

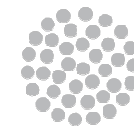


CIBERSEGURIDAD INDUSTRIAL

Situación y Desafíos

Carlos Jaureche B.

cjaureche@indracompany.com



indra

CIBERSEGURIDAD INDUSTRIAL

- **Ciberseguridad Industrial:** conjunto de prácticas, procesos y tecnologías diseñadas para gestionar el riesgo proveniente del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información utilizada en las organizaciones e infraestructuras industriales, utilizando las perspectivas de personas, procesos y tecnologías.
- Los sistemas de control industrial son fundamentales para la sociedad y la economía de los países. Las infraestructuras como sus sistemas se han convertido en objetivos de ataque.

DESAFÍO: Construir una cultura de la Ciberseguridad Industrial destinada a mejorar la seguridad de las instalaciones industriales

CONTEXTO

- Proceso de **convergencia e interdependencia** entre sistemas TIC clásicos y sistemas de control industrial.
- Abandono de sistemas y protocolos limitados al mundo industrial a favor de **estándares abiertos y tecnologías de uso común** en ámbitos TIC.
- Las instalaciones actuales deben **adaptarse** para combatir amenazas para las que no están diseñadas.

AMENAZAS, DESAFIOS Y PRIORIDADES

- **Cultura de Ciberseguridad**
- **Medir y analizar el riesgo**
- **Protección: reducir el riesgo y mitigar los impactos**
- **Detección y gestión de incidentes**
- **Colaboración y Coordinación**
- **Investigación**

Fuente: Centro Ciberseguridad Industrial de España

AMENAZAS, DESAFÍOS Y PRIORIDADES

CULTURA DE CIBERSEGURIDAD

Establecimiento de responsabilidades dentro de las organizaciones

Financiación de medidas complicada cuando la Dirección desconoce el tema

Falta de estándares específicos

Escasa coordinación entre iniciativas gubernamentales y privadas

Necesidades diferentes para para sectores industriales diferentes

Fomentar la Ciberseguridad en Industria igual que física / laboral / procesos

Desarrollo de currículo, programa formativo para carreras relacionadas

AMENAZAS, DESAFÍOS Y PRIORIDADES

MEDIR Y ANALIZAR EL RIESGO

Inventario de activos implicados en ciberseguridad no es adecuadamente conocido

No existe conocimiento formal del riesgo, amenazas y vulnerabilidades

Falta de herramientas prácticas y eficientes para evaluación del riesgo

Integración de los riesgos de ciberseguridad dentro de las herramientas y sistemas de gobierno corporativo que incluyen la gestión de otros riesgos de negocio.

AMENAZAS, DESAFÍOS Y PRIORIDADES

PROTECCIÓN: REDUCIR EL RIESGO Y MITIGAR LOS IMPACTOS

Conectividad sin control entre sistemas de control y redes TIC

Acceso remoto de múltiples partes sin control adecuado

Sistemas diseñados para operar en entornos fiables

Escasez de parches y actualizaciones. Dificultad para aplicarlos

Herramientas que permitan la captura y retención de logs de los sistemas en tiempo real de cara al análisis forense

Falta de entornos de prueba (testbeds)

AMENAZAS, DESAFÍOS Y PRIORIDADES

DETECCIÓN Y GESTIÓN DE INCIDENTES

Medidas de seguridad pueden afectar negativamente respuesta a emergencias

Incremento de la sofisticación de herramientas y ataques

No existen medidas equivalentes a los entornos TIC tradicionales

Definir proceso de identificación de vulnerabilidades y notificación de incidentes

Detectar incidentes en curso

AMENAZAS, DESAFÍOS Y PRIORIDADES

COLABORACIÓN Y COORDINACIÓN

Resistencia a compartir información potencialmente debilitadora

Ausencia de normativa específica

Establecer medidas de seguridad no es prioridad de los negocios

AMENAZAS, DESAFÍOS Y PRIORIDADES INVESTIGACIÓN

Escasez de iniciativas específicas en Ciberseguridad Industrial

Gran espacio de mejora en las herramientas y servicios relacionados a Ciberseguridad Industrial

Falta de conocimiento específico en el tema

Escasa vigilancia tecnológica en Ciberseguridad Industrial

ASEGURAMIENTO DE LA CADENA DE VALOR (I...)

