Ciberseguridad en Entornos Industriales

Lucena, 9 de octubre de 2018

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA
SECRETARÍA DE ESTADO PARA EL AVANCE DIGITAL

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

¿Qué es INCIBE?

Entidad de referencia para el **desarrollo de la ciberseguridad** y de la **confianza digital** de:

Ciudadanos

Empresas**, en especial sectores estratégicos**

Sociedad Mercantil Estatal y Medio Propio dependiente de la Secretaría de Estado para el Avance Digital que lidera diferentes actuaciones para la Ciberseguridad a nivel nacional e internacional.

Nuestra historia

2006

Nace INTECO

Instituto Nacional de
Tecnologías de la Comunicación

2012

INTECO

Se focaliza en
el mundo de la ciberseguridad

2014

Se transforma en INCIBE

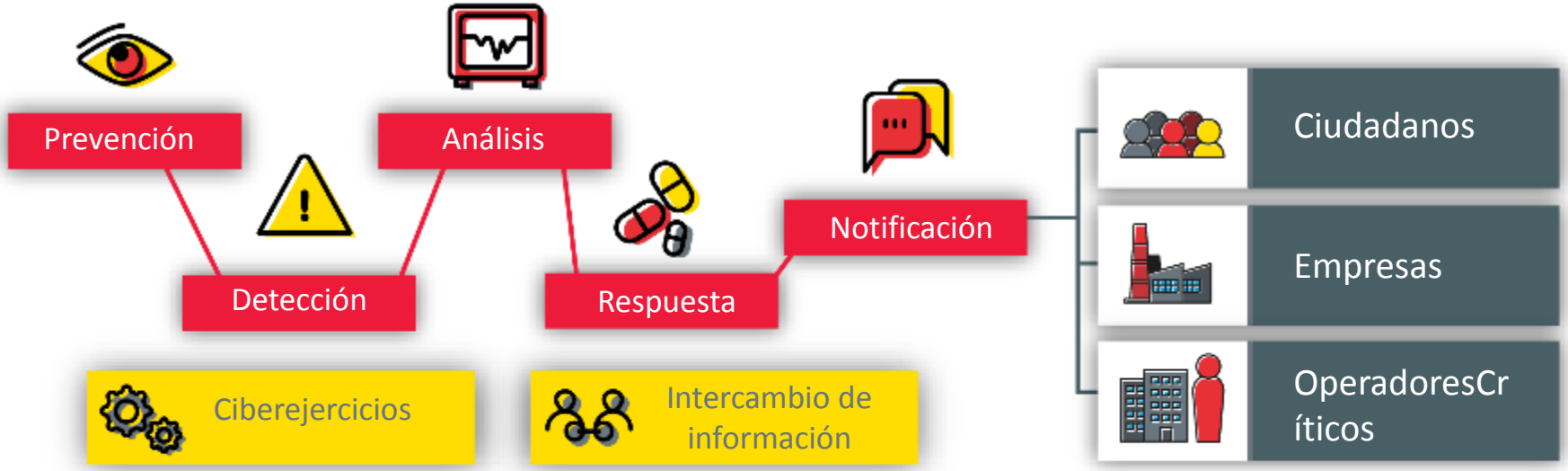
Instituto Nacional
de Ciberseguridad de España

¿Qué hacemos?


Respuesta ante incidentes y ciberataques
Concienciación
Servicios de Ciberseguridad
Desarrollo de la industria nacional
Apoyo al desarrollo de la industria, I+D+I y talento
Fomento I+D+I
Promoción e identificación de talento
incibe_
Desarrollo de Tecnologías de Ciberseguridad
Tecnologías de Ciberseguridad
Inteligencia en el ciberespacio
Diseño e implementación de Sistemas de Gestión

