

Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Aval/Membresía



tech
universidad



Grand Master Oficial
Universitario
MBA en Dirección
de Ciberseguridad
(CISO, Chief Information
Security Officer)

Idioma: **Español**

Modalidad: **100% online**

Duración: **2 años**

Créditos: **120 ECTS**

Acceso web: www.techtute.com/informatica/grand-master-oficial-universitario/grand-master-oficial-universitario-mba-direccion-ciberseguridad-ciso-chief-information-security-officer

Índice

01

Presentación del programa

pág. 4

02

¿Por qué estudiar en TECH?

pág. 8

03

Plan de estudios

pág. 12

04

Convalidación
de asignaturas

pág. 34

05

Objetivos docentes

pág. 40

06

Salidas profesionales

pág. 44

07

Idiomas gratuitos

pág. 48

08

Metodología de estudio

pág. 52

09

Cuadro docente

pág. 64

10

Triple titulación

pág. 84

11

Homologación del título

pág. 88

12

Requisitos de acceso

pág. 92

13

Proceso de admisión

pág. 96

01

Presentación del programa

La ciberdelincuencia genera pérdidas globales que superan los 8 billones de dólares anuales, una cifra comparable al PIB de Japón, en un contexto marcado por más de 3,5 millones de vacantes de profesionales en el sector. Además, el 81% de los CISO declara operar con presupuestos insuficientes frente a una superficie de ataque en constante expansión (Forrester). Esta convergencia de amenazas crecientes, escasez de talento y restricciones financieras redefine el rol del Chief Information Security Officer como un actor estratégico clave, responsable de diseñar resiliencia mediante la integración de gobernanza, inteligencia tecnológica y alineación con los objetivos corporativos. En este escenario, TECH ofrece un programa universitario 100% online, flexible y orientado a facilitar la conciliación profesional y personal.

Este es el momento, te estábamos esperando

“

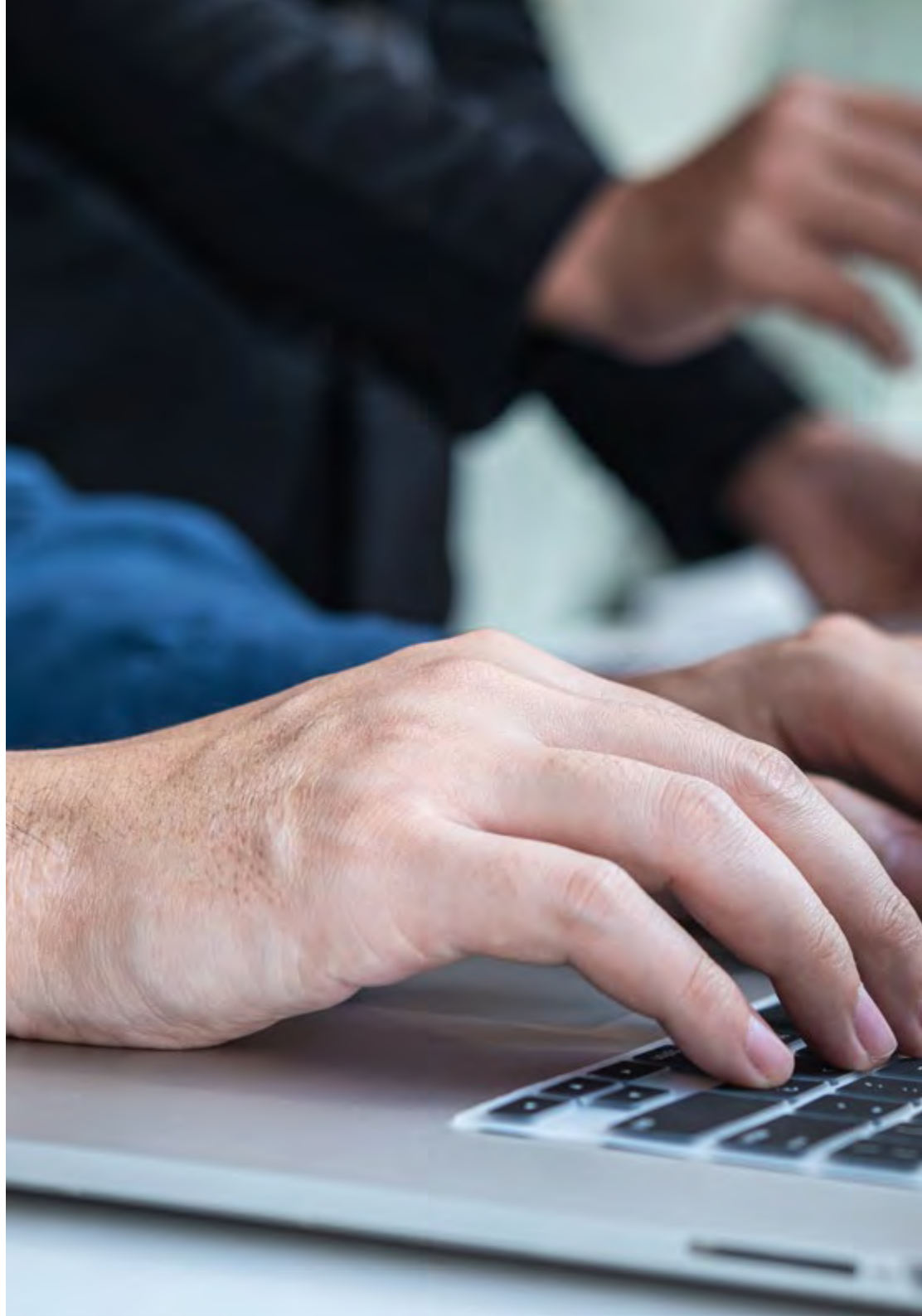
*Un programa exhaustivo y 100% online,
exclusivo de TECH y con una perspectiva
internacional respaldada por nuestra afiliación
con Business Graduates Association”*

La transformación digital ha consolidado la ciberseguridad como un pilar esencial no solo para la gestión tecnológica, sino para la continuidad operativa y la resiliencia estratégica de toda organización. Ante esta creciente dependencia de infraestructuras digitales, se requiere un liderazgo que domine tanto la complejidad técnica como la dimensión ejecutiva del riesgo. Para responder a esta necesidad, TECH presenta el Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer), diseñado para desarrollar profesionales con visión integral, preparados para dirigir la seguridad desde una perspectiva holística que integra gestión, tecnología y organización.

Esta visión se traduce en un plan de estudios estructurado que combina, en primer lugar, competencias directivas fundamentales como liderazgo, estrategia corporativa y gobierno con, en segundo lugar, conocimientos técnicos avanzados en ciberinteligencia, seguridad ofensiva y defensiva, e inteligencia artificial aplicada a la seguridad. Por consiguiente, el programa prepara al profesional para cerrar la brecha entre la alta dirección y las operaciones técnicas, diseñando estrategias de ciberseguridad alineadas con los objetivos de negocio.

Con el objetivo de adaptarse a las demandas del profesional en activo, este programa se imparte bajo una metodología 100% online y flexible. Gracias a un enfoque práctico basado en casos reales y recursos digitales avanzados, los participantes pueden integrar el aprendizaje en su rutina profesional, avanzando en su desarrollo directivo sin interrumpir sus responsabilidades laborales y personales, y preparándose así para asumir roles de máxima responsabilidad en un ámbito estratégico.

Asimismo, gracias a que TECH es miembro de **Business Graduates Association (BGA)**, el alumno podrá acceder a recursos exclusivos y actualizados que fortalecerán su formación continua y su desarrollo profesional, así como descuentos en eventos profesionales que facilitarán el contacto con expertos del sector. Además, podrá ampliar su red profesional, conectando con especialistas de distintas regiones, favoreciendo el intercambio de conocimientos y nuevas oportunidades laborales.





“

Tu desarrollo profesional cuenta con una metodología innovadora y Directores Invitados internacionales, una fórmula diseñada para liderar con éxito en cualquier sector”

02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Te damos +

“

*Estudia en la mayor universidad digital
del mundo y asegura tu éxito profesional.
El futuro empieza en TECH”*

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

Forbes
Mejor universidad
online del mundo

Plan
de estudios
más completo

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistuba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

Profesorado
TOP
Internacional



La metodología
más eficaz

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en once idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

nº1
Mundial
Mayor universidad
online del mundo

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.



Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.



La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.



03

Plan de estudios

El plan de estudios propone un recorrido progresivo y coherente que integra visión estratégica y especialización técnica. En primer lugar, desarrolla capacidades directivas para comprender cómo la Ciberseguridad influye en la organización y en la toma de decisiones. A continuación, profundiza en el análisis de amenazas, vulnerabilidades y mecanismos de defensa en entornos corporativos y digitales. Además, incorpora la Inteligencia Artificial generativa para reforzar la prevención y la gestión de incidentes. Finalmente, el Trabajo Final de Máster consolida este enfoque orientado a la ciberresiliencia.

