SEGURIDAD TELCO 2018

Ciberseguridad en un mundo conectado

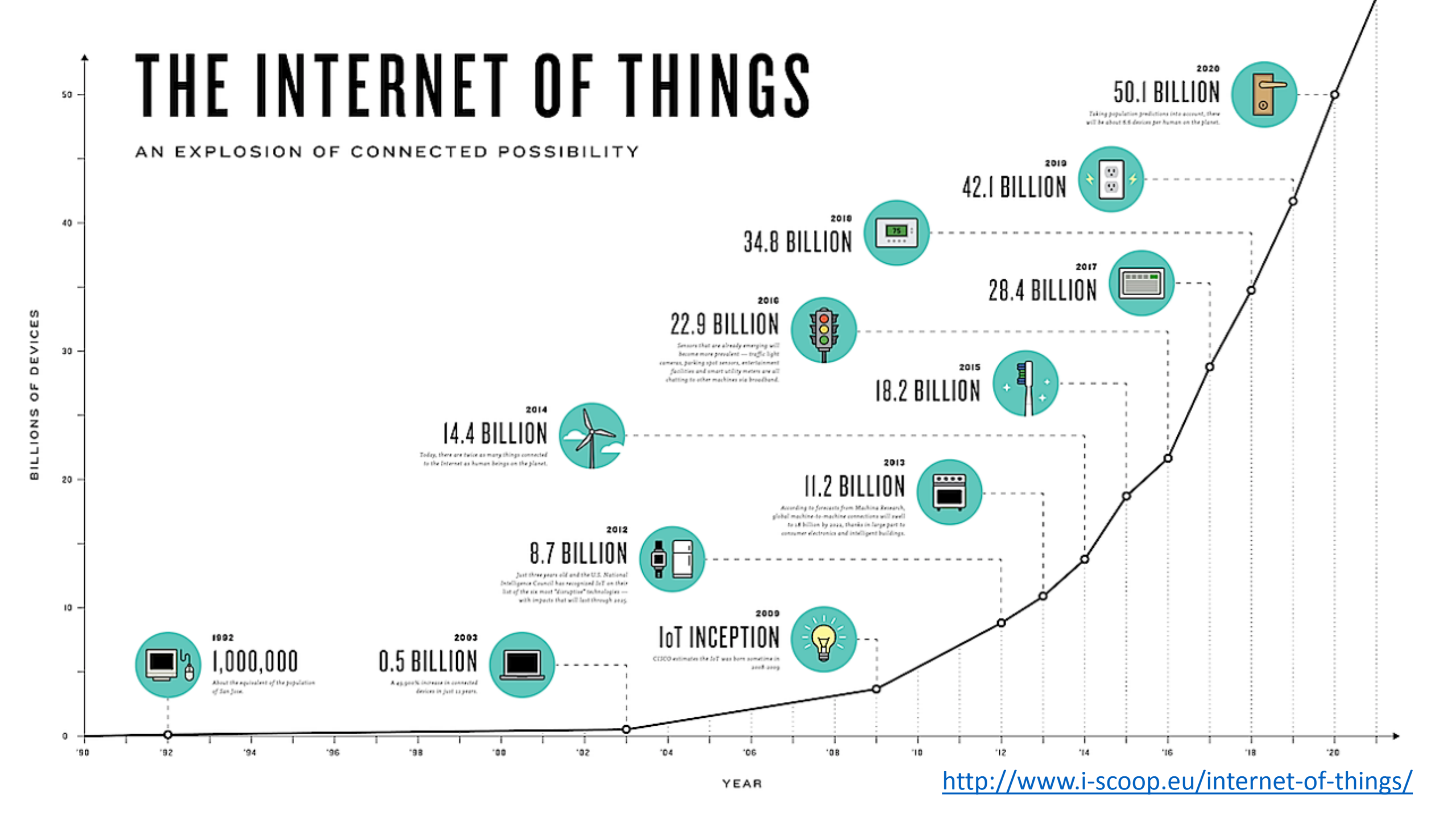
ELENA GARCÍA DÍEZ

21 febrero 2018

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

¿Qué es la conectividad?



http://www.i-scoop.eu/internet-of-things/


¿Qué está pasando?