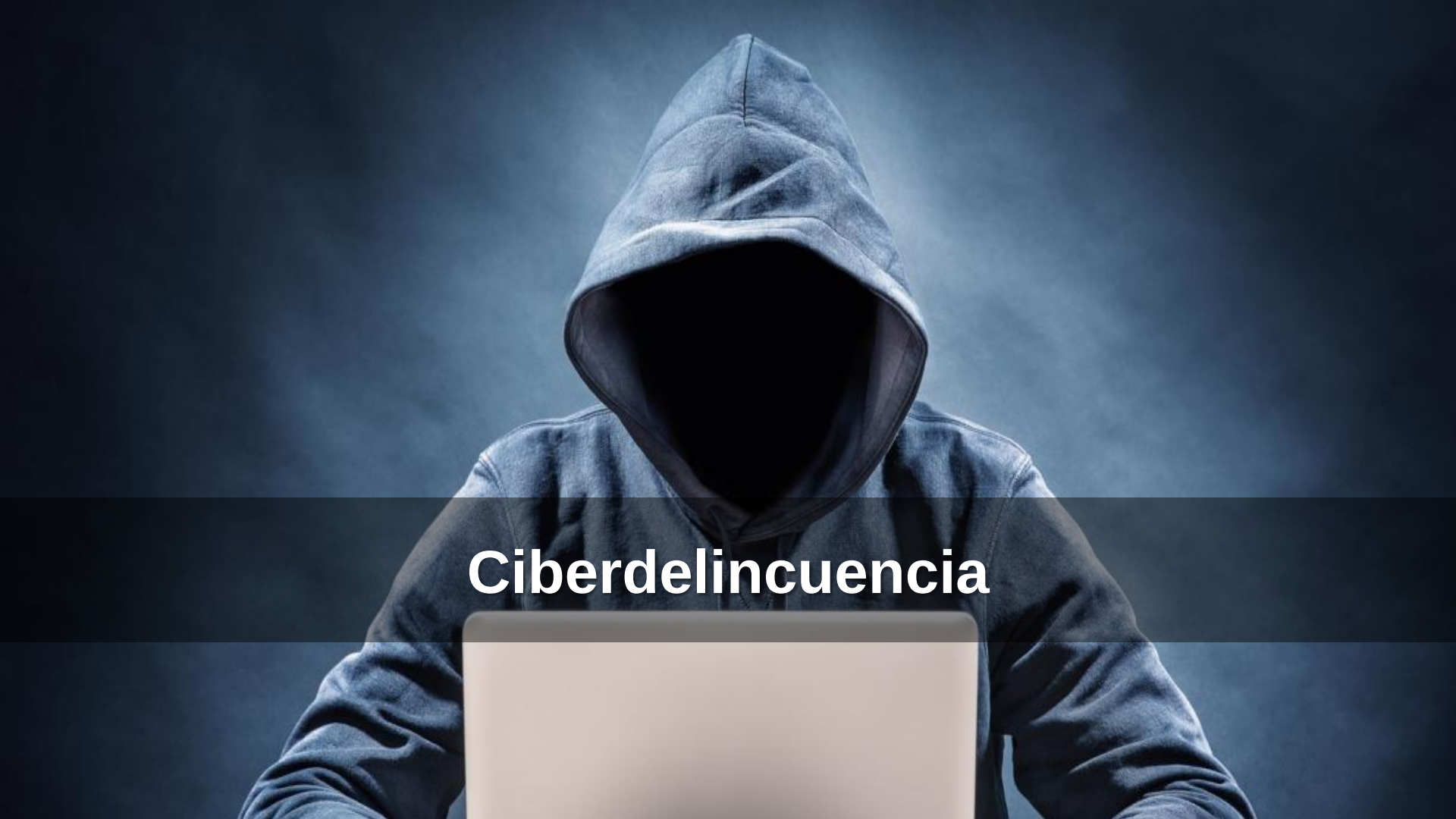
incibe cert_

Referencia para la resolución técnica de incidentes de ciberseguridad que afectan a ciudadanos y empresas