*Un temario
completo y bien
desarrollado*



“

El temario de esta titulación académica te posicionará a la vanguardia de la dirección empresarial y de la ciberseguridad”

El Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) de TECH se distingue como un programa intensivo que prepara a los alumnos para afrontar retos y decisiones empresariales tanto a nivel nacional como internacional. Su contenido está pensado para favorecer el desarrollo de competencias directivas que permitan la toma de decisiones con un mayor rigor en entornos inciertos.

A lo largo de 2 años de estudio, el alumno analizará multitud de casos prácticos mediante el trabajo individual, logrando un aprendizaje de gran calidad que podrá aplicar, posteriormente, a su práctica diaria. Se trata, por tanto, de una auténtica inmersión en situaciones reales de negocio.

Este programa aborda los principales desafíos del mercado, ya que integra gestión, tecnología y anticipación del riesgo digital. Así, cubre desde la alineación de la ciberseguridad con los objetivos de negocio hasta la protección de infraestructuras críticas y la respuesta ante incidentes complejos. Además, permite desarrollar profesionales con visión estratégica, liderazgo y capacidad para tomar decisiones en entornos de alto riesgo.

Desarrolla competencias estratégicas y técnicas para liderar la ciberseguridad corporativa, aplicando metodologías avanzadas y herramientas innovadoras como análisis de amenazas asistido por IA, recursos multimedia interactivos: todo con la flexibilidad y excelencia que ofrece TECH.

Asignatura 1	Liderazgo, Ética y Responsabilidad Social
Asignatura 2	Dirección Estratégica y <i>Management</i> Directivo
Asignatura 3	Dirección de Personas y Gestión del Talento
Asignatura 4	Dirección Económico - Financiera
Asignatura 5	Dirección de Operaciones y Logística
Asignatura 6	Dirección de Sistemas de Información
Asignatura 7	Dirección Comercial, Marketing Estratégico y Comunicación Corporativa
Asignatura 8	Innovación y Dirección de Proyectos
Asignatura 9	<i>Management</i> Directivo
Asignatura 10	Trabajo Final de Máster (TFM)
Asignatura 11	Ciberinteligencia y Ciberseguridad
Asignatura 12	Seguridad en <i>Host</i>
Asignatura 13	Seguridad en Red (Perimetral)
Asignatura 14	Seguridad en <i>Smartphones</i>

Asignatura 15	Seguridad en IoT
Asignatura 16	Hacking Ético
Asignatura 17	Ingeniería Inversa
Asignatura 18	Desarrollo Seguro
Asignatura 19	Análisis Forense
Asignatura 20	Retos Actuales y Futuros en Seguridad Informática
Asignatura 21	Ciberseguridad y Análisis de Amenazas Modernas con ChatGPT
Asignatura 22	Detección y Prevención de Intrusiones Usando Modelos de Inteligencia Artificial Generativa
Asignatura 23	Criptografía Moderna con Asistencia de ChatGPT en la Protección de Datos
Asignatura 24	Análisis forense digital y respuesta a incidentes asistida por Inteligencia Artificial
Asignatura 25	Modelos Predictivos de Defensa Proactiva en Ciberseguridad usando ChatGPT

Trabajo Final de Máster

El Trabajo Final del Máster (TFM) tendrá un enfoque teórico y/o práctico y su finalidad primordial será acreditar los conocimientos adquiridos a través de este programa universitario. Este ejercicio deberá estar orientado a propuestas innovadoras vinculadas a cuestiones de actualidad y relacionados a los contenidos abordados en la titulación. Además, todos los TFM serán realizados bajo la supervisión de un tutor académico, encargado de asesorar y planificar las diferentes etapas de desarrollo de este proyecto investigativo.

El TFM está dispuesto a mitad del plan de estudios para poder iniciar su desarrollo mientras se llevan a cabo el resto de las asignaturas específicas, permitiendo al estudiante compatibilizar ambas tareas y lograr finalizar el programa en el plazo de 2 años.



Ampliarás tus habilidades metodológicas e investigativas a través del desarrollo de un Trabajo Final de Máster”

Asignatura 1

Liderazgo, Ética y Responsabilidad Social

1.1. Globalización y Gobernanza

- 1.1.1. Gobernanza y Gobierno Corporativo
- 1.1.2. Fundamentos del Gobierno Corporativo en las empresas
- 1.1.3. El Rol del Consejo de Administración en el marco del Gobierno Corporativo

1.2. Liderazgo

- 1.2.1. Liderazgo: una aproximación conceptual
- 1.2.2. Liderazgo en las empresas
- 1.2.3. La importancia del líder en la dirección de empresas

1.3. Cross Cultural Management

- 1.3.1. Concepto de *Cross Cultural Management*
- 1.3.2. Aportaciones al Conocimiento de Culturas Nacionales
- 1.3.3. Gestión de la Diversidad

1.4. Desarrollo directivo y liderazgo

- 1.4.1. Concepto de desarrollo directivo
- 1.4.2. Concepto de liderazgo
- 1.4.3. Teorías del liderazgo
- 1.4.4. Estilos de liderazgo
- 1.4.5. La inteligencia en el liderazgo
- 1.4.6. Los desafíos del líder en la actualidad

1.5. Ética empresarial

- 1.5.1. Ética y Moral
- 1.5.2. Ética Empresarial
- 1.5.3. Liderazgo y ética en las empresas

1.6. Sostenibilidad

- 1.6.1. Sostenibilidad y desarrollo sostenible
- 1.6.2. Agenda 2030
- 1.6.3. Las empresas sostenibles

1.7. Responsabilidad Social de la Empresa

- 1.7.1. Dimensión internacional de la Responsabilidad Social de las Empresas
- 1.7.2. Implementación de la Responsabilidad Social de la Empresa
- 1.7.3. Impacto y medición de la Responsabilidad Social de la Empresa

1.8. Sistemas y herramientas de Gestión responsable

- 1.8.1. RSC: la responsabilidad social corporativa
- 1.8.2. Aspectos esenciales para implantar una estrategia de gestión responsable
- 1.8.3. Pasos para la implantación de un sistema de gestión de responsabilidad social corporativa
- 1.8.4. Herramientas y estándares de la RSC

1.9. Multinacionales y derechos humanos

- 1.9.1. Globalización, empresas multinacionales y derechos humanos
- 1.9.2. Empresas multinacionales frente al derecho internacional
- 1.9.3. Instrumentos jurídicos para multinacionales en materia de derechos humanos

1.10. Entorno legal y Corporate Governance

- 1.10.1. Normas internacionales de importación y exportación
- 1.10.2. Propiedad intelectual e industrial
- 1.10.3. Derecho Internacional del Trabajo

Asignatura 2

Dirección Estratégica y Management Directivo

2.1. Análisis y diseño organizacional

- 2.1.1. Marco Conceptual
- 2.1.2. Factores clave en el diseño organizacional
- 2.1.3. Modelos básicos de organizaciones
- 2.1.4. Diseño organizacional: tipologías

2.2. Estrategia Corporativa

- 2.2.1. Estrategia corporativa competitiva
- 2.2.2. Estrategias de Crecimiento: tipologías
- 2.2.3. Marco conceptual

2.3. Planificación y Formulación Estratégica

- 2.3.1. Marco Conceptual
- 2.3.2. Elementos de la Planificación Estratégica
- 2.3.3. Formulación Estratégica: proceso de la Planificación Estratégica

2.4. Pensamiento estratégico

- 2.4.1. La empresa como un sistema
- 2.4.2. Concepto de organización

2.5. Diagnóstico Financiero

- 2.5.1. Concepto de Diagnóstico Financiero
- 2.5.2. Etapas del Diagnóstico Financiero
- 2.5.3. Métodos de Evaluación para el Diagnóstico Financiero

2.6. Planificación y Estrategia

- 2.6.1. El Plan de una Estrategia
- 2.6.2. Posicionamiento Estratégico
- 2.6.3. La Estrategia en la Empresa

2.7. Modelos y Patrones Estratégicos

- 2.7.1. Marco Conceptual
- 2.7.2. Modelos Estratégicos
- 2.7.3. Patrones Estratégicos: Las Cinco P's de la Estrategia

2.8. Estrategia Competitiva

- 2.8.1. La Ventaja Competitiva
- 2.8.2. Elección de una Estrategia Competitiva
- 2.8.3. Estrategias según el Modelo del Reloj Estratégico
- 2.8.4. Tipos de Estrategias según el ciclo de vida del sector industrial

2.9. Dirección Estratégica

- 2.9.1. El concepto de Estrategia
- 2.9.2. El proceso de dirección estratégica
- 2.9.3. Enfoques de la dirección estratégica

2.10. Implementación de la Estrategia

- 2.10.1. Sistemas de Indicadores y Enfoque por Procesos
- 2.10.2. Mapa Estratégico
- 2.10.3. Alineamiento Estratégico

2.11. Management Directivo

- 2.11.1. Marco conceptual del *Management Directivo*
- 2.11.2. *Management Directivo*. El Rol del Consejo de Administración y herramientas de gestión corporativas

2.12. Comunicación Estratégica

- 2.12.1. Comunicación interpersonal
- 2.12.2. Habilidades comunicativas e influencia
- 2.12.3. La comunicación interna
- 2.12.4. Barreras para la comunicación empresarial

