CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL

Autor: Henry Alfonso Romero Mestre

8 de enero de 2018

Directora: Angela María García Valdés

Universidad Abierta de Cataluña

Máster Interuniversitario en Seguridad de las TICs

Empresa: INCIBE

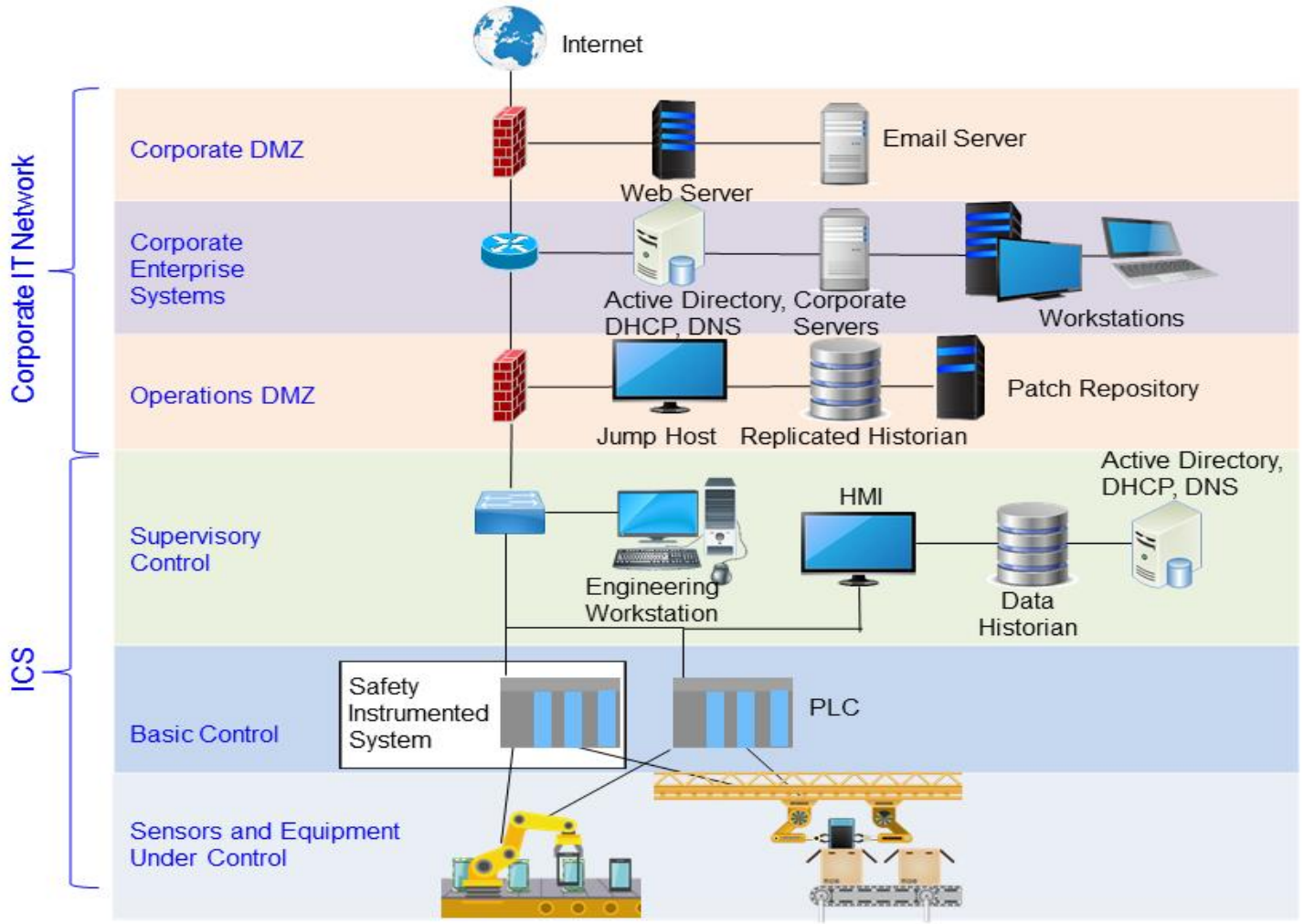
Ciberseguridad en Sistemas de Control Industrial ICSs

- Definición
- Arquitecturas, protocolos y partes de un ICS
- Relación entre las TIs y los ICSs
- Seguridad en ICSs
  - Riesgos informáticos
    - Ataques
    - Vulnerabilidades
- Recomendaciones de Securización para ICSs
- Conclusiones

