



Asociación Latinoamericana de
Metros y Subterráneos

EL RETO DE LA GESTIÓN DE LA CIBERSEGURIDAD EN EL TRANSPORTE METROPOLITANO

Isaac Centellas García

Responsable División de Instalaciones y Sistemas de Información
Metro de Madrid.

Índice



El Contexto



La Ciberseguridad y el entorno Smart OT



Hacia un Metro Protegido Digitalmente



Conclusiones



El Contexto



Un Metro conectado

La tecnología como
medio para
desarrollar la
innovación alrededor
de la movilidad ...

Tecnologías de la Comunicación
y de la Información.

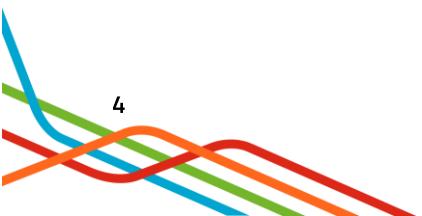
4.0. IIoT

Control del Tráfico e Instalaciones
Centralizado

Automatización de procesos

Eficiencia Energética

Mantenimiento según Condición



La transformación digital

1. Liderar con visión
2. Cliente
3. La comunicación
4. El gobierno del dato
5. Las personas
6. La innovación
7. La tecnología
8. La Ciberseguridad

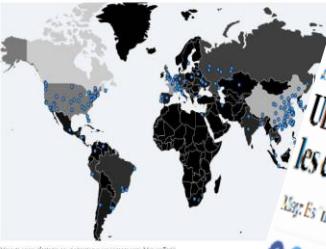


El Contexto

El Confidencial

Viernes negro para la ciberseguridad. Un ataque masivo de ransomware que comenzó turbiando a Telefónica se ha extendido paralizando a medio planeta. Ya hay 100 países afectados

MAPA DE PAISES AFFECTADOS POR EL CIBERATAQUE CON RANSOMWARE. (MENOSFOOT)



EL PAÍS

Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero

Mapa: un ataque internacional que afecta países y regiones y un uso ilegal

PERFILES. EL DEBATE. CONVERSACIONES CON FUTURO. TRIBUNA INTERNACIONAL

Tus datos son tóxicos

El rastro de información que los usuarios dejan en Internet puede ser usado en su contra. En la era digital, proteger la privacidad es la única forma de conseguir una sociedad libre



6

EL PAÍS

ESTADOS UNIDOS

CASO CAMBRIDGE ANALYTICA

Una fuga de datos de Facebook abre una tormenta

Políticos de EE UU y Reino Unido reclaman que Zuckerberg dé explicaciones tras la revelación de que una consultora electoral manipuló información de 50 millones de usuarios de la red social

PERFILES. EL DEBATE. CONVERSACIONES CON FUTURO. TRIBUNA INTERNACIONAL

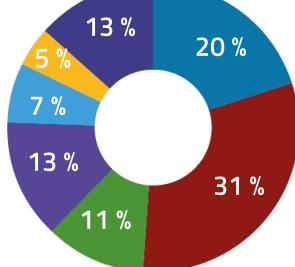
Los datos son vulnerables, y por eso hacen vulnerable tanto a quien los almacena (una fuga de información puede desvelar secretos empresariales o terminar en una costosa demanda) como a los sujetos de esos datos. Esa información que se recoge es peligrosa porque no es fácil de proteger.

