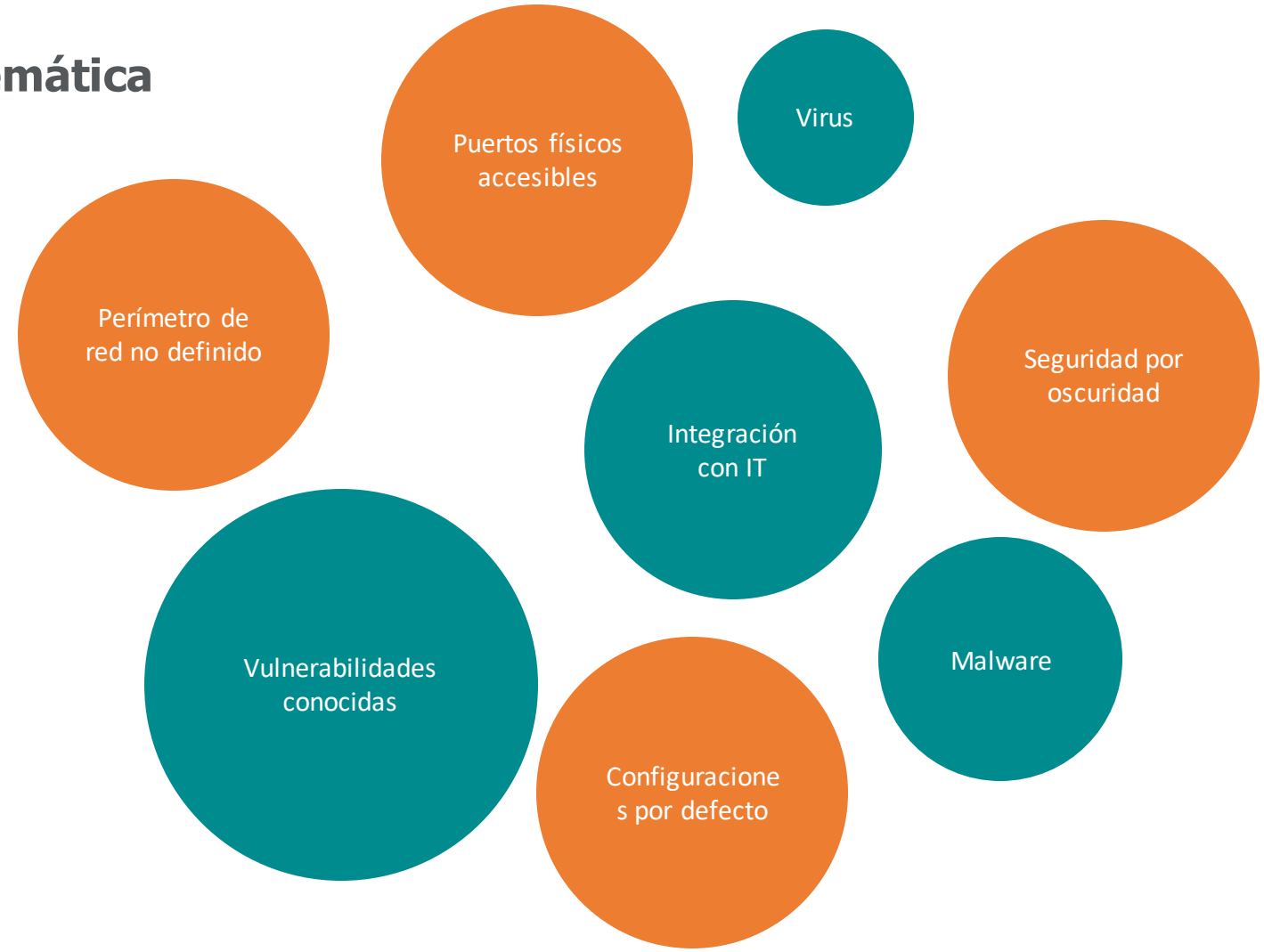
Sothis

Sothis SICS (Secured Industrial Control System)

Ciberseguridad Industrial. Problemática

Los entornos industriales se han visto cada vez más amenazados en los últimos años, debido en gran parte a:

- La estandarización de tecnologías IT en el ámbito industrial
- Proliferación del acceso web a los sistemas SCADA
- Adopción de paradigmas como cloud, móvil, BYOD, IIoT, Industria 40.0
- Hoy en día casi cualquier dispositivos dispone de conexión RJ45 y funciona bajo ethernet
- No siempre es posible desplegar las mismas contramedidas que en IT



Hoy en día, el panorama de amenazas industriales sigue siendo en gran parte desconocido, debido a la falta de recopilación de datos en las redes industriales, y existe una escasez crítica de profesionales con experiencia en seguridad cibernética de ICS para analizar los datos en busca de amenazas.

