

**Propuesta de Máster de Formación
Permanente
Ciberseguridad Industrial aplicada a la
industria del automóvil**

Universidad Euneiz

ÍNDICE

1. Resumen	3
2. Denominación, número de créditos. Modalidad, año de implantación y número de plaza.....	4
2.1 Denominación.....	4
2.2 Año de implantación.....	5
2.3 Número de créditos y duración	5
2.4 Modalidad	5
2.5 Oferta de plazas	5
3. Dirección y Equipo docente	5
3.1 Dirección	5
3.2 Equipo docente	5
4. Justificación de la titulación y formación.	6
5. Objetivo formativo y resultados de aprendizaje a alcanzar, Habilidades y Evidencias	7
5.1 Objetivos formativos.....	7
5.2 Resultados de formación y aprendizaje a alcanzar: contenidos, competencias, habilidades o destrezas y evidencias	7
6. Destinatarios, Requisitos y Perfil de ingreso	8
6.1 Destinatarios	8
6.2 Requisitos y perfil de ingreso	8
7. Plan de estudios y extinción	8
7.1 Plan de estudios y contenidos (asignaturas y ECTS)	8
7.2 Distribución asignaturas por semestre u otra periodificación (cronograma)	9
7.3. Derecho a tutoría académica y examen en caso de extinción	9
8. Prácticas Externas	9
8.1 Detalle y desarrollo de las Prácticas Externas.	9
8.2 Entidades colaboradoras.	9
9. Recursos requeridos.....	10
9.1. Número de grupos, aulas y horario previsible	10

9.2. Infraestructuras.....	10
9.3. Material específico	10
9.3.1. Material existente o compartido	10
9.3.2. Material propio o exclusivo.....	10
10. Indicadores	10
10.1. Indicadores de seguimiento	10

1. Resumen

1.1. Denominación del título	Máster de Formación Permanente en Ciberseguridad Industrial aplicada a la industria del automóvil
1.2. Ámbito de conocimiento	Ingeniería informática y de sistemas
1.3. Facultad	Nuevas Tecnologías Interactivas

1.4. Responsable	Josué Sallent
1.5. Entidades participantes	Universidad Euneiz y BaM (Basque Automotive Manufacturing Center)
1.6. Modalidad de enseñanza	Presencial
1.7. Número total de ECTS	60
1.8. Idiomas de impartición	Castellano
1.9. Número total de plazas	25
1.10. Porcentaje profesorado Euneiz	25%
1.11 Duración y distribución temporal	De octubre de 2026 a septiembre de 2027 Jueves y viernes de 15:30 a 20:30

2. Denominación, número de créditos. Modalidad, año de implantación y número de plaza

2.1 Denominación

Máster de Formación Permanente en Ciberseguridad Industrial aplicada a la industria del automóvil.

Denominación comercial: Máster en Ciberseguridad Industrial aplicada a la industria del automóvil.

2.2 Año de implantación

El año de implantación es 2026.

2.3 Número de créditos y duración

60 ECTS distribuidos en un curso académico. 1500 horas de dedicación.

- 400 horas de docencia presencial, con enfoque aplicado y orientado a casos reales del sector.
- 600 horas de trabajo autónomo del estudiante, incluyendo estudio, resolución de casos y preparación de entregables.
- 250 horas de prácticas en empresa (módulo optativo/sustituible por ampliación del TFM).
- 250 horas de Trabajo Fin de Máster, ampliables a 500 horas en caso de no realizar las prácticas externas.

2.4 Modalidad

Presencial, con sesiones de 5 horas los jueves y viernes por la tarde.

2.5 Oferta de plazas

Plazas ofrecidas: 25

Número mínimo para impartición: 17 estudiantes

3. Dirección y Equipo docente

3.1 Dirección

- Director académico: Josuè Sallent.
- Codirector: Jorge Aranzabal (BaM).
- Coordinador: Lorenzo Fanari.