Las etapas de la cadena de valor que se benefician del modelo son las siguientes:







- **Planificación producción**
- **Fabricación y Distribución**
- **Ingeniería**
- **Mantenimiento**
- **Centros de Operación y Control**



OBJETIVO: Implantar un modelo dinámico y de mejora continua de la seguridad mediante la aplicación de prácticas, procesos y tecnologías diseñadas para proteger los activos que soportan LA CADENA DE VALOR.

ASEGURAMIENTO DE LA CADENA DE VALOR (...II...)

Y, ¿DÓNDE DEBEN PROTEGERSE?

| <p>EJEMPLOS A TENER EN CUENTA PARA LA SEGURIDAD</p>  | <p>PLANIFICACIÓN</p>  <p>Plan Director Arquitectura de Red</p> | <p>INGENIERÍA</p>  <p>Diseño Arquitectura de la Red Nuevas instalaciones Balance rendimientos</p> | <p>MANTENIMIENTO</p>  <p>Correctivo Preventivo, Predictivo Ejecución Análisis</p> | <p>CENTRO CONTROL</p>  <p>Preparar cortes programados Gestión de la red de Tiempo Real y de los cortes programados</p> | <p>FABRICACIÓN</p>  <p>Planificación Diseño Ejecución Órdenes de Trabajo</p> |
|---|---|---|--|---|---|
| <p>➤ Adquisición de datos online.</p> | | | ✓ | ✓ | ✓ |
| <p>➤ Actualización HW/SW de dispositivos distribuidos</p> | | | ✓ | ✓ | ✓ |
| <p>➤ Importación/Exportación de información sensible (con terceros)</p> | ✓ | ✓ | ✓ | ✓ | ✓ |
| <p>➤ Cadena de suministro de servicios y activos (contratistas/fabricantes)</p> | | ✓ | ✓ | ✓ | ✓ |
| <p>➤ Transmisión de órdenes de servicio (movilidad)</p> | | ✓ | ✓ | ✓ | ✓ |

ASEGURAMIENTO DE LA CADENA DE VALOR (...III...)

PERO, ¿A QUÉ SE ENFRENTAN LAS ORGANIZACIONES?

Proliferación de dispositivos embebidos vulnerables.

El nivel de interconexión entre redes y dispositivos es cada vez mayor.

Coexistencia de dispositivos de antigüedad muy heterogénea.

Los dispositivos seguros de hoy presentarán vulnerabilidades mañana.

La seguridad por simplicidad reemplazará a la seguridad por oscuridad.

Dificultad para establecer estándares internacionales.

Más información pública sobre herramientas y modos de ataque.

Los operadores tienen un conocimiento parcial de los riesgos existentes.

Seguridad física, ciberseguridad y cumplimiento legal deben estar alineados.

Buscar la resiliencia de las infraestructuras como equilibrio entre medidas de prevención, detección y respuesta.

ASEGURAMIENTO DE LA CADENA DE VALOR (...IV...)

Y, ¿CÓMO?



INDEX

SEGURIDAD PARA INFRAESTRUCTURAS INDUSTRIALES

Aseguramiento de la Cadena de Valor

Protección de las Infraestructuras Físicas

Arquitectura de Seguridad en Redes de Control

Seguridad en la “Última Milla”

Gobierno de la Seguridad

Formación y Concientización de Seguridad



indra

PROTECCIÓN DE LAS INFRAESTRUCTURAS FÍSICAS



La migración de los grandes sistemas analógicos de la industria hacia la digitalización, el mundo TIC y la creciente interconexión de sistemas, ha supuesto el aumento del riesgo y añadido complejidad a las soluciones.

Protección de los sistemas y redes que operan las infraestructuras críticas. Desarrollo e implantación de planes de Seguridad del Operador (**PSO**) y Planes de Protección Específicos (**PPE**) para Plantas de Producción, sistemas de control, redes de distribución...



PROTECCIÓN DE LAS INFRAESTRUCTURAS FÍSICAS

INTEGRACIÓN DE SISTEMAS

- Unión inteligente de sistemas diversos.
- Interconexión de sistemas complejos de seguridad.
- Creación de centros de control integrados.
- Coexistencia de sistemas diferentes en una única solución.
- Incorporación de distintos tipos de alarmas y productos de terceros.
- Flexibilidad y adaptación a cambios y ampliaciones.
- Simplicidad de operación y mantenimiento.
- Integración de todo tipo de comunicaciones (PDA's, móviles, ...).



