26º CONGRESO ESPAÑOL ITS

INSTITUTO DE LA INGENIERIA DE ESPAÑA

INTELLIGENT TRANSPORT SYSTEM ITS ESPAÑA

Relevancia de los ITS en la Fiabilidad y Resiliencia de los Sistemas de Transporte

J Javier LARRAÑETA
Secretario General
PESI

PESI
PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

Madrid
24-26 marzo 2026

Nota aclaratoria

La actual presentación no ha sido desarrollada con ninguna herramienta de Inteligencia Artificial.

Tan sólo con la limitada Inteligencia Natural del Autor y el conocimiento, información documental y experiencias acumuladas en 43 años de actividad académica, empresarial y profesional (CC. Físicas, formación tecnológica en TIC-KET y empresarial en Dirección y marketing; Tco. Sup. en PRL/3 especialidades; Director de Seguridad habilitado por el MINT)

PESI cuenta con una ayuda de la Agencia Estatal de Investigación (MICINN) dentro del Programa PTE (Expediente: PTR2024-002956)

Actividades de PESI en el ámbito de la Movilidad (segura) - 1

- **Foco de la Movilidad Segura en la Persona (empleados y externos de la cadena de valor)**

Movilidad segura que atañe a las ***Personas (Conductor, pasajero, usuario vulnerable en la Vía)***, sea por sus *desplazamientos* en *misión* como en *in-itinere*. Pero no exclusivamente a los Trabajadores y Empleados de la propia organización, sino también al Personal de toda la **cadena de valor del negocio y las cadenas de suministro y logística;** la accidentalidad que pueda producirse deriva en responsabilidades que se encuadran en la labor de los **Departamentos de PRL-SST** y el área de Personal; los cuales deben responder ante la **Inspección de Trabajo** y **DGT.**

- ***Transporte de Mercancías peligrosas*** (sistemas embarcados, carta de porte en la nube…)
- ***Movilidad segura:*** directamente relacionada con las ***Personas*** y la ***Organización*** empresarial,

Factores añadidos a Infraestructura y Vehículo, => nuevo ***Modelo de Seguridad Vial (4 Elementos)***, superando modelo clásico (Persona-Vehículo-Infraestructura).

- Modelo de ***4 Factores (Infraestructura-Vehículo -Persona- Organización empresarial)*** reflejado en el ***Marco de Referencia de la Movilidad empresarial segura y sostenible*** (incluye *Seguridad Vial Laboral*)

Este Marco de Referencia, gratuito, promovido por PESI con la colaboración de **FESVIAL y** el Centro Tecnológico **TECNALIA,** está adscrito al ***MGA*** *Modelo de Gestión avanzada* (modelo de calidad en la gestión empresarial, derivado de la Euro-Q) también gratuito, compatible con los modelos basados en **ISO** (9001, 14001, 27001, 45001 ...).

- Uso de la ***IA (algoritmos) en la Movilidad***, tanto en el Vehículo autónomo como en los *ITS, APPs* y aplicaciones de ayuda al Usuario (pasajero/conductor-copiloto), requiere un tratamiento **Humanístico** acorde con la *Legislación Europea* y la de los Estados miembros en la **UE**.

Este enfoque humanístico de la IA está siendo desarrollado por la Confederación Europea de Organizaciones de Profesionales de la PRL-SST (expertos de PESI).

Actividades de PESI en el ámbito de la Movilidad (segura) - 2

- La ***Resiliencia climática*** de las Infraestructuras críticas y Servicios esenciales a la Sociedad, entre los que se encuentran las ***Infraestructuras de Transporte*** (carretera, vías férreas...) y los medios para la Movilidad (Transporte público y de mercancías, Energía y Telecomunicaciones y los propios los Centros de Control e ITS...).

Esto se suma al modelo de ***Gestión integral de Riesgos, GRC y Resiliencia*** que se aplica igualmente a las Infraestructuras de Transporte y Movilidad, tanto públicas como privadas. El modelo incluye herramientas para la categorización de los *elementos críticos, dependencias* de otras infraestructuras críticas (energía eléctrica y combustibles, telecomunicaciones...) y evaluación de los posibles *efectos en cascada*, que dañen no sólo las propias infraestructuras y/o medios sino también la ***Continuidad de las Infraestructuras y Servicios de Movilidad, como parte de su Resiliencia.***