Asignatura 3**Dirección de Personas y Gestión del Talento****3.1. Comportamiento Organizacional**

- 3.1.1. Comportamiento Organizacional. Marco Conceptual
- 3.1.2. Principales factores del comportamiento organizacional

3.2. Las personas en las organizaciones

- 3.2.1. Calidad de vida laboral y bienestar psicológico
- 3.2.2. Equipos de trabajo y la dirección de reuniones
- 3.2.3. *Coaching* y gestión de equipos
- 3.2.4. Gestión de la igualdad y diversidad

3.3. Dirección Estratégica de personas

- 3.3.1. Dirección Estratégica y recursos humanos
- 3.3.2. Dirección estratégica de personas

3.4. Evolución de los Recursos. Una visión integrada

- 3.4.1. La importancia de RR. HH
- 3.4.2. Un nuevo entorno para la gestión y dirección de personas
- 3.4.3. Dirección estratégica de RR. HH

3.5. Selección, dinámicas de grupo y reclutamiento de RR. HH

- 3.5.1. Aproximación al reclutamiento y la selección
- 3.5.2. El reclutamiento
- 3.5.3. El proceso de selección

3.6. Gestión de recursos humanos por competencias

- 3.6.1. Análisis del potencial
- 3.6.2. Política de retribución
- 3.6.3. Planes de carrera / sucesión

3.7. Evaluación del rendimiento y gestión del desempeño

- 3.7.1. La gestión del rendimiento
- 3.7.2. Gestión del desempeño: objetivos y proceso

3.8. Gestión de la formación

- 3.8.1. Las teorías del aprendizaje
- 3.8.2. Detección y retención del talento
- 3.8.3. Gamificación y la gestión del talento
- 3.8.4. La formación y la obsolescencia profesional

3.9. Gestión del talento

- 3.9.1. Claves para la gestión positiva
- 3.9.2. Origen conceptual del talento y su implicación en la empresa
- 3.9.3. Mapa del talento en la organización
- 3.9.4. Coste y valor añadido

3.10. Innovación en gestión del talento y las personas

- 3.10.1. Modelos de gestión del talento estratégico
- 3.10.2. Identificación, formación y desarrollo del talento
- 3.10.3. Fidelización y retención
- 3.10.4. Proactividad e innovación

3.11. Motivación

- 3.11.1. La naturaleza de la motivación
- 3.11.2. La teoría de las expectativas
- 3.11.3. Teorías de las necesidades
- 3.11.4. Motivación y compensación económica

3.12. Employer Branding

- 3.12.1. *Employer branding* en RR. HH
- 3.12.2. Personal Branding para profesionales de RR. HH

3.13. Desarrollo de equipos de alto desempeño

- 3.13.1. Los equipos de alto desempeño: los equipos autogestionados
- 3.13.2. Metodologías de gestión de equipos autogestionados de alto desempeño

3.14. Desarrollo competencial directivo

- 3.14.1. ¿Qué son las competencias directivas?
- 3.14.2. Elementos de las competencias
- 3.14.3. Conocimiento
- 3.14.4. Habilidades de dirección
- 3.14.5. Actitudes y valores en los directivos
- 3.14.6. Habilidades directivas

3.15. Gestión del tiempo

- 3.15.1. Beneficios
- 3.15.2. ¿Cuáles pueden ser las causas de una mala gestión del tiempo?
- 3.15.3. Tiempo
- 3.15.4. Las ilusiones del tiempo
- 3.15.5. Atención y memoria
- 3.15.6. Estado mental
- 3.15.7. Gestión del tiempo
- 3.15.8. Proactividad
- 3.15.9. Tener claro el objetivo
- 3.15.10. Orden
- 3.15.11. Planificación

3.16. Gestión del cambio

- 3.16.1. Gestión del cambio
- 3.16.2. Tipo de procesos de gestión del cambio
- 3.16.3. Etapas o fases en la gestión del cambio

3.17. Negociación y gestión de conflictos

- 3.17.1. Negociación
- 3.17.2. Gestión de Conflictos
- 3.17.3. Gestión de Crisis

3.18. Comunicación directiva

- 3.18.1. Comunicación interna y externa en el ámbito empresarial
- 3.18.2. Departamentos de Comunicación
- 3.18.3. El responsable de comunicación de la empresa. El perfil del Dircom

3.19. Gestión de Recursos humanos y equipos PRL

- 3.19.1. Gestión de recursos humanos y equipos
- 3.19.2. Prevención de riesgos laborales

3.20. Productividad, atracción, retención y activación del talento

- 3.20.1. La productividad
- 3.20.2. Palancas de atracción y retención de talento

3.21. Compensación monetaria vs. No monetaria

- 3.21.1. Compensación monetaria vs. no monetaria
- 3.21.2. Modelos de bandas salariales
- 3.21.3. Modelos de compensación no monetaria
- 3.21.4. Modelo de trabajo
- 3.21.5. Comunidad corporativa
- 3.21.6. Imagen de la empresa
- 3.21.7. Salario emocional

3.22. Innovación en gestión del talento y las personas

- 3.22.1. Innovación en las Organizaciones
- 3.22.2. Nuevos retos del departamento de Recursos humanos
- 3.22.3. Gestión de la Innovación
- 3.22.4. Herramientas para la Innovación

3.23. Gestión del conocimiento y del talento

- 3.23.1. Gestión del conocimiento y del talento
- 3.23.2. Implementación de la gestión del conocimiento

3.24. Transformación de los recursos humanos en la era digital

- 3.24.1. El contexto socioeconómico
- 3.24.2. Nuevas formas de organización empresarial
- 3.24.3. Nuevas metodologías

Asignatura 4

Dirección Económico - Financiera

4.1. Entorno Económico

- 4.1.1. Entorno macroeconómico y el sistema financiero nacional
- 4.1.2. Instituciones financieras
- 4.1.3. Mercados financieros
- 4.1.4. Activos financieros
- 4.1.5. Otros entes del sector financiero

4.2. La financiación de la empresa

- 4.2.1. Fuentes de financiación
- 4.2.2. Tipos de costes de financiación

4.3. Contabilidad Directiva

- 4.3.1. Conceptos básicos
- 4.3.2. El Activo de la empresa
- 4.3.3. El Pasivo de la empresa
- 4.3.4. El Patrimonio Neto de la empresa
- 4.3.5. La Cuenta de Resultados

4.4. De la contabilidad general a la contabilidad de costes

- 4.4.1. Elementos del cálculo de costes
- 4.4.2. El gasto en contabilidad general y en contabilidad de costes
- 4.4.3. Clasificación de los costes

4.5. Sistemas de información y Business Intelligence

- 4.5.1. Fundamentos y clasificación
- 4.5.2. Fases y métodos de reparto de costes
- 4.5.3. Elección de centro de costes y efecto

4.6. Presupuesto y Control de Gestión

- 4.6.1. El modelo presupuestario
- 4.6.2. El Presupuesto de Capital
- 4.6.3. El Presupuesto de Explotación
- 4.6.4. El Presupuesto de Tesorería
- 4.6.5. Seguimiento del Presupuesto

4.7. Gestión de tesorería

- 4.7.1. Fondo de Maniobra Contable y Fondo de Maniobra Necesario
- 4.7.2. Cálculo de Necesidades Operativas de Fondos
- 4.7.3. *Credit management*

4.8. Responsabilidad fiscal de las empresas

- 4.8.1. Conceptos tributarios básicos
- 4.8.2. El impuesto de sociedades
- 4.8.3. El impuesto sobre el valor añadido
- 4.8.4. Otros impuestos relacionados con la actividad mercantil
- 4.8.5. La empresa como facilitador de la labor del Estado

4.9. Sistemas de control de las empresas

- 4.9.1. Análisis de los estados financieros
- 4.9.2. El Balance de la empresa
- 4.9.3. La Cuenta de Pérdidas y Ganancias
- 4.9.4. El Estado de Flujos de Efectivo
- 4.9.5. Análisis de Ratios

4.10. Dirección Financiera

- 4.10.1. Las decisiones financieras de la empresa
- 4.10.2. El departamento financiero
- 4.10.3. Excedentes de tesorería
- 4.10.4. Riesgos asociados a la dirección financiera
- 4.10.5. Gestión de riesgos de la dirección financiera



4.11. Planificación Financiera

- 4.11.1. Definición de la planificación financiera
- 4.11.2. Acciones a efectuar en la planificación financiera
- 4.11.3. Creación y establecimiento de la estrategia empresarial
- 4.11.4. El cuadro *Cash Flow*
- 4.11.5. El cuadro de circulante

4.12. Estrategia Financiera Corporativa

- 4.12.1. Estrategia corporativa y fuentes de financiación
- 4.12.2. Productos financieros de financiación empresarial

4.13. Contexto Macroeconómico

- 4.13.1. Contexto macroeconómico
- 4.13.2. Indicadores económicos relevantes
- 4.13.3. Mecanismos para el control de magnitudes macroeconómicas
- 4.13.4. Los ciclos económicos