INDEX

SEGURIDAD PARA INFRAESTRUCTURAS INDUSTRIALES

Aseguramiento de la Cadena de Valor

Protección de las Infraestructuras Físicas

Arquitectura de Seguridad en Redes de Control

Seguridad en la “Última Milla”

Gobierno de la Seguridad

Formación y Concientización de Seguridad



indra

ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL



- ➔ DISEÑO DE PLATAFORMAS SEGURAS
- ➔ BENCHMARKING DE SOLUCIONES DE SEGURIDAD
- ➔ IMPLANTACIÓN DE SOLUCIONES TECNOLÓGICAS
- ➔ SECURIZACIÓN DE INFRAESTRUCTURAS TECNOLÓGICAS

- Soluciones de seguridad específicas para entornos **SCADA/DCS**:
 - Detección de **puntos de acceso** vulnerables.
 - Tests de intrusión y despliegue de honey-pots para seguimiento de **amenazas**.
 - Implantación de **seguridad perimetral**: Firewall, NAC, IPS/IDS, Diodos de datos, etc.
 - **Control de comportamiento** de procesos: Whitelisting, Sandboxing, Virtual Patching, etc.
 - Soluciones personalizadas **por ámbitos**:
 - Seguridad en planta.
 - Seguridad de redes: aislamiento de segmentos y células de seguridad.
 - Seguridad de dispositivos embebidos.
 - Seguridad de sistemas de control.