Hackers hacen saltar 156 alarmas de emergencia en Dallas

07/04/2017

La noche del pasado viernes, el sistema de alarmas de tornados de Dallas compuesto por 156 sirenas, fue hackeado provocando que todas empezaran a sonar al mismo tiempo, poniendo así en alerta a los ciudadanos.

Según afirma el alcalde de la ciudad, Mike Rawlings, se trataría de un ciberataque hacia los sistemas de emergencia de la ciudad, el cual está siendo investigado para encontrar a los responsables.

Referencias:

08/04/2017	usatoday.com	Hacker sets off all 156 emergency sirens in Dallas
09/04/2017	computerhoy.com	Hackean 156 sirenas de emergencia en Dallas, causando el páni...
09/04/2017	edition.cnn.com	Hacker sets off emergency alarms, frightening Dallas residents
10/04/2017	xataka.com	Hackean las 156 sirenas de aviso de tornado de Dallas y las hace...
10/04/2017	thehackernews.com	Hacker Caused Panic in Dallas by Turning ON Every Emergency S...

Etiquetas: Cibercrimen Incidente

Ir atrás

Ataque dirigido

Últimas actualizadas

Fuga de información en Swisscom afecta a 800.000 clientes
Actualizado el 13/02/2018

La botnet Smominru utiliza el Malware WannaMine para minar criptodivisas
Actualizado el 09/02/2018

Roban 500 millones de dólares en la criptomoneda NEM a CoinCheck
Actualizado el 08/02/2018

Aplicación de fitness Strava filtra la ubicación d bases militares secretas
Actualizado el 05/02/2018

Un adolescente detenido por obtener información confidencial de la CIA y FBI
Actualizado el 02/02/2018

Múltiples vulnerabilidades en Siemens SPCanywhere

Fecha de publicación: 06/03/2015
Importancia: 3 - Media

Recursos afectados:

- SPCanywhere para Android. Todas las versiones
- SPCanywhere para iOS. Todas las versiones

Descripción:

Se han descubierto varias vulnerabilidades que permitirían a un atacante manipular la aplicación Sismens SPCanywhere o extraer información sensible de la comunicación entre la misma y el sistema de alarmas.

Solución:

Actualizar el software a la última versión a traves de Google Play o Apple App Store.

Detalle:

Siemens SPCanywhere es una aplicación móvil que permite gestionar remotamente sistemas de alarma desde el teléfono. Se han identificado las siguientes vulnerabilidades relacionadas con la misma.

Falta de cifrado en datos sensibles

Puede obtenerse la IP de un sistema de alarma debido a que la resolución de ID a IP se hace sin cifrar. (CVE-2015-1595)

La validación del certificado SSL no se realiza correctamente, lo que permite a un atacante manipular o capturar sesiones protegidas con SSL/TLS. Se ha reservado el identificador CVE-2015-1596.

Eliminación incorrecta de información sensible

La carga de código sin cifrar permite a un atacante manipular la aplicación y ejecutar código (sólo afecta a Android). Se ha reservado el identificador CVE-2015-1597.

Contraseñas almacenadas en un formato recuperable

Las contraseñas son almacenadas de tal forma que un atacante [illegible] (CVE-2015-1598)

Sorteo de la autenticación

Un atacante con acceso físico al dispositivo puede saltarse el control de acceso debido a las características del sistema de ficheros. Se ha reservado el identificador CVE-2015-1598.

Últimos avisos

Múltiples vulnerabilidades en productos OSIsoft
14/02/2018

Múltiples vulnerabilidades en cliente web Saperion
13/02/2018

Vulnerabilidad en IGSS SCADA de Schneider
07/02/2018

Vulnerabilidad en la herramienta de actualización Vyaire Medical CareFusion
07/02/2018

Incorrecto control de acceso en MicroSCADA Pro SYS600 9.x de ABB
07/02/2018

Software vulnerable

Vulneran la seguridad del Mitsubishi Outlander PHEV

06/06/2016

Investigadores de seguridad han conseguido vulnerar la seguridad del híbrido Mitsubishi Outlander. A través de un ordenador portátil han logrado acceder de forma no autorizada a varias de las funciones del vehículo, como encender o apagar las luces, desactivar la alarma antirrobo. Esto permitiría el acceso al interior del vehículo a través de las ventanillas y una vez dentro acceder al puerto de diagnóstico del vehículo que permite acceder a funciones vitales del coche. Mitsubishi está trabajando para corregir este problema.

