IEC 62443. Ciberseguridad de los sistemas de control

Juan Manuel Escaño González
Universidad de Sevilla
jescano@us.es

Tendencias en ciberseguridad en ICS

- Las empresas han informado de un mayor número de intentos no autorizados y de un marcado aumento de los ataques con códigos maliciosos.
- Los sistemas de control utilizan más software y hardware "comercial" (COTS).
- Uso común de protocolos de Internet (IP)
- Mayor uso de la supervisión y el acceso remotos
- Disponibilidad generalizada de herramientas para automatizar los ataques

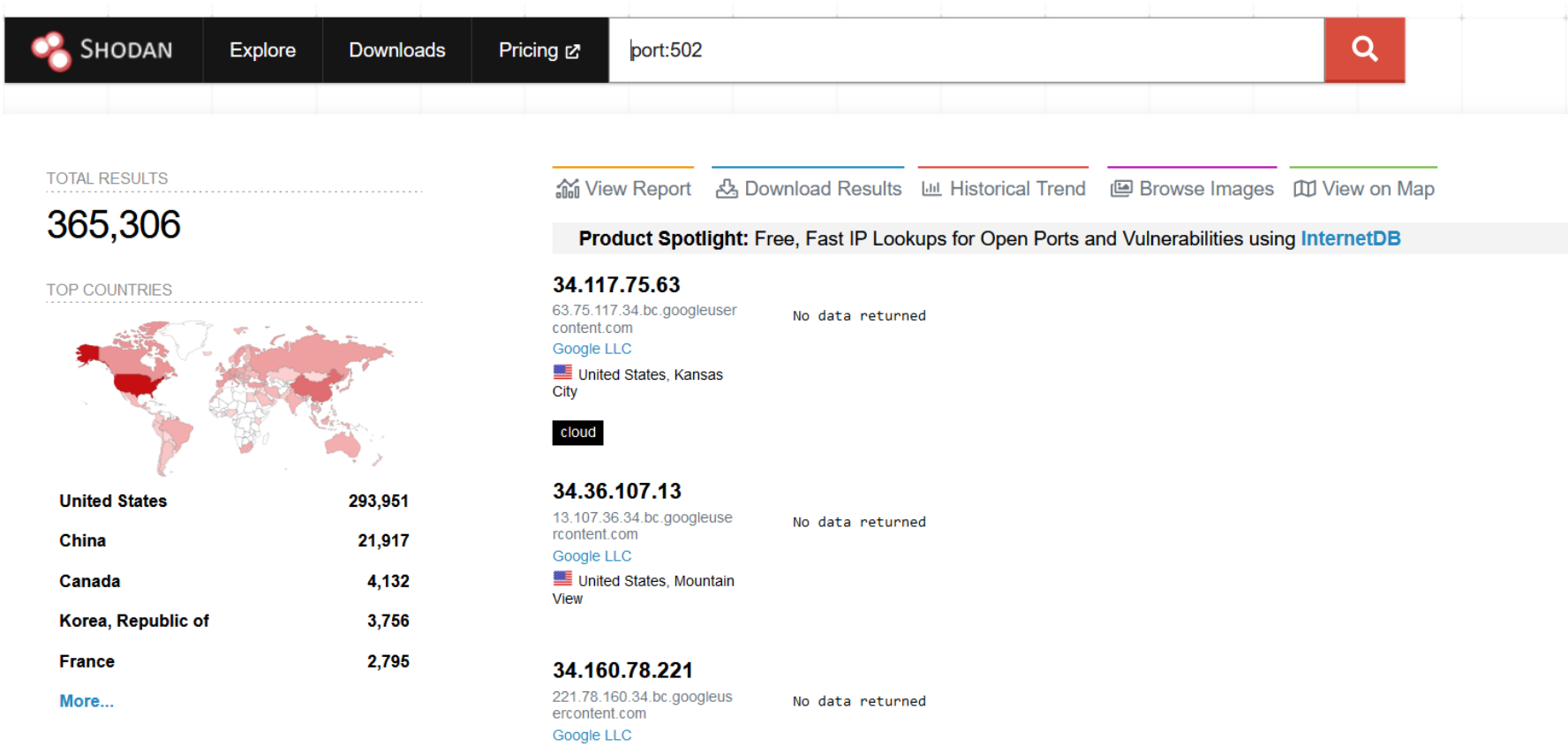
Mitos sobre la ciberseguridad OT

- “No nos conectamos a Internet”
- “Nuestros sistemas de control están detrás de un cortafuegos”
- “Los piratas informáticos no entienden de sistemas de control”
- “Nuestras instalaciones no son un objetivo”
- “Nuestros sistemas de seguridad nos protegen”