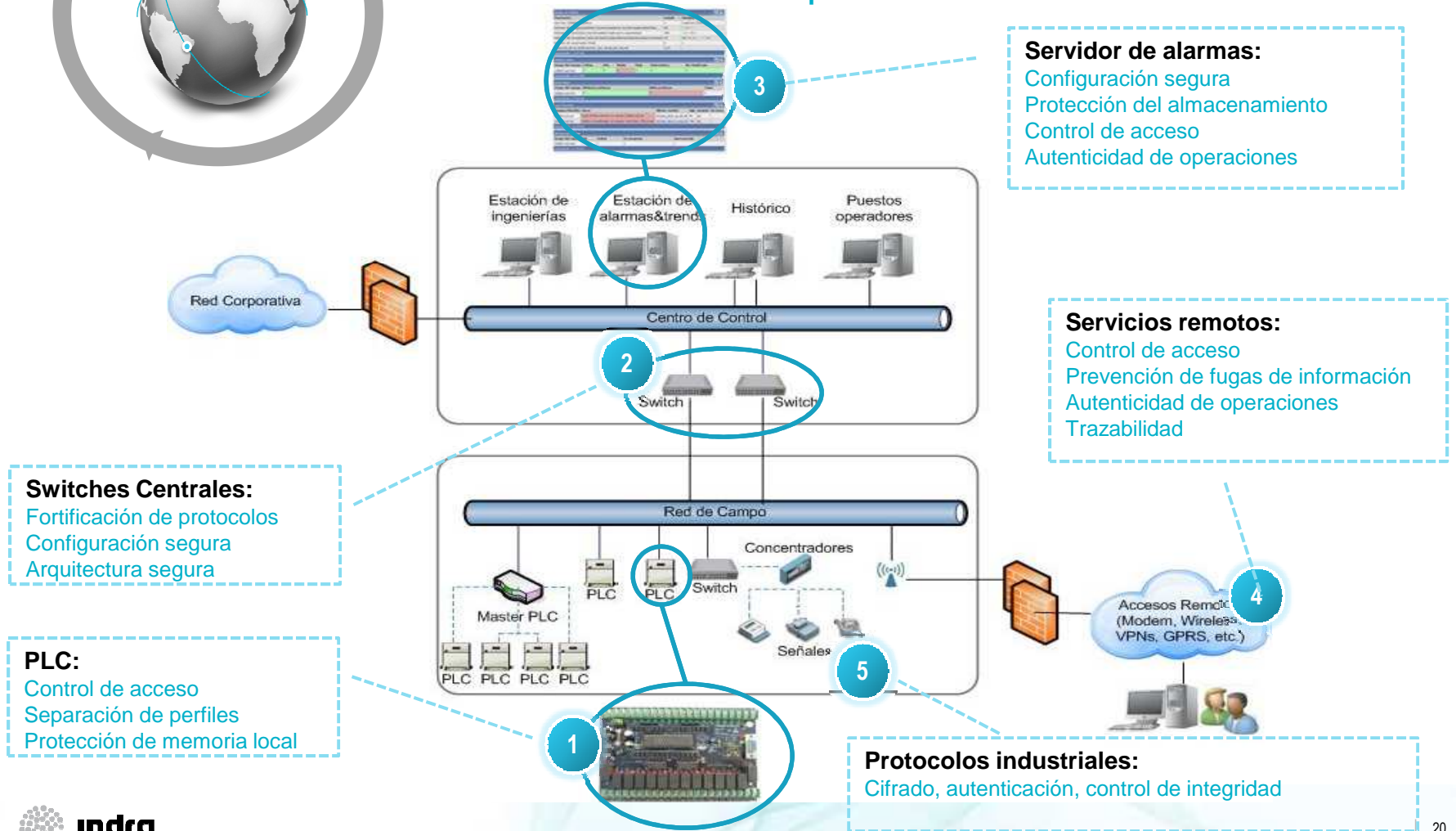


ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL



- Soluciones de seguridad específicas para entornos **SCADA/DCS**:

- Detección de **puntos** vulnerables.

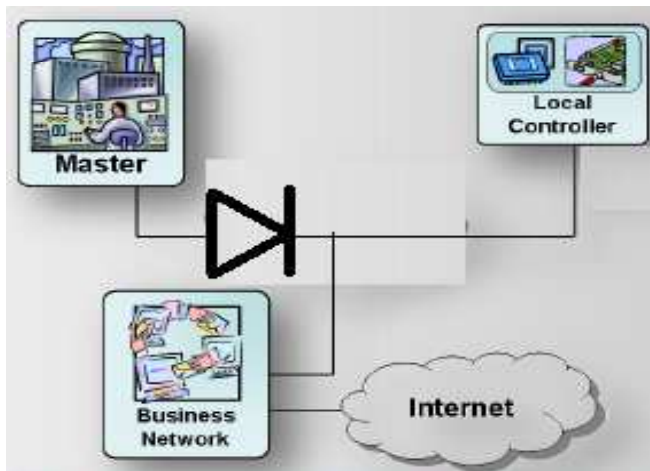


ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL

Barreras lógicas

- Confinamiento para redes de proceso críticas.
- Solución más allá del firewall y/o del datadiodo.
- Elimina la mayor parte de las potenciales amenazas, pero no todas, por lo que debe complementarse con niveles de contención adicionales.

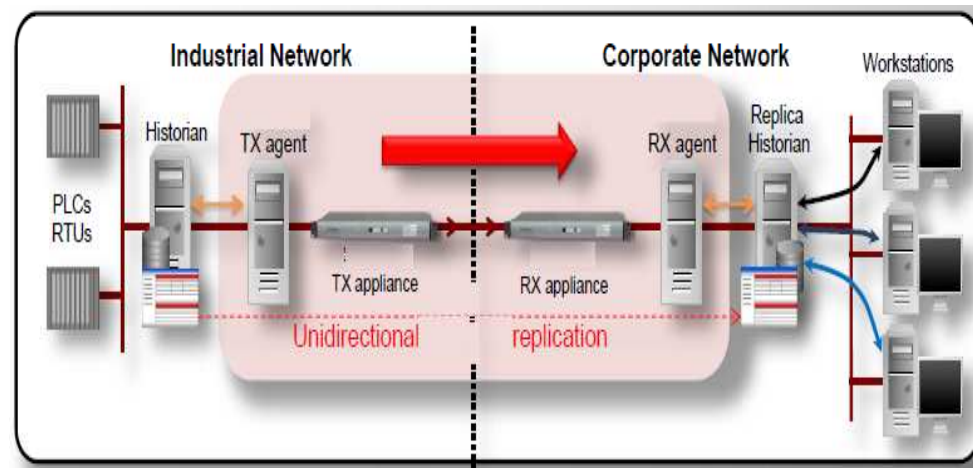
ANTES (datadiodo)



- *Dificultad de monitorización de seguridad fuera de la red de proceso.*
- *Dificultad de visibilidad de negocio fuera de la red de proceso.*
- *Dificultad de mantenimiento .*



DESPUÉS (Gateway unidireccional con) conectores



- *Monitorización tanto de seguridad como de negocio fuera de las redes de proceso.*
- *Replicación segura en tiempo real fuera de las redes de proceso.*
- *Amplia implantación en USA.*

ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL

Quioscos de sanitización

Permiten comprobar que los elementos externos (*) que deban conectarse a las redes internas de proceso en planta, en muchos casos redes aisladas, están libres de malware. De este modo, las tareas de revisión y mantenimiento no se convierten en una fuente de vulnerabilidades.