Referencias:

06/06/2016	pentesterpartners.com	Hacking the Mitsubishi Outlander PHEV hybrid
06/06/2016	cnet.com	British security firm hacks Mitsubishi Outlander via mobile app, ...
06/06/2016	theguardian.com	Yet another car can be hacked – this time it's the Mitsubishi Outl...

Etiquetas: Vulnerability

Ir atrás

Últimas actualizadas

Fuga de información en Swisscom afecta a 800.000 clientes
Actualizado el 13/02/2018

La botnet Smominru utiliza el Malware WannaMine para minar criptodivisas
Actualizado el 09/02/2018

Roban 500 millones de dólares en la criptomoneda NEM a CoinCheck
Actualizado el 08/02/2018

Aplicación de fitness Strava filtra la ubicación de bases militares secretas
Actualizado el 05/02/2018

Un adolescente detenido por obtener información confidencial de la CIA y FBI
Actualizado el 02/02/2018

Fallos de diseño

La seguridad física y la ciberseguridad se dan la mano: CCTV

Publicado el 17/11/2015, por Daniel Fírvida (INCIBE)

En los últimos años han aparecido diferentes noticias relacionadas con ataques a cámaras web y cámaras IP, desde vulnerabilidades propias de cualquier sistema, credenciales embebidas, y el más conocido, cámaras abiertas sin contraseña... y muchos otros ejemplos.

Estos fallos de seguridad no son ajenos a sistemas más profesionales, como grabadores de vídeo o DVR y cámaras de circuitos "cerrados" de televisión o CCTV.

Configuración inadecuada

Hace pocos días se ha hecho público un nuevo ataque [illegible] Incapsula (filial del fabricante Imperva) de una botnet que [illegible] cámaras de circuitos "cerrados" de televisión (CCTV) para hacer ataques de DDoS.

En el ataque, detectado por Incapsula, además de informarse del volumen y ubicación de algunas cámaras, se explica cómo se producía el ataque en estos sistemas, pese a no ser algo especialmente novedoso...

Últimas entradas

Introducción a los sistemas embebidos
Publicado el 08/02/2018, por INCIBE

Hoy en día no somos capaces de imaginarnos de un coche sin sistema de manos libres, una televisión que no sea Smart y un montón de dispositivos que tienen un procesamiento de información. Esto se...

Greatest hits 2017: De aquellos barros vienen estos lodos
Publicado el 30/01/2018, por Juan D. Peláez (INCIBE)

El objetivo de la Bitácora ciberseguridad de INCIBE es recoger las noticias relevantes con el mundo de la ciberseguridad a lo largo del año. Este es el artículo de resumen de aquellas noticias que...

Medidas de protección frente ataques de denegación de servicio (DoS)
Publicado el 26/01/2018, por Alejandro Fernández Castrillo

Los ataques de denegación de servicio son un tipo de ataque informático a través del cual se reduce o anula la capacidad de servidores o recursos

