIDACIÓN Y ANÁLISIS FORENSE
AUDITORÍA Y ANÁLISIS
Estrategias de Defensa en Profundidad
MAASERISv2.1
Metodología para el Análisis, Auditoría de Seguridad y Evaluación del Riesgo Operativo de Redes Industriales y Sistemas SCADA
Diseño de modelo de control
Soluciones para la detección y respuesta
Contramedidas para la prevención
Definición de políticas y procedimientos
Análisis de amenazas y vulnerabilidades
Evaluación estratégica del riesgo operativo
Propuesta de arquitecturas de referencia
Plan Director de Ciberseguridad Industrial
OT
Evaluar nivel de madurez actual
Determinar nivel de madurez deseado
CONSULTORÍA ESTRATÉGICA Y OPERATIVA
Ley 8/2011 de Protección de Infraestructuras Críticas (PIC) | Formación, concienciación y sensibilización


Se
SEGURIDAD
Alternativas para la segmentación y fo de redes industriale
En infraestructuras críticas del secto
Aplicación de soluc antimalware off-line
En los sistemas de gestión de tien en la industria química
Reducción de amenazas, vulnerabilidades y riesgos asociados a las redes OT
A través de la utilización de protocolos industriales seguros, whitelisting de protocolos y la fortificación de servidores de comunicaciones

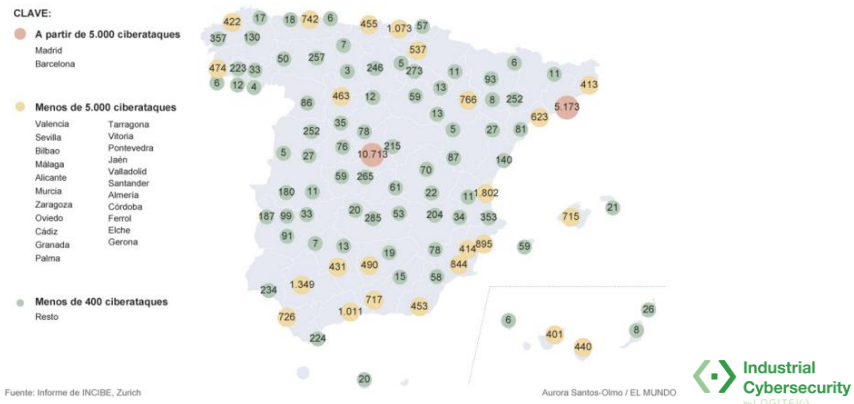
2

La Ley PIC

Industrial Cybersecurity by LOGITEK

Noticia del 26 de octubre de 2015 · El Mundo

- 63 'ciberataques' en lo que va de año contra infraestructuras críticas del Estado



La Ley PIC

Dentro del marco normativo asociado a la ciberseguridad industrial, tiene especial importancia en España:

- **La Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011).**
- **Complementada por el Real Decreto 704/2011**
- **Las disposiciones 18439 y 10060 donde se establecen los contenidos mínimos de los PSO y los PPE**

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

Dos grandes objetivos

Catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad

Diseñar **un planeamiento** que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la **seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones**

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

La Ley PIC define como **infraestructuras críticas** aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los **servicios esenciales.**

Estos a su vez, se definen como los servicios necesarios para el mantenimiento de **las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos**, o **el eficaz funcionamiento** de las Instituciones del Estado y las **Administraciones Públicas.**

Por último define como **infraestructuras estratégicas** las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

Asociados a TIC

Industrial Cybersecurity by LOGITEK

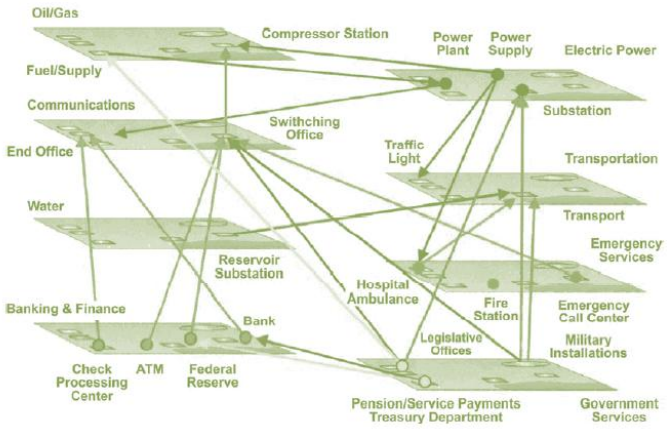
Objetivos y alcance de la Ley PIC

Una infraestructura se considera crítica teniendo en cuenta:

- El número de personas afectadas
- El impacto económico
- El impacto medioambiental
- El impacto público y social