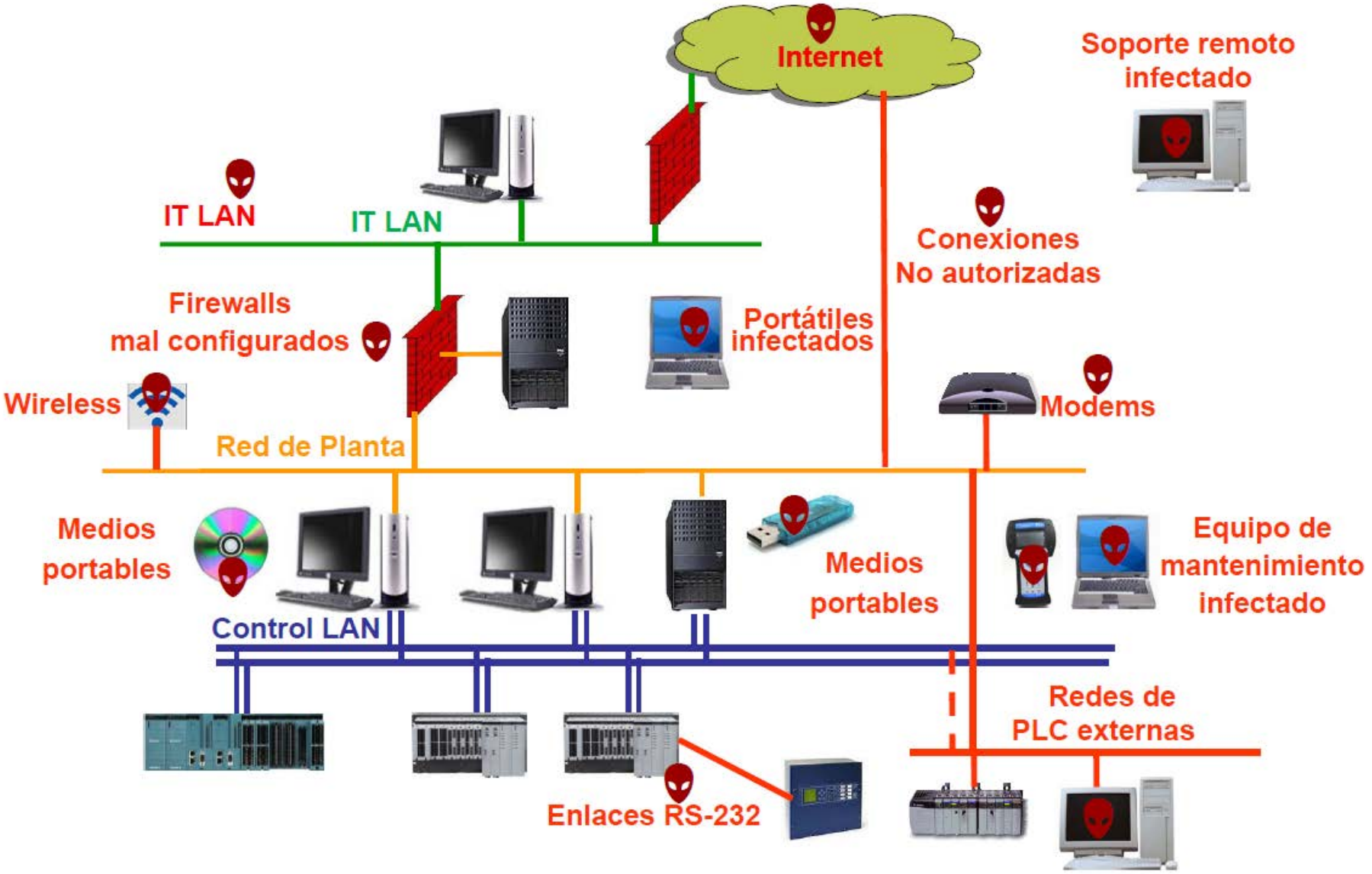
Mito 1

“No nos conectamos a Internet”

https://www.shodan.io/explore/category/industrial-control-systems



“No nos conectamos a Internet”



Mito 2

“Nuestros sistemas de control están detrás de un cortafuegos”

Estudio de 2004 sobre 37 cortafuegos de empresas financieras, energéticas, de telecomunicaciones, medios de comunicación, automoción y seguridad… "Casi el 80 por ciento de los cortafuegos permiten tanto el servicio "Cualquiera" en las reglas entrantes como el acceso inseguro a los cortafuegos.

Estudio de 2010 revisa las conclusiones de 2004

- 84 cortafuegos evaluados
- Los cortafuegos siguen estando mal configurados
- El software de configuración moderno no ayuda a los administradores a cometer menos errores
- Un estudio de 2014 y 2015 revela que la principal debilidad cibernética de los sistemas de control fue la insuficiente protección de los límites de la red

Aunque se configuren correctamente hay vulnerabilidades publicadas

Mito 3

“Los piratas informáticos no entienden de sistemas de control”