Problemas de seguridad de los sistemas de Automatización Industrial "tradicionales"

Los sistemas de control y automatización industrial 4.0 comparten características con los sistemas TI

La forma de resolverlo

Es indispensable, la incorporación de tecnologías de monitorización y vigilancia, que ayuden a detectar anomalías de forma temprana en las redes OT y que se integren totalmente con los SOCs

Vigilancia y Monitorización

Es necesario identificar los activos y entender a qué riesgos se enfrentan, entender las amenazas internas y externas, y desarrollar medidas que ayuden a reducir el impacto que pudiera provocar que una amenaza se materialice

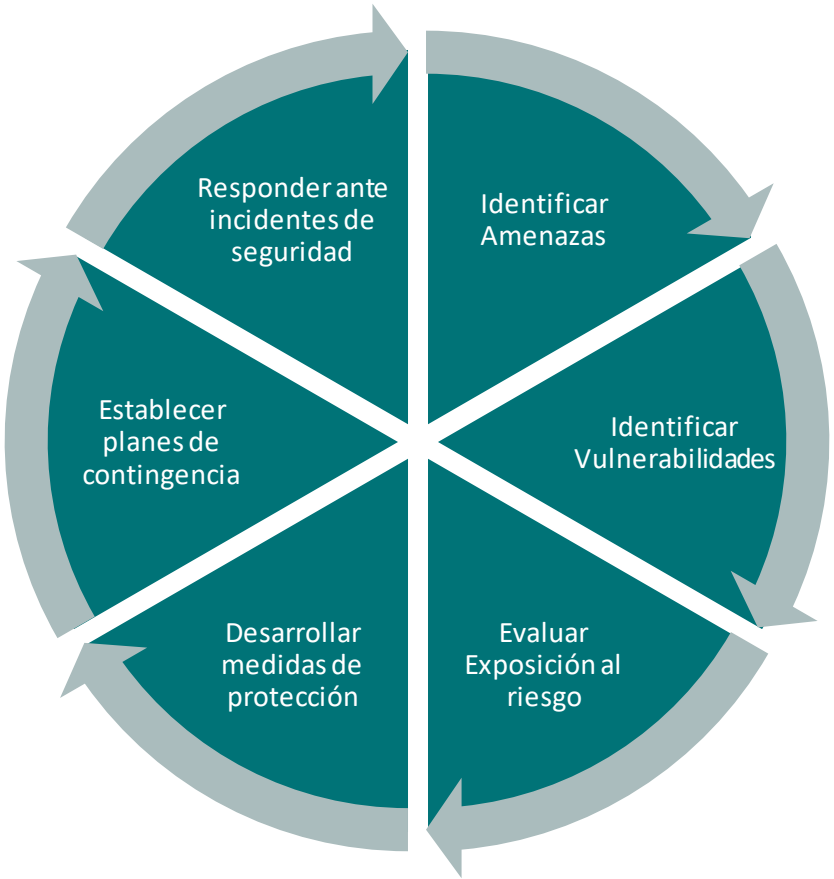
Servicios Auditoria

La ciberseguridad industrial empieza por la selección de los elementos HW/SW adecuados. Cualquier servicio a este respecto debe integrar no sólo un profundo conocimiento de la parte IT sino también de Entornos Industriales y de Automatismo y Control