constante evolución…


como en la delincuencia…

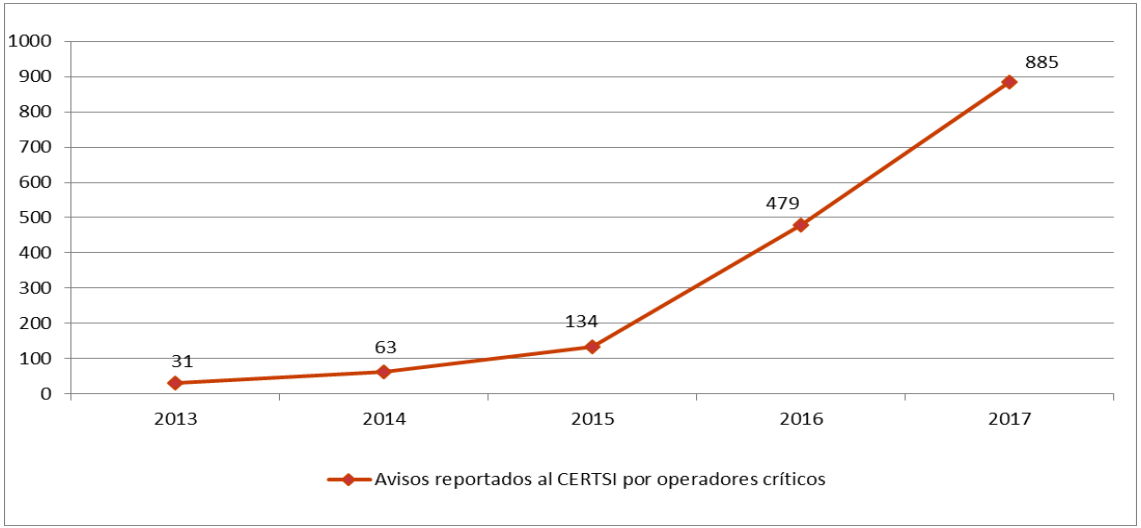

Ciberdelincuencia

¿Y la ciberseguridad?, ¿Realmente afecta a la industria?

¿Qué está pasando en el ciberespacio?


Cyber Security
Situational Awareness
World Security Threats
+
–
SPAIN
SEARCH
?
0,12M
INTERNAL
THREATS
31,6K
EXTERNAL
THREATS
SPAIN
EXT: 31.592
INT: 119.230
¿Qué pasa en el mundo?
Top Countries by
Threat number
UNITED STATES 11035
GERMANY 2559
JAPAN 2263
CHINA 2185
FRANCE 1381
RUSSIAN FEDERATION 1066
UNITED KINGDOM 957
NETHERLANDS 896
CANADA 569
BRAZIL 508

Evolución de incidentes en operadores críticos



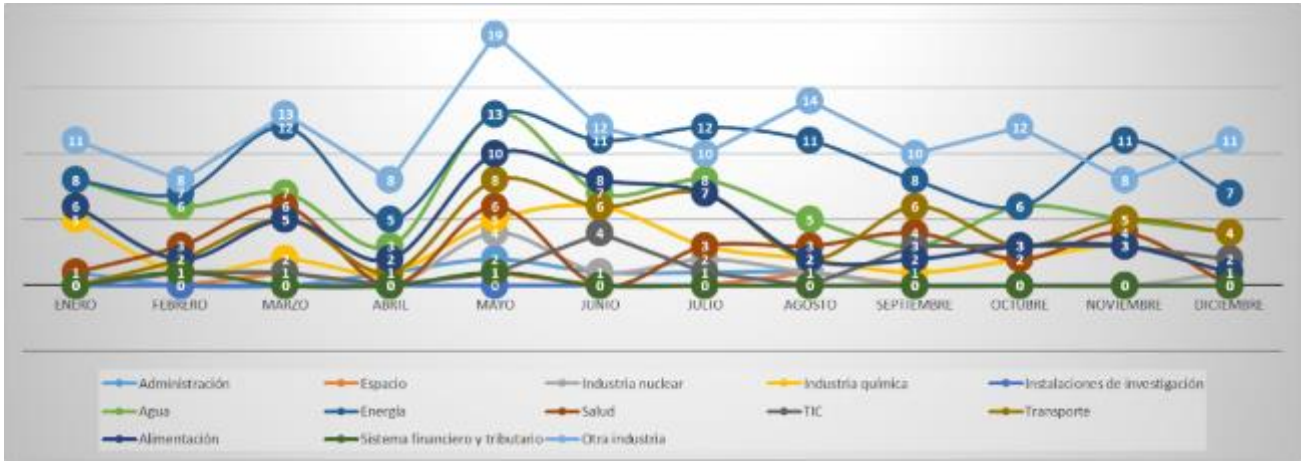
Operadores críticos

La preocupación por la Ciberseguridad en entornos TI ha sufrido un incremento significativo durante los últimos años.

¿Podemos decir los mismo para los entornos Tecnologías de la Operación (OT)?

