



SIEMENS Mobility - Alamys:

Ciberseguridad para sistemas ferroviarios

Noviembre 2021

Camilo Cerda
SIEMENS Mobility

SIEMENS

Tendencias Clave

Ciberseguridad Ferroviaria



SIEMENS

Tendencia: Nuevos ciberataques

Gobiernos aumentan su atención a los ciberataques que apuntan a industrias críticas.



The Colonial Pipeline Crisis Is a Taste of Things to Come

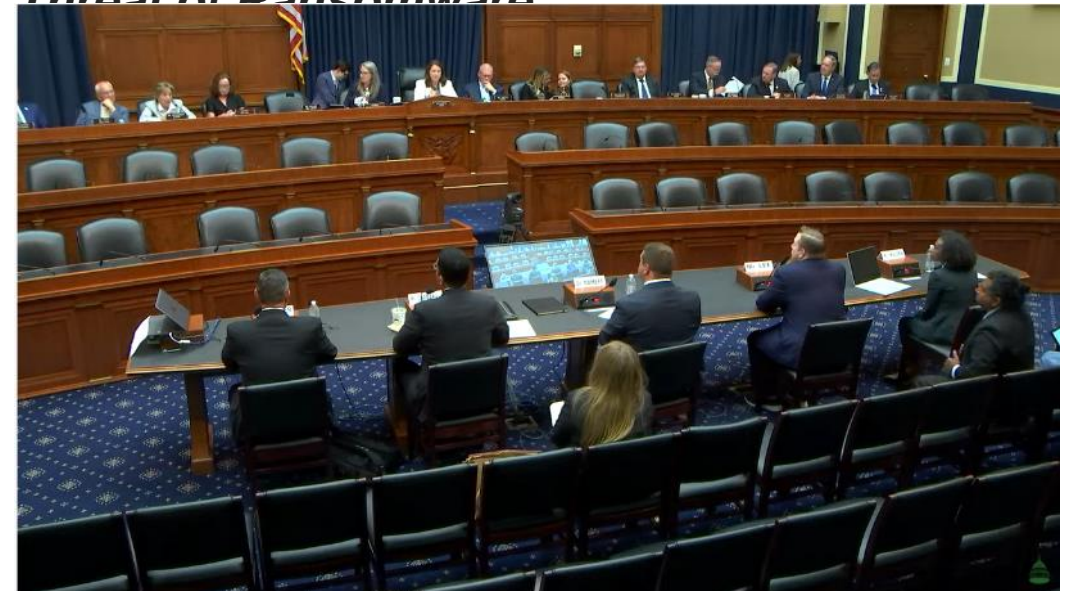
Biden must act now to protect the energy system from the rising threat of cyberattacks and natural disasters.

By [Jason Bordoff](#), a columnist at *Foreign Policy* and the co-founding dean of the Columbia Climate School.



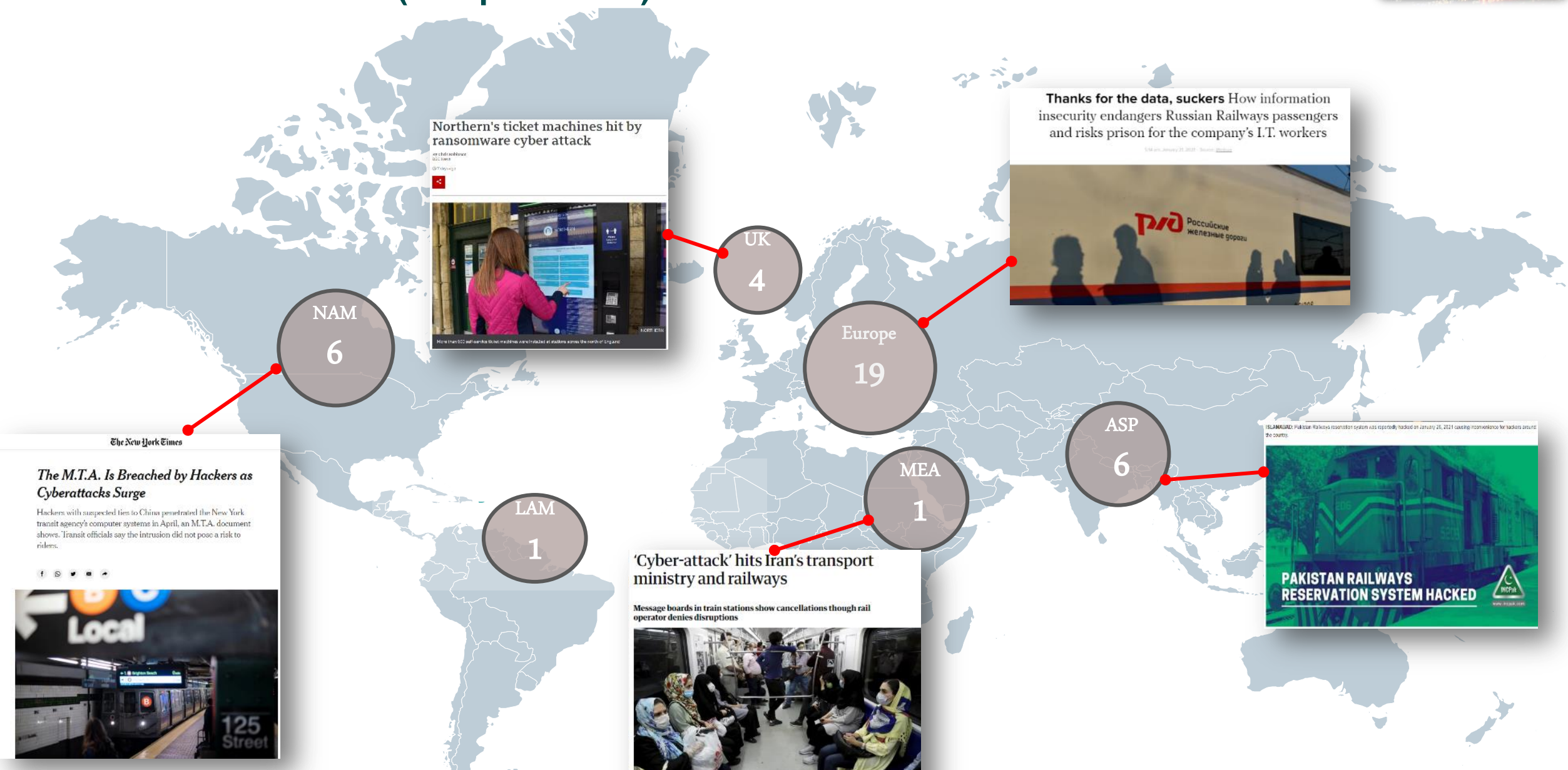
Committee on Energy and Commerce hearing:

"Stopping Digital Thieves: The Growing Threat of Ransomware"



Tendencia: Ciber incidentes son titulares de la prensa en el 2021

Más de 36 incidentes (búsqueda web)



Tendencia: Nueva regulación y estándares

Las regulaciones de ciberseguridad para infraestructura se están haciendo más estrictas



Revised Directive on Security of Network & Information Systems (NIS2)-

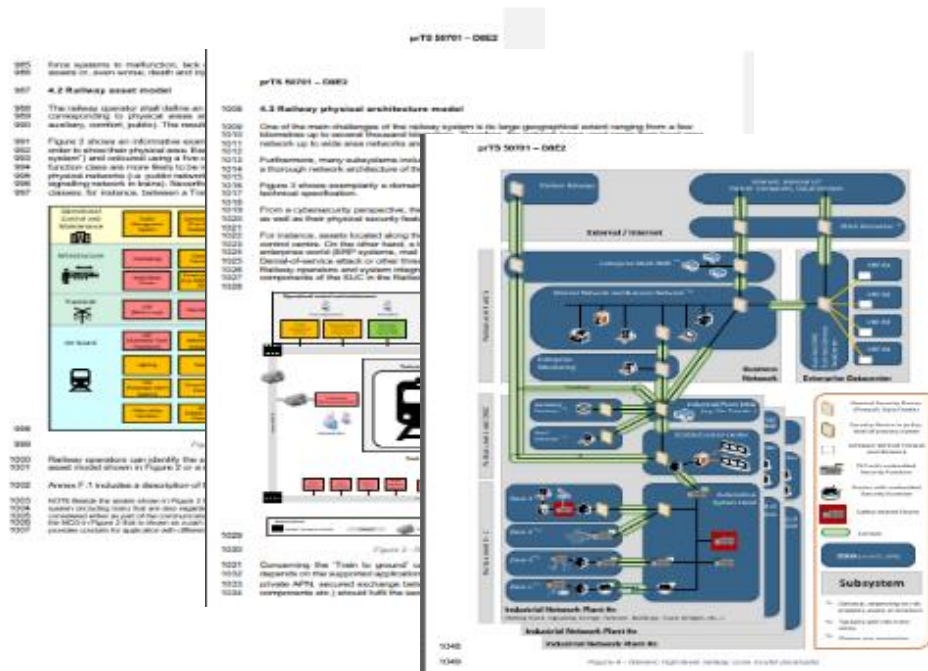
proposed on 16 December 2020



- **Multas de hasta 10 MM EUR** o 2% de ventas anuales mundiales
- **Obligación de compartir información** y cooperación
- Comunicación coordinada de **vulnerabilidades nuevas**
- Requerimientos básicos de seguridad con una lista de medidas clave, incluyendo **respuesta a incidentes**, **administración de crisis**, manejo de vulnerabilidad, **pruebas de ciberseguridad** y uso efectivo de encriptación
- Foco en ciberseguridad de la **cadena de suministro**
- **Responsabilidad personal del management** de las compañías por el cumplimiento de regulaciones de administración de riesgo de ciberseguridad
- Obligación de **reporte de incidentes**, contenido mínimo y plazos.

Tendencia: Nueva regulación y estándares

Nueva especificación técnica para ciberseguridad ferroviaria TS 50701



Reference: CLC/TS 50701:2021
Title: Aplicaciones Ferroviarias- Ciberseguridad

Abstract/Alcance:

Este documento entrega guías y especificaciones para **operadores ferroviarios**, integradores de sistemas y proveedores de productos, sobre como debe **administrarse la ciberseguridad** en el context del proceso de ciclo de vida de EN 50126-1 RAMS. El objetivo de este documento es implementar un **enfoque consistente a la administración de la seguridad de sistemas ferroviarios**.