4.14. Financiación Estratégica

- 4.14.1. La autofinanciación
- 4.14.2. Ampliación de fondos propios
- 4.14.3. Recursos Híbridos
- 4.14.4. Financiación a través de intermediarios

4.15. Mercados monetarios y de capitales

- 4.15.1. El Mercado Monetario
- 4.15.2. El Mercado de Renta Fija
- 4.15.3. El Mercado de Renta Variable
- 4.15.4. El Mercado de Divisas
- 4.15.5. El Mercado de Derivados

4.16. Análisis y planificación financiera

- 4.16.1. Análisis del Balance de Situación
- 4.16.2. Análisis de la Cuenta de Resultados
- 4.16.3. Análisis de la Rentabilidad

4.17. Análisis y resolución de casos / problemas

- 4.17.1. Información financiera de Industria de Diseño y Textil, S.A. (INDITEX)

Asignatura 5**Dirección de Operaciones y Logística****5.1. Dirección y Gestión de Operaciones**

- 5.1.1. La función de las operaciones
- 5.1.2. El impacto de las operaciones en la gestión de las empresas
- 5.1.3. Introducción a la estrategia de Operaciones
- 5.1.4. La dirección de Operaciones

5.2. Organización industrial y logística

- 5.2.1. Departamento de Organización Industrial
- 5.2.2. Departamento de Logística

5.3. Estructura y tipos de producción (MTS, MTO, ATO, ETO, etc.)

- 5.3.1. Sistema de producción
- 5.3.2. Estrategia de producción
- 5.3.3. Sistema de gestión de inventario
- 5.3.4. Indicadores de producción

5.4. Estructura y tipos de aprovisionamiento

- 5.4.1. Función del aprovisionamiento
- 5.4.2. Gestión de aprovisionamiento
- 5.4.3. Tipos de compras
- 5.4.4. Gestión de compras de una empresa de forma eficiente
- 5.4.5. Etapas del proceso de decisión de la compra

5.5. Control económico de compras

- 5.5.1. Influencia económica de las compras
- 5.5.2. Centro de costes
- 5.5.3. Presupuestación
- 5.5.4. Presupuestación vs. gasto real
- 5.5.5. Herramientas de control presupuestario

5.6. Control de las operaciones de almacén

- 5.6.1. Control de inventario
- 5.6.2. Sistema de ubicación
- 5.6.3. Técnicas de gestión de stock
- 5.6.4. Sistema de almacenamiento

5.7. Gestión estratégica de compras

- 5.7.1. Estrategia empresarial
- 5.7.2. Planeación estratégica
- 5.7.3. Estrategia de compras

5.8. Tipologías de la Cadena de Suministro (SCM)

- 5.8.1. Cadena de suministro
- 5.8.2. Beneficios de la gestión de la cadena de suministro
- 5.8.3. Gestión logística en la cadena de suministro

5.9. Supply Chain Management

- 5.9.1. Concepto de Gestión de la Cadena de Suministro (SCM)
- 5.9.2. Costes y eficiencia de la cadena de operaciones
- 5.9.3. Patrones de Demanda
- 5.9.4. La estrategia de operaciones y el cambio

5.10. Interacciones de la SCM con todas las áreas

- 5.10.1. Interacción de la cadena de suministro
- 5.10.2. Interacción de la cadena de suministro. Integración por partes
- 5.10.3. Problemas de integración de la cadena de suministro
- 5.10.4. Cadena de suministro 4.0

5.11. Costes de la logística

- 5.11.1. Costes logísticos
- 5.11.2. Problemas de los costes logísticos
- 5.11.3. Optimización de costes logísticos

5.12. Rentabilidad y eficiencia de las cadenas logísticas: KPIS

- 5.12.1. Cadena logística
- 5.12.2. Rentabilidad y eficiencia de la cadena logística
- 5.12.3. Indicadores de rentabilidad y eficiencia de la cadena logística

5.13. Gestión de procesos

- 5.13.1. La gestión de procesos
- 5.13.2. Enfoque basado en procesos: mapa de procesos
- 5.13.3. Mejoras en la gestión de procesos

5.14. Distribución y logística de transportes

- 5.14.1. Distribución en la cadena de suministro
- 5.14.2. Logística de transportes
- 5.14.3. Sistemas de Información Geográfica como soporte a la Logística

5.15. Logística y clientes

- 5.15.1. Análisis de Demanda
- 5.15.2. Previsión de Demanda y Ventas
- 5.15.3. Planificación de Ventas y Operaciones
- 5.15.4. Planeamiento participativo, pronóstico y reabastecimiento (CPFR)

5.16. Logística internacional

- 5.16.1. Procesos de exportación e importación
- 5.16.2. Aduanas
- 5.16.3. Formas y medios de pago internacionales
- 5.16.4. Plataformas logísticas a nivel internacional

5.17. Outsourcing de operaciones

- 5.17.1. Gestión de operaciones y *outsourcing*
- 5.17.2. Implantación del outsourcing en entornos logísticos

5.18. Competitividad en operaciones

- 5.18.1. Gestión de Operaciones
- 5.18.2. Competitividad operacional
- 5.18.3. Estrategia de Operaciones y ventajas competitivas

5.19. Gestión de la calidad

- 5.19.1. Cliente interno y cliente externo
- 5.19.2. Los costes de calidad
- 5.19.3. La mejora continua y la filosofía de Deming

Asignatura 6

Dirección de Sistemas de Información

6.1. Entornos tecnológicos

- 6.1.1. Tecnología y globalización
- 6.1.2. Entorno económico y tecnología
- 6.1.3. Entorno tecnológico y su impacto en las empresas

6.2. Sistemas y tecnologías de la información en la empresa

- 6.2.1. Evolución del modelo de IT
- 6.2.2. Organización y departamento IT
- 6.2.3. Tecnologías de la información y entorno económico

6.3. Estrategia corporativa y estrategia tecnológica

- 6.3.1. Creación de valor para clientes y accionistas
- 6.3.2. Decisiones estratégicas de SI / TI
- 6.3.3. Estrategia corporativa vs. estrategia tecnológica y digital

6.4. Dirección de sistemas de información

- 6.4.1. Gobierno Corporativo de la tecnología y los sistemas de información
- 6.4.2. Dirección de los sistemas de información en las empresas
- 6.4.3. Directivos expertos en sistemas de información: roles y funciones

6.5. Planificación estratégica de Sistemas de Información

- 6.5.1. Sistemas de información y estrategia corporativa
- 6.5.2. Planificación estratégica de los sistemas de información
- 6.5.3. Fases de la planificación estratégica de los sistemas de información

6.6. Sistemas de información para la toma de decisiones

- 6.6.1. *Business intelligence*
- 6.6.2. *Data Warehouse*
- 6.6.3. BSC o Cuadro de mando Integral

6.7. Explorando la información

- 6.7.1. SQL: bases de datos relacionales. Conceptos básicos
- 6.7.2. Redes y comunicaciones
- 6.7.3. Sistema operacional: modelos de datos normalizados
- 6.7.4. Sistema estratégico: OLAP, modelo multidimensional y *dashboards* gráfico
- 6.7.5. Análisis estratégico de BBDD y composición de informes

6.8. Business Intelligence empresarial

- 6.8.1. El mundo del dato
- 6.8.2. Conceptos relevantes
- 6.8.3. Principales características
- 6.8.4. Soluciones en el mercado actual
- 6.8.5. Arquitectura global de una solución BI
- 6.8.6. Ciberseguridad en BI y Data Science

6.9. Nuevo concepto empresarial

- 6.9.1. ¿Por qué BI?
- 6.9.2. Obtención de la información
- 6.9.3. BI en los distintos departamentos de la empresa
- 6.9.4. Razones para invertir en BI

6.10. Herramientas y soluciones BI

- 6.10.1. ¿Cómo elegir la mejor herramienta?
- 6.10.2. Microsoft Power BI, MicroStrategy y Tableau
- 6.10.3. SAP BI, SAS BI y Qlikview
- 6.10.4. Prometheus

6.11. Planificación y dirección Proyecto BI

- 6.11.1. Primeros pasos para definir un proyecto de BI
- 6.11.2. Solución BI para la empresa
- 6.11.3. Toma de requisitos y objetivos

6.12. Aplicaciones de gestión corporativa

- 6.12.1. Sistemas de información y gestión corporativa
- 6.12.2. Aplicaciones para la gestión corporativa
- 6.12.3. Sistemas *Enterprise Resource Planning* o ERP

6.13. Transformación Digital

- 6.13.1. Marco conceptual de la transformación digital
- 6.13.2. Transformación digital: elementos clave, beneficios e inconvenientes
- 6.13.3. Transformación digital en las empresas

6.14. Tecnologías y tendencias

- 6.14.1. Principales tendencias en el ámbito de la tecnología que están cambiando los modelos de negocio
- 6.14.2. Análisis de las principales tecnologías emergentes