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC



Características

- Automatización
- Amenazas
- Distribución geográfica
- Dependencias

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- En España se consideran sectores críticos los siguientes:

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia. Ministerio Interior. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio. Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación. Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad. Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Ciencia e Innovación. Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad. Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

Gas
Petroleo
Electricidad

Marítimo
Ferrovario
Aéreo
Carretera

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

La protección de infraestructuras críticas se define como:

El conjunto de actividades destinadas a **asegurar la funcionalidad, continuidad e integridad** de las infraestructuras críticas con el fin de…	**Prevenir, paliar y neutralizar el daño causado** por un ataque deliberado contra dichas infraestructuras y a …	**Garantizar la integración de estas actuaciones** con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

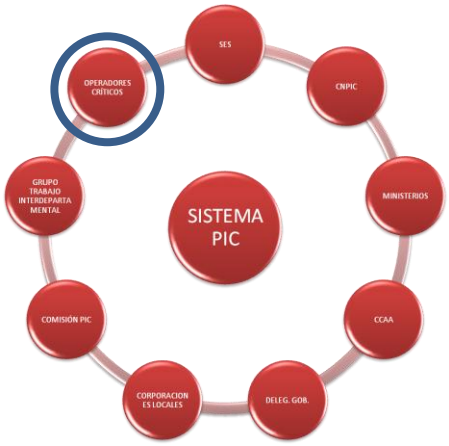
- La Ley 8/2011 PIC transpone a la legislación nacional las medidas incluidas en la ya mencionada Directiva 2008/114/CE.
  - Dicha Ley es completada por el Real Decreto 704/2011 y por las disposiciones adicionales.
  - Tiene como **principales objetivos**:

- Crear el **Sistema Nacional PIC**
- Poner las bases para el **Sistema de Planificación PIC**
- Generar el **Catálogo Nacional de Infraestructuras Estratégicas**
- **Establecer el CERT** para la gestión de incidentes de ciberseguridad

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- **Crear el Sistema Nacional de Protección de Infraestructuras Críticas** que contiene aquellas instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos. Estos son: los **operadores críticos**, el CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas), ministerios, CCAA, corporaciones locales, grupos de trabajo sectoriales, etc.



Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

Los **Operadores Críticos** son las entidades u organismos responsables de las inversiones o del funcionamiento de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica por proporcionar un servicio indispensable para la sociedad.

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- **Poner las bases para el Sistema de Planificación PIC**. Se trata de un conjunto de textos normativos que definen una serie de medidas para la protección de las infraestructuras críticas que se concretan en actuaciones que deben llevar a cabo los integrantes del Sistema de Protección de Infraestructuras Críticas.

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

PES	PSO	PPE	PAO
Enfoque sectorial. Normativas, tipologías de infraestructuras, interdependencias y niveles de criticidad	Definirán la política general del operador para garantizar la seguridad integral del conjunto de instalaciones o sistemas de su propiedad o gestión	Son los documentos operativos donde se deben definir las medidas concretas ya adoptadas y las que se vayan a adoptar por los operadores críticos para garantizar la seguridad integral (física y lógica) de cada una de sus infraestructuras críticas	Plan para cada una de las infraestructuras críticas, elaborado por los cuerpos de seguridad del estado, supervisado por delegación del gobierno y aprobado por la SES

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- Contenidos de los PES (Planes Estratégicos Sectoriales)

1. Analizar normativa sectorial para evitar fricciones con Ley PIC
2. Estructurar y segmentar por ámbitos de actividad
3. Establecer tipología de infraestructuras e identificar operadores críticos
4. Analizar interdependencias intra e inter sectoriales
5. Establecer tabla de criticidad (6 niveles)
6. Establecer análisis de riesgos sectorial
7. Establecer mecanismos coordinación PNPIC

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- Contenidos de los **PSO (Plan de Seguridad del Operador):**

1. Política general de seguridad del operador y marco de gobierno
2. Relación de Servicios Esenciales prestados por el Operador Crítico
3. Metodología de análisis de riesgo (amenazas físicas y lógicas)
4. Criterios de aplicación de Medidas de Seguridad Integral
5. Documentación complementaria

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- Contenidos de los **PPE (Plan de Protección Específico)**

1. Organigrama de seguridad

2. Descripción de la infraestructura

3. Resultado de análisis de riesgo
   - Amenazas
   - Medidas
   - Valores de riesgo

4. Plan de acción por activo

5. Documentación complementaria

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- Contenidos de los PAO (Plan de Apoyo Operativo):

1. Plan para cada una de las IC

2. Elaborado por cuerpos de seguridad del estado

3. Supervisado por delegación del gobierno y aprobado por la SES

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

- **Generar el Catálogo Nacional de Infraestructuras Estratégicas** que contiene la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.
- Para facilitar esta información se ha desarrollado el sistema **HERMES** a través del cual, los operadores críticos podrán dar de alta, acceder y modificar la información relativa a aquellas infraestructuras que gestionen.