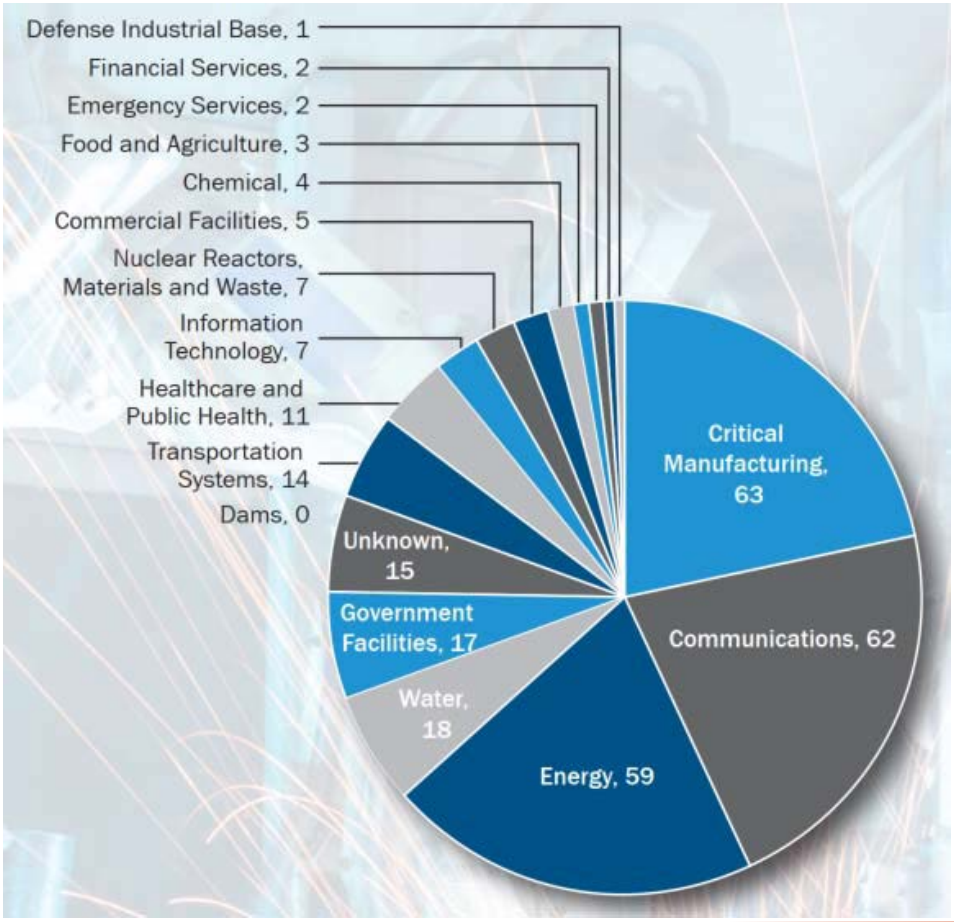
- Esto ya no es cierto
- El pirateo informático ya no es sólo una diversión: los piratas informáticos venden exploits de día cero a la delincuencia organizada.
- El hacking como servicio se ha generalizado
  - Ya no sólo en la web oscura clandestina
  - Ofertas de empleo
- Los sistemas SCADA y de control de procesos son temas habituales en las conferencias "DEFCON" y "Blackhat

Mito 3

- MaaS:Malware as a Service
- Haas: Hacking as a Service
- CaaS: Crimeware as a Service
- FaaS: Fraud as a Service

Mito 4

“Nuestras instalaciones no son un objetivo”



Mito 4

“Nuestras instalaciones no son un objetivo”

- Infraestructuras de tratamiento de aguas en Noruega en 2021
- Dos plantas de tratamiento de aguas residuales en San Francisco y Florida (EE.UU.) en 2021
- Una empresa de distribución en Kansas (EE.UU.) en 2019
- Una empresa de distribución en Carolina del Norte (EE.UU.) en 2018
- Un proveedor público en Michigan (EE.UU.) en 2016
- Una planta de agua potable en Georgia (EE.UU.) en 2013
- Un sistema de canales en California (EE.UU.) en 2007
- Una planta de tratamiento de aguas residuales en el condado de Maroochy (Australia) en 2000.
- Un depósito de agua reciclada en Israel en 2020
- Bombas de agua en Israel en 2020
- Estaciones de bombeo e instalaciones de tratamiento en Israel en 2020

https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water

Mito 5

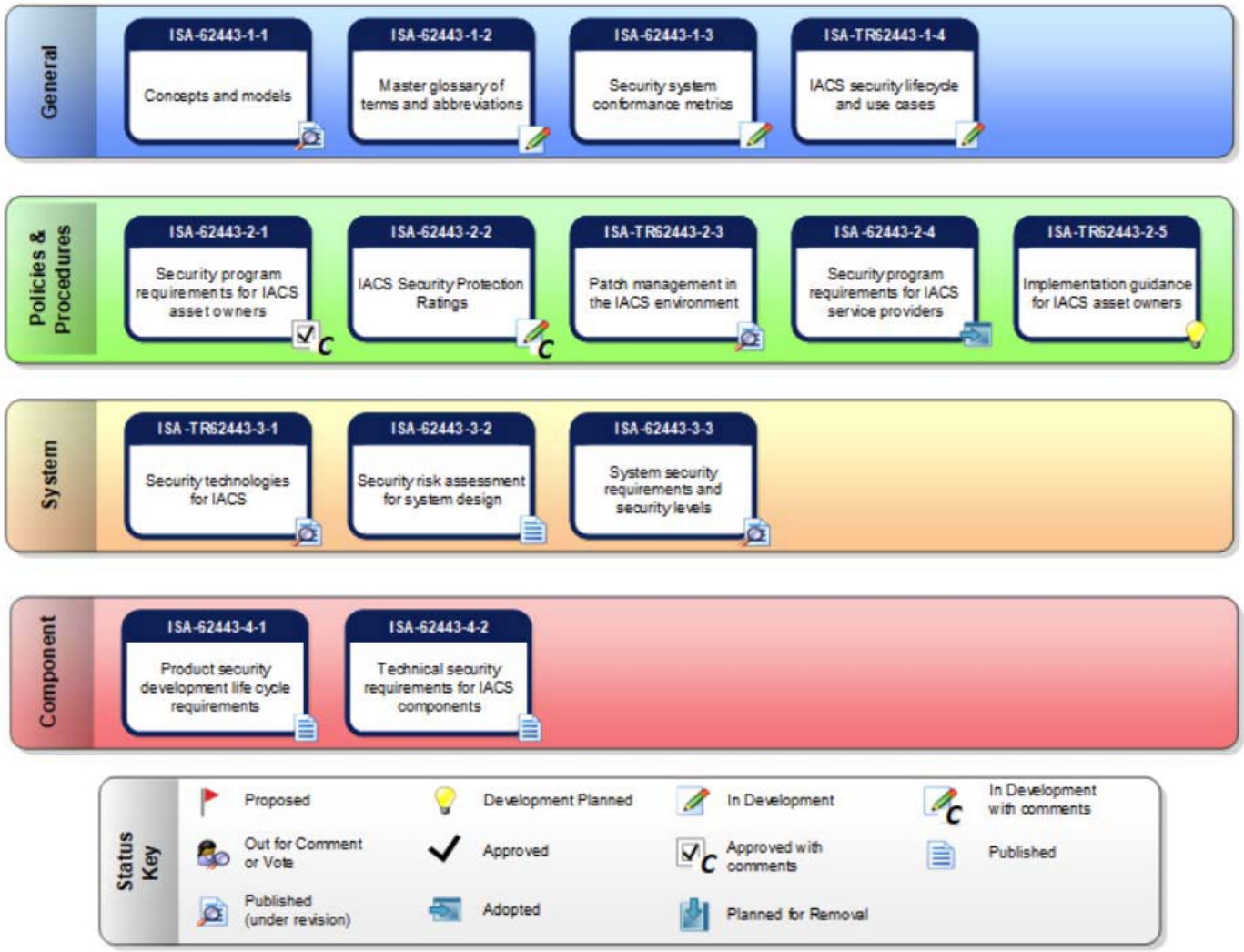
Nuestros sistemas de seguridad nos protegerán