6.15. Outsourcing de TI

- 6.15.1. Marco conceptual del *outsourcing*
- 6.15.2. *Outsourcing* de TI y su impacto en los negocios
- 6.15.3. Claves para implementar proyectos corporativos de *outsourcing* de TI

Asignatura 7

Gestión Comercial, Marketing Estratégico y Comunicación Corporativa

7.1. Dirección comercial

- 7.1.1. Marco conceptual de la dirección comercial
- 7.1.2. Estrategia y planificación comercial
- 7.1.3. El rol de los directores comerciales

7.2. Marketing

- 7.2.1. Concepto de marketing
- 7.2.2. Elementos básicos del marketing
- 7.2.3. Actividades de marketing de la empresa

7.3. Gestión Estratégica del Marketing

- 7.3.1. Concepto de marketing estratégico
- 7.3.2. Concepto de planificación estratégica de marketing
- 7.3.3. Etapas del proceso de planificación estratégica de marketing

7.4. Marketing digital y comercio electrónico

- 7.4.1. Objetivos del Marketing digital y comercio electrónico
- 7.4.2. Marketing Digital y medios que emplea
- 7.4.3. Comercio electrónico. Contexto general
- 7.4.4. Categorías del comercio electrónico
- 7.4.5. Ventajas y desventajas del e-commerce frente al comercio tradicional

7.5. Managing digital business

- 7.5.1. Estrategia competitiva ante la creciente digitalización de los medios
- 7.5.2. Diseño y creación de un plan de Marketing Digital
- 7.5.3. Análisis del ROI en un plan de Marketing Digital

7.6. Marketing digital para reforzar la marca

- 7.6.1. Estrategias online para mejorar la reputación de tu marca
- 7.6.2. *Branded Content & Storytelling*

7.7. Estrategia de Marketing Digital

- 7.7.1. Definir la estrategia del Marketing Digital
- 7.7.2. Herramientas de la estrategia de Marketing Digital

7.8. Marketing digital para captar y fidelizar clientes

- 7.8.1. Estrategias de fidelización y vinculación a través de Internet
- 7.8.2. *Visitor Relationship Management*
- 7.8.3. Hipersegmentación

7.9. Gestión de campañas digitales

- 7.9.1. ¿Qué es una campaña de publicidad digital?
- 7.9.2. Pasos para lanzar una campaña de *marketing online*
- 7.9.3. Errores de las campañas de publicidad digital

7.10. Plan de marketing online

- 7.10.1. ¿Qué es un plan de *marketing online*?
- 7.10.2. Pasos para crear un plan de *marketing online*
- 7.10.3. Ventajas de disponer un plan de *marketing online*

7.11. Blended marketing

- 7.11.1. ¿Qué es el *blended marketing*?
- 7.11.2. Diferencias entre *marketing online* y *offline*
- 7.11.3. Aspectos a tener en cuenta en la estrategia de *blended marketing*
- 7.11.4. Características de una estrategia de *blended marketing*
- 7.11.5. Recomendaciones en *blended marketing*
- 7.11.6. Beneficios del *blended marketing*

7.12. Estrategia de ventas

- 7.12.1. Estrategia de ventas
- 7.12.2. Métodos de ventas

7.13. Comunicación Corporativa

- 7.13.1. Concepto
- 7.13.2. Importancia de la comunicación en la organización
- 7.13.3. Tipos de la comunicación en la organización
- 7.13.4. Funciones de la comunicación en la organización
- 7.13.5. Elementos de la comunicación
- 7.13.6. Problemas de la comunicación
- 7.13.7. Escenarios de la comunicación

7.14. Estrategia de Comunicación Corporativa

- 7.14.1. Programas de motivación, acción social, participación y entrenamiento con RR. HH
- 7.14.2. Instrumentos y soportes de comunicación interna
- 7.14.3. El plan de comunicación interna

7.15. Comunicación y reputación digital

- 7.15.1. Reputación online
- 7.15.2. ¿Cómo medir la reputación digital?
- 7.15.3. Herramientas de reputación online
- 7.15.4. Informe de reputación online
- 7.15.5. *Branding* online

7.16. Publicidad

- 7.16.1. Antecedentes históricos de la Publicidad
- 7.16.2. Marco conceptual de la Publicidad: principios, concepto de briefing y posicionamiento
- 7.16.3. Agencias de publicidad, agencias de medios y profesionales de la publicidad
- 7.16.4. Importancia de la publicidad en los negocios
- 7.16.5. Tendencias y retos de la publicidad

7.17. Desarrollo del plan de Marketing

- 7.17.1. Concepto del Plan de Marketing
- 7.17.2. Análisis y Diagnóstico de la Situación
- 7.17.3. Decisiones Estratégicas de Marketing
- 7.17.4. Decisiones Operativas de Marketing

7.18. Estrategias de promoción y Merchandising

- 7.18.1. Comunicación de Marketing Integrada
- 7.18.2. Plan de Comunicación Publicitaria
- 7.18.3. El *Merchandising* como técnica de Comunicación

7.19. Planificación de medios

- 7.19.1. Origen y evolución de la planificación de medios
- 7.19.2. Medios de comunicación
- 7.19.3. Plan de medios

7.20. Fundamentos de la dirección comercial

- 7.20.1. La función de la Dirección Comercial
- 7.20.2. Sistemas de análisis de la situación competitiva comercial empresa / mercado
- 7.20.3. Sistemas de planificación comercial de la empresa
- 7.20.4. Principales estrategias competitivas

7.21. Negociación comercial

- 7.21.1. Negociación comercial
- 7.21.2. Las cuestiones psicológicas de la negociación
- 7.21.3. Principales métodos de negociación
- 7.21.4. El proceso negociador



7.22. Toma de decisiones en gestión comercial

- 7.22.1. Estrategia comercial y estrategia competitiva
- 7.22.2. Modelos de toma de decisiones
- 7.22.3. Analíticas y herramientas para la toma de decisiones
- 7.22.4. Comportamiento humano en la toma de decisiones

7.23. Dirección y gestión de la red de ventas

- 7.23.1. *Sales Management*. Dirección de ventas
- 7.23.2. Redes al servicio de la actividad comercial
- 7.23.3. Políticas de selección y formación de vendedores
- 7.23.4. Sistemas de remuneración de las redes comerciales propias y externas
- 7.23.5. Gestión del proceso comercial. Control y asistencia a la labor de los comerciales basándose en la información

7.24. Implementación de la función comercial

- 7.24.1. Contratación de comerciales propios y agentes comerciales
- 7.24.2. Control de la actividad comercial
- 7.24.3. El código deontológico del personal comercial
- 7.24.4. Cumplimiento normativo
- 7.24.5. Normas comerciales de conducta generalmente aceptadas

7.25. Gestión de cuentas clave

- 7.25.1. Concepto de la Gestión de Cuentas Clave
- 7.25.2. El *Key Account Manager*
- 7.25.3. Estrategia de la Gestión de Cuentas Clave

7.26. Gestión financiera y presupuestaria

- 7.26.1. El umbral de rentabilidad
- 7.26.2. El presupuesto de ventas. Control de gestión y del plan anual de ventas
- 7.26.3. Impacto financiero de las decisiones estratégicas comerciales
- 7.26.4. Gestión del ciclo, rotaciones, rentabilidad y liquidez
- 7.26.5. Cuenta de resultados

Asignatura 8

Innovación y Dirección de Proyectos

8.1. Innovación

- 8.1.1. Introducción a la innovación
- 8.1.2. Innovación en el ecosistema empresarial
- 8.1.3. Instrumentos y herramientas para el proceso de innovación empresarial

8.2. Estrategia de Innovación

- 8.2.1. Inteligencia estratégica e innovación
- 8.2.2. Estrategia de innovación

8.3. Project Management para startups

- 8.3.1. Concepto de *startup*
- 8.3.2. Filosofía *Lean Startup*
- 8.3.3. Etapas del desarrollo de una *startup*
- 8.3.4. El rol de un gestor de proyectos en una *startup*

8.4. Diseño y validación del modelo de negocio

- 8.4.1. Marco conceptual de un modelo de negocio
- 8.4.2. Diseño y validación de modelos de negocio

8.5. Dirección y Gestión de Proyectos

- 8.5.1. Dirección y Gestión de proyectos: identificación de oportunidades para desarrollar proyectos corporativos de innovación
- 8.5.2. Principales etapas o fases de la dirección y gestión de proyectos de innovación

8.6. Gestión del cambio en proyectos: gestión de la formación

- 8.6.1. Concepto de Gestión del Cambio
- 8.6.2. El Proceso de Gestión del Cambio
- 8.6.3. La implementación del cambio

8.7. Gestión de la comunicación de proyectos

- 8.7.1. Gestión de las comunicaciones del proyecto
- 8.7.2. Conceptos clave para la gestión de las comunicaciones
- 8.7.3. Tendencias emergentes
- 8.7.4. Adaptaciones al equipo
- 8.7.5. Planificar la gestión de las comunicaciones
- 8.7.6. Gestionar las comunicaciones
- 8.7.7. Monitorear las comunicaciones

