FUNDACIÓN PARA EL FOMENTO DE LA INNOVACIÓN INDUSTRIAL

# Taller práctico
# Análisis de riesgos y buenas prácticas de seguridad en la cadena de suministro

6 de Noviembre 2024

Tecnogetafe, Calle Erik Kandel 1, 28906 Getafe

Cuota de inscripción: 360 € + IVA

## Objetivos del Taller:

La duración completa de este curso tiene una estimación aproximada de 8 horas, durante las cuales se completarán los siguientes objetivos:

- Comprender el proceso y los puntos clave para realizar un análisis de riesgos, según la metodología TARA, tano a nivel de sistema de gestión como de componentes individuales para dar cumplimiento a los requisitos del reglamento R155 de UNECE.
- Desarrollar competencias en la evaluación y mitigación de riesgos de ciberseguridad en la cadena de suministro.
- Preparar a los participantes en la creación y el uso de herramientas documentales como matrices RASIC y acuerdos SLA.

## Detalle del programa:

### Bloque 1: Introducción a TARA y la normativa R155.

**Duración:** 1 hora.

**Contenido:**

- Contexto del reglamento R155 y su impacto en la industria.
- Principios básicos de la metodología TARA y su aplicación en el sistema de gestión y componentes del vehículo.
- Diferencias entre evaluación de riesgos a nivel sistema y de componente.

- Ejemplos de amenazas comunes en la cadena de suministro y su impacto en la seguridad: Gestión de amenazas y vulnerabilidades.

## Bloque 2: Metodología TARA según ISO/SAE 21434

**Duración:** 2 horas

**Contenido:**

- Revisión de los pasos de un TARA según la norma ISO/SAE 21434:
  1. Definición de ítems.
  2. Identificación de los activos.
  3. Identificación de escenarios de amenaza.
  4. Valoración del impacto y análisis de rutas de ataque.
  5. Calificación de viabilidad de los ataques y determinación del valor del riesgo.
  6. Decisiones de tratamiento.
- Ejercicio: Análisis completo de un componente de vehículo .

## Bloque 3: Seguridad en la cadena de suministro.

**Duración:** 1,5 horas

**Contenido:**

- Importancia de la gestión de riesgos en la cadena de suministro según los requisitos del reglamento R155.
- Proceso de evaluación y supervisión de proveedores conforme a ISO/SAE 21434:
  - Estrategias para identificar y mitigar riesgos asociados a los proveedores.
  - Introducción del uso de herramientas como la matriz RASIC o acuerdos SLA para garantizar la seguridad en la cadena de suministro.
  - Mecanismos de intercambio de información y validación de ciberseguridad (ISO 27001 y TISAX) y acuerdos de confidencialidad.
- Ejercicio: Redacción de los puntos clave de un procedimiento de proveedores.

## Bloque 4: Ejercicio combinado de SLA y Matriz RASIC.

**Duración:** 2 horas

**Contenido:**

- Parte 1: Definición de un SLA:
  Se identificarán y definirán los elementos clave de un SLA para un proveedor de servicios, incluyendo:
  - Indicadores de clave de rendimiento (KPIs): Tiempos de respuesta a incidentes, frecuencia de auditorías de seguridad y condiciones para la evaluación de vulnerabilidades.
  - Tiempos de respuesta: Especificar los tiempos de respuesta para incidentes de ciberseguridad (por ejemplo, incidentes críticos en 24 horas).
  - Mantenimiento de ciberseguridad: Definición de los requisitos de actualización y revisión periódica de controles de ciberseguridad.
- Parte 2: Creación de la matriz RASIC:
  Se identificarán y definirán los elementos clave de una matriz RASIC según ISO/SAE 21434:
  - R → Responsable (Responsible)
  - A → Autoridad (Accountable)
  - S → Apoyo (supporting)
  - I → Informado (Informed)
  - C → Consultado (Consulted)
  - Fase del vehículo.
  - Work Product afectado.
  - Documentación de referencia.
  - Nivel de confidencialidad de la documentación asociada.
- Ejercicio: Los participantes deberán elaborar un SLA y una matriz RASIC .