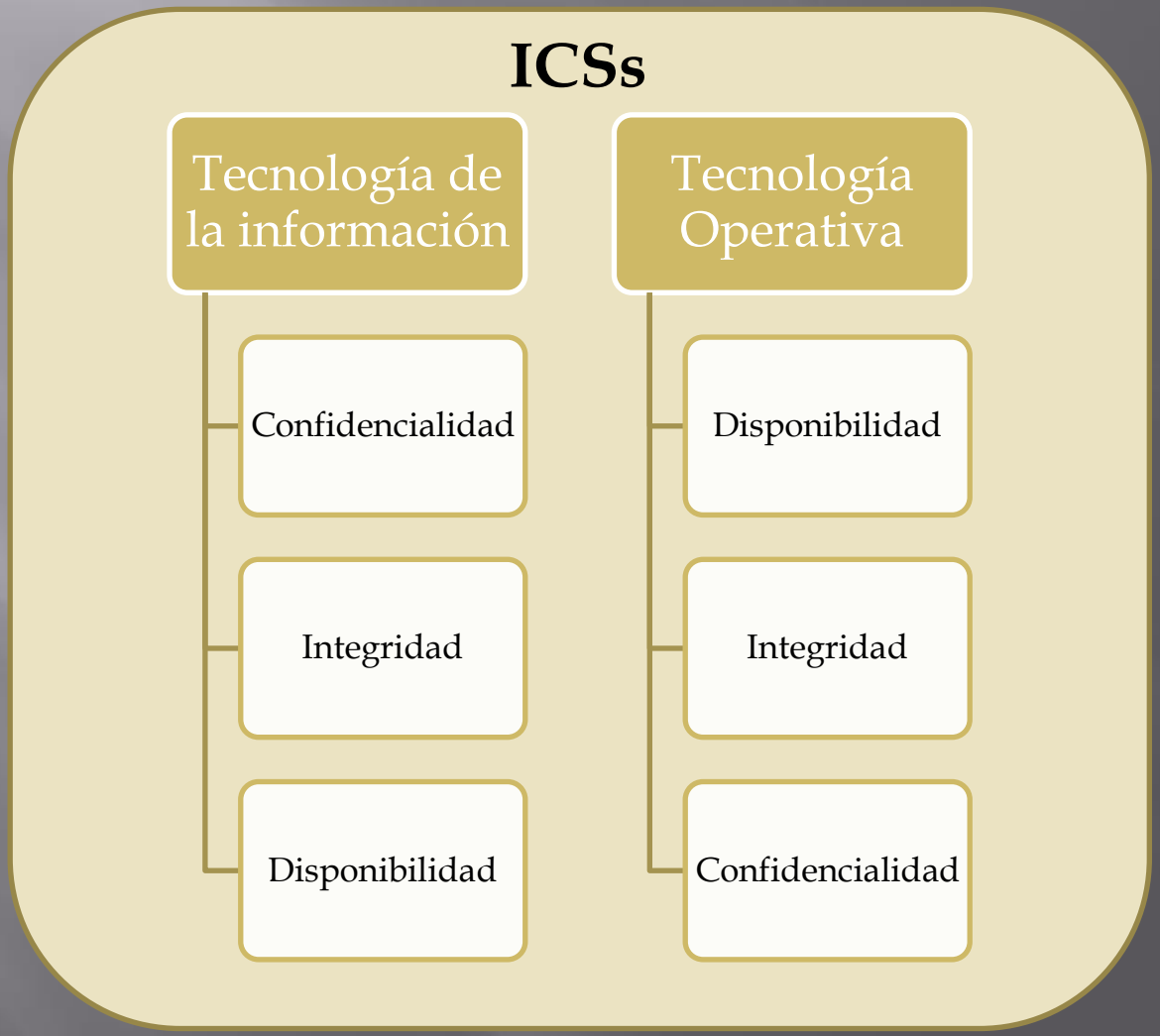
Ciberseguridad en Sistemas de Control Industrial ICSs

- ICS: sistemas compuestos por computadoras, equipos de red, buses de datos, dispositivos lógicos, dispositivos eléctricos, hidráulicos y mecánicos, y procesos manuales supervisados por humanos que monitorean y que controlan todo tipo de proceso físico.