8.8. Metodologías tradicionales e innovadoras

- 8.8.1. Metodologías innovadoras
- 8.8.2. Principios básicos del Scrum
- 8.8.3. Diferencias entre los aspectos principales del Scrum y las metodologías tradicionales

8.9. Creación de una startup

- 8.9.1. Creación de una *startup*
- 8.9.2. Organización y cultura
- 8.9.3. Los diez principales motivos por los cuales fracasan las *startups*
- 8.9.4. Aspectos legales

8.10. Planificación de la gestión de riesgos en los proyectos

- 8.10.1. Planificar riesgos
- 8.10.2. Elementos para crear un plan de gestión de riesgos
- 8.10.3. Herramientas para crear un plan de gestión de riesgos
- 8.10.4. Contenido del plan de gestión de riesgos

Asignatura 9

Management Directivo

9.1. General Management

- 9.1.1. Concepto de *General Management*
- 9.1.2. La acción del *Manager General*
- 9.1.3. El Director General y sus funciones
- 9.1.4. Transformación del trabajo de la Dirección

9.2. El directivo y sus funciones. La cultura organizacional y sus enfoques

- 9.2.1. El directivo y sus funciones. La cultura organizacional y sus enfoques

9.3. Dirección de operaciones

- 9.3.1. Importancia de la dirección
- 9.3.2. La cadena de valor
- 9.3.3. Gestión de calidad

9.4. Oratoria y formación de portavoces

- 9.4.1. Comunicación interpersonal
- 9.4.2. Habilidades comunicativas e influencia
- 9.4.3. Barreras en la comunicación

9.5. Herramientas de comunicación personal y organizacional

- 9.5.1. La comunicación interpersonal
- 9.5.2. Herramientas de la comunicación interpersonal
- 9.5.3. La comunicación en la organización
- 9.5.4. Herramientas en la organización

9.6. Comunicación en situaciones de crisis

- 9.6.1. Crisis
- 9.6.2. Fases de la crisis
- 9.6.3. Mensajes: contenidos y momentos

9.7. Preparación de un plan de crisis

- 9.7.1. Análisis de posibles problemas
- 9.7.2. Planificación
- 9.7.3. Adecuación del personal

9.8. Inteligencia emocional

- 9.8.1. Inteligencia emocional y comunicación
- 9.8.2. Asertividad, empatía y escucha activa
- 9.8.3. Autoestima y comunicación emocional

9.9. Branding Personal

- 9.9.1. Estrategias para desarrollar la marca personal
- 9.9.2. Leyes del branding personal
- 9.9.3. Herramientas de la construcción de marcas personales

9.10. Liderazgo y gestión de equipos

- 9.10.1. Liderazgo y estilos de liderazgo
- 9.10.2. Capacidades y desafíos del líder
- 9.10.3. Gestión de Procesos de cambio
- 9.10.4. Gestión de Equipos Multiculturales

Asignatura 10

Trabajo Final de Máster (TFM)

Asignatura 11

Ciberinteligencia y Ciberseguridad

11.1. Ciberinteligencia

- 11.1.1. Ciberinteligencia
 - 11.1.1.1. La inteligencia
 - 11.1.1.1.1. Ciclo de inteligencia
 - 11.1.1.2. Ciberinteligencia
 - 11.1.1.3. Ciberinteligencia y ciberseguridad
- 11.1.2. El analista de inteligencia
 - 11.1.2.1. El rol del analista de inteligencia
 - 11.1.2.2. Los sesgos del analista de inteligencia en la actividad evaluativa

11.2. Ciberseguridad

- 11.2.1. Las capas de seguridad
- 11.2.2. Identificación de las ciberamenazas
 - 11.2.2.1. Amenazas externas
 - 11.2.2.2. Amenazas internas
- 11.2.3. Acciones adversas
 - 11.2.3.1. Ingeniería social
 - 11.2.3.2. Métodos comúnmente usados

11.3. Técnicas y herramientas de inteligencia

- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuciones de Linux y herramientas
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologías de evaluación

- 11.4.1. El análisis de inteligencia
- 11.4.2. Técnicas de organización de la información adquirida
- 11.4.3. Fiabilidad y credibilidad de las fuentes de información
- 11.4.4. Metodologías de análisis
- 11.4.5. Presentación de los resultados de la inteligencia

11.5. Auditorías y documentación

- 11.5.1. La auditoría en seguridad informática
- 11.5.2. Documentación y permisos para auditoría
- 11.5.3. Tipos de auditoría
- 11.5.4. Entregables
 - 11.5.4.1. Informe técnico
 - 11.5.4.2. Informe ejecutivo

11.6. Anonimato en la red

- 11.6.1. Uso de anonimato
- 11.6.2. Técnicas de anonimato (Proxy, VPN)
- 11.6.3. Redes TOR, Freenet e IP2

11.7. Amenazas y tipos de seguridad

- 11.7.1. Tipos de amenazas
- 11.7.2. Seguridad física
- 11.7.3. Seguridad en redes
- 11.7.4. Seguridad lógica
- 11.7.5. Seguridad en aplicaciones web
- 11.7.6. Seguridad en dispositivos móviles

11.8. Normativa y compliance

- 11.8.1. RGPD
- 11.8.2. La estrategia nacional de ciberseguridad 2019
- 11.8.3. Familia ISO 27000
- 11.8.4. Marco de ciberseguridad NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normativas *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Análisis de riesgos y métricas

- 11.9.1. Alcance de riesgos
- 11.9.2. Los activos
- 11.9.3. Las amenazas
- 11.9.4. Las vulnerabilidades
- 11.9.5. Evaluación del riesgo
- 11.9.6. Tratamiento del riesgo

11.10. Organismos importantes en materia de ciberseguridad

- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Asignatura 12

Seguridad en Host

12.1. Copias de seguridad

- 12.1.1. Estrategias para las copias de seguridad
- 12.1.2. Herramientas para Windows
- 12.1.3. Herramientas para Linux
- 12.1.4. Herramientas para MacOS

12.2. Antivirus de usuario

- 12.2.1. Tipos de antivirus
- 12.2.2. Antivirus para Windows
- 12.2.3. Antivirus para Linux
- 12.2.4. Antivirus para MacOS
- 12.2.5. Antivirus para smartphones

12.3. Detectores de intrusos - HIDS

- 12.3.1. Métodos de detección de intrusos
- 12.3.2. Sagan
- 12.3.3. Aide
- 12.3.4. Rkhunter

12.4. Firewall local

- 12.4.1. *Firewalls* para Windows
- 12.4.2. *Firewalls* para Linux
- 12.4.3. *Firewalls* para MacOS

12.5. Gestores de contraseñas

- 12.5.1. *Password*
- 12.5.2. LastPass
- 12.5.3. KeePass
- 12.5.4. StickyPassword
- 12.5.5. RoboForm

12.6. Detectores de phishing

- 12.6.1. Detección del *phishing* de forma manual
- 12.6.2. Herramientas *antiphishing*

12.7. Spyware

- 12.7.1. Mecanismos de evitación
- 12.7.2. Herramientas *antispyware*

12.8. Rastreadores

- 12.8.1. Medidas para proteger el sistema
- 12.8.2. Herramientas anti - rastreadores

12.9. EDR (End Point Detection and Response)

- 12.9.1. Comportamiento del Sistema EDR
- 12.9.2. Diferencias entre EDR y antivirus
- 12.9.3. El futuro de los sistemas EDR

12.10. Control sobre la instalación de software

- 12.10.1. Repositorios y tiendas de software
- 12.10.2. Listas de software permitido o prohibido
- 12.10.3. Criterios de actualizaciones
- 12.10.4. Privilegios para instalar software

Asignatura 13**Seguridad en Red (Perimetral)****13.1. Sistemas de detección y prevención de amenazas**

- 13.1.1. Marco general de los incidentes de seguridad
- 13.1.2. Sistemas de defensa actuales: *Defense in Depth* y SOC
- 13.1.3. Arquitecturas de red actuales
- 13.1.4. Tipos de herramientas para la detección y prevención de incidentes
 - 13.1.4.1. Sistemas basados en red
 - 13.1.4.2. Sistemas basados en *host*
 - 13.1.4.3. Sistemas centralizados
- 13.1.5. Comunicación y detección de instancias / *hosts*, contenedores y *serverless*

13.2. Firewall

- 13.2.1. Tipos de *firewalls*
- 13.2.2. Ataques y mitigación
- 13.2.3. *Firewalls* comunes en *kernel* Linux
 - 13.2.3.1. UFW
 - 13.2.3.2. *Nftables* e *iptables*
 - 13.2.3.3. *Firewalld*
- 13.2.4. Sistemas de detección basados en *logs* del sistema
 - 13.2.4.1. TCP Wrappers
 - 13.2.4.2. BlockHosts y DenyHosts
 - 13.2.4.3. Fail2ban

13.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)

- 13.3.1. Ataques sobre IDS/IPS
- 13.3.2. Sistemas de IDS/IPS
 - 13.3.2.1. Snort
 - 13.3.2.2. Suricata