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

Establecer el CERT (Cyber Emergency Response Team) para la gestión de incidentes de ciberseguridad. Apoyando al CNPIC, **INCIBE y dentro de él CERTSI** se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional.

- La misión del CE ntes de seguridad especializado e de problemas e incidencias de se

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

https://www.incibe.es/CERT/Respuesta_y_Soporte/

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

1. ¿Qué objetivos persigue?
2. ¿Cómo define la Ley PIC las infraestructuras críticas, los servicios esenciales y las infraestructuras estratégicas?
3. ¿Qué sectores se han designado como prestadores de servicios esenciales?
4. ¿Qué se entiende por protección de infraestructuras críticas?
5. ¿Cuáles son las principales aportaciones de la Ley PIC?
6. ¿Cómo puede afectar la Ley PIC a mi empresa u organismo?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

¿Puede mi empresa u organismo ser designado como operador crítico?

- Para la designación de una empresa u organismo como operador crítico, bastará con que al menos una de las infraestructuras por él gestionadas reúna la consideración de infraestructura crítica.

¿Quién realiza esta comunicación?

- El CNPIC es el encargado de realizar la comunicación, elaborando una propuesta de resolución y notificándola al titular o administrador de las infraestructuras.

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

¿A qué me obligan los Planes de Seguridad del Operador (PSO) y los Planes Específicos de Protección (PPE)?

Industrial Cybersecurity by LOGITEK

Objetivos y alcance de la Ley PIC

Aspecto	PSO	PPE
Alcance	Políticas generales	Medidas concretas (adoptadas o a adaptar) para garantizar seguridad física y lógica
Plazo de elaboración a partir de notificación CNPIC	6 meses	4 meses (tras aprobación PSO)
Contenidos esenciales	Metodología de análisis de riesgo y criterios de aplicación de medidas de seguridad	Medidas permanentes de protección y medidas de seguridad temporales y graduadas
Órgano resolutorio	Secretaría Estado u órgano delegado tras informe del CNPIC	Secretaría Estado u órgano delegado tras informe del CNPIC
Plazo respuesta	Máximo de 2 meses	Máximo de 2 meses
Plazo revisión	Cada dos años	Cada dos años

4

El análisis de riesgos dentro de los PSO y los PPE

Industrial Cybersecurity by LOGITEK

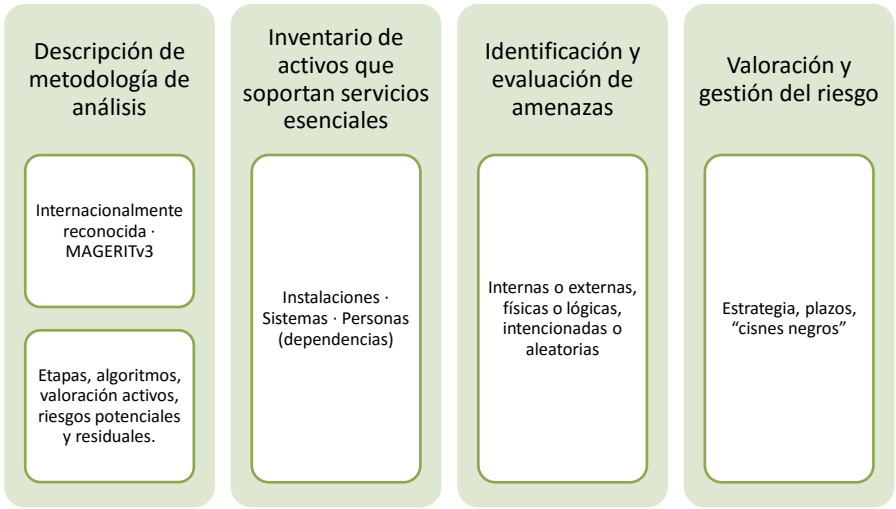
4. El análisis de riesgos dentro de los PSO y los PPE

- La Ley solicita esta documentación dentro de los PSO

Descripción de metodología de análisis
Inventario de activos que soportan servicios esenciales
Identificación y evaluación de amenazas
Valoración y gestión del riesgo

Industrial Cybersecurity by LOGITEK

4. El análisis de riesgos dentro de los PSO y los PPE



Industrial Cybersecurity by LOGITEK

4. El análisis de riesgos dentro de los PSO y los PPE

- La Ley se refiere a la gestión de riesgos dentro de los PPE de esta manera:
  - Resultados de análisis de riesgo

Definición de medidas permanentes y temporales/graduales

Identificación de medidas por capas

Valores de riesgo

Industrial Cybersecurity by LOGITEK

4. El análisis de riesgos dentro de los PSO y los PPE

Definición de medidas permanentes y temporales/graduales

- Permanentes son las ya adoptadas o las que se desplegarán tras el análisis de riesgos.
- Temporales, las que se incorporarán en caso de incrementar el nivel de seguridad.