Este documento también puede ser utilizado para **asegurar la seguridad de los sistemas** y componentes/equipos desarrollados independiente de EN 50126.

Este documento aplica a los dominios de Comunicaciones, Señalización y Procesamiento, Material Rodante, e Instalaciones Fijas.



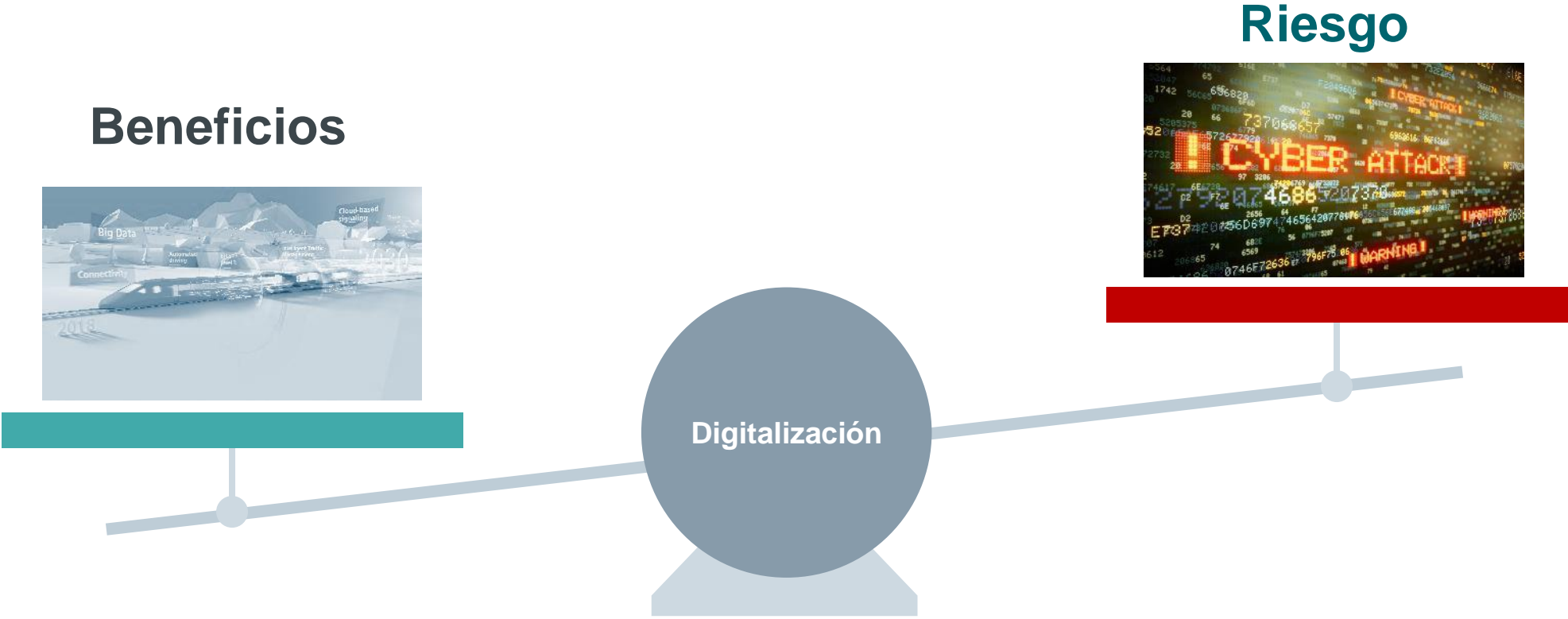
Consecuencias y Posibilidades

Ciberseguridad Ferroviaria



SIEMENS

Consecuencias: **Los operadores ferroviarios deben encontrar un equilibrio**
Maximizar los beneficios de la digitalización y minimizer los ciber riesgos.



Posibilidades: Integrar la ciberseguridad de los OEM e Integradores en las nuevas licitaciones.