- Una parte relevante de las Infraestructuras de Transporte y Movilidad han sido declaradas ***"Infraestructuras críticas/esenciales"*** que deben cumplir con la ***Ley PIC y la nueva Directiva Europea de Resiliencia.***
- La gestión de la ***Ciberseguridad*** (tecnologías y sistemas de las infraestructuras, ITS y vehículos -autónomos, eléctricos y convencionales-): actividades de innovación del Grupo Inter-Plataformas de Ciberseguridad.
- La ***Cultura Preventiva*** del Trabajador, también como **conductor** de vehículos. (punto central del Grupo de Cultura Preventiva, seguridad y salud Laboral, en el que incluye la seguridad vial laboral.
- Los **medios pedagógicos** innovadores y sistemas tecnológicos para la *concienciación, información y formación* de los trabajadores en una *Cultura de Seguridad (Vial)*:

Área de importante actividad en PESI (eLearning, gamificación, realidad virtual, aumentada y mixta VR/AR/XR, Big data, simulación, IA, gemelos digitales...) compartido por el Grupo de Safety-Industria 5.0 en los procesos de ***transformación digital e incorporación de las KET*** en las Organizaciones.

Resiliencia y desastres/accidentes industriales:

nuevos riesgos y efectos cascada en instalaciones/Red de Transporte/servicios esenciales

La actividad industrial/económica está llena de incidentes de diferente naturaleza, gravedad y afección, pero los accidentes industriales combinados con nuevos riesgos generan situaciones insospechadas:

- Fukushima: accidente nuclear derivado de un tsunami provocado por un terremoto, afectando instalaciones críticas (Japón, 11 de marzo de 2011)
- Ciberataques (WannaCry, Dragonfly…): paralización durante varios días de servicios centrales de operadores críticos en la UE (energía, telecomunicaciones, ITS…)
- PANDEMIA COVID-19 (2020 –2021): afección global en el funcionamiento de todos los Operadores críticos (cadena de suministro). Nuevas: Gripe aviar…
- Cambio Climático y desastres naturales: Terremotos/ Tormentas /Incendios en España/ DANA en Levante… (grave afección a toda la Sociedad, infraestructuras urbanas, de transporte e industriales).
- Apagón eléctrico (2025): afección Sociedad e Infraestructuras críticas (dependencia)
- Explosiones solares (radiación): riesgo de “apagón” de Telecomunicaciones

Otros:

- Barco embarranca en Canal de Suez (2021): paralización del transporte mundial
- Situación geopolítica: Terrorismo y conflictos bélicos: guerra de Rusia en Ukrania (crisis energética/ciberataques), Israel en Gaza; USA con Venezuela/ ataques a Irán…
- Políticas proteccionistas (guerras comerciales entre Bloques): acceso a RR naturales…
- Crisis humanitarias África/Asia/LATAM y migraciones masivas.

Seguridad y Resiliencia industrial: riesgos y efectos en cascada

(Industria e Infraestructuras –transporte, energía, redes de suministro…)

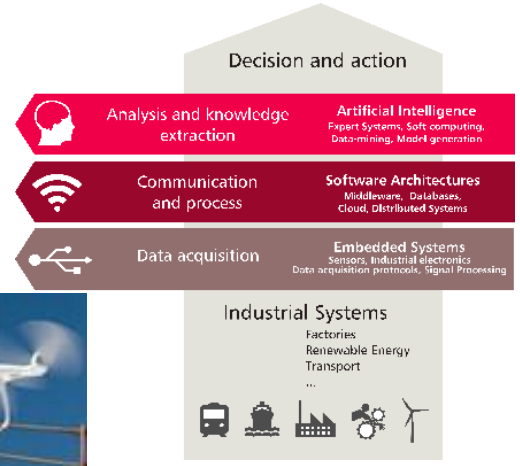
- Desastres naturales (más frecuentes y de mayor intensidad debido al cambio climático): inadecuada evaluación de riesgos climáticos y efectos sobre infraestructuras, instalaciones, operación y servicios.
- Insuficiente evaluación de las dependencias de una instalación, más si es crítica, tanto internas como de otras infraestructuras (IC: energía, telecomunicaciones, agua, transporte, emergencias…) para evitar/minimizar efectos en cascada.
- Falta de mecanismos eficientes de alerta temprana, información y actuación coordinada entre operadores (Infraestructuras Críticas y/o Servicios esenciales) y su Cadena Valor (subcontratas, logística, mantenimiento, proveedores).
- Diversas causas (ciberataques, ataque terrorista, pandemia, sabotaje, fallos técnicos de diseño, mantenimiento, errores humanos, otros…) también pueden ocasionar una concatenación de similares consecuencias (directas y en las Cadenas de Valor).
- Adicionalmente tienen una influencia directa en la Seguridad y Salud Laboral: afección a los Trabajador@s (seguridad física y salud psicosocial inc.), tanto el personal interno como los colaboradores externos (toda la cadena de Valor).
- Todo ello implica una imprescindible coordinación de las Direcciones operativas (O&M/ Ingeniería/Logística/Personas-PRL…) con las de Seguridad (Security-Cyber IT-OT y Emergencias) y continuidad de Negocio.