13.4. Firewalls de siguiente generación (NGFW)

- 13.4.1. Diferencias entre NGFW y *firewall* tradicional
- 13.4.2. Capacidades principales
- 13.4.3. Soluciones comerciales
- 13.4.4. *Firewalls* para servicios de *cloud*
 - 13.4.4.1. Arquitectura Cloud VPC
 - 13.4.4.2. Cloud ACLs
 - 13.4.4.3. Security Group

13.5. Proxy

- 13.5.1. Tipos de *proxy*
- 13.5.2. Uso de *proxy*. Ventajas e inconvenientes

13.6. Motores de antivirus

- 13.6.1. Contexto general del *malware* e IOC's
- 13.6.2. Problemas de los motores de antivirus

13.7. Sistemas de protección de correo

- 13.7.1. Antispam
 - 13.7.1.1. Listas blancas y negras
 - 13.7.1.2. Filtros bayesianos
- 13.7.2. Mail Gateway (MGW)

13.8. SIEM

- 13.8.1. Componentes y arquitectura
- 13.8.2. Reglas de correlación y casos de uso
- 13.8.3. Retos actuales de los sistemas SIEM

13.9. SOAR

- 13.9.1. SOAR y SIEM: enemigos o aliados
- 13.9.2. El futuro de los sistemas SOAR

13.10. Otros sistemas basados en red

- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots y HoneyNets
- 13.10.4. CASB

Asignatura 14**Seguridad en Smartphones****14.1. El mundo del dispositivo móvil**

- 14.1.1. Tipos de plataformas móviles
- 14.1.2. Dispositivos iOS
- 14.1.3. Dispositivos Android

14.2. Gestión de la seguridad móvil

- 14.2.1. Proyecto de seguridad móvil OWASP
 - 14.2.1.1. Top 10 vulnerabilidades
- 14.2.2. Comunicaciones, redes y modos de conexión

14.3. El dispositivo móvil en el entorno empresarial

- 14.3.1. Riesgos
- 14.3.2. Políticas de seguridad
- 14.3.3. Monitorización de dispositivos
- 14.3.4. Gestión de dispositivos móviles (MDM)

14.4. Privacidad del usuario y seguridad de los datos

- 14.4.1. Estados de la información
- 14.4.2. Protección y confidencialidad de los datos
 - 14.4.2.1. Permisos
 - 14.4.2.2. Encriptación
- 14.4.3. Almacenamiento seguro de los datos
 - 14.4.3.1. Almacenamiento seguro en iOS
 - 14.4.3.2. Almacenamiento seguro en Android
- 14.4.4. Buenas prácticas en el desarrollo de aplicaciones

14.5. Vulnerabilidades y vectores de ataque

- 14.5.1. Vulnerabilidades
- 14.5.2. Vectores de ataque
 - 14.5.2.1. *Malware*
 - 14.5.2.2. Exfiltración de datos
 - 14.5.2.3. Manipulación de los datos

14.6. Principales amenazas

- 14.6.1. Usuario no formado
- 14.6.2. *Malware*
 - 14.6.2.1. Tipos de *malware*
- 14.6.3. Ingeniería social
- 14.6.4. Fuga de datos
- 14.6.5. Robo de información
- 14.6.6. Redes wifi no seguras
- 14.6.7. Software desactualizado
- 14.6.8. Aplicaciones maliciosas
- 14.6.9. Contraseñas poco seguras
- 14.6.10. Configuración débil o inexistente de seguridad
- 14.6.11. Acceso físico
- 14.6.12. Pérdida o robo del dispositivo
- 14.6.13. Suplantación de identidad (integridad)
- 14.6.14. Criptografía débil o rota
- 14.6.15. Denegación de servicio (DoS)

14.7. Principales ataques

- 14.7.1. Ataques de *phishing*
- 14.7.2. Ataques relacionados con los modos de comunicación
- 14.7.3. Ataques de *smishing*
- 14.7.4. Ataques de *criptojacking*
- 14.7.5. *Man in the middle*

14.8. Hacking

- 14.8.1. *Rooting* y *jailbreaking*
- 14.8.2. Anatomía de un ataque móvil
 - 14.8.2.1. Propagación de la amenaza
 - 14.8.2.2. Instalación de *malware* en el dispositivo
 - 14.8.2.3. Persistencia
 - 14.8.2.4. Ejecución del *payload* y extracción de la información
- 14.8.3. *Hacking* en dispositivos iOS: mecanismos y herramientas
- 14.8.4. *Hacking* en dispositivos Android: mecanismos y herramientas

14.9. Pruebas de penetración

- 14.9.1. iOS *pentesting*
- 14.9.2. Android *pentesting*
- 14.9.3. Herramientas

14.10. Protección y seguridad

- 14.10.1. Configuración de seguridad
 - 14.10.1.1. En dispositivos iOS
 - 14.10.1.2. En dispositivos Android
- 14.10.2. Medidas de seguridad
- 14.10.3. Herramientas de protección

Asignatura 15

Seguridad en IoT

15.1. Dispositivos

- 15.1.1. Tipos de dispositivos
- 15.1.2. Arquitecturas estandarizadas
 - 15.1.2.1. ONEM2M
 - 15.1.2.2. IoTWF
- 15.1.3. Protocolos de aplicación
- 15.1.4. Tecnologías de conectividad

15.2. Dispositivos IoT. Áreas de aplicación

- 15.2.1. *SmartHome*
- 15.2.2. *SmartCity*
- 15.2.3. Transportes
- 15.2.4. *Wearables*
- 15.2.5. Sector salud
- 15.2.6. IIoT

15.3. Protocolos de comunicación

- 15.3.1. MQTT
- 15.3.2. LWM2M
- 15.3.3. OMA - DM
- 15.3.4. TR - 069

15.4. SmartHome

- 15.4.1. Domótica
- 15.4.2. Redes
- 15.4.3. Electrodomésticos
- 15.4.4. Vigilancia y seguridad

15.5. SmartCity

- 15.5.1. Iluminación
- 15.5.2. Meteorología
- 15.5.3. Seguridad

15.6. Transportes

- 15.6.1. Localización
- 15.6.2. Realización de pagos y obtención de servicios
- 15.6.3. Conectividad

15.7. Wearables

- 15.7.1. Ropa inteligente
- 15.7.2. Joyas inteligentes
- 15.7.3. Relojes inteligentes

15.8. Sector salud

- 15.8.1. Monitorización de ejercicio / ritmo cardiaco
- 15.8.2. Monitorización de pacientes y personas mayores
- 15.8.3. Implantables
- 15.8.4. *Robots* quirúrgicos

15.9. Conectividad

- 15.9.1. Wifi / Gateway
- 15.9.2. Bluetooth
- 15.9.3. Conectividad incorporada

15.10. Securitización

- 15.10.1. Redes dedicadas
- 15.10.2. Gestor de contraseñas
- 15.10.3. Uso de protocolos cifrados
- 15.10.4. Consejos de uso

Asignatura 16

Hacking Ético

16.1. Entorno de trabajo

- 16.1.1. Distribuciones Linux
 - 16.1.1.1. Kali Linux - Offensive Security
 - 16.1.1.2. Parrot OS
 - 16.1.1.3. Ubuntu
- 16.1.2. Sistemas de virtualización
- 16.1.3. *Sandbox*
- 16.1.4. Despliegue de laboratorios

16.2. Metodologías

- 16.2.1. OSSTMM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. Footprinting

- 16.3.1. Inteligencia de fuentes abiertas (OSINT)
- 16.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 16.3.3. Uso de herramientas pasivas

16.4. Escaneo de redes

- 16.4.1. Herramientas de escaneo
 - 16.4.1.1. Nmap
 - 16.4.1.2. Hping3
 - 16.4.1.3. Otras herramientas de escaneo
- 16.4.2. Técnicas de escaneo
- 16.4.3. Técnicas de evasión de *firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagramas de red

16.5. Enumeración

- 16.5.1. Enumeración SMTP
- 16.5.2. Enumeración DNS
- 16.5.3. Enumeración de NetBIOS y Samba
- 16.5.4. Enumeración de LDAP
- 16.5.5. Enumeración de SNMP
- 16.5.6. Otras técnicas de enumeración

16.6. Análisis de vulnerabilidades

- 16.6.1. Soluciones de análisis de vulnerabilidades
 - 16.6.1.1. Qualys
 - 16.6.1.2. Nessus
 - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemas de puntuación de vulnerabilidades
 - 16.6.2.1. CVSS
 - 16.6.2.2. CVE
 - 16.6.2.3. NVD

16.7. Ataques a redes inalámbrica

- 16.7.1. Metodología de *hacking* en redes inalámbricas
 - 16.7.1.1. Wifi *Discovery*
 - 16.7.1.2. Análisis de tráfico
 - 16.7.1.3. Ataques del *aircrack*
 - 16.7.1.3.1. Ataques WEP
 - 16.7.1.3.2. Ataques WPA / WPA2
 - 16.7.1.4. Ataques de *Evil Twin*
 - 16.7.1.5. Ataques a WPS
 - 16.7.1.6. *Jamming*
- 16.7.2. Herramientas para la seguridad inalámbrica