Alamys | Uniendo Destinos

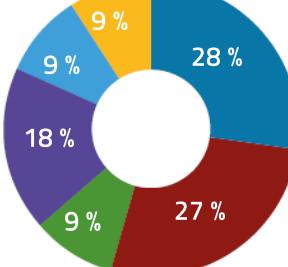
El contexto

TIPOLOGÍA DE INCIDENTES

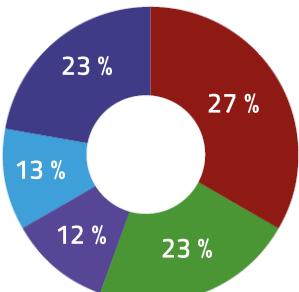
SERVICIOS ESENCIALES



SECTOR ENERGÍA

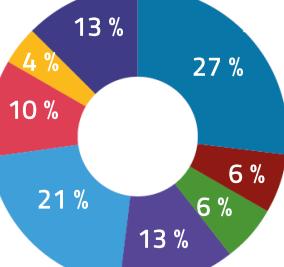


SECTOR TRANSPORTE

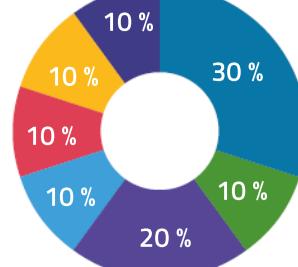


CONSECUENCIAS DE LOS INCIDENTES

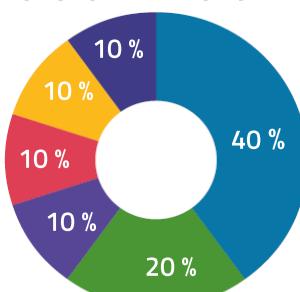
SERVICIOS ESENCIALES



SECTOR ENERGÍA



SECTOR TRANSPORTE



- Ataques dirigidos
- Malware
- Dos o DDoS
- Intrusión
- Compromiso de Información
- Fraude
- Violación de normas

- Pérdida de servicio
- Acceso ilícito a equipos
- Pérdida de control de sistemas
- Pérdida de visibilidad
- Consecuencias ambientales
- Consecuencias físicas
- Incumplimiento regulatorio
- Impacto reputacional

Fuente CCI (Centro de Ciberseguridad Industrial). Encuesta realizada en España en el año

2019

7

A photograph of a subway car interior. Several passengers are visible, mostly focused on their mobile devices. In the foreground, a person's hand holds a smartphone displaying a news article from 'EL MUNDO' with the headline 'El coronavirus se ha convertido en la mayor amenaza para la salud mental'. The background is blurred, showing other passengers and subway infrastructure.

La Ciberseguridad y el entorno Smart OT

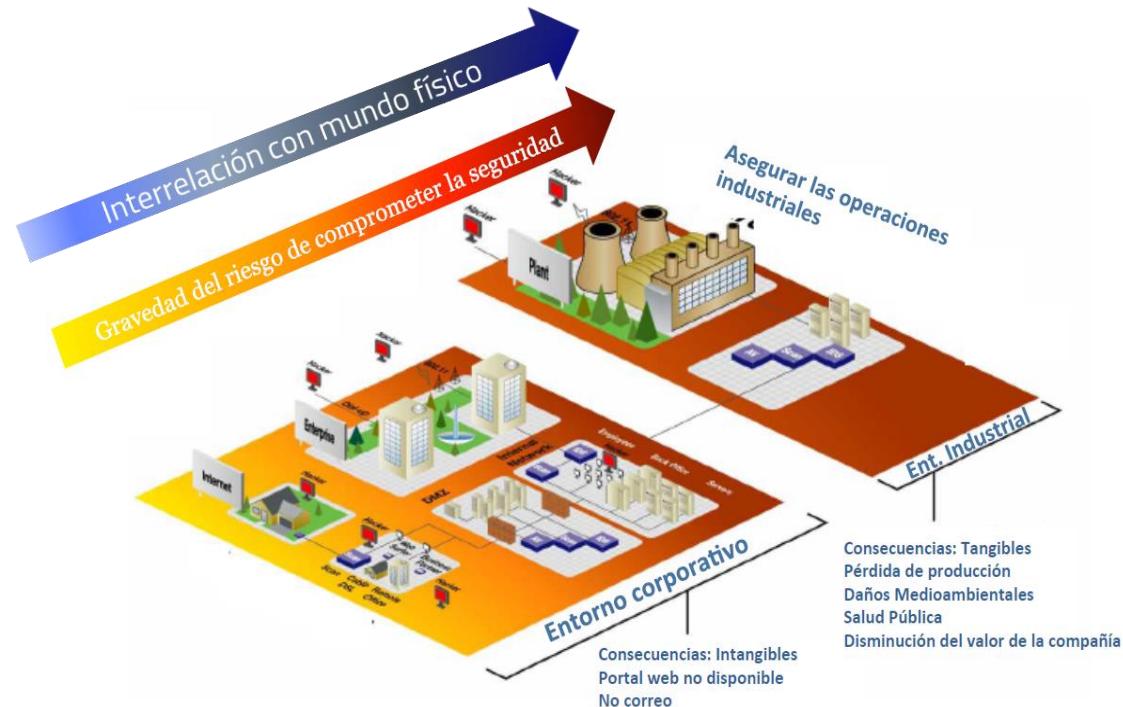
Ciberseguridad

Conjunto de medidas encaminadas a **proteger las operaciones, los datos, la información y los sistemas implicados en la prestación del servicio contra cualquier amenaza.**



Dos entornos en los Metros

Una nueva conectividad entre sistemas para operar los Metros ha dado lugar a nuevos escenarios de riesgo.