Seguridad Física

SICS 360º

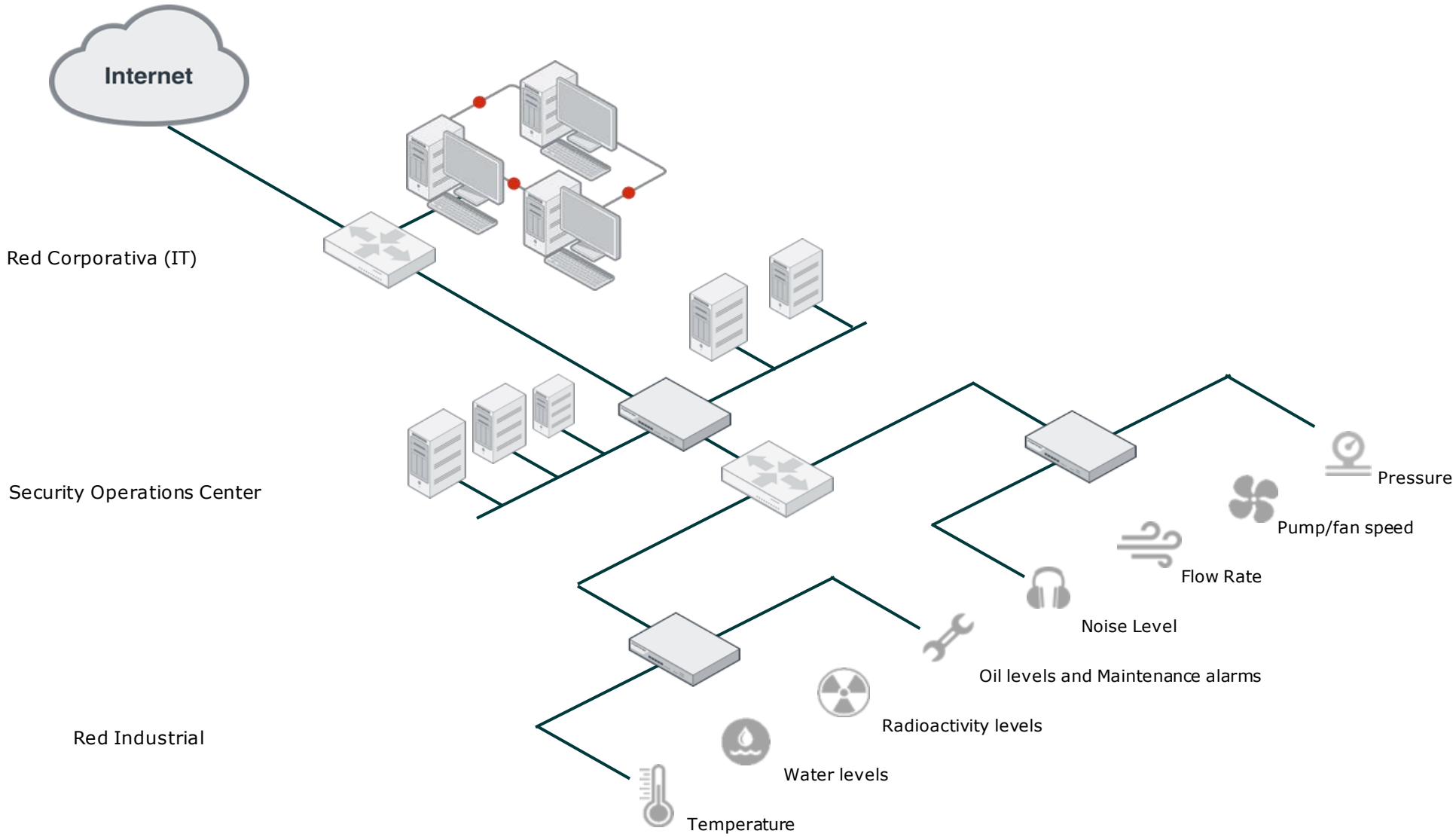
- **Identificar amenazas**: entender las amenazas externas e internas de ciberseguridad por uso inapropiado o falta de conocimiento.
- **Identificar vulnerabilidades**: identificar todos los activos y entender los riesgos a los que se enfrentan.
- **Evaluar Exposición al riesgo**: Determinar las probabilidad de que las vulnerabilidades puedan ser explotadas.
- **Desarrollar medidas de protección**: Reducir el impacto que pudiera provocar que una amenaza se materialice
- **Establecer planes de contingencia**: Desarrollar un plan de acción para reducir el impacto de las amenazas
- **Responder ante incidentes de seguridad**: Responder y recuperar el estado de normalidad tras un incidente de seguridad