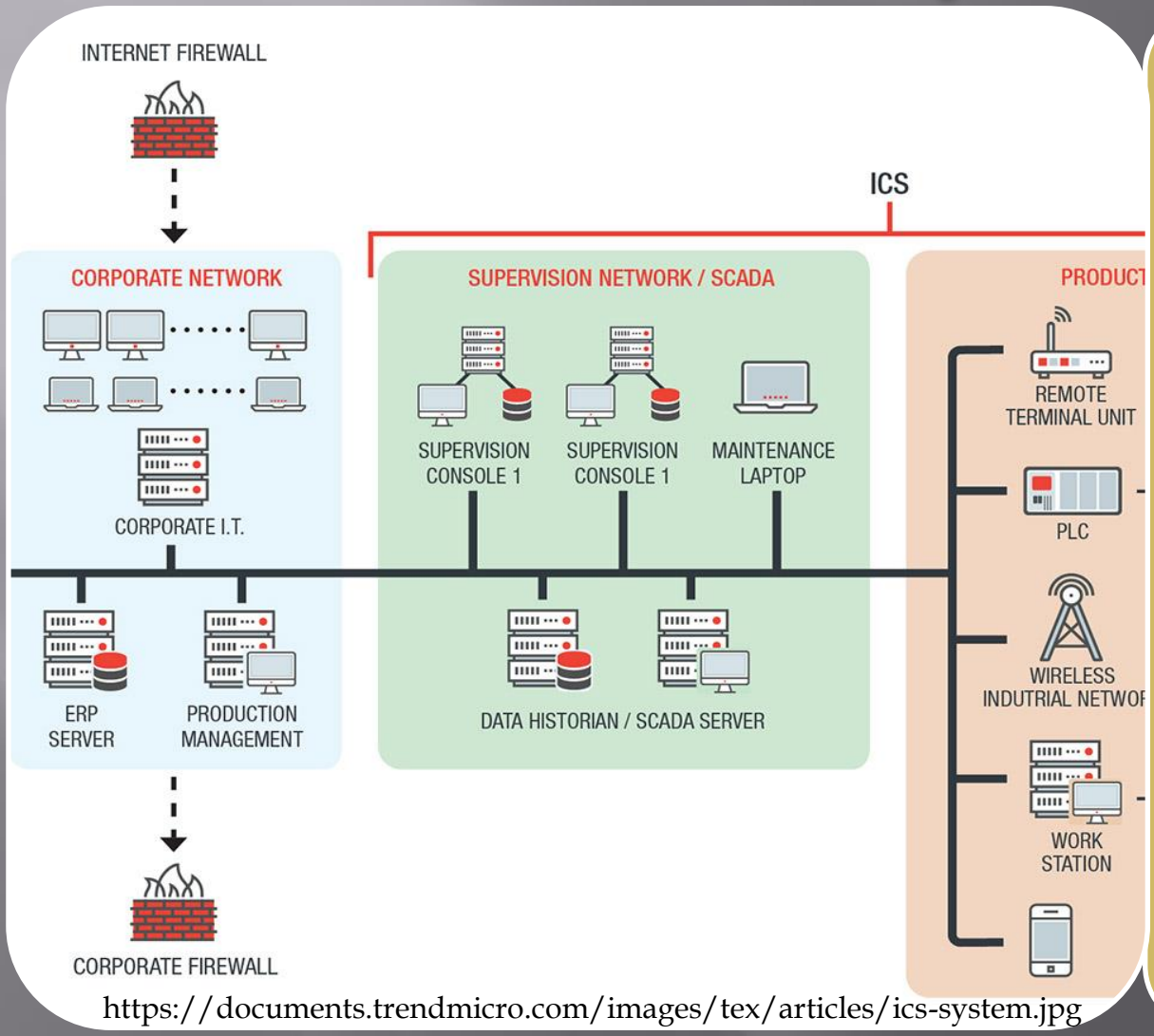
Sistemas de Control Industrial ICSs - Esquema



Sistemas de Control Industrial ICSs Tecnología de la Información TI y Tecnología Operativa TO