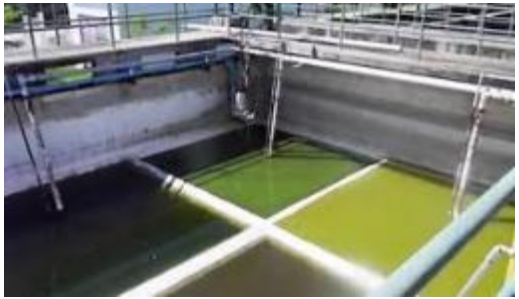
Clasificación de avisos de vulnerabilidad por sector

Avisos de vulnerabilidad publicados **2017** **199**



- Uno de los sectores más afectados sigue siendo en de Energía
- Gran parte de los avisos afectan a varios sectores
- Este dato no quiere decir que el nivel de seguridad de un sector sea menor

Incidentes reales: sector agua



FUENTE: http://csrc.nist.gov

Maroochy (Australia, 2000)

Vertido de 2 millones de litros de aguas no tratadas en ríos, parques, etc. en un paraje natural

- Ex-empleado suplanta una estación de bombeo, de forma remota.
- Causo mas de **46 incidentes** premeditados en menos de **3 meses**.

Incidentes reales: sector marítimo

FUENTE: http://csrc.nist.gov

Barcelona (España, 2017)

Cierre de terminales de carga controladas por la empresa APM

- Versión modificada de Petya afecta a los sistemas informáticos y obliga a parar la producción
- Causo pérdidas de entre **200 y 300 millones** de dólares a la naviera danera **Maersk**

Incidentes reales: sector logístico

FUENTE: https://www.easyenvio.com/es

Estados Unidos (2013-2014)

Al menos 8 compañías comprometidas

- El malware "Zombie Zero" infecta al hardware de escáner utilizado en distintas unidades logísticas
- De los 64 escáneres analizados, 16 estaban infectados. Los atacantes obtuvieron detalles financieros de todos los clientes y envíos

Incidentes reales: sector transporte

FUENTE: http://www.theregister.co.uk

Lodz (Polonia, 2008)

Descarrilamiento de trenes

- Joven de 14 años convierte el mando de su TV en un mando para cambiar las agujas de las vías de tren
- 4 tranvías descarrilados y varios heridos

Incidentes reales: sector energía

FUENTE: https://www.certsi.es

Ucrania (2015)

Corte de suministro eléctrico a la población

- Primer ataque exitoso conocido a una red de distribución eléctrica
- Alrededor de **1,5 millones** de habitantes sin electricidad
- Más de **30 subestaciones** desconectadas

Incidentes reales: sector energía

TIMELINE DE INCIDENTES DE SEGURIDAD

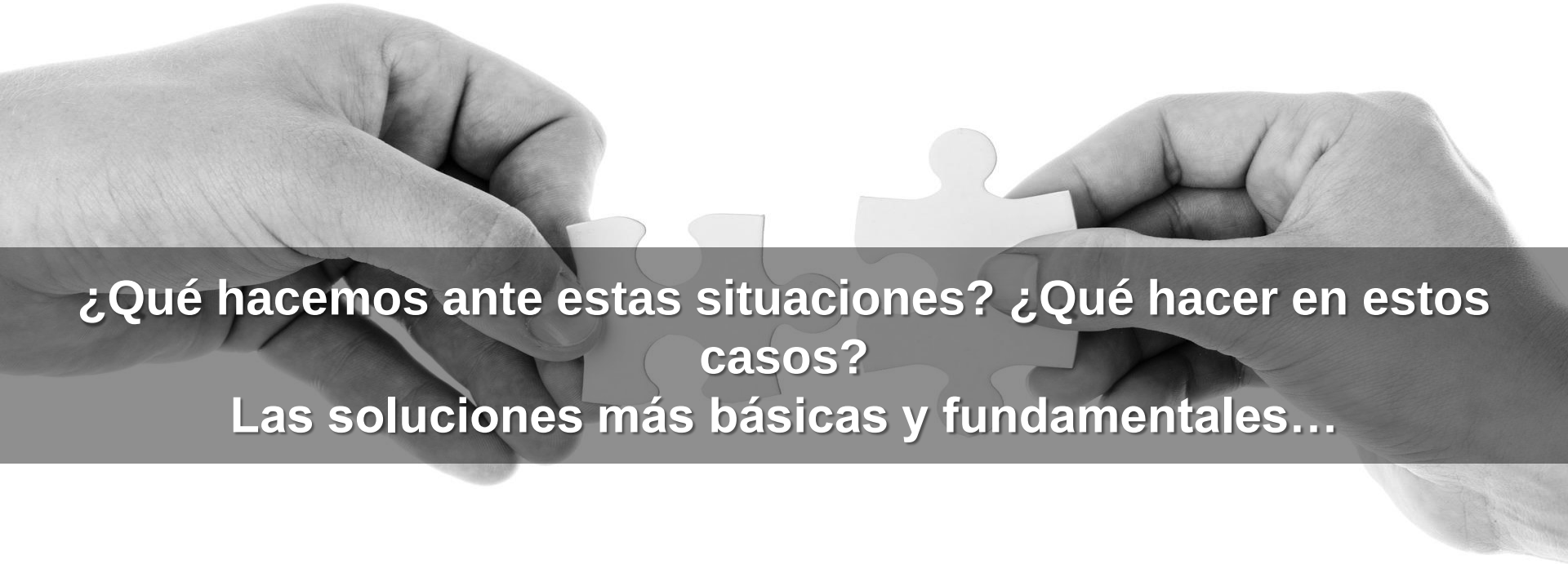
¿Y la ciberseguridad?, ¿Realmente afecta a la industria?