- Los sistemas de seguridad modernos son sistemas programables basados en microprocesadores que se configuran con un PC Windows.
- Ahora es habitual integrar sistemas de control y seguridad mediante comunicaciones Ethernet con protocolos abiertos e inseguros (Modbus TCP, OPC, etc.).
- Muchos módulos de interfaz de comunicación de sistemas de seguridad ejecutan sistemas operativos integrados y pilas Ethernet que presentan vulnerabilidades conocidas.
- El malware "Triton" o "Trisis" interrumpe una función de parada de emergencia en el sistema instrumentado de seguridad (SIS) Triconex y paraliza las operaciones.

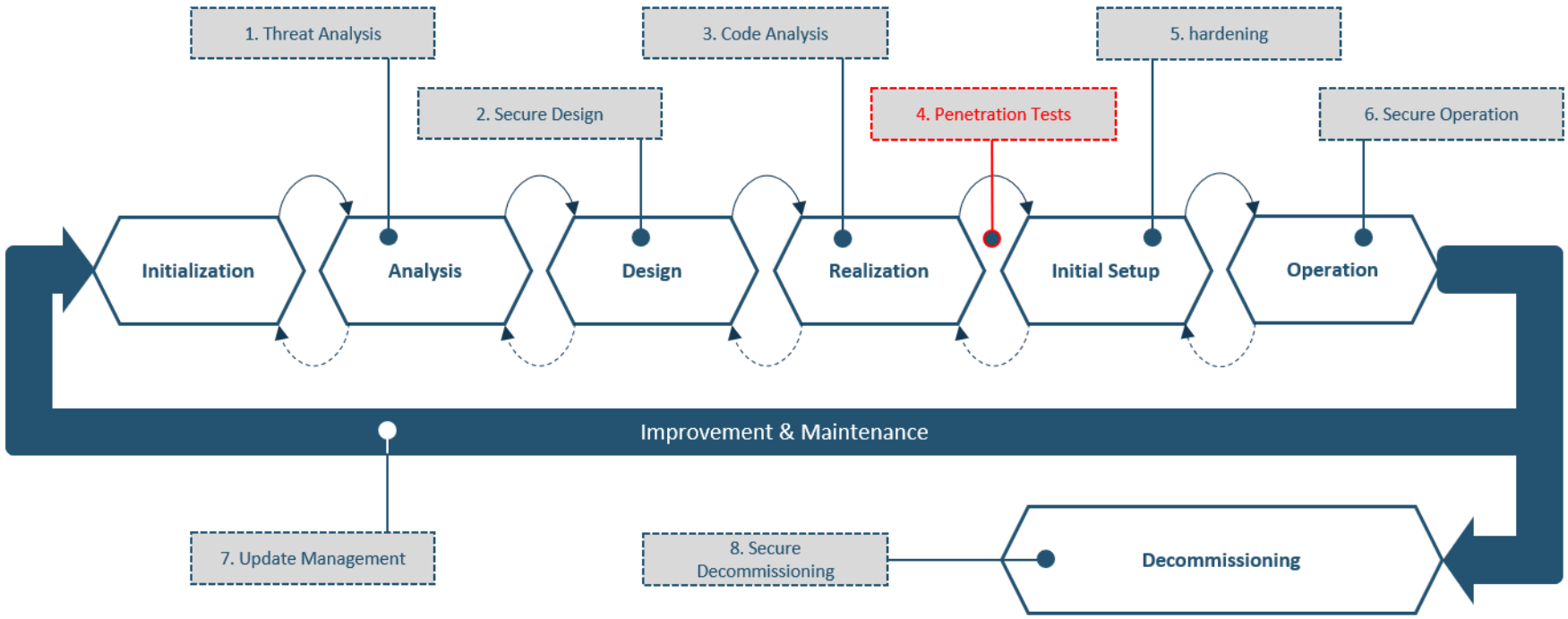
IEC 62443

- Establece requisitos y pautas de seguridad cibernética en los sistemas de control industrial.
- Define los conceptos genéricos de seguridad que aplican a los sistemas de automatización y de aplicaciones críticas
- Se utiliza para definir dominios de seguridad
- Identifica aspectos clave que influyen en la disponibilidad
  – Procesos, Tecnología y Personas
- Analiza la seguridad en todo el ciclo de vida del producto/sistema