3.2 Equipo docente

Tabla I. Resumen de profesorado previsto (Volumen de profesorado % Euneiz)

Nombre o perfil del profesor/a	Nº de créditos asignados	Asignaturas
Dr. especializado en redes de telecomunicaciones (Euneiz)	55 horas	Módulos 1 y 2
Dr. en derecho digital (Euneiz)	45 horas	Módulos 1, 3, 4 y 5

Ingeniero industrial organización del sector automóvil	30 horas	Módulo 1
Ingeniero Especialista en ciberseguridad industrial	90 horas	Módulo 5
Ingeniero Especialista en ciberseguridad industrial	90 horas	Módulo 3
Ingeniero Especialista en ciberseguridad en plantas de automóvil	90 horas	Módulo 4

4. Justificación de la titulación y formación.

La impartición de un máster en ciberseguridad industrial orientado a la industria del automóvil en Euskadi responde a la necesidad de formar especialistas capaces de proteger entornos cada vez más conectados, automatizados y dependientes del software.

El sector de la automoción evoluciona hacia el vehículo conectado, eléctrico y autónomo, incorporando sistemas OT, IoT, comunicaciones vehículo-cloud, actualizaciones OTA y cadenas de suministro digitales. Esta transformación amplía la superficie de ataque y exige perfiles con conocimientos específicos en ciberseguridad industrial, automoción, normativa, gestión del riesgo y protección de sistemas críticos.

Euskadi cuenta con un ecosistema industrial y tecnológico altamente vinculado a la automoción, la fabricación avanzada, la máquina-herramienta, la robótica y los sistemas embebidos. Implantar este máster permitiría responder a la demanda de talento especializado de empresas tractoras, proveedores tecnológicos, centros de investigación y pymes industriales.

Además, reforzaría la competitividad del tejido productivo vasco, facilitaría la transferencia de conocimiento universidad-empresa y contribuiría a mejorar la resiliencia de infraestructuras, procesos y productos clave para la industria del automóvil.

Este máster presenta un carácter especialmente novedoso en el panorama español y europeo porque combina tres ámbitos que habitualmente se abordan por separado: **ciberseguridad industrial OT, vehículo conectado/electrificado y protección de la cadena de suministro de automoción.**

Aunque existen programas de ciberseguridad industrial y formaciones vinculadas a movilidad conectada, la orientación específica a la industria del automóvil, desde la fábrica digital hasta el vehículo y sus servicios cloud/OTA, responde a una necesidad emergente reconocida por organismos europeos como ENISA, que identifica riesgos específicos en smart cars, movilidad conectada y conducción autónoma.

Esta especialización convierte al máster en una propuesta diferencial, alineada con los retos actuales del sector y con una demanda todavía poco cubierta por la oferta formativa tradicional.

5. Objetivo formativo y resultados de aprendizaje a alcanzar, Habilidades y Evidencias

5.1 Objetivos formativos

El máster tiene como objetivo formar profesionales capaces de analizar, diseñar e implantar medidas de ciberseguridad en entornos industriales y, de forma específica, en la industria del automóvil.

La propuesta integra una visión técnica, de gestión y legal para responder a los riesgos derivados del vehículo conectado, los sistemas OT, la robótica industrial y la cadena de suministro automotriz.

El programa combina fundamentos, prácticas de laboratorio, análisis de incidentes reales, simulaciones y trabajo aplicado orientado a la empleabilidad.

5.2 Resultados de formación y aprendizaje a alcanzar: contenidos, competencias, habilidades o destrezas y evidencias

Los resultados de aprendizaje se articulan de forma progresiva desde los fundamentos hasta la aplicación avanzada en automoción, OT y supply chain, y se resumen en la siguiente tabla:

Tabla II. Resultados de formación y aprendizaje (RFA) por tipología

Código y tipología	Resultado de formación y aprendizaje	Módulos principales
RFA-C1 Contenidos / conocimientos	Comprender los fundamentos de la ciberseguridad y su aplicación a sistemas críticos	M1
RFA-C2 Contenidos / conocimientos	Interpretar el vehículo como sistema ciberfísico complejo	M1, M3
RFA-COMP1 Competencias	Evaluar la ciberseguridad del vehículo conectado	M3
RFA-COMP2 Competencias	Diseñar soluciones de desarrollo seguro y monitorización	M3
RFA-COMP3 Competencias	Aplicar marcos de gestión del riesgo y segmentación OT	M4
RFA-COMP4 Competencias	Gestionar la ciberseguridad en la cadena de suministro	M5
RFA-COMP45 Competencias	Desarrollar un proyecto aplicado en contexto profesional	M6, M7
RFA-HD1 Habilidades o destrezas	Analizar redes y protocolos de comunicación	M2