Sistemas de Control Industrial ICSs - Componentes

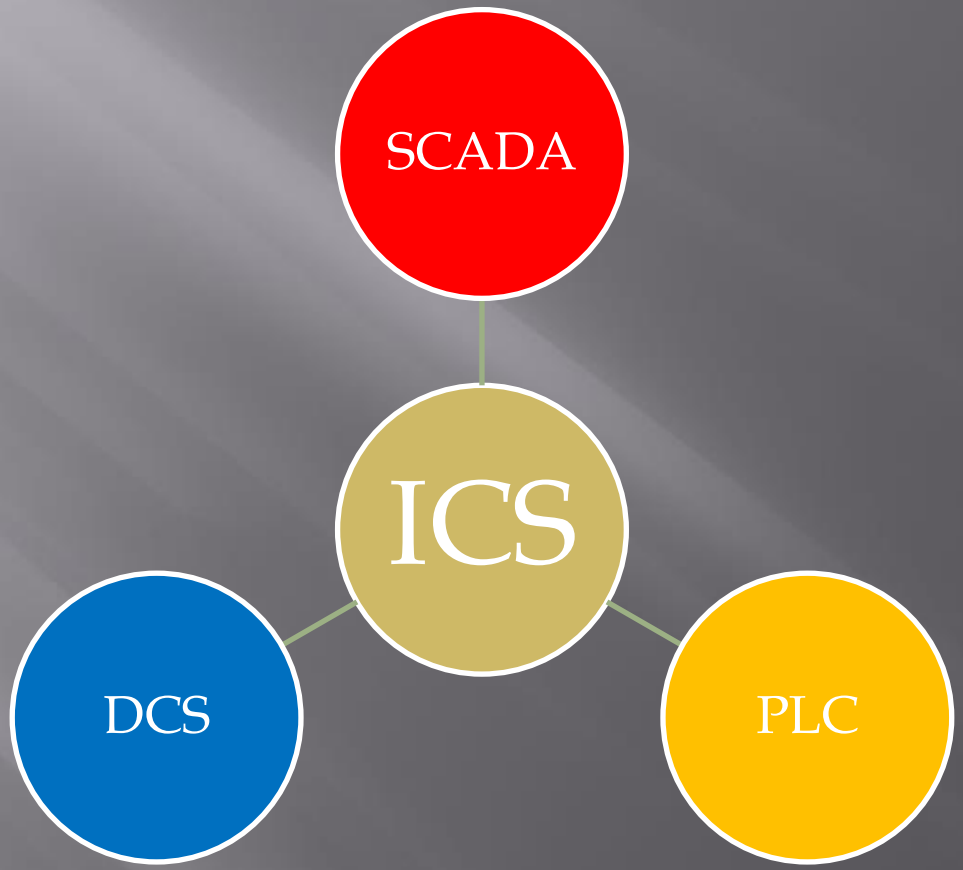


https://documents.trendmicro.com/images/tex/articles/ics-system.jpg

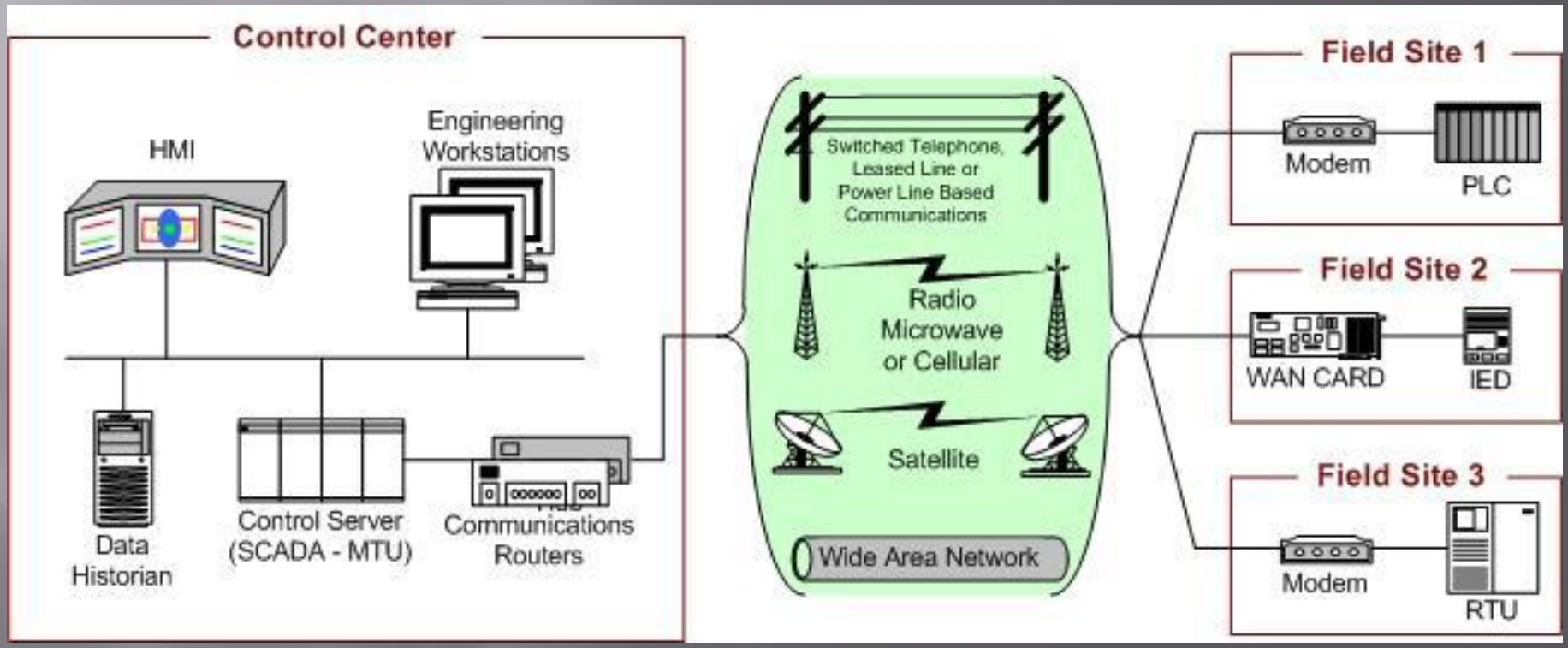
Sistemas ICSs

- PLC
- MTU
- Servidor de Control/Supervisión
- Historiadores
- HMI
- RTU
- IED
- Servidor de E/S
- Equipo de Ingeniería
- Red de Buses de Campo
- Red de Control
- Router
- Firewall
- Modem
- Punto de Acceso Remoto
- Dispositivo de Campo