ROTUNDAMENTE SÍ


La cuestión, no es si un dispositivo va a sufrir un ciberataque, sino cuando lo va a sufrir y si estamos protegidos


Porque a veces pasa esto...


Petya
Petya
Petya
Petya
Petya
!Y esto!



¿Qué hacemos ante estas situaciones? ¿Qué hacer en estos casos?
Las soluciones más básicas y fundamentales…

Buenas prácticas

- Limitación y control de puertos de red, protocolos y servicios
- Configuraciones de dispositivos de red como cortafuegos
- Capacidades de recuperación de datos
- Diseño de red seguro
- Implementación de canales de comunicación segura
- Encriptación o autenticación incorporado en los sistemas de navegación
- Concienciación en ciberseguridad y formación a los operarios

Iniciativas Tecnológicas para elevar el nivel de Ciberseguridad en entornos industriales

Iniciativas tecnológicas: RNLI

Red Nacional de Laboratorios Industriales

Objetivo

Disponer de una Red de Laboratorios con capacidad para **TESTEO, EXPERIMENTACIÓN e INVESTIGACIÓN**.

- Potenciar la **oferta y la demanda** de la ciberseguridad en los entornos industriales a nivel nacional
- **Promoción** de capacidades de los laboratorios
- Fomento de la colaboración y cooperación entre los actores involucrados: **NUEVOS SERVICIOS**

rnli_
Red Nacional de Laboratorios Industriales

Mostrando: 24 laboratorios

Nombre

Arkossa Smart Solutions

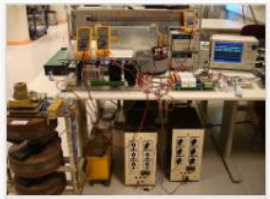
Energía, Electricidad

Laboratorio para Análisis de Redes PRIME

Embedded Lab

Administración, Agua, Alimentació...

El Embedded Lab de SCASSI ayuda a las empresas a...



Embedded Systems Secur...

Agua, Energía, Electricidad, Gas, Es...

Laboratorio de ciberseguridad de sistemas...

EMI Security Laboratory

Agua, Energía, Electricidad, Gas, Es...

Laboratorio de seguridad física/lógica basado en...

ERESMA GRID

Energía, Electricidad, Instalaciones...

Laboratorio de investigación y docencia en nuevas...

EY Advanced Security Lab

Agua, Tratamiento del agua, Energ...

Laboratorio especializado en el estudio de la...

ICS21sec Evals

Industria Química, Energía, Electric...

Laboratorio de evaluaciones de seguridad

ICSSY Lab

Energía, Electricidad, Gas, Instalaci...

Laboratorio de Ciberseguridad Industrial y Safety...

¿Cómo adherirse a la iniciativa?

- Disponer de dispositivos de control industrial
- Permitir a INCIBE acceso a los dispositivos
- Contacto: rnli@incibe.es

¿Cómo saber si mis sistemas de control son vulnerables?

Iniciativas tecnológicas: ESCILA

Detección de vulnerabilidades en entornos controlados

Descripción

ESCILA consiste en una solución diseñada para evaluar el nivel de seguridad de los dispositivos que constituyen los Sistemas de Control Industrial (SCI)

- Interfaz amigable
- Implantación simple
- Generación inmediata del informe
- ¿Asumo riesgo o mejoro?
- Tests específicos orientados a Sistemas de Control

escila_
Evaluación de Sistemas de Control Industrial y Automatización

¿Cómo adherirse a la iniciativa?