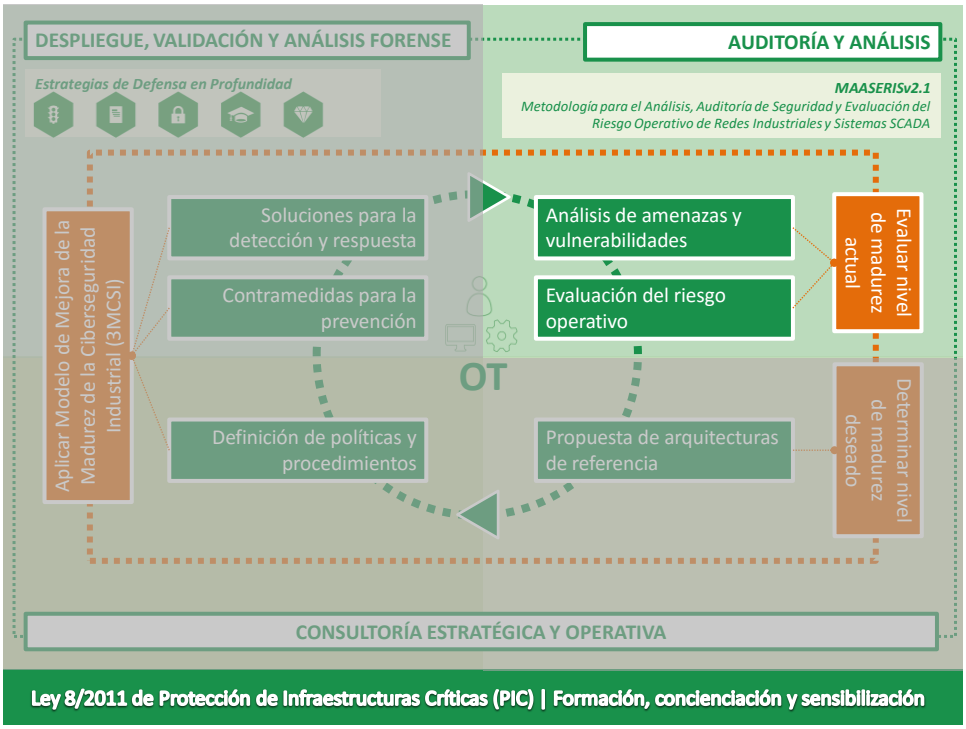
Identificación de medidas por capas

- Técnicas, procedimentales y de gestión

Valores de riesgo

- Quién ha evaluado / aprobado el riesgo y la estrategia de tratamiento asociada

Industrial Cybersecurity by LOGITEK

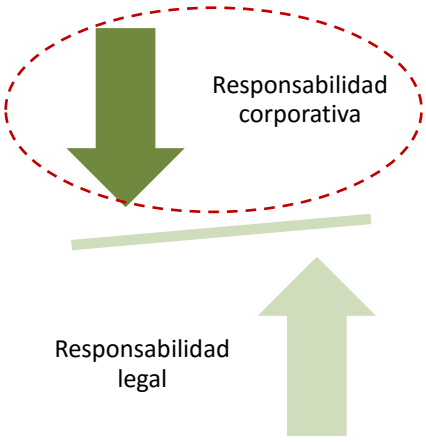


4. El análisis de riesgos dentro de los PSO y los PPE

- MAASERISv2.1 (Metodología para el Análisis, Auditoría de seguridad y Evaluación de Riesgo operativo de redes Industriales y sistemas SCADA) es un conjunto de procesos, herramientas y entregables que permiten:

Industrial Cybersecurity by LOGITEK

7. Conclusiones



- Proceso & Proyecto
- La alta dirección se acerca a la seguridad
- Seguridad de forma integral

Industrial Cybersecurity by LOGITEK

Industrial Cybersecurity by LOGITEK

iberquimia
Congreso de Industria Química

MADRID - 27 y 28 abril 2016

La Ley PIC en la Industria Química

¿A qué me obligan los PSO y los PPE?
¿Cómo puede ayudarme Logitek?

Dr. Fernando Sevillano
Solution Managers Director
fernando.sevillano@logitek.es