Amenazas de los dispositivos conectados

Configuración inadecuada

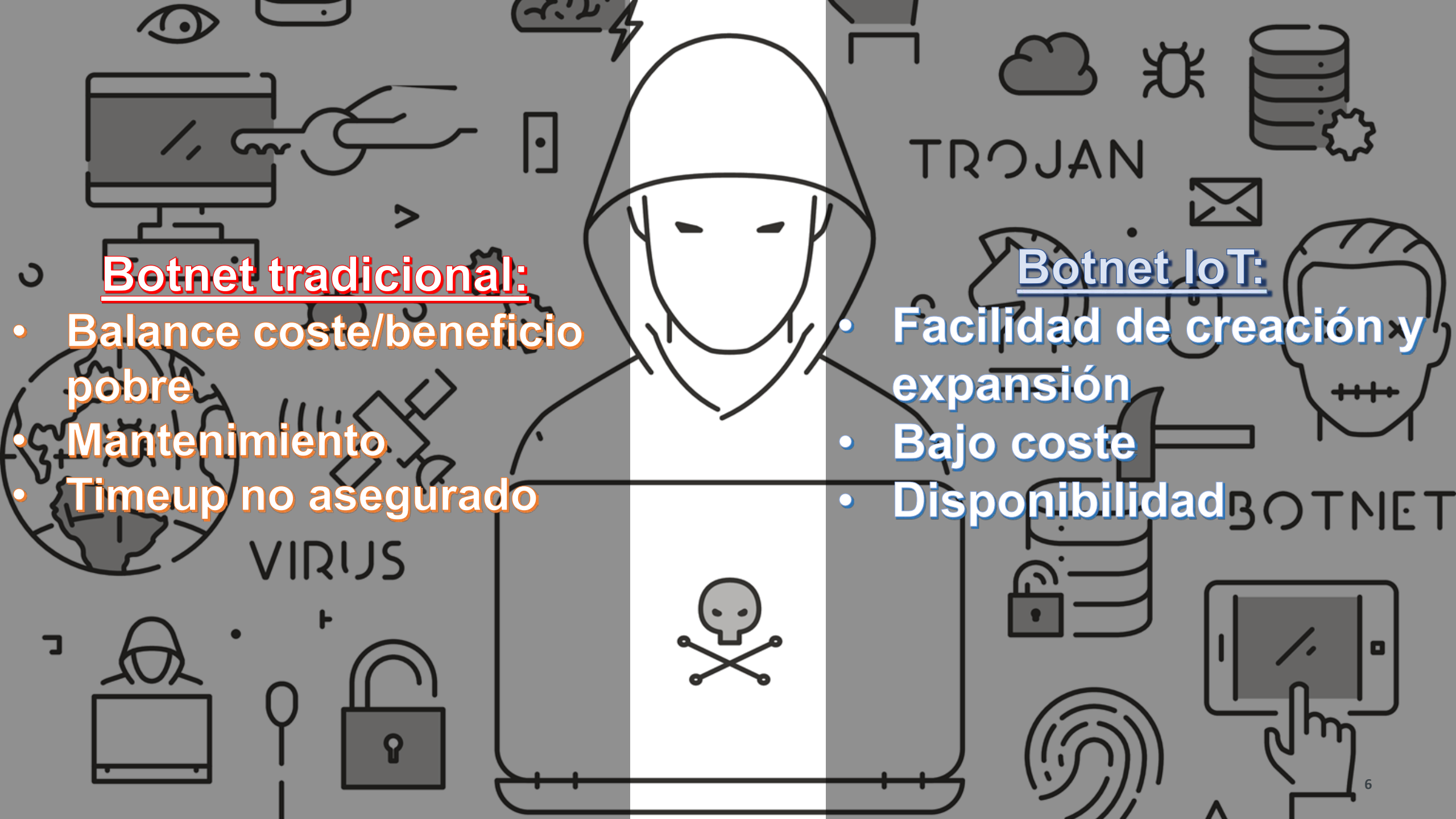
- Falta de autenticación/autorización
- Contraseñas por defecto/débiles
- Servicios innecesarios e interfaces de administración

Comunicaciones y datos

- Cifrado débil o inexistente
- Privacidad datos
- Bloqueo de cuentas, protección fuerza bruta
- Acceso físico

Software/firmware vulnerable

- Falta de auditoría
- Falta actualizaciones e incluso imposibilidad
- Soporte y abandono
- Backdoors
- Fallos de diseño



Botnet tradicional:

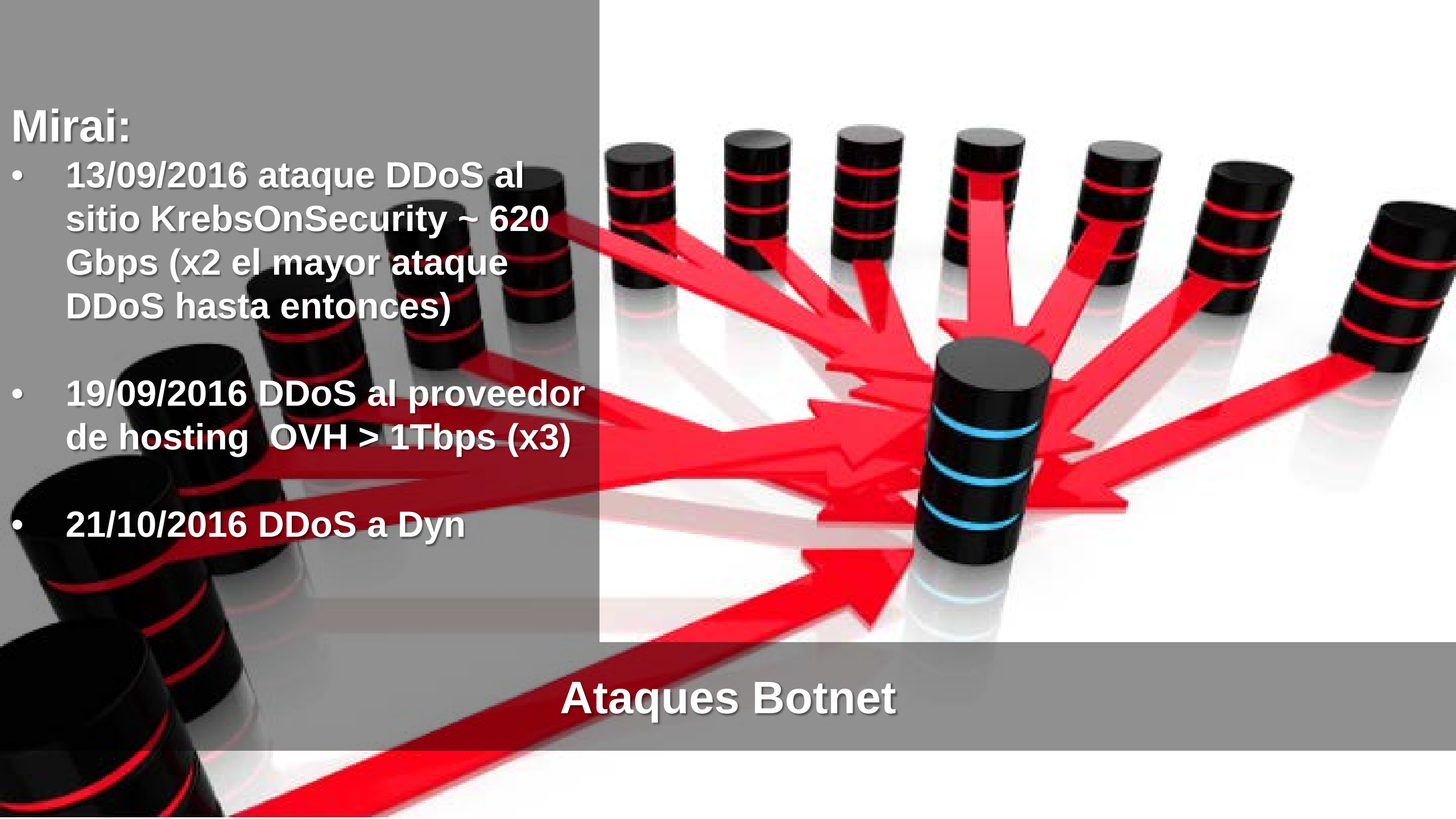
- Balance coste/beneficio pobre
- Mantenimiento
- Timeup no asegurado

Botnet IoT:

- Facilidad de creación y expansión
- Bajo coste
- Disponibilidad

Mirai:

- 13/09/2016 ataque DDoS al sitio KrebsOnSecurity ~ 620 Gbps (x2 el mayor ataque DDoS hasta entonces)
- 19/09/2016 DDoS al proveedor de hosting OVH > 1Tbps (x3)
- 21/10/2016 DDoS a Dyn



Ataques Botnet

Configuración
Auditoría
Actualizaciones

Cifrado
Autenticación

Dispositivo

Red

Aplicaciones
y Servicios

Confidencialidad y privacidad
Seguridad datos (acceso, cifrado)