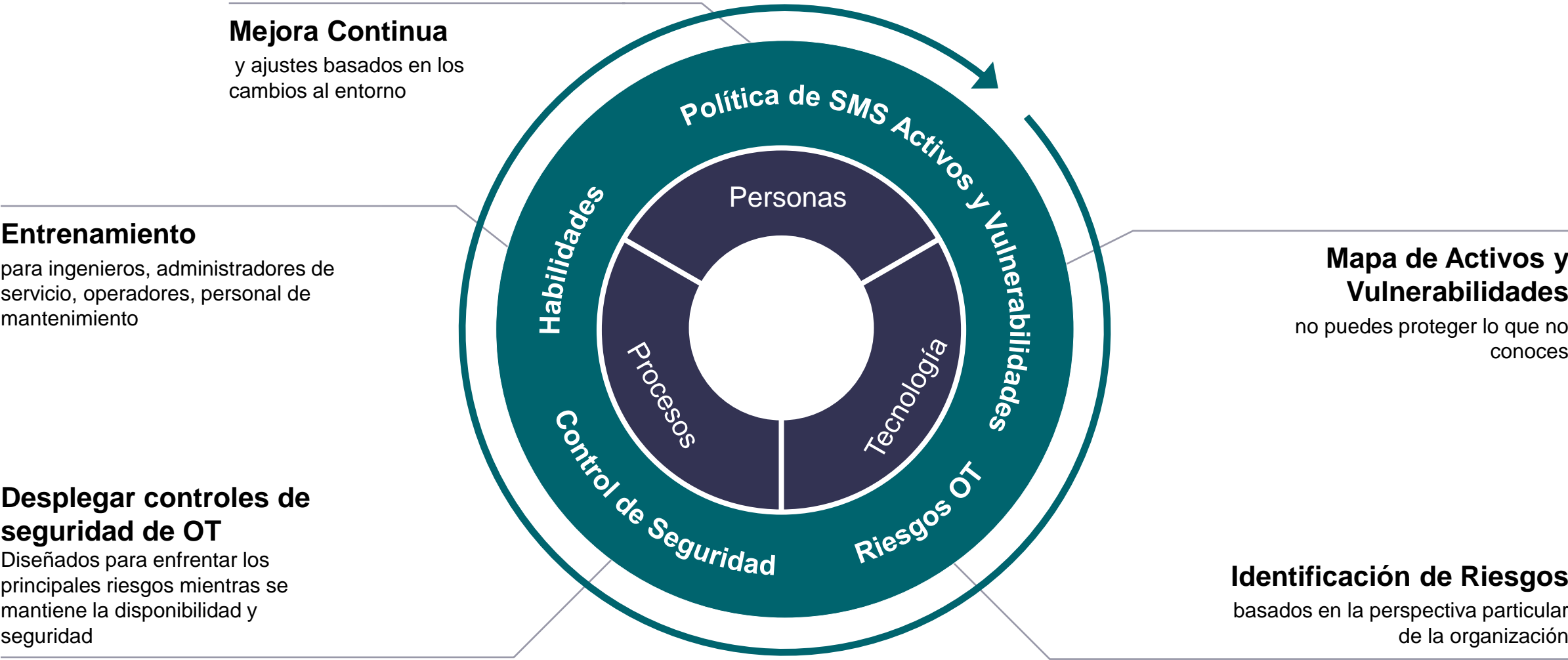
Por ejemplo, IEC62443-3-3 Security Level 3

FR>	IAC	UC	SI	DC	RDF	TRE	RA		tot
SL 1	10	8	5	2	4	1	7		37
SL 2	6	4	5	2	2	1	3		23
SL 3	6	9	6	1	4	1	3		30
SL 4	2	3	3	1	1	0	0		10
tot	24	24	19	6	11	3	13		100