RFA-HD2 Habilidades o destrezas	Aplicar medidas de seguridad en Edge, Cloud y OTA	M3
RFA-HD3 Habilidades o destrezas	Evalúa vulnerabilidades en PLC, SCADA, redes OT y células robotizadas con impacto operativo y físico.	M4
RFA-HD4 Habilidades o destrezas	Analizar riesgos en sistemas OT y robótica industrial	M4

6. Destinatarios, Requisitos y Perfil de ingreso

6.1 Destinatarios

El programa está dirigido a titulados y tituladas universitarios/as del ámbito de la ingeniería y las tecnologías aplicadas al sector del automóvil.

6.2 Requisitos y perfil de ingreso

Pueden acceder al Máster de formación permanente en Ciberseguridad Industrial aplicada a la industria del automóvil, todas aquellas personas con titulación universitaria en ingeniería de telecomunicación, informática, electrónica o ingeniería industrial vinculada al sector del automóvil.

Adicionalmente, se ofrece a todas aquellas personas que aún sin titulación universitaria, estén interesados/as en dicho ámbito, y a las cuales, se les expedirá un certificado tras su finalización.

Excepcionalmente, los módulos 3 y 4 podrán cursarse de forma independiente, tanto las personas con titulación universitaria, que en el caso de que superen dichos módulos obtendrán un Diploma de Experto, como las personas sin titulación universitaria que, en el caso de que superen dichos módulos, obtendrán un certificado con la denominación concreta del programa cursado.

7. Plan de estudios y extinción

7.1 Plan de estudios y contenidos (asignaturas y ECTS)

El plan de estudios se estructura en siete módulos:

- Módulo 1. Fundamentos de la ciberseguridad industrial y automoción (4 ECTS).
- Módulo 2. Seguridad en redes y protocolos de comunicación (4 ECTS).
- Módulo 3. Ciberseguridad en vehículos conectados (15 ECTS).
- Módulo 4. Seguridad en sistemas de producción y robots industriales (12 ECTS).
- Módulo 5. Seguridad en la cadena de suministro (5 ECTS).
- Módulo 6. Prácticas en empresa (10 ECTS).

- Módulo 7. Proyecto Final de Máster (10 ECTS). El módulo de prácticas podrá sustituirse por una ampliación del TFM hasta 20 ECTS cuando no se realicen prácticas externas.

7.2 Distribución asignaturas por semestre u otra periodificación (cronograma)

Distribución propuesta:

- Primer periodo (octubre 2026 – febrero 2027): Módulos 1 y 2, e inicio del Módulo 3.
- Segundo periodo (febrero 2027 – junio 2027): finalización del Módulo 3, desarrollo completo de los Módulos 4 y 5.
- Tercer periodo (junio 2027 – septiembre 2027): realización de prácticas externas y/o desarrollo del Proyecto Final de Máster, con seguimiento tutorial individualizado.

7.3. Derecho a tutoría académica y examen en caso de extinción

En caso de extinción del programa, el estudiantado mantendrá el derecho a tutoría académica, evaluación y convocatoria extraordinaria en los términos establecidos por la normativa de enseñanzas propias de la universidad, garantizando un periodo razonable para la superación de las asignaturas pendientes y la defensa del TFM.

8. Prácticas Externas

8.1 Detalle y desarrollo de las Prácticas Externas.

Se contempla la posibilidad de realizar 250 horas de prácticas externas en empresas del sector del automóvil o bien en empresas del ámbito de la ciberseguridad que presten servicios en la industria del automóvil de modo que los estudiantes puedan poner en práctica los conceptos, competencias y habilidades aprendidas en el máster.