Dos entornos IT OT

Sistemas IT
(Gestión del Negocio)



CONFIDENCIALIDAD

INTEGRIDAD

DISPONIBILIDAD

+ importancia -

Sistemas OT
(Explotación Ferroviaria)



- importancia +

Dos realidades muy distintas

IT

Confidencialidad, Disponibilidad, Integridad
2/3 años. Muchos proveedores

Normativas genéricas

Metodologías estándar y automatizables

Común y fácil de desplegar y actualizar

Fácil despliegue

Habituales con conocimientos

OT

Disponibilidad, Integridad, Confidencialidad
10/20 años. Proveedores de nicho

Normativas específicas y sectoriales

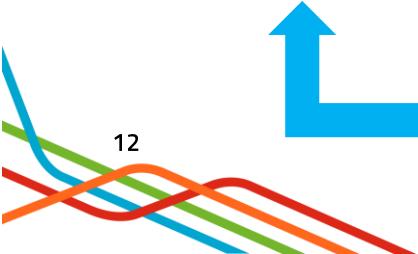
Sin metodologías estándar. Testeo de nicho

Impacto rendimiento / No soportado

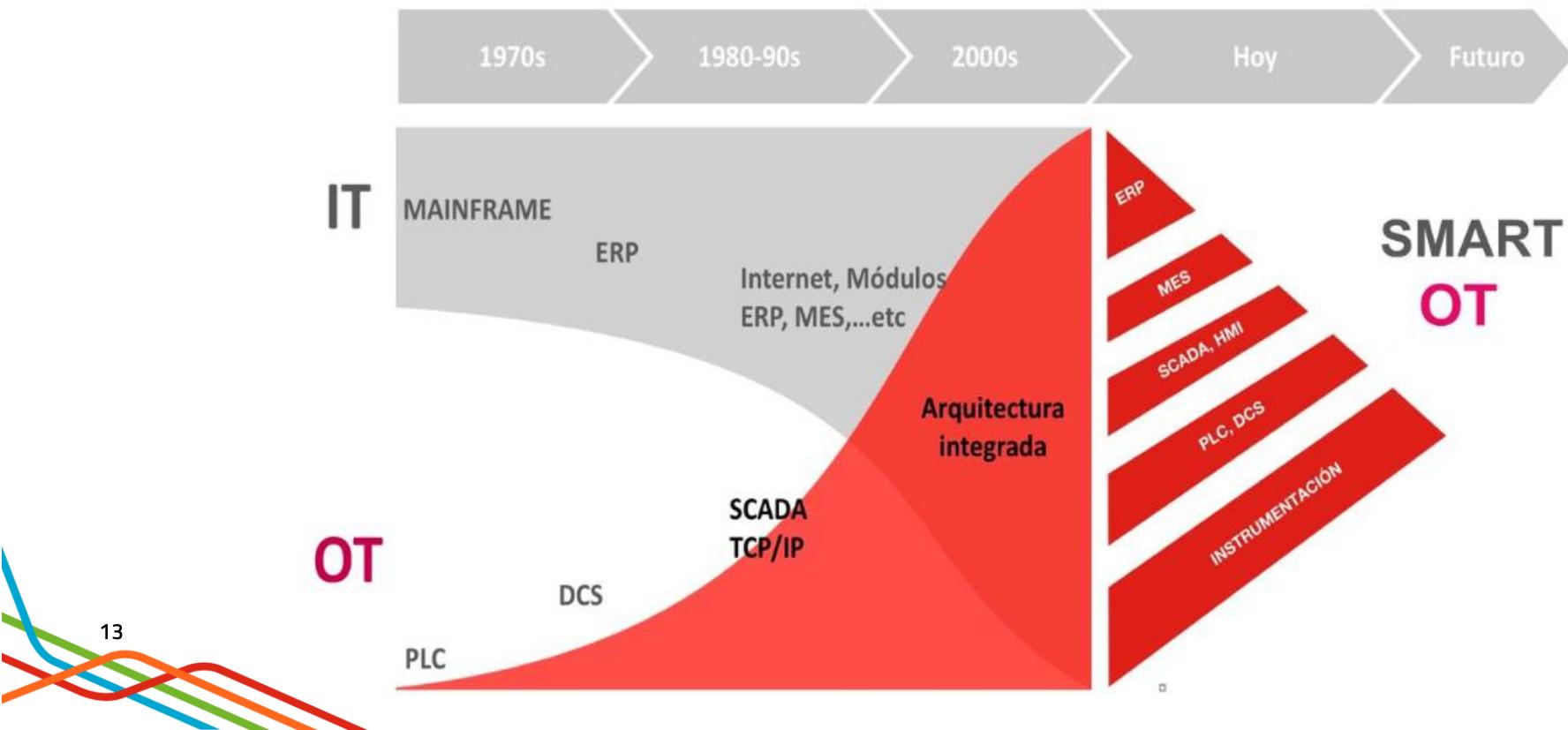
Difícil despliegue

Escasos perfiles con conocimientos

OBJETIVOS
CICLO DE VIDA
CUMPLIMIENTO NORMATIVO
TESTEO Y AUDITORIAS
ANTIVIRUS Y PARCHES
RTA. INCIDENTES / ANÁLISIS FORENSE
PERFILES



Convergencia IT OT



Una nueva inteligencia empresarial

“Debemos de buscar una nueva inteligencia empresarial, desde el aprovechamiento de la inteligencia de negocio y la inteligencia de operación, y ponerla al servicio de nuestros grupos de interés”



La ciberseguridad en los Metros

La ciberseguridad en los Metros debe de aproximarse a esas dos realidades distintas, IT y OT, con sus características **diferenciales** pero con una **estrategia común**.



¿Contamos con las **medidas necesarias** para hacer frente a las amenazas de la ciberseguridad ?

¿Son las **medidas** con las que contamos **proporcionales** al **impacto** que puede tener en **nuestras empresas** un ataque de esta naturaleza?





Hacia un Metro Protegido
Digitalmente

La Gestión de la Ciberseguridad

La gestión de la ciberseguridad de nuestras compañías se debe **basar en**:

- **Liderazgo** por parte de la dirección
- **Cumplimiento** legal y normativo
- **Gestión** eficiente de los **riesgos**