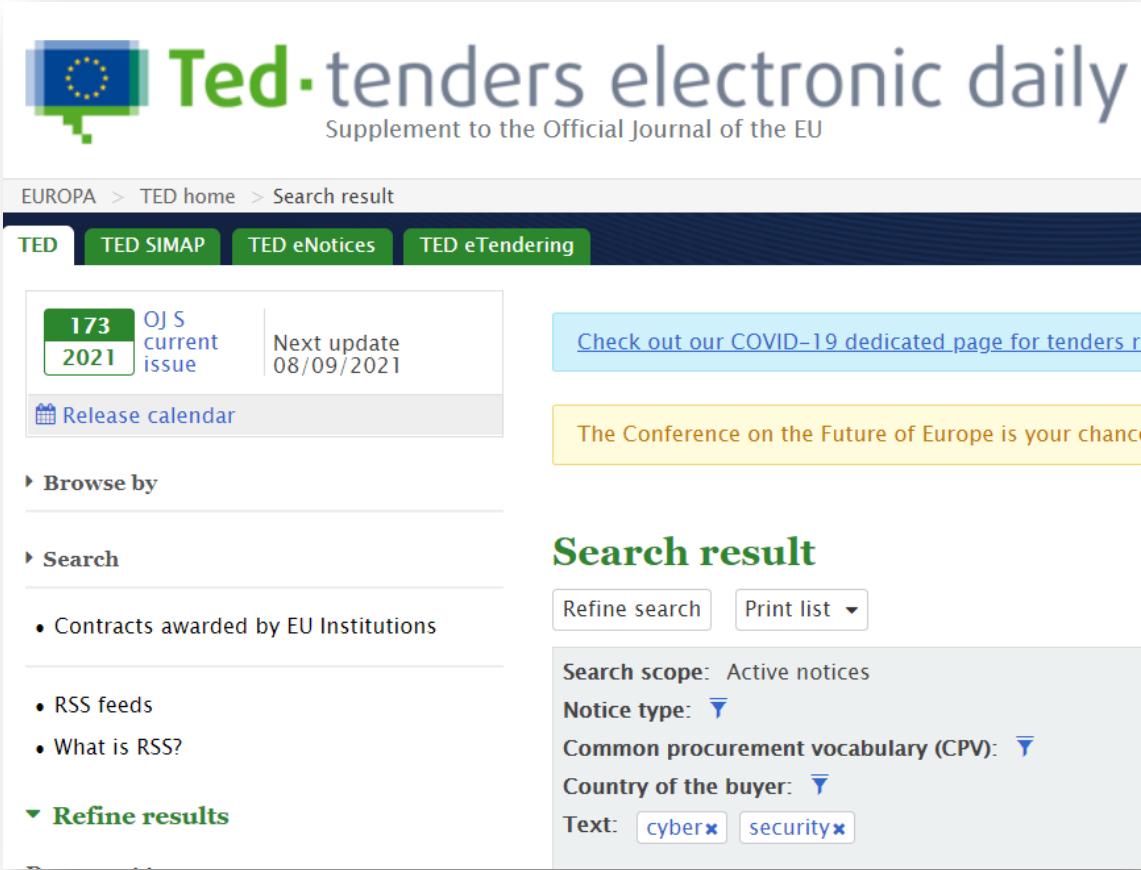
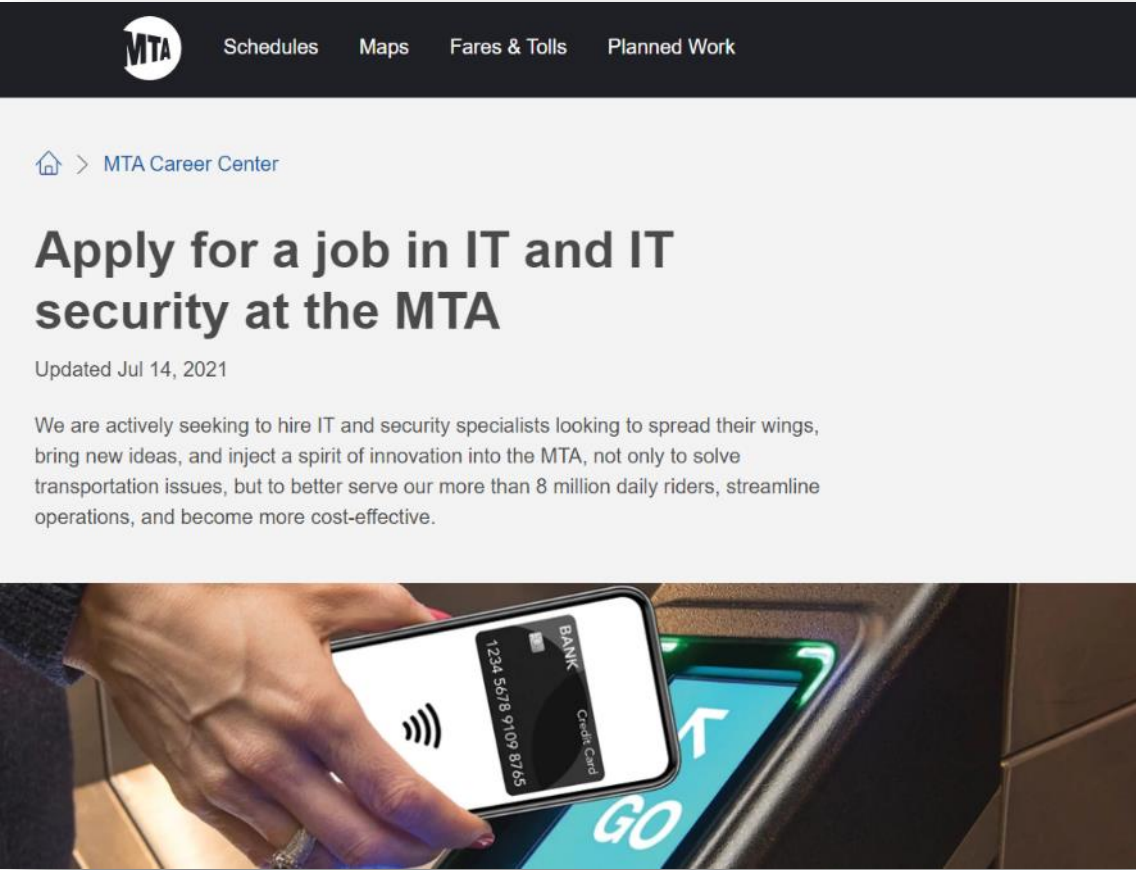
*Number of system requirements
given in IEC 62443-3-3:2019,
per FR groups and SL values*

Posibilidades: **Establecer un proceso y un presupuesto**
Identificar los activos clave, los riesgos del negocio y una estrategia para enfrentarlos



Posibilidades: Contratar expertos en ciber seguridad o externalizar el servicio

Administrar las tareas de ciberseguridad



SOLUCIONES

Ciberseguridad Ferroviaria



SIEMENS

Soluciones: Digitalización con Smart Security:

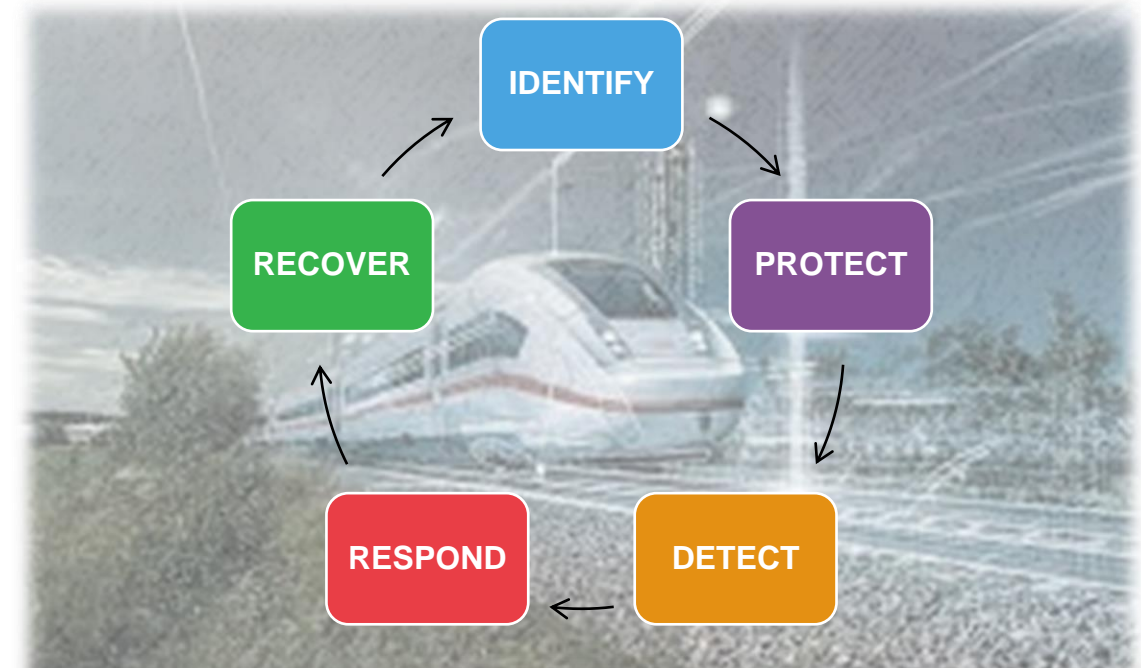
Cumplir requerimientos legales y administrar riesgos de negocio y seguridad

Puntos Clave / UC's

IDENTIFY riesgos de negocio
PROTECT operaciones ferroviarias
DETECT anomalías, causa raíz & reporter incidencias
RESPOND & **RECOVER** para minimizar ciber impacto

Beneficios

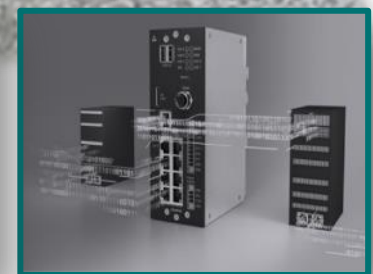
- Cumplimiento de Leyes de Ciberseguridad y privacidad de datos
- Reducir Riesgo (financiero, cumplimiento, seguridad y reputacional)
- Soporte para crear caso de negocio de seguridad
- Consultores con conocimientos ferroviarios y en ciberseguridad
- Red global de +1200 expertos en ciberseguridad (1)
- Soluciones específicas para trenes de Siemens y sus partners
- Procesos y productos certificados ISO27001 y IEC62443
- Referencias con operadores ferroviarios y otras industrias