Partes de la norma



IEC 62433-4-1



Secure Development Lifecycle with mapping to IEC 62443-4-1 practices

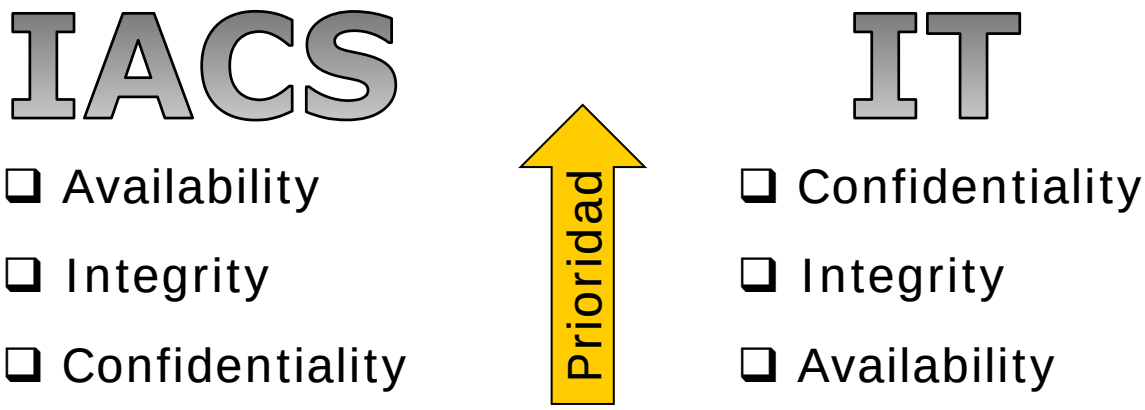
Conceptos fundamentales

- Programa de seguridad
  - Implementación y mantenimiento de personal, políticas y procedimientos, y capacidades basadas en tecnología que reducen el riesgo de ciberataques.
- Gestión de riesgos
  - Evaluación de riesgos
  - Zonas y conductos
  - Especificación de requisitos de ciberseguridad
- Requisitos Fundamentales
- Niveles de seguridad
  - Medida de la fortaleza de los requisitos técnicos
- Niveles de madurez
  - Medida de la fortaleza de los procesos (personas, políticas y procedimientos).
- Principios de diseño

IT vs IACS

- Existen diferencias importantes entre IT e IACS
- Los problemas surgen porque los supuestos que son válidos en un entorno IT pueden no serlo en la planta y viceversa.
- La ciberseguridad del IACS debe abordar cuestiones de seguridad, lo que no suele ser un problema con la ciberseguridad de IT convencional.
- Comprender las diferentes necesidades de seguridad de los sistemas IACS y de IT, conduce a la cooperación y colaboración entre campos históricamente desconectados

Prioridades



- TOMAR prestadas las tecnologías y prácticas de seguridad y aprender a utilizarlas correctamente en el IACS.
- El IACS utiliza tecnologías informáticas como Windows, TCP/IP y Ethernet.
- Gran parte de la política y la tecnología de IT funcionarán para los sistemas de control.
- El entorno informático no se ocupa de la seguridad, sólo de la protección.

Diferentes requisitos de funcionamiento

IT	IACS
La respuesta debe ser fiable	La respuesta además es urgente
Alto rendimiento	Rendimiento modesto
Se tolera un gran retraso	El gran retraso es muy preocupante
Interacción de emergencia no crítica	Crítica respuesta a las emergencias
Protocolos IT	IT y protocolos industriales

Diferentes requisitos de disponibilidad

IT	IACS
Funcionamiento programado	Funcionamiento continuo
Fallos ocasionales tolerados	Cortes intolerables
Se tolera el reinicio	El reinicio puede no ser aceptable
Pruebas beta sobre el terreno aceptables	Pruebas de control de cal. minuciosas en un entorno de no-producción
Modificaciones posibles con poco papeleo	Puede exigirse una certificación formal después de cualquier cambio