Leyes, normativas y estándares

Formación y concienciación

ICS Security

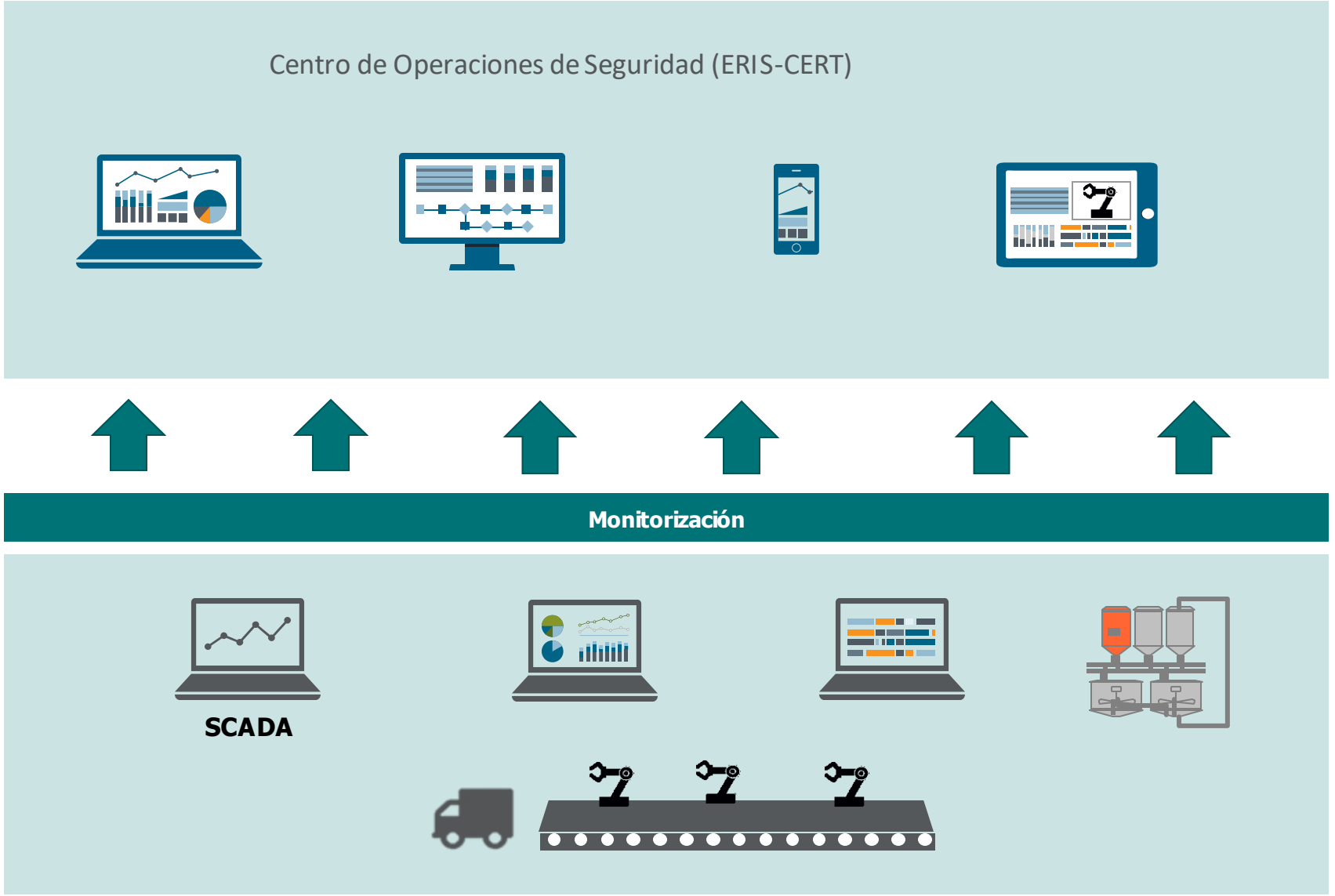


¿Cómo se hace?

Lo principal es la incorporación de tecnologías de monitorización y vigilancia que ayuden a detectar anomalías de forma temprana en las redes OT y que se integren totalmente con los servicios de SOC.

Así, desde el SOC se debe poder monitorizar, entre otros:

- Cambios en el Firmware de los PLC
- Latencia en las respuestas de los PLC
- Cambios en el Firmware del HMI
- Login fallido en el HMI
- Creación de cuentas de usuario en el Sistema Operativo
- Incremento del "payload" de los paquetes de datos
- Cambios de dispositivos HW en PLC/RTU



Sothis

PATERNA – VALENCIA (HQ)
Ronda Auguste y Louis Lumière, 23
Naves 20, 19 y 18
Parque Tecnológico de Paterna
Paterna 46980 Valencia

VALENCIA
Edificio América, Plaza
América, 2
Planta 4ª y 5ª
46004 Valencia

MADRID
C/ Torrelaguna, 77
Planta 2ª
28043 Madrid

BARCELONA
Edificio Diagonal
Mar B2 C/ Josep Plà
2 – Planta 8
08019 Barcelona

VALLADOLID
C/ Cobalto, 15
Polígono San Cristóbal
47012 Valladolid

Phone. +34 902 88 35 33
Fax. +34 902 90 89 49

www.sothis.tech