- **Soluciones** coordinadas y **multidisciplinares**
- **Prevención**
- **Formación** y concienciación



... debemos transformar nuestras organizaciones hacia **organizaciones protegidas digitalmente**.

Promover un **M**etro **P**rotegido **D**igitalmente



Hacia un Metro Protegido Digitalmente

Ocho preguntas para la reflexión:



1. ¿Disponemos de una Política de Ciberseguridad?
2. ¿Nuestro plan estratégico contempla la ciberseguridad?
3. ¿Tenemos identificados nuestros activos digitales?
4. ¿Disponemos de tecnología de protección?
5. ¿Tenemos implantados procesos de detección de amenazas?
6. ¿Contamos con la organización necesaria?
7. ¿Tenemos destinadas partidas presupuestarias a esta materia?
8. ¿Tenemos planes de respuesta ante incidentes?



Hacia un Metro Protegido Digitalmente

Cómo afrontar el futuro



- | | | | |
|---|--|---|--|
| 1. Seguridad en el diseño – Protección de los existente | 1. Análisis y gestión de vulnerabilidades | 1. Detección, análisis y gestión de los incidentes de seguridad | 1. Lecciones aprendidas |
| 2. Definición de la criticidad | 2. Servicios de seguridad y vigilancia avanzada | 2. Gestión de crisis | 2. Adaptación de la infraestructura, procedimientos y planes |
| 3. Análisis y gestión de riesgo e impacto | 3. Monitorización continua – Inteligencia aplicada | 3. Coordinación y colaboración | 3. Ejecución de pruebas y simulacros |
| 4. Coordinación y colaboración | 4. Continuidad, redundancia y operación del servicio | 4. Ejecución planes de continuidad del servicio | |
| 5. Concienciación, capacitación y formación | | | |

Hacia un Metro Protegido Digitalmente

Cómo afrontar el futuro



Conclusiones



Una nueva realidad, nuevos escenarios.



No podemos renunciar a una
nueva inteligencia empresarial



Debemos transformar
nuestras organizaciones hacia
Metros Protegidos Digitalmente.