**Expertos Seguridad
Ferroviaria**



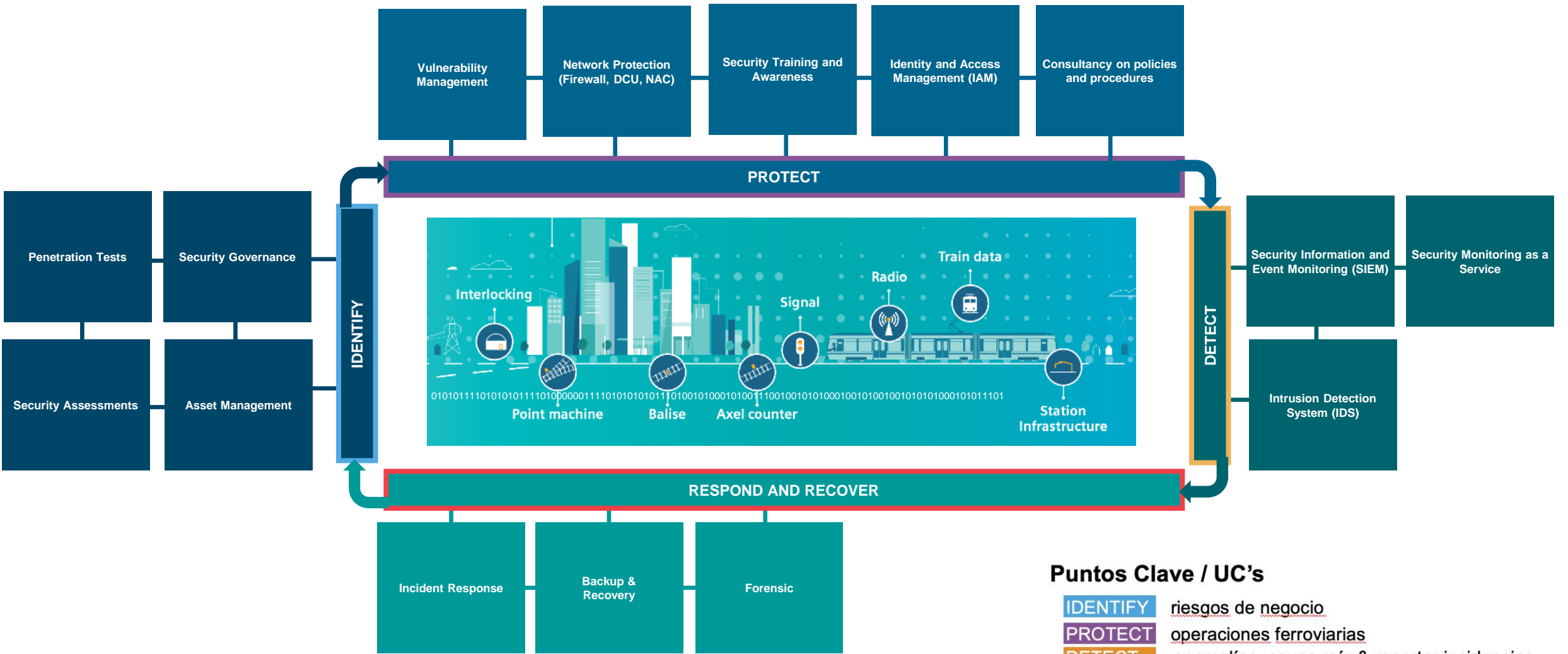
**Proceso
Certificado**



**Soluciones
Ferroviarias**

Soluciones: Elementos del portafolio de ciberseguridad en Siemens Mobility

Cumplir requerimientos legales y administrar riesgos de negocio y seguridad



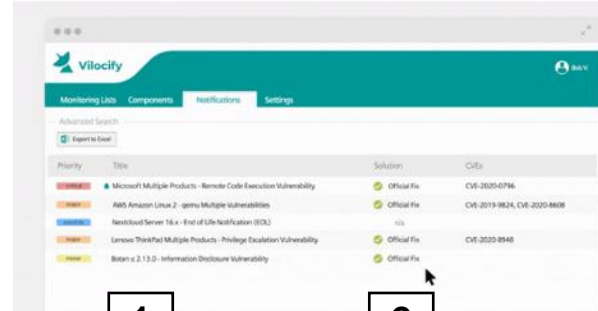
Soluciones: Nuevos servicios

Pruebas de Seguridad, Administración de Vulnerabilidades y Detección de Intrusiones



Identificar (Pruebas de Seguridad)

- Cambios de configuración
- Cambios de version de software
- Vulnerabilidades de software y configuración
- Cumplimiento de políticas de seguridad



Specify components



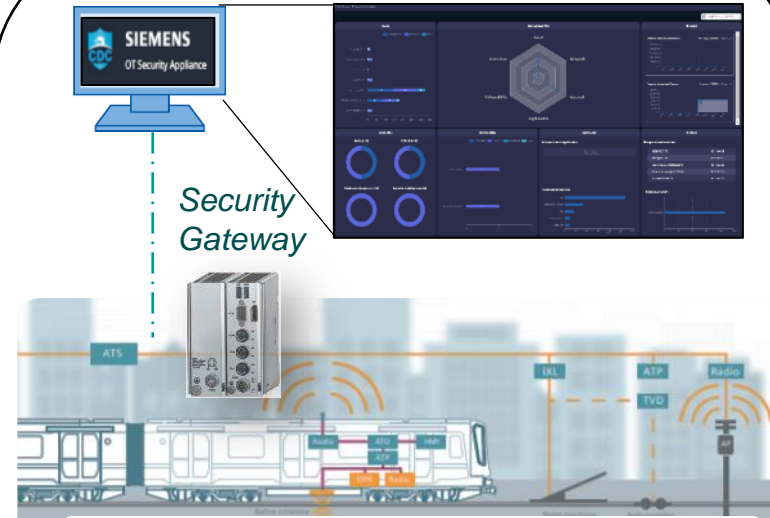
Monitor



Alarm & Report

Monitoreo y Seguimiento (VM)

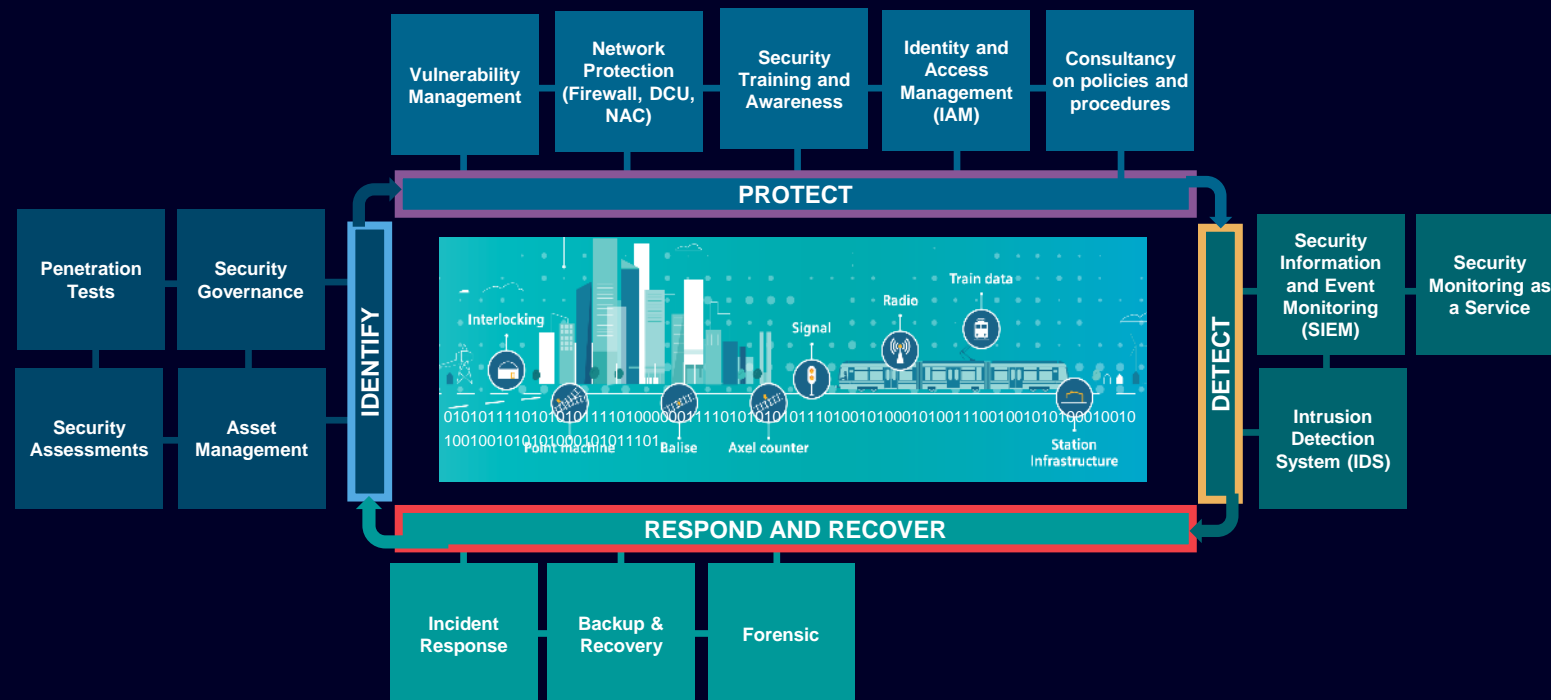
- Vulnerabilidades de software con nivel de severidad (CVSS)
- Planificación de parches y otras medidas de mitigación
- Base de datos > 90k componentes de software