Diferentes entornos operativos

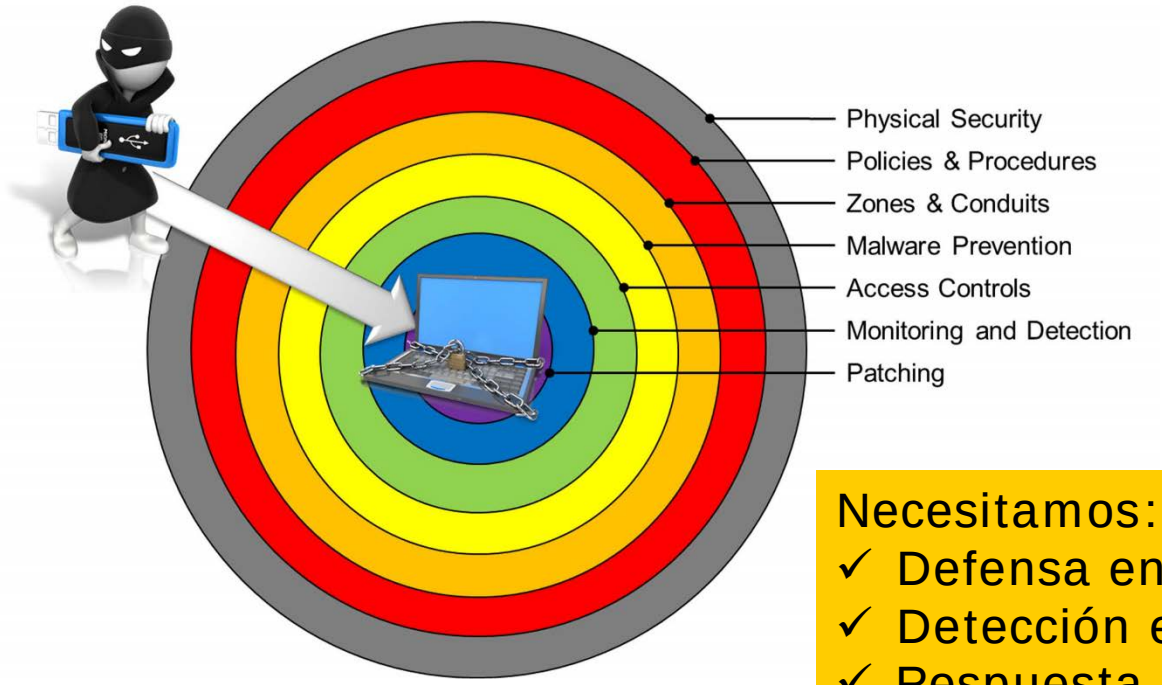
IT	IACS
Aplicaciones "ofimáticas" típicas	Aplicaciones especiales
Sistemas operativos estándar	Sistemas operativos estándar y embebidos
Las actualizaciones son sencillas	Las actualizaciones son un reto pueden impactar en el hardware, la lógica, etc…
La tecnología se renueva a menudo con Tecnología comercial (COTS), (de 3 a 5 años)	Sistemas antiguos (15-20 años)
Recursos abundantes (memoria, ancho de banda)	Recursos restringidos
Centro de datos, sala de servidores o entorno de oficina.	Entornos industriales

Diferentes objetivos de gestión de riesgos

IT	IACS
Confidencialidad e integridad de los datos primordial	HSE y la producción son primordiales (integridad y disponibilidad)
El impacto del riesgo es la pérdida de datos, el retraso de las operaciones comerciales	El riesgo Impacto es la pérdida de vidas, equipos o producto
Recuperación por reinicio	Tolerancia a fallos esencial

- Ejemplo: Procedimientos de bloqueo de contraseña:
  - ✓ IT: Bloqueo de TODOS los accesos durante los 10 minutos posteriores a 3 intentos fallidos de inicio de sesión.
  - ✓ IACS: Facilitar el acceso del operador y hacerlo infalible.
- El operario entra en pánico durante una fuga de cloro y escribe mal su contraseña tres veces. La HMI bloquea TODOS los accesos durante 10 minutos.
  - ✓ El resultado puede ser desastroso

Defensa en profundidad



- ✓ Los malos acabarán entrando.
- ✓ No basta con instalar un cortafuegos y olvidarse de la seguridad.
- ✓ Debemos reforzar la red de sistemas de control

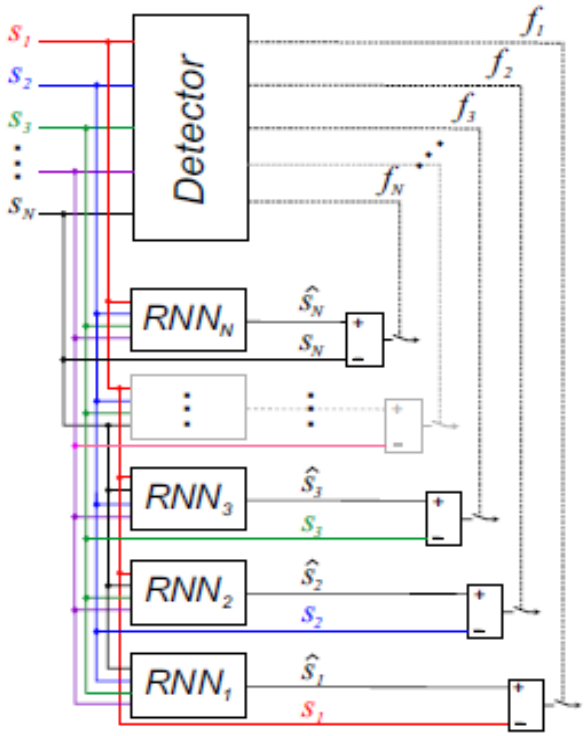
Necesitamos:

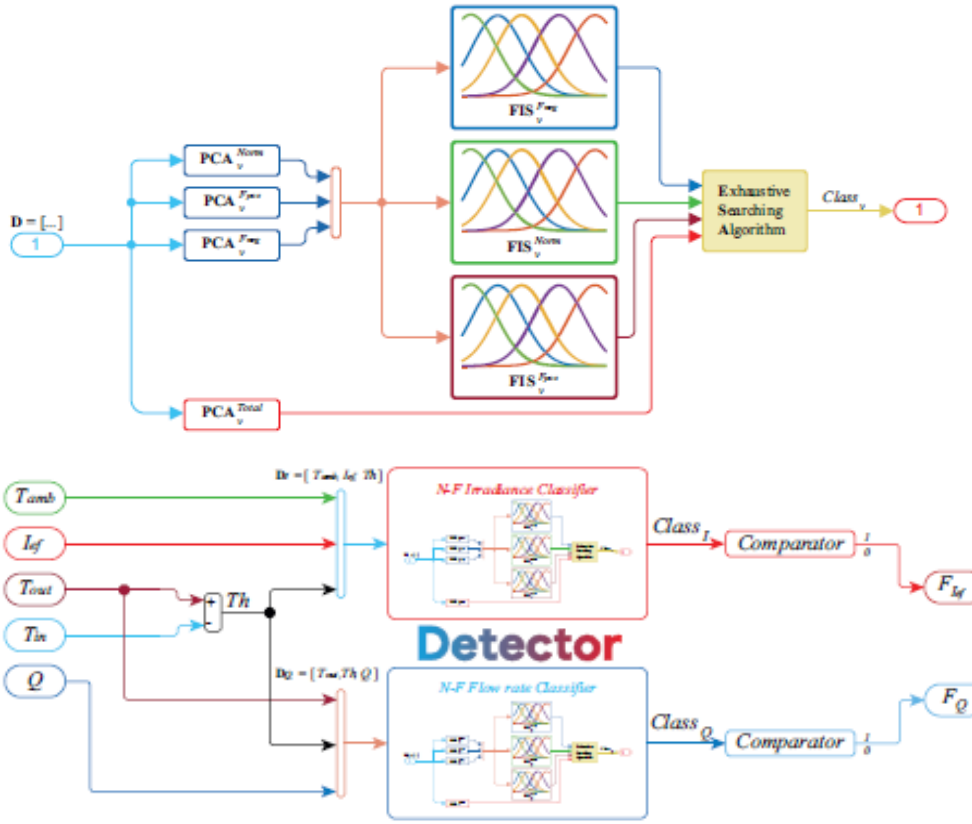
- ✓ Defensa en profundidad
- ✓ Detección en profundidad
- ✓ Respuesta responsable y oportuna a los incidentes

False Data Injection

Man in the middle

Detección de fallos



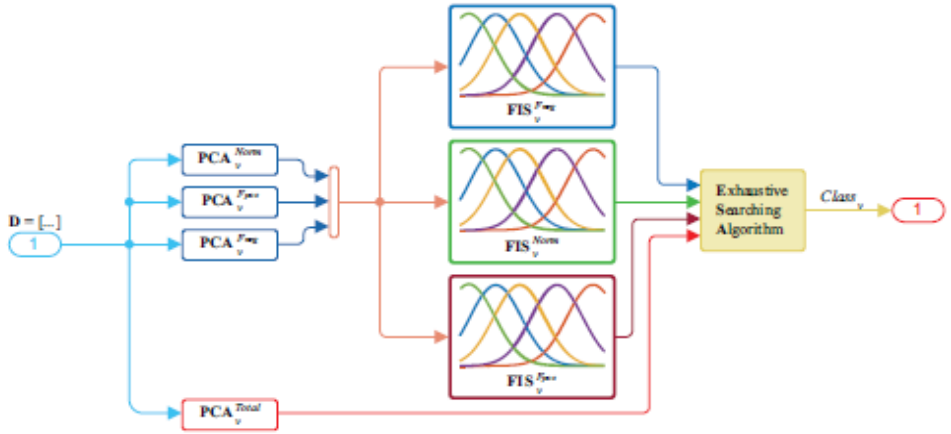


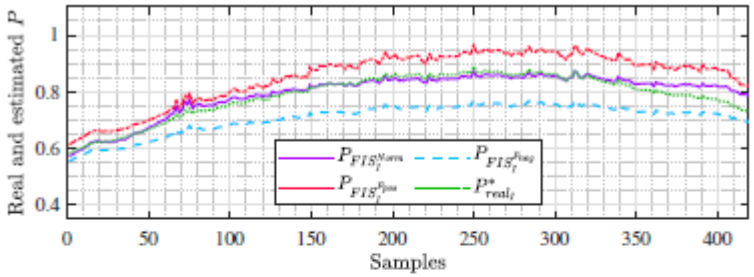
Predicted Classes

Actual	F_{neg}	Norm	F_{pos}
F_{neg}	419	0	0
Norm	0	400	19
F_{pos}	0	19	400

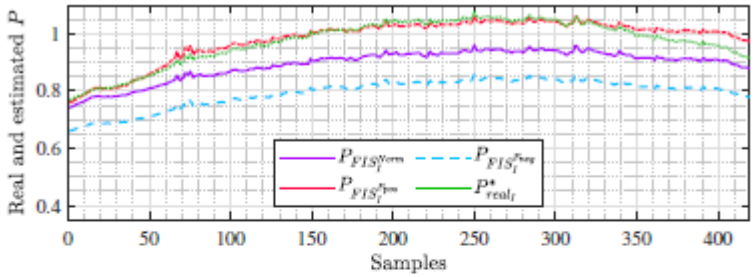
Precision	100 %	95.47 %	95.47 %
Recall	100 %	95.47 %	95.47 %
Accuracy	96.98 %		