(*) Memorias USB, portátiles, CDs/DVDs, etc...



- La tecnología multiscaning multiplica la eficacia frente al antivirus tradicional.
- La tecnología OPSWAT es muy utilizada en EEUU. Las principales compañías con infraestructuras críticas lo utilizan.
- Facilita cumplimientos regulatorios presentes y/o futuros.

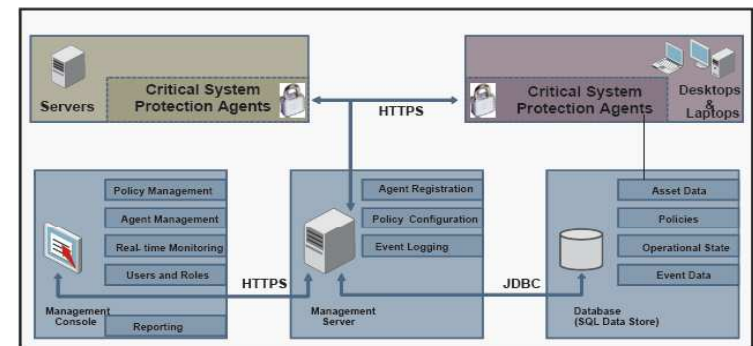
ARQUITECTURAS DE SEGURIDAD EN REDES DE CONTROL

LA SEGURIDAD MULTINIVEL

3º NIVEL: SANDBOXING Y BASTIONADO

Mitigación de riesgos inherentes bloqueando servicios innecesarios que pudieran explotar vulnerabilidades presentes en equipos desactualizados (*), permitiendo:

- Realizar un **bastionado** del sistema:
 - Supervisión de integridad de archivos
 - Supervisión de la configuración
 - Políticas de prevención de intrusión
 - Administración centralizada
 - Integración con plataformas SIEM
- Controlar los **privilegios de control de acceso**
- Desplegar en **múltiples tipos de SO**: Vmware, Windows, Solaris, Linux, AIX, HP-UX, etc.
- Soporte de múltiples releases de **Sistemas Operativos NO parcheables**



(*) *Windows XP descontinuado soporte en 2014.*

INDEX

SEGURIDAD PARA INFRAESTRUCTURAS INDUSTRIALES

Aseguramiento de la Cadena de Valor

Protección de las Infraestructuras Físicas

Arquitectura de Seguridad en Redes de Control

Seguridad en la “Última Milla”

Gobierno de la Seguridad

Formación y Concientización de Seguridad



indra

SEGURIDAD EN LA “ULTIMA MILLA”



- ⇒ SEGURIDAD, OPERACIÓN Y RENDIMIENTO
- ⇒ GESTIÓN DE SUMINISTRADORES
- ⇒ PREVENCIÓN DEL FRAUDE A GRAN ESCALA

- Soluciones de seguridad específicas para **Smart Metering**:
 - Seguridad en las especificaciones para el **sistema central de telegestión**:
 - Protocolos seguros.
 - Autenticación de concentradores y RTUs.
 - Autenticación de procesos.
 - Seguridad en las especificaciones para los dispositivos del entorno PLC (**DLMS/COSEM y PRIME**):
 - Securización de la información y las órdenes.
 - Protección de uso de TPLs y Smart-phones.
 - Gestión segura de las claves de contadores, concentradores y RTUs.
 - Ajuste fino de medidas de seguridad para no impactar en los KPIs de comunicaciones.