Soluciones

Incidentes por público objetivo

Incidentes gestionados
en 2017

123.064

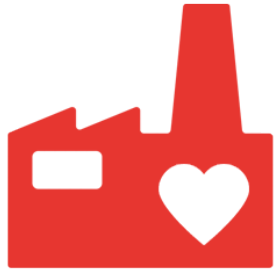
116.642

Ciudadanos
y empresas

Red IRIS

5.537

Red Académica
(RedIRIS)

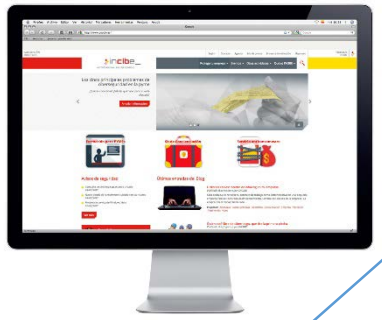


885

Operadores
estratégicos

Ciberseguridad para Profesionales

certsi_
CERT DE SEGURIDAD E INDUSTRIA

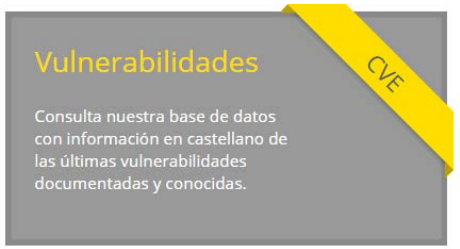


certsi_
CERT DE SEGURIDAD E INDUSTRIA

www.certsi.es
@certsi_

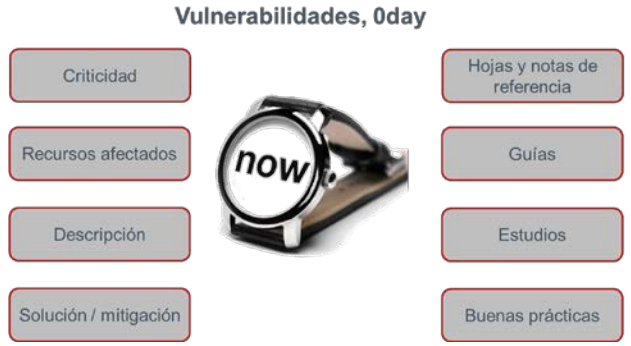
www.incibe.es/formacion

Alerta Temprana



Publicaciones: BLOG, BITÁCORA, GUÍAS, ESTUDIOS Y ENSI.

Información para OOCC



Formación especializada

- Ciberseguridad para micropymes y autónomos
- Curso avanzado de ciberseguridad en dispositivos móviles
- Seguridad en sistemas de control y automatización industrial
- Ciberseguridad básica para fuerzas y cuerpos de seguridad
- Ciberseguridad avanzada para fuerzas y cuerpos de seguridad

Ciberseguridad para Empresas

protege tu empresa

Información

- Blog
- Avisos de seguridad
- ¿Qué te interesa?
- Boletines

Formación

- Hackend
- Curso para micro-pymes y autónomos
- Talleres
- Formación sectorial
- Guías

Herramientas

- Antibotnet
- Antiransomware
- ¿Conoce tus riesgos?
- Kit de concienciación
- Respuesta y soporte
- Catálogo
- Sellos de confianza
- Políticas de seguridad


La ciberseguridad no es una opción

Síguenos en…

CONTACTO	**Instituto Nacional de Ciberseguridad (INCIBE)** info@incibe.es
VISÍTANOS	**Instituto Nacional de Ciberseguridad (INCIBE)** https://www.incibe.es
INFÓRMATE	**CERT de Seguridad e Industria (CERTSI)** https://www.certsi.es **Oficina de Seguridad del Internauta (OSI)** https://www.osi.es **CyberCamp** https://www.cybercamp.es **Internet Segura for Kids** https://www.is4k.es/
SÍGUENOS	**Twitter, YouTube, Facebook, LinkedIn, G+.** @Incibe @protegeempresa @Certsi_ @Osiseguridad @is4kids @CyberCampEs @CiberEmprende_
REPÓRTANOS	**Incidentes, vulnerabilidades, fraude online, phishing, malware, etc.** incidencias@certsi.es, empresas@incibe.es y consultas@osi.es