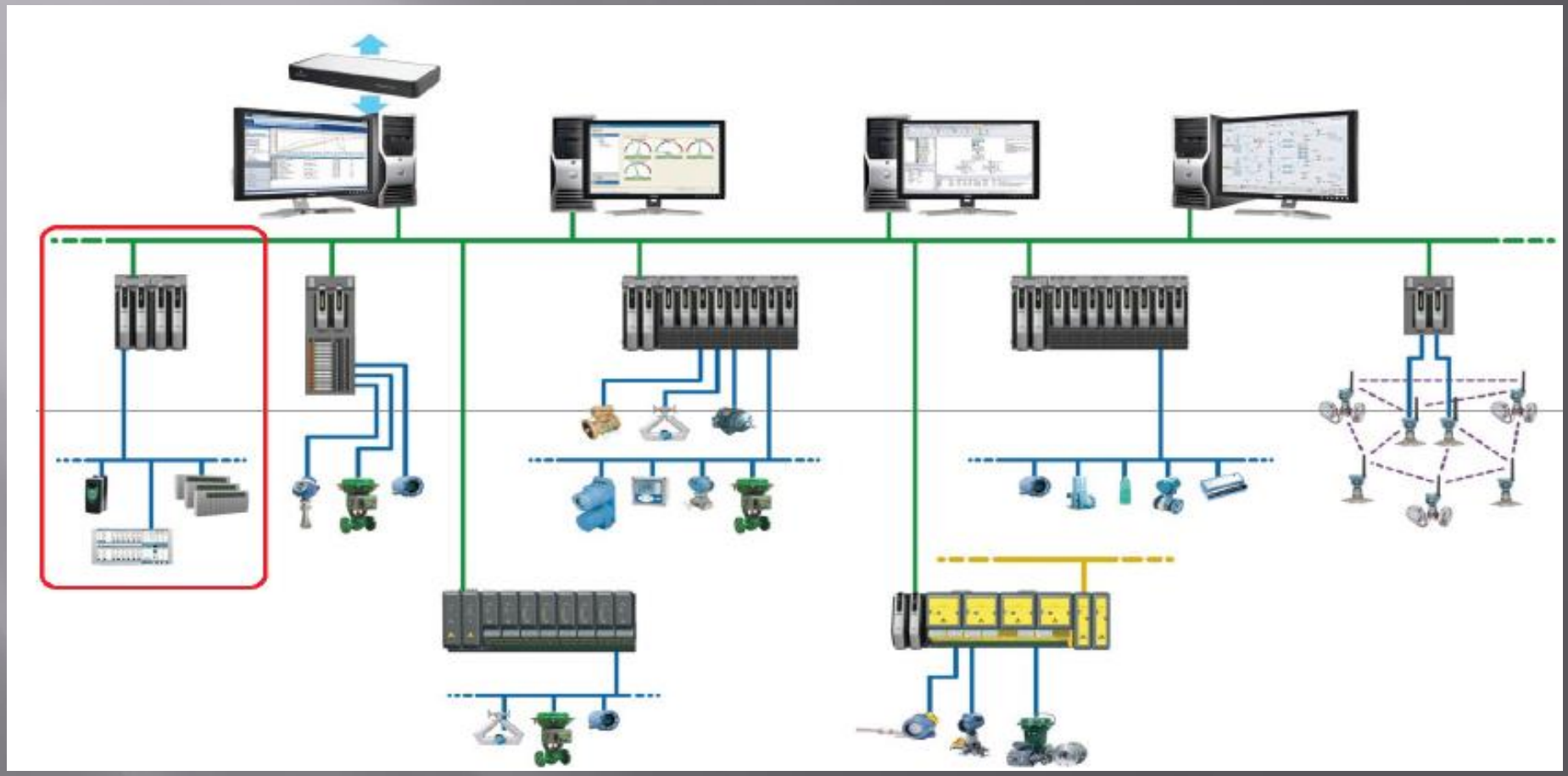
Sistemas de Control Industrial
ICSs - Tipos



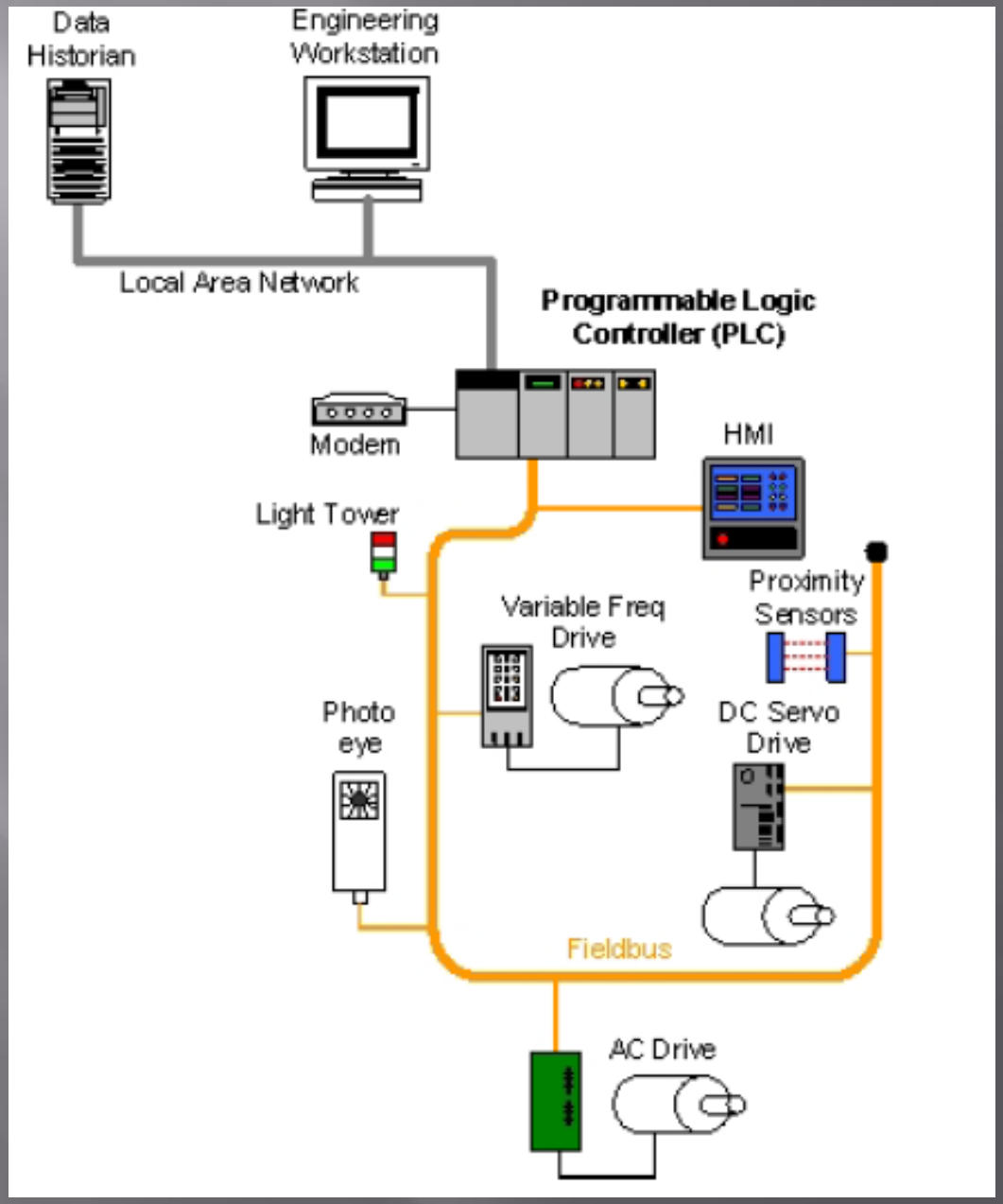
Sistemas de Control Industrial ICSs - SCADA