INDEX

SEGURIDAD PARA INFRAESTRUCTURAS INDUSTRIALES

Aseguramiento de la Cadena de Valor

Protección de las Infraestructuras Físicas

Arquitectura de Seguridad en Redes de Control

Seguridad en la “Última Milla”

Gobierno de la Seguridad

Formación y Concientización de Seguridad



indra

GOBIERNO DE LA SEGURIDAD



- ⇒ CONSULTORÍA DE SEGURIDAD.
- ⇒ PLANIFICACIÓN Y DIAGNÓSTICO
- ⇒ CONTROL, GOBIERNO Y AUDITORÍA
- ⇒ ACREDITACIÓN

- **REORDENAR** Definición de la función de la seguridad.
- Aseguramiento de la cadena de suministro.
- Adecuación a la legislación vigente.
- Alineamiento con normas y estándares.
- Acreditación (Common Criteria, FIPS...)
- Auditorías normativas (ISO, SOX, PCI...).
- Consultoría técnica de seguridad.
- Definición planes de ciberseguridad y continuidad de negocio.
- Auditorías técnicas (Hacking ético, análisis de vulnerabilidad, SCA...).
- Auditorías de políticas internas. Identificación y cumplimiento de la reglamentación propia
- Análisis forense. Revisiones “post-mortem” de incidentes.



INDEX

SEGURIDAD PARA INFRAESTRUCTURAS INDUSTRIALES

Aseguramiento de la Cadena de Valor

Protección de las Infraestructuras Físicas

Arquitectura de Seguridad en Redes de Control

Seguridad en la “Última Milla”

Gobierno de la Seguridad

Formación y Concientización de Seguridad

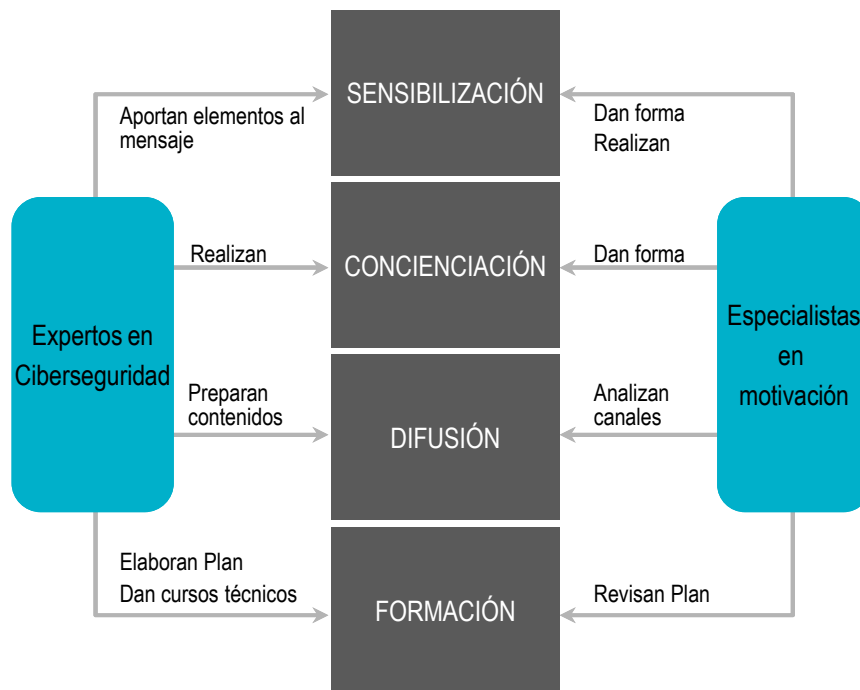


indra

FORMACIÓN Y CONCIENTIZACIÓN



Tan importante como la existencia de un nivel de seguridad adecuado a los riesgos existentes, es la percepción del nivel de seguridad y de riesgo que tienen los actores, y la concienciación de los mismos en su rol para preservar la seguridad.



○ Por ello cada vez es más necesario dotar a los diferentes actores de entrenamiento y documentación de apoyo.

- Elaboración de **planes de formación, divulgación y concienciación**.
- **Impartición** de cursos y seminarios.
- **Guías de Uso**. Definición de arquitecturas de seguridad homologadas. Libros blancos de desarrollo seguro y procedimientos de configuración segura (PoS).
- **Simulación y Entrenamiento**.

“La seguridad es
un proceso,
no un producto”





Security Solutions & Services

**SOLUCIONES Y SERVICIOS
EN EL ÁMBITO DE
LA SEGURIDAD**



indra