Los alumnos que no realicen las prácticas deberán destinar las 250 horas al proyecto fin de máster

8.2 Entidades colaboradoras.

Se prevé la realización de prácticas en las siguientes empresas:

- JakinCode.
- Mercedes Benz.
- BaM.

9. Recursos requeridos

9.1. Número de grupos, aulas y horario previsible

Se prevé la impartición de un único grupo de hasta 25 estudiantes. La docencia se desarrollará en horario de tarde, los jueves y viernes de 15:30 a 20:30, en aulas docentes y espacios de laboratorio adecuados para actividades teóricas y prácticas.

9.2. Infraestructuras

El programa requerirá aulas equipadas con medios audiovisuales, conectividad, y acceso a entornos de laboratorio, no se requiere aula informatizada.

Asimismo, se contemplará el uso de espacios vinculados a simulación, análisis de redes y prácticas sobre escenarios industriales y de automoción.

9.3. Material específico

Para la realización de tareas prácticas se contempla el uso de:

- Laboratorio de ciberseguridad de Euneiz con los equipos y materiales de redes de telecomunicaciones, IoT y ciberseguridad industrial.
- Plataforma TryhackMe: se prevé el uso de esta plataforma de pago de Capture the Flag por parte de todos los alumnos para poder resolver casos prácticos de los distintos módulos del máster.

9.3.1. Material existente o compartido

Aulas docentes, equipos informáticos, proyectores, red de comunicaciones, software de productividad, herramientas de virtualización y plataformas generales de laboratorio disponibles en Euneiz y/o entidades colaboradoras.

9.3.2. Material propio o exclusivo

Entornos específicos para prácticas de ciberseguridad en automoción y OT, laboratorios de análisis de comunicaciones, recursos para simulación de incidentes, materiales de casos prácticos y acceso a conocimiento sectorial aportado por profesionales y entidades colaboradoras.

10. Indicadores

10.1. Indicadores de seguimiento

Los indicadores recogidos a continuación permitirán realizar el seguimiento académico, de demanda, rendimiento y satisfacción del título, así como valorar su sostenibilidad y mejora continua.

Tabla III. Indicadores de seguimiento

Indicador	Objetivo	Valor o parámetro aceptable
Nº de plazas ofertadas.	Ajustar la oferta al mercado y asegurar grupos viables y sostenibles.	25
Nº de solicitudes recibidas.	Garantizar una demanda que justifique la continuidad del máster.	30
Ratio solicitudes/plaza.	Mantener una demanda adecuada de solicitudes por plaza para asegurar competitividad.	1,2
Nº total de estudiantes matriculados/as.	Alcanzar o superar el mínimo necesario para la viabilidad económica y académica.	-
Tasa de matriculación (matriculas/admitidos/as).	Lograr que al menos un buen porcentaje de admitidos formalicen matrícula.	75%
Tasa de ocupación (matricula/plazas).	Alcanzar una ocupación alta de las plazas disponibles.	90%
Nº de créditos ofertados.	Garantizar que la oferta académica cumple los requisitos del plan de estudios.	60
Tasa de créditos matriculados (nº de créditos matriculados / nº de créditos ofertados).	Mantener una matriculación alta de los créditos ofertados.	90%
Tasa de créditos superados (nº de créditos superados / nº de créditos matriculados).	Lograr que los/as estudiantes superen un % alto de los créditos matriculados.	≥ 90%
Perfil del alumno/a (edad, perfil profesional, género...).	Conocer y conseguir un grupo adecuado de enfoque profesional del máster.	-
Tasa de rendimiento.	Mantener valores	≥ 80–90%
Tasa de éxito.	Alcanzar tasas de éxito	≥ 90–95%
Tasa de abandono.	Mantenerla igual o por debajo del 5%	≤ 5%
Nota media global del máster.	Garantizar un nivel formativo alto.	media entre 7 y 8,5
Satisfacción del alumnado con la docencia.	Obtener valoraciones.	Escala 1-5 (3,5-5)
Satisfacción del profesorado.	Obtener valoraciones.	Escala 1-5 (3,5-5)
% de estudiantes trabajadores a tiempo completo		-