Sistemas de Control Industrial ICSs - DCS



Sistemas de Control Industrial ICSs - PLC



Sistemas de Control Industrial ICSs
Amenazas, Ataques y Vulnerabilidades

Fuentes de Amenazas

- Ciberdelincuentes
- Terroristas
- Gobiernos hostiles
- Competidores

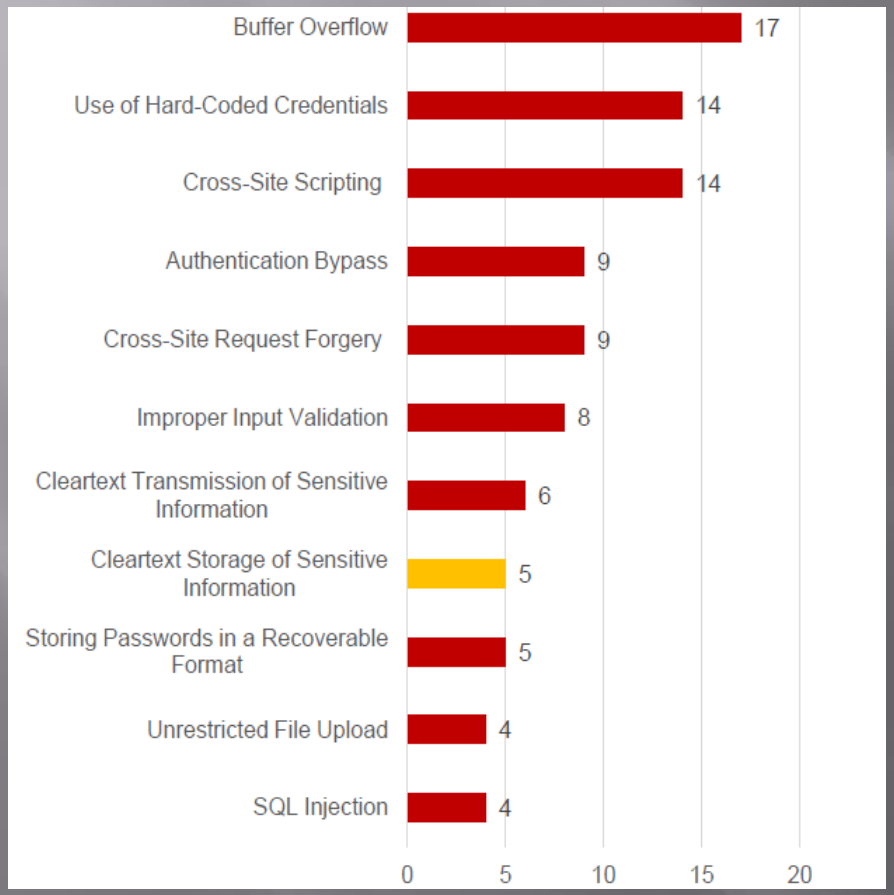
Sistemas de Control Industrial ICSs Amenazas, Ataques y Vulnerabilidades