Seguridad y Resiliencia industrial (infraestructuras e ITS): retos y ámbitos de mejora

- Falta de Estrategias de Resiliencia (continuidad de los Servicios Esenciales – Business Continuity Plans – coordinadas dentro de la Empresa y de los Operadores IC (privados) con Municipio/Comarca/Región
- Falta de protocolos de actuación coordinados ante emergencias híbridas simultáneas (industrial y catástrofe natural, Ciberataque, pandemia, guerra…) (sí se dispone de Planes de Protección Civil y ejercicios /simulacros de forma independiente): apoyo con Sistemas avanzados basados en KET-IA
- Incorporar Tecnologías de uso Dual para el desarrollo de Sistemas avanzados
- En especial: foco en el FACTOR HUMANO (propio y el de la cadena de valor): Equipos críticos, formación/entrenamiento (Tecnologías, Cultura de Seguridad /Ciberseguridad, riesgos Psicosociales)
- Mejorar la coordinación entre los Operadores, especialmente las “Entidades Esenciales” (Colaboración público-privada + SI-KET-TD:
  - Interna en las Empresas: Dirección, RSC, Personas, SST-PRL, Sistemas, Seguridad, Gerencia de Riesgos, O&M, Logística,...
  - Cadenas de Valor (Operadores-Proveedores-Serv. Técnicos)
  - Gestión Municipal/CCAA (Servicios Esenciales a la Sociedad)
  - Seguridad Pública (Defensa en su caso) Emergencias/Protección Civil



PESI: modelo integrado de Gestión de Riesgos hacia la Continuidad de Negocio y Resiliencia (Infraestructuras –Movilidad 5.0)

Integración de Modelos y Técnicas de evaluación y gestión de Riesgos (incidentes, Crisis, Emergencias) y Continuidad de Negocio (O&M Infraestr.): Resiliencia

El **Negocio** es: producir energía, vehículos, agua, transportar viajeros y mercancías, mantener la infraestructura (carretera, túneles, puentes, luz, ITS…)

¿cómo integrar la gestión operativa (riesgos intrínsecos de la Infraestructura e ITS) en la Seguridad integral?

¿Y en las Cadenas de Valor industrial (proveedores, subcontratación, cadenas logísticas, etc.)?

AMPLIAR EL MODELO DE SEGURIDAD INTEGRAL A LA CADENA DE VALOR

Visión integral: Seguridad y Gobernanza de Riesgos para la Resiliencia

Industria, Redes e Infraestructuras 5.0 y Servicios Públicos

Estrategia de Resiliencia (Inteligencia, Seguridad y Gobernanza, GRC)

Gestión de Procesos y Activos 5.0: Fiabilidad y Seguridad - O&M (RAMS) (**Transporte y Mov.: ITS**)

SeguridadMedioambiental (+riesgos Cambio Climático)

Organiz. **Cadena de Valor** Proveedores y **Logística**

Gestión de Emergencias (Planes Autoprotección)

Personas y Cultura de Seguridad Industria 5.0

Gerencia de Riesgos y Organización de Seguridades (Continuidad de negocio) Seguros, cumplimiento Legal

Ciberseguridad (IT y OT)

Seguridad Física (Protección activos físicos y personas)

Factor Humano en Seguridad L. PREC (Personnel Security)

Seguridad y Salud Laboral PRL, Bienestar, Adicciones Movilidad-Seguridad Vial, Factor Generacional/Género