- Formar parte de la Red Nacional de Laboratorios Industriales
- Compartir feedback con INCIBE para la mejora del servicio
- Contacto: escila@incibe.es

Iniciativas tecnológicas: ICS-Arsenal

Distribución Linux orientada a entornos industriales

Objetivo

Distribución de software basada en Linux que recoge un conjunto de herramientas y otros recursos de seguridad orientados a evaluar y elevar el nivel de seguridad de los Sistemas de Control Industrial

- Identificación de herramientas y recursos focalizadas en Sistemas y Control Industrial
- Repositorio de INCIBE con recursos propios
- - Fase piloto en curso

¿Cómo adherirse a la iniciativa?

- Formar parte de la Red Nacional de Laboratorios Industriales
- Compartir feedback con INCIBE para la mejora del servicio
- Contacto: ics-arsenal@incibe.es

¿Cómo os puede ayudar INCIBE?

Protege tu Empresa

https://www.incibe.es/protege-tu-empresa

INCIBE CERT

- Respuesta 24x7
- Notificaciones y análisis ad-hoc
- Contenidos especializados PIC
- CyberEx
- ICARO
- Information gathering
- Detector de incidentes

Actualidad

https://www.incibe-cert.es/

Debemos preguntarnos....

Preguntas que nos debemos de hacer…

- Los PC de mi sistema de control industrial, ¿disponen de antivirus? ¿Está actualizado?
- El sistema operativo, ¿es la última versión? ¿O continuamos con sistemas operativos del siglo XX?
- Si no me es posible mantener mis sistemas actualizados, ¿dispongo de medidas de seguridad complementarias?
- Las memorias portátiles USB suelen ser un mecanismo común de entrada de malware. ¿Qué gestión hacemos de estos dispositivos? ¿Uso el mismo pendrive para descargas de internet y para introducir los programas de fabricación en mis máquinas?
- ¿Quién tiene acceso a mi sistema? ¿Está conectado a internet? ¿Hay terceras empresas que se conecten para hacer mantenimiento remoto? ¿Qué políticas de seguridad siguen esas empresas?

Preguntas que nos debemos de hacer…

- El acceso a los terminales de control de mis máquinas ¿Está protegido por contraseña? ¿No tendrás escrita esa contraseña en un post-it pegado a la pantalla?
- Si el técnico al que no renové el contrato el mes pasado quisiese conectarse de nuevo a mi sistema, ¿podría hacerlo?
- ¿Dispongo de copias de seguridad actualizadas de los programas que se ejecutan en mis autómatas programables? Si mañana se borrase la memoria de esos equipos, ¿cuánto tardaría en volver a la producción a un ritmo normal?
- ¿Es realmente necesario conectarme desde cualquier lugar para ver cómo va la producción? Por ejemplo, a través de uno de esos puntos de acceso wi-fi gratuitos de las cafeterías…
- ¿Quién se encarga en mi empresa de la ciberseguridad de los sistemas de control industrial? ¿Cómo la gestionamos?
- A modo de resumen, ¿cuál es el estado de la ciberseguridad industrial de mi negocio? ¿Cuánto tiempo voy a esperar para averiguarlo?

Conclusiones

Un incidente de Ciberseguridad en tu INDUSTRIA, puede provocar
PÉRDIDA DE REPUTACIÓN

UTILIZA LOS 5 SENTIDOS PARA EVITAR INCIDENTES DE CIBERSEGURIDAD

«Una cadena es tan fuerte como su eslabón más débil»

«El usuario es el eslabón más IMPORTANTE de la cadena de la seguridad»

Síguenos en…

CONTACTO	Instituto Nacional de Ciberseguridad **(INCIBE)** **info@incibe.es**
VISÍTANOS	Instituto Nacional de Ciberseguridad **(INCIBE)** **https://www.incibe.es**
INFÓRMATE	INCIBE CERT **https://www.incibe-cert.es/** Portal de protección del menor **https://www.is4k.es** CyberCamp **https://www.cybercamp.es**
SÍGUENOS	Twitter, YouTube, Facebook, LinkedIn **@Incibe @incibe_cert @Osiseguridad @CyberCampEs @CiberEmprende_**
REPÓRTANOS	incidentes, vulnerabilidades, fraude online, phishing, malware, etc. **incidencias@incibe-cert.es**