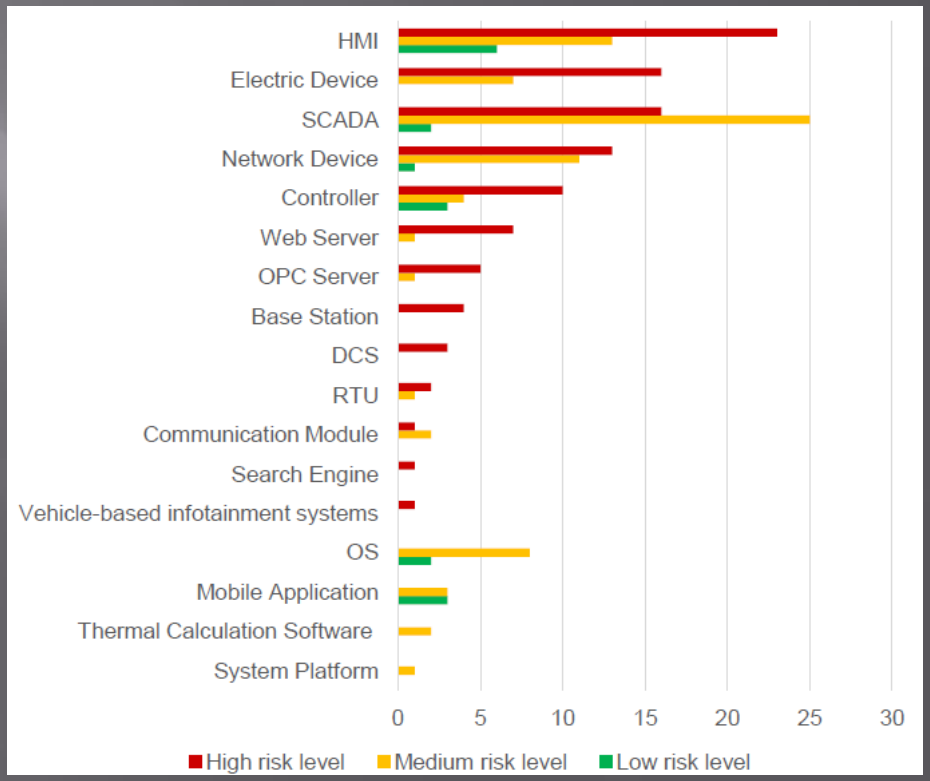
Vulnerabilidades

- Buffer overflow
- Cross Site Scripting
- Falta de una política de control de acceso adecuada
- Falta de política de contraseñas
- Mala o nula gestión de parches
- Falta de política de protección de datos
- Sistema operativo y parches de seguridad sin mantenimiento
- Utilización de software desactualizado
- Falta de instalaciones de prueba
- Uso doble de NIC
- Falta de seguridad de acceso remoto
- Vulnerabilidades de DoS y DDoS
- Uso de texto plano
- Falta de Sistema de Detección de Intrusiones (IDS) y Sistema de Prevención de Intrusiones (IPS)
- Mantenimiento deficiente del registro
- Falta de software de protección AV o Malware adecuado

Sistemas de Control Industrial ICSs Amenazas, Ataques y Vulnerabilidades

Vulnerabilidades mas frecuentes y componentes de ICSs





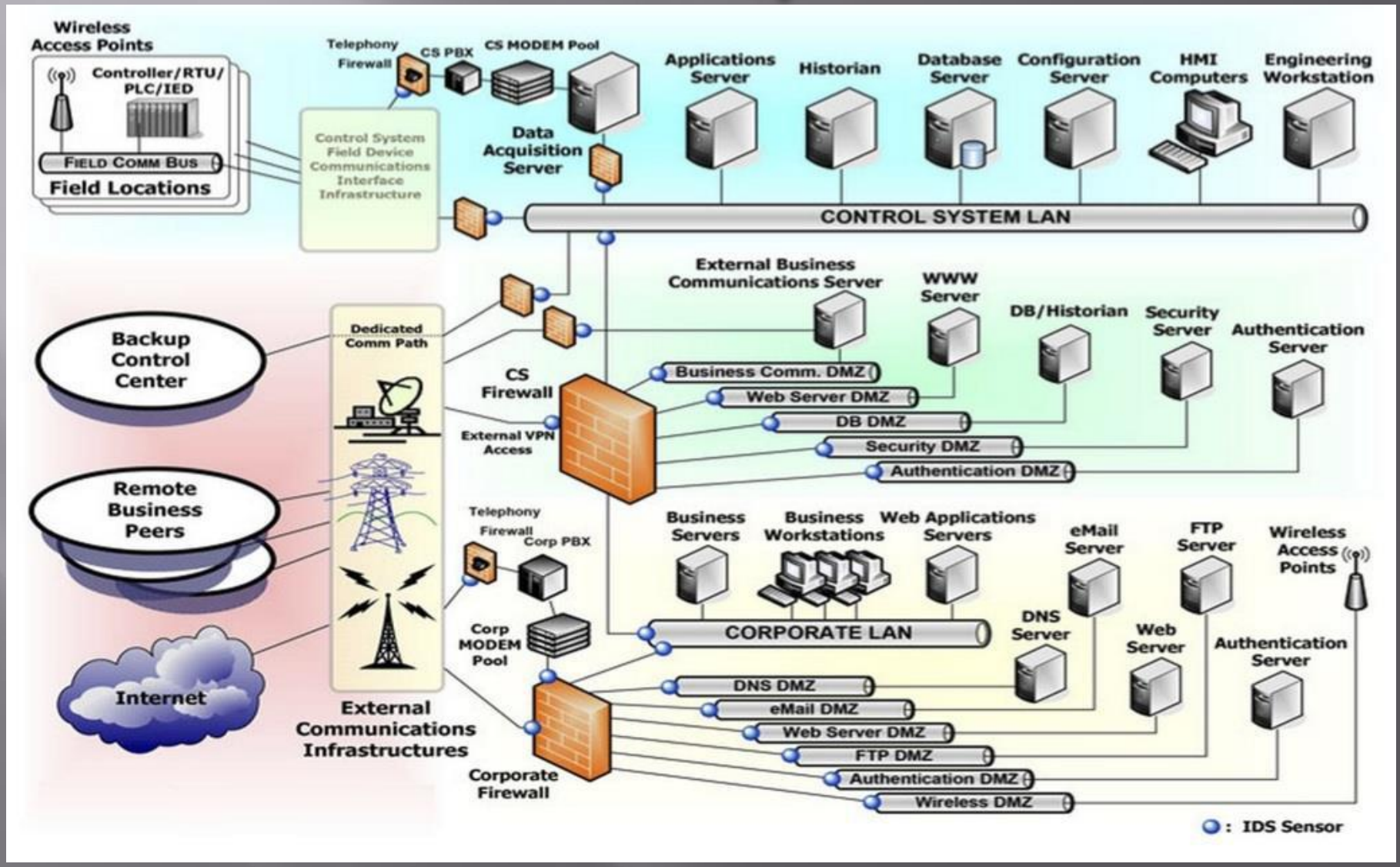
Recomendaciones de Securización para ICSs