NIS2 Network & Information Systems Directive

Cyber Resilience Act

Gestión de Riesgos en Instalaciones: riesgos Climáticos y Tecnológicos

1. **Metodologías AR (Análisis y Evaluación de Riesgos)**
   1. Identificación de Amenazas y Riesgos (global de Instalaciones)
   2. Valoración de posible afección (elementos afectados/ grado)
   3. Efectos en cascada (dependencias internas y externas)
   4. **Integrar SST y herramientas Ciber (factor humano/ organizacional –seguridad integral-)**
2. **Sistemas de Detección y Alerta temprana**
   1. **Monitorización Instalaciones ("gemelo digital" y simulación)**
   2. Sistemas multi-canal de información (e Inteligencia de Seguridad)
3. **Medidas de Remediación**
   1. Evitar Riesgos (Seguridad desde el Diseño): físico y digital
   2. Plan: mejoras en Elementos (instalaciones) y Procesos (incrementar la Resiliencia) (mejoras físicas, Sec y Ciber)
   3. **Participación del Equipo Humano (Cultura Seguridad -SST,Sec, Cyber- mediante formación y comunicación)**
   4. Contratos de Seguros (+Ciberseguros)
4. **Colaboración Público-Privada en Crisis y Emergencias**
   1. Protocolos (interno) Gestión de Crisis: planes (Autoprotección, Ciber)
   2. Protocolos colaboración Equipos de Emergencias (Protec. Civil, INCIBE)
   3. Plan de Comunicación a la Sociedad

HERRAMIENTAS Y TECNOLOGÍAS

- **Riesgos** Climáticos: Análisis Riesgo/vectores frente (Instalaciones/Servº, Procesos, Materiales/peligross
- Plataformas (SW) **RA/RM** – Integración BIM
- **Modelo** Criticidad y Evaluación Dependencias: efectos cascada (plan de choque)
- **Personal** Crítico (role crisis y comunicación)
- Resto Personal (perfiles riesgo): PRL-Riesgo CC
- Sist.Gestión **Desastres** e info Emergencias (Gob.)
- Gemelos Digitales –elem.críticos (afección clim.)
- Integración SI planta/Infra: SCADA O&M-ITS- Sª de Seguridad-CRA/PCI-Seguridad(Security)-Cybersec.
- Industria 5.0 (SWE, IIoT, BigData, IA, RV/XR
- Assest Management (Mantenimiento)
- Facility Management 5.0 (energía, climatización, calidad ambiente, sist. seguridad, PCI, CCTV…)
- **Monitorización** elem./procesos críticos (**RAMS**)
- **Comité de Resiliencia** (DG, O&M, Personas, Logística, Seguridad, Emergencias, Rel. Inst.)
- Plan de **Continuidad de Negocio** (BCP)
- Dashboard Gestión Crisis (SW , comm. interna)
- Servicio de Prevención: Plan Prevención Riesgos climáticos/desastres naturales (accidente/cascada)
- Formación y Ejercicios (Emerg., Ciberataques)
- Pólizas de **Seguros** (acorde R. Climáticos/Cyber)
- Plan **Comunicación** (medios y Redes Sociales)

Intra/Inter-dependencias de Elementos/Sistemas Críticos

(elementos críticos: Ciberseguros # Directiva Ciber-Resiliencia: -> Certificación !!)

	INTER-DEPENDENCIES	Direct Impacts	Energy	Gas/oil	Water	Telecoms (voice, data &ISP)	Location & Environment	Transport Infrast. (road, train	Logistics (& purveyance)	Security, Civil Protection & Emergencies	Others
Categories	Critical Elements of the CI										
I	Control Rooms (Operation, Security, Integral)					5					
I	- Security Control Rooms					5					
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)										
III	Staff - Crisis Committee										
III	- essential teams (Op&Maint, Emerg, ITC)										
III	- other personnel & subcontractors										
IV	Critical Processes (industrial/essential service, restricted areas...; design, organization, tasks, safety systems)										
IV	Critical Process-2								4		
IV	Critical Process-n										
V	Security Equipment & Systems										
VI	Equipment & appliances (esential)										
VII	Infraestructure (buildings, installations)										
VIII	External Services &Supplies (Subcontr&Providers)										
IX	*Economic & Legal (Stability); Societal acceptance*										
X	Others (specific in the CI)										

Risk Analysis and BIA (Dependencies assesment)