Detección de Intrusión (IDS)

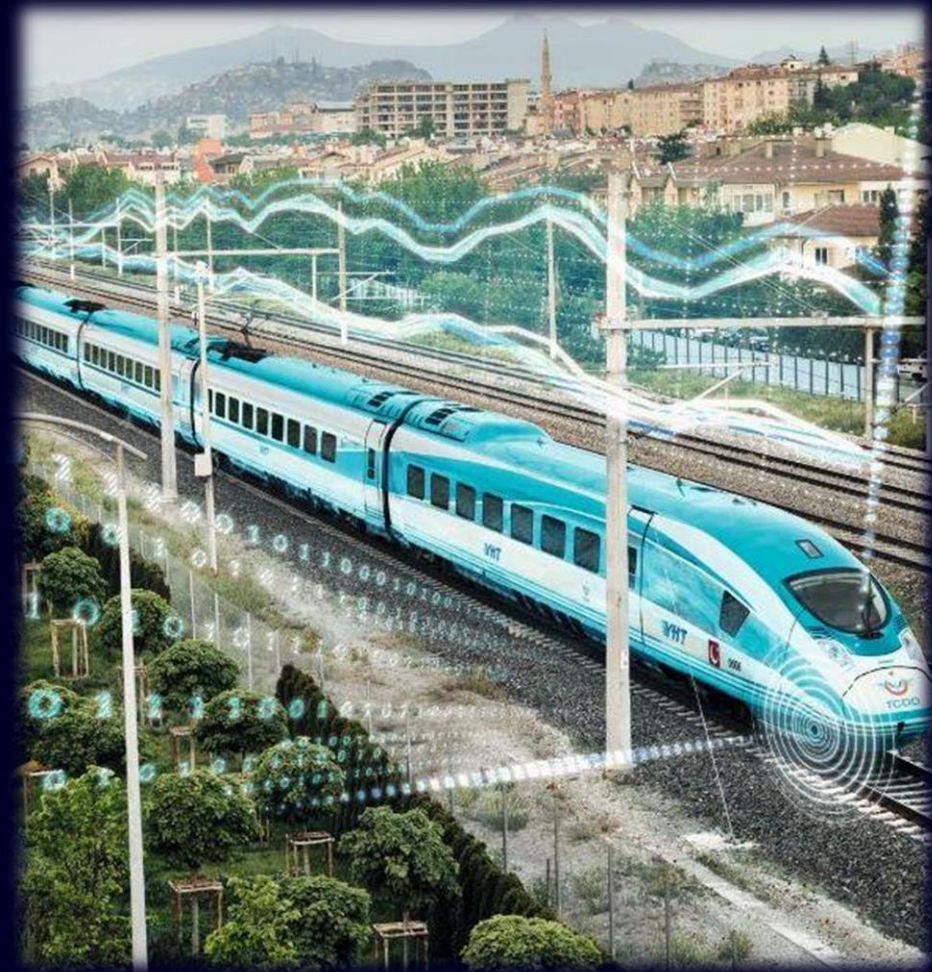
- Para material rodante y señalización
- Sistemas basados en firma y en IA
- SIEMENS IDS y Security Gateway
- Soluciones de Partners

| Preguntas



SIEMENS

Muchas gracias!



Camilo Cerda

Siemens Mobility Spa

CEO Chile

<mailto:camilo.cerda@siemens.com>

[siemens.com/mobility-services](https://www.siemens.com/mobility-services)

SIEMENS