- Tener un plan de actualización periódica de contraseñas y uso de contraseñas robustas
- Capacitar a los usuarios de la red corporativa respecto a los riesgos de seguridad que pueden afectar el sistema, tales como Phishing, Vishing, Baiting, entre otros. la Ingeniería social es una técnica que aprovecha los errores humanos para comprometer las seguridad de los sistemas,
- Agregar routers redundantes y establecer enlaces duales hacia cada uno desde las capas inferiores, tener fuentes de alimentación redundantes, suministros de energía independientes, utilizar motores de enrutamiento/redirección redundantes.
- Actualizar los equipos, por aquellos que soporten IPV6, tales como routers, firewalls, sensores y actuadores en general.
- Segmentar correctamente la red
- Construir un centro de control redundante geográficamente
- Ubicar en la zona desmilitarizada del centro de control, equipos que permitan la auditoría de los datos de los canales de comunicación con la red corporativa

Recomendaciones de Securización para ICSs

- Controlar los servicios en ejecución y/o puertos abiertos que no se utilizan.
- Cifrar las comunicaciones.
- Implementar servicios de seguridad en TCP/IP
- Usar adecuadamente los cortafuegos (o firewalls)
- Aislar a los PLCs mediante switches y routers y usar firewalls para controlar su acceso.
- Controlar el acceso físico de los elementos de los ICSs
- Usar ductería para el cableado de dispositivos de campo y red.
- Usar sistemas de prevención y/o detección de intrusiones (IDS)
- Usar paquetes antivirus/antimalware
- Implementar redes privadas virtuales (VPN) basadas en IPsec.
- implantación de:
  - Un cortafuegos
  - Red Desmilitarizada (DMZ)

Solución de Securización recomendada por el NIST



Conclusiones

- En una primera fase del proyecto se definieron los tipos de ICSs, las partes principales que lo conforman y la relación entre las OTs y las ITs. Con este estudio teórico se pudo evidenciar que existen diferentes tipos de amenazas y vulnerabilidades que se pueden presentar en los ICSs y que se derivan de él.
- Debido a la importancia de los ICSs tanto para el sector público, respecto al control de infraestructura crítica como la de generación y transporte de gas, electricidad, agua y aguas residuales; y para el sector privado, industria química, manufacturera, de ensamblaje de automóviles, entre otras; atacantes de diversas índoles y motivaciones han puesto su atención en estos y se han dedicado a encontrar deficiencias en su securización para obtener beneficios individuales y colectivos.
- En el estudio de los ICSs se encuentra que el rezago en su securización se presenta por una multiplicidad de factores, desde los concernientes a los humanos hasta los relacionados componentes presentes en las etapas finales tales como sensores y actuadores. Lo anterior nos debe llevar a la reflexión de la importancia en la capacitación especializada del personal de TI y TO en los temas de ciberseguridad para evitar o mitigar daños en los ICSs. Adicionalmente, en los diferentes estudios sobre ciberseguridad se ha encontrado que el principal factor de riesgo en la infraestructura de las empresas es el error humano lo que debe llevarnos a pensar en la realización de campañas de capacitación al personal diferente al de las áreas de TI y TO.

Conclusiones

- En muchos casos las industrias usaban ICSs con configuraciones, equipos y protocolos de comunicación propietarios, lo anterior llevaba a pensar a los encargados de las TIs y TOs que se encontraban blindados contra ataques y no tomaban medidas de seguridad. Si por algún motivo se perdía la confidencialidad de los ICSs cabía la posibilidad subsecuentes ataques.
- En los ICSs se debe tener en cuenta que hay existen otros factores importantes en sus procesos y procedimientos operacionales, así como en las consecuencias de salud, seguridad y medio ambiente debido a un fallo de un sistema o componente.
- Como los sistemas de control industrial tales como SCADA, DCS, PLCs, y otras redes de control de procesos, usan cada vez más equipos que usan internet se exponen a ataques por explotación de vulnerabilidades inherentes a ella, tales como: troyanos, gusanos, puertas trasera, etc. La amenaza de mayor resonancia ha sido el gusano Stuxnet.

Gracias