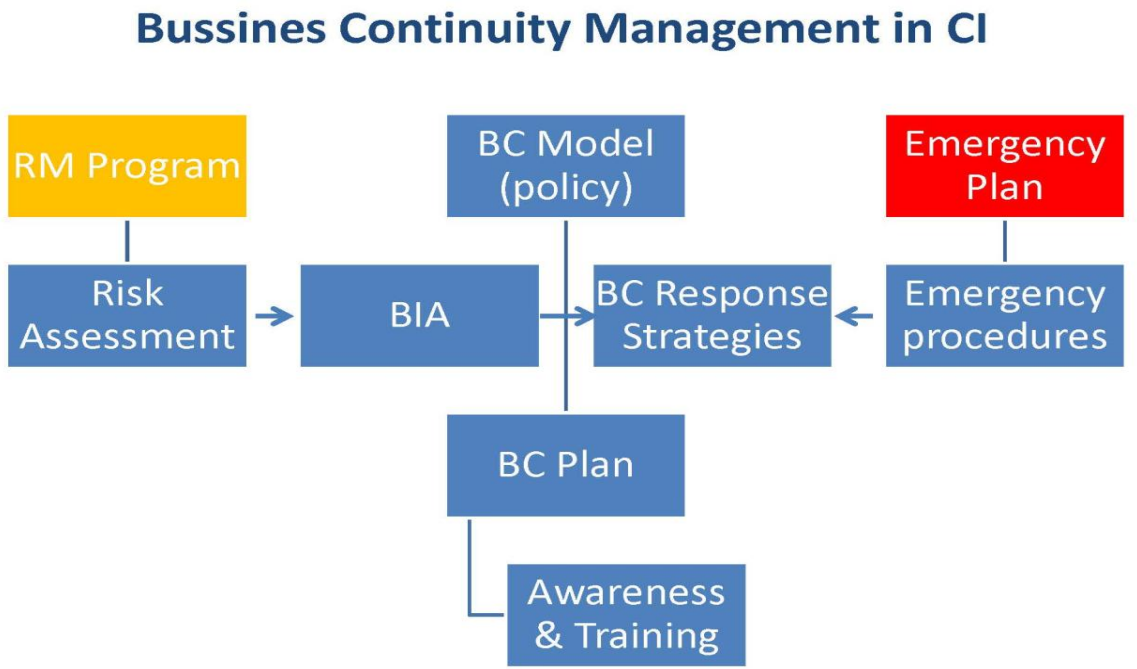
- **Risk and Dependencies Assesment:**
  - **Functions and Services** evaluation (***criticity*** *level*)
  - **Resources** (requirements):
    - Personnel
    - Equipment
    - Systems (SW, ITC, ITS...) and **Cybersecurity**
    - Utilities (Inter-dependencies)
    - Materials ...
- **Business Impact Analysis:**
  - Intra-dependencies
  - Inter-dependencies (external CIs)
  - Cascading effects (up-stream & down-stream)

PESI: marco sistémico para la Gestión de Riesgos, Continuidad del Negocio y Resiliencia

(Infrastructuras Críticas, servicios esenciales a la Sociedad)

Metodologías y herramientas PESI (modelo de criticidad y evaluación de dependencias Intra-Externa)

Categories	Critical Elements of the CI	INTRA-DEPENDENCIES: Direct Impacts	Control Rooms (Operation)	Security Control Rooms	Info Systems (OT/IT, ciber) &Comm	Staff - Mgnt Board & Crisis Committee	Essential Teams	other staff & ext personnel	Critical Proc-1	Critical Proc-2	Critical Proc-n	Security Equipment & Systems	(essential) Equipment & appliances	Infraestructures (buildings)	External Services &Supplies	Others
I	Control Rooms (Operation, Security, Integral)															
I	- Security Control Rooms															
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)															
III	Staff - Mgnt Board & Crisis Committee															
III	- essential Teams (Op&Maint, Emerg, ITC)															
III	- other personnel & subcontractors															
IV	Critical Processes (industrial/essential service, restricted areas...; safety systems)															
IV	Critical Process-2															
IV	Critical Process-n															
V	Security Equipment & Systems															
VI	Equipment & appliances (esential)															
VII	Infraestructure (buildings, installations)															
VIII	External Services &Supplies (Subcontr&Providers)															
IX-X	Others (economic, legal, Soc accept., specific)															