Detector

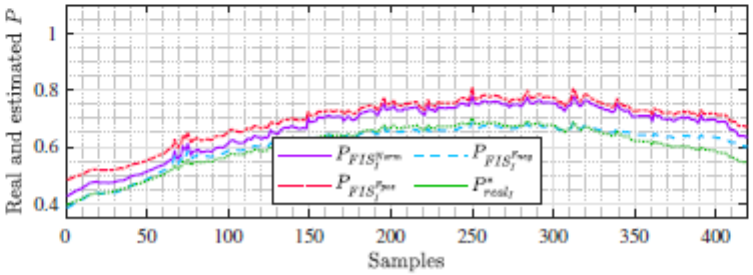




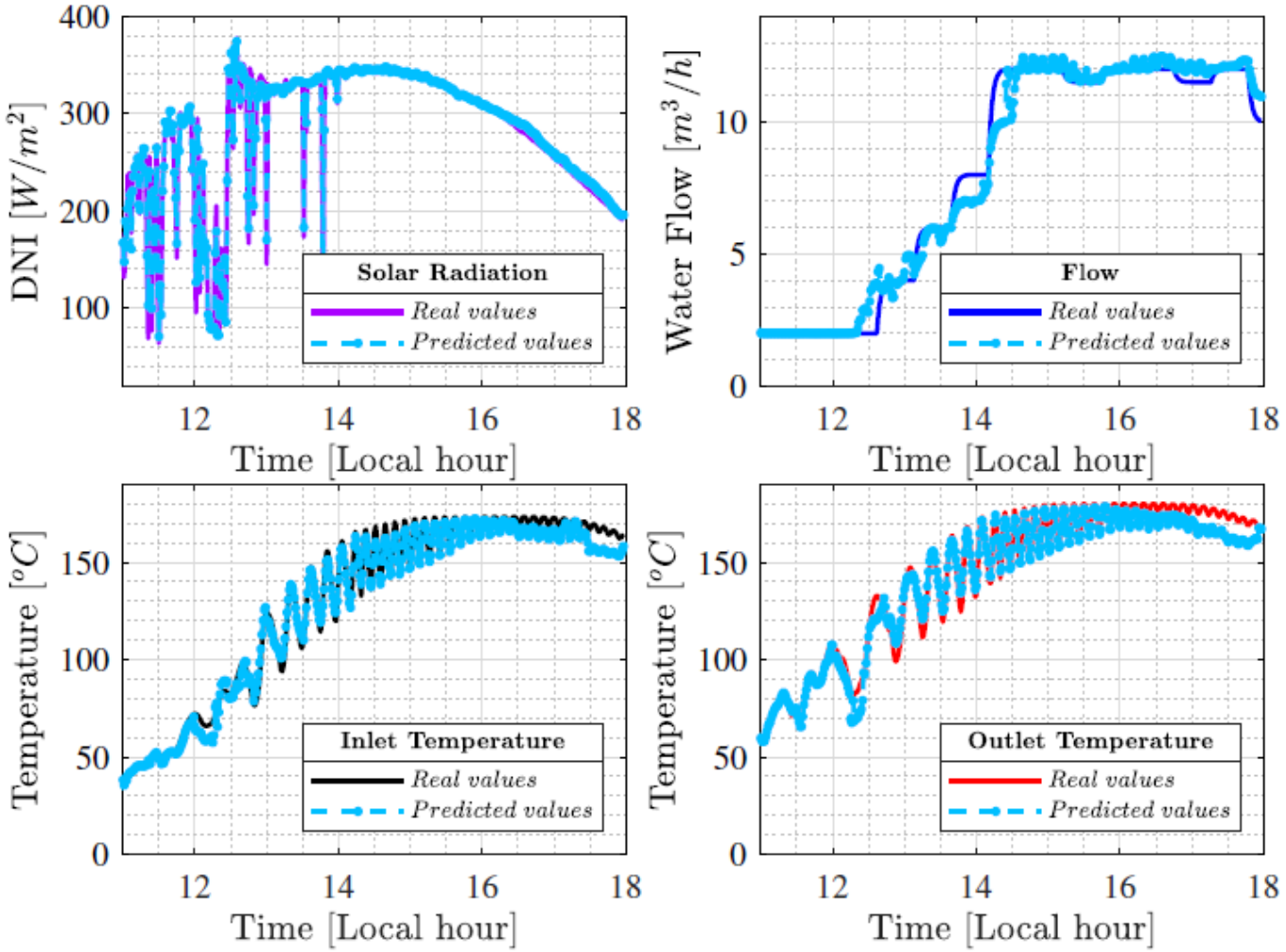
(a) *Norm* Prototypes



(b) F_{pos} Prototypes



Regresores


DNI $[W/m^2]$
Solar Radiation
Real values
Predicted values
Time [Local hour]
Water Flow $[m^3/h]$
Flow
Real values
Predicted values
Time [Local hour]
Temperature $[^oC]$
Inlet Temperature
Real values
Predicted values
Time [Local hour]
Temperature $[^oC]$
Outlet Temperature
Real values
Predicted values
Time [Local hour]

Gracias por su atención

Juan Manuel Escaño González
Universidad de Sevilla
jescano@us.es