Directiva Europea de Resiliencia de Entidades Críticas (CER): Ley PREC

- La **Ley PREC** (**Protección y Resiliencia de Entidades Críticas –ECs-**), recientemente aprobada Consejo Ministros del 17-marzo-2026, corresponde a la trasposición en España de la **Directiva Europea de Resiliencia (CER)** de **2023**.
- La Ley busca fortalecer la seguridad de los **servicios esenciales (energía, transporte, sanidad, telecomunicaciones/digital, agua, etc.)** ante amenazas (ciberataques, desastres naturales, terrorismo… y efectos en cascada que afecten al funcionamiento), para que las "entidades designadas" implementen **planes de resiliencia**, notifiquen incidentes y aseguren su continuidad, vital para la sociedad.
- Las Entidades Críticas deberán ser definidas antes del 17 Julio de 2026. La Ley **PIC** (Protección de Infraestructuras Críticas), derogada por la nueva Ley **PREC**, en sus +15 años de aplicación ha permitido la elaboración del actual **Catálogo de ICs (ECs)**.
- Esta ley impone **obligaciones** como evaluaciones de riesgo, planes de contingencia, y controles de personal en puestos sensibles,
- La autoridad nacional responsable es la **Secretaría de Estado de Seguridad** a través del **CNPREC** Centro Nacional de Protección y Resiliencia de Entidades Críticas (actual **CNPIC**).

Marco de la Seguridad y Resiliencia Corporativa en Infraestructuras Críticas (España): Estrategias Nacionales de Seguridad, Ciberseguridad y nueva Ley PREC (antes PIC)

Actual Ley PIC (CNPIC/CNPREC, trasposición Dirª Resiliencia -> Ley PREC):

- Sectores Críticos: Infraestructuras y Servicios esenciales « Entidades Críticas »:
  - Operadores Privados (tipo industrial: Energía, Transporte, Agua, Telecom…)
  - Administración Pública (inc. Sanidad, Patrimonio…)
- Sectores: Estudios sectoriales (8 de 13 sectores con tipología industrial)
- PSO Plan de Seguridad del Operador -> **Infras. Transporte y Movilidad**
- PPE Plan de Protección Específico (instalación: Carretera/Vía F./túnel/puente…)
- Planes y Organización de la Seguridad Corporativa
  - Estrategia y Gestión de Riesgos integral (Safety-Security-Cyber)
  - Certificación de los Planes y sistemas (CNPIC)
- Ciberseguridad: ISO-2700x/ENS, ya NIS2 (y próxima Dirª E. Ciber-Resiliencia)

+ Nueva Ley de Seguridad Privada (gestionada: servicios de seguridad física y Ciberseguridad subcontratados: SOC…)

Directiva Europea de Resiliencia de Entidades Críticas (CER): Ley PREC (aprobada 17Mar2026)

Objetivos clave de la Ley PREC (Directiva Europea CER)

- **Reforzar la Resiliencia:** Mejorar la capacidad de prevenir, resistir, absorber y recuperarse de incidentes.
- **Garantizar servicios esenciales:** Asegurar la continuidad de funciones sociales y económicas vitales (**Inf. Transporte y Movilidad**)
- **Armonización europea:** Adaptar la legislación española a los estándares de la Directiva (UE) 2022/2557.

Obligaciones para las Entidades Críticas

- **Planes de Resiliencia:** Desarrollar medidas organizativas y técnicas contra riesgos.
- **Notificación de Incidentes:** Informar rápidamente sobre interrupciones significativas.
- **Evaluación de Riesgos:** Identificar amenazas propias y transversales.
- **Comprobación de Personal:** Revisar antecedentes de empleados en puestos clave.
- **Responsable de Seguridad y Resiliencia:** Designar un enlace con las autoridades.

Elementos diferenciadores con la Ley PIC

- **Modelo más avanzado e integral de la Seguridad:** Integración de las evaluaciones de riesgos aisladas (responsabilidades funcionales: O&M, Centros de Control e ITS, Medioambiente, PRL-RRHH, Safety, Emergencias, Security, Ciberseg.): **Modelo PESI**
- **Factor Humano** en la seguridad (personal crítico)
- **Cadena de Valor**: responsabilidad de la Entidad propietaria u operadora de la Infra/instalación crítica de asegurar la continuidad del “servicio” y Resiliencia de toda la Cadena de Valor (empresas subcontratadas, servicios esenciales externos, cadena de suministro y logística…)

26º CONGRESO ESPAÑOL ITS

INSTITUTO DE LA INGENIERIA DE ESPAÑA

INTELLIGENT TRANSPORT SYSTEM ITS ESPAÑA

¡MUCHAS GRACIAS!

J Javier LARRAÑETA
Secretario General
(Javier.larraneta@pesi-seguridadindustrial.org)

Actividad de la Plataforma financiada con ayuda de la AEI (Plataformas Tecnológicas PTR2024-002956

PESI
PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

GOBIERNO DE ESPAÑA | MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES | AGENCIA ESTATAL DE INVESTIGACIÓN

Madrid
24-26 marzo 2026