16.8. Hacking de servidores webs

- 16.8.1. *Cross Site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQL Injection*

16.9. Explotación de vulnerabilidades

- 16.9.1. Uso de *exploits* conocidos
- 16.9.2. Uso de *metasploit*
- 16.9.3. Uso de *malware*
 - 16.9.3.1. Definición y alcance
 - 16.9.3.2. Generación de *malware*
 - 16.9.3.3. *Bypass* de soluciones antivirus

16.10. Persistencia

- 16.10.1. Instalación de *rootkits*
- 16.10.2. Uso de *ncat*
- 16.10.3. Uso de tareas programadas para *backdoors*
- 16.10.4. Creación de usuarios
- 16.10.5. Detección de HIDS

Asignatura 17

Ingeniería Inversa

17.1. Compiladores

- 17.1.1. Tipos de códigos
- 17.1.2. Fases de un compilador
- 17.1.3. Tabla de símbolos
- 17.1.4. Gestor de errores
- 17.1.5. Compilador GCC

17.2. Tipos de análisis en compiladores

- 17.2.1. Análisis léxico
 - 17.2.1.1. Terminología
 - 17.2.1.2. Componentes léxicos
 - 17.2.1.3. Analizador léxico LEX
- 17.2.2. Análisis sintáctico
 - 17.2.2.1. Gramáticas libres de contexto
 - 17.2.2.2. Tipos de análisis sintácticos
 - 17.2.2.2.1. Análisis descendente
 - 17.2.2.2.2. Análisis ascendente
 - 17.2.2.3. Árboles sintácticos y derivaciones
 - 17.2.2.4. Tipos de analizadores sintácticos
 - 17.2.2.4.1. Analizadores LR (*Left To Right*)
 - 17.2.2.4.2. Analizadores LALR
- 17.2.3. Análisis semántico
 - 17.2.3.1. Gramáticas de atributos
 - 17.2.3.2. S-Atribuidas
 - 17.2.3.3. L - Atribuidas

17.3. Estructuras de datos en ensamblador

- 17.3.1. Variables
- 17.3.2. *Arrays*
- 17.3.3. Punteros
- 17.3.4. Estructuras
- 17.3.5. Objetos

17.4. Estructuras de código en ensamblador

- 17.4.1. Estructuras de selección
 - 17.4.1.1. *If, else if, Else*
 - 17.4.1.2. *Switch*
- 17.4.2. Estructuras de iteración
 - 17.4.2.1. *For*
 - 17.4.2.2. *While*
 - 17.4.2.3. Uso del *break*
- 17.4.3. Funciones

17.5. Arquitectura Hardware x86

- 17.5.1. Arquitectura de procesadores x86
- 17.5.2. Estructuras de datos en x86
- 17.5.3. Estructuras de código en x86

17.6. Arquitectura hardware ARM

- 17.6.1. Arquitectura de procesadores ARM
- 17.6.2. Estructuras de datos en ARM
- 17.6.3. Estructuras de código en ARM

17.7. Análisis de código estático

- 17.7.1. Desensambladores
- 17.7.2. IDA
- 17.7.3. Reconstructores de código

17.8. Análisis de código dinámico

- 17.8.1. Análisis del comportamiento
 - 17.8.1.1. Comunicaciones
 - 17.8.1.2. Monitorización
- 17.8.2. Depuradores de código en Linux
- 17.8.3. Depuradores de código en Windows

17.9. Sandbox

- 17.9.1. Arquitectura de un *sandbox*
- 17.9.2. Evasión de un *sandbox*
- 17.9.3. Técnicas de detección
- 17.9.4. Técnicas de evasión
- 17.9.5. Contramedidas
- 17.9.6. Sandbox en Linux
- 17.9.7. Sandbox en Windows
- 17.9.8. Sandbox en MacOS
- 17.9.9. Sandbox en Android

17.10. Análisis de *malware*

- 17.10.1. Métodos de análisis de *malware*
- 17.10.2. Técnicas de ofuscación de *malware*
 - 17.10.2.1. Ofuscación de ejecutables
 - 17.10.2.2. Restricción de entornos de ejecución
- 17.10.3. Herramientas de análisis de *malware*

Asignatura 18

Desarrollo Seguro

18.1. Desarrollo seguro

- 18.1.1. Calidad, funcionalidad y seguridad
- 18.1.2. Confidencialidad, integridad y disponibilidad
- 18.1.3. Ciclo de vida del desarrollo de software

18.2. Fase de requerimientos

- 18.2.1. Control de la autenticación
- 18.2.2. Control de roles y privilegios
- 18.2.3. Requerimientos orientados al riesgo
- 18.2.4. Aprobación de privilegios

18.3. Fases de análisis y diseño

- 18.3.1. Acceso a componentes y administración del sistema
- 18.3.2. Pistas de auditoría
- 18.3.3. Gestión de sesiones
- 18.3.4. Datos históricos
- 18.3.5. Manejo apropiado de errores
- 18.3.6. Separación de funciones

18.4. Fase de implementación y codificación

- 18.4.1. Aseguramiento del ambiente de desarrollo
- 18.4.2. Elaboración de la documentación técnica
- 18.4.3. Codificación segura
- 18.4.4. Seguridad en las comunicaciones

18.5. Buenas prácticas de codificación segura

- 18.5.1. Validación de datos de entrada
- 18.5.2. Codificación de los datos de salida
- 18.5.3. Estilo de programación
- 18.5.4. Manejo de registro de cambios
- 18.5.5. Prácticas criptográficas
- 18.5.6. Gestión de errores y *logs*
- 18.5.7. Gestión de archivos
- 18.5.8. Gestión de Memoria
- 18.5.9. Estandarización y reutilización de funciones de seguridad

18.6. Preparación del servidor y *hardening*

- 18.6.1. Gestión de usuarios, grupos y roles en el servidor
- 18.6.2. Instalación de software
- 18.6.3. *Hardening* del servidor
- 18.6.4. Configuración robusta del entorno de la aplicación

18.7. Preparación de la BBDD y *Hardening*

- 18.7.1. Optimización del motor de BBDD
- 18.7.2. Creación del usuario propio para la aplicación
- 18.7.3. Asignación de los privilegios precisos para el usuario
- 18.7.4. *Hardening* de la BBDD

18.8. Fase de pruebas

- 18.8.1. Control de calidad en controles de seguridad
- 18.8.2. Inspección del código por fases
- 18.8.3. Comprobación de la gestión de las configuraciones
- 18.8.4. Pruebas de caja negra

18.9. Preparación del Paso a producción

- 18.9.1. Realizar el control de cambios
- 18.9.2. Realizar procedimiento de paso a producción
- 18.9.3. Realizar procedimiento de *rollback*
- 18.9.4. Pruebas en fase de preproducción

18.10. Fase de mantenimiento

- 18.10.1. Aseguramiento basado en riesgos
- 18.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 18.10.3. Pruebas de mantenimiento de seguridad de caja negra

Asignatura 19

Análisis Forense

19.1. Adquisición de datos y duplicación

- 19.1.1. Adquisición de datos volátiles
 - 19.1.1.1. Información del sistema
 - 19.1.1.2. Información de la red
 - 19.1.1.3. Orden de volatilidad
- 19.1.2. Adquisición de datos estáticos
 - 19.1.2.1. Creación de una imagen duplicada
 - 19.1.2.2. Preparación de un documento para la cadena de custodia
- 19.1.3. Métodos de validación de los datos adquiridos
 - 19.1.3.1. Métodos para Linux
 - 19.1.3.2. Métodos para Windows

19.2. Evaluación y derrota de técnicas antiforenses

- 19.2.1. Objetivos de las técnicas antiforenses
- 19.2.2. Borrado de datos
 - 19.2.2.1. Borrado de datos y ficheros
 - 19.2.2.2. Recuperación de archivos
 - 19.2.2.3. Recuperación de particiones borradas
- 19.2.3. Protección por contraseña
- 19.2.4. Esteganografía
- 19.2.5. Borrado seguro de dispositivos
- 19.2.6. Encriptación

19.3. Análisis forense del sistema operativo

- 19.3.1. Análisis forense de Windows
- 19.3.2. Análisis forense de Linux
- 19.3.3. Análisis forense de Mac

19.4. Análisis forense de la red

- 19.4.1. Análisis de los *logs*
- 19.4.2. Correlación de datos
- 19.4.3. Investigación de la red
- 19.4.4. Pasos a seguir en el análisis forense de la red

19.5. Análisis forense web

- 19.5.1. Investigación de los ataques webs
- 19.5.2. Detección de ataques
- 19.5.3. Localización de direcciones IP

19.6. Análisis forense de Bases de Datos

- 19.6.1. Análisis forense en MSSQL
- 19.6.2. Análisis forense en MySQL
- 19.6.3. Análisis forense en PostgreSQL
- 19.6.4. Análisis forense en MongoDB

19.7. Análisis forense en *cloud*

- 19.7.1. Tipos de crímenes en *cloud*
 - 19.7.1.1. *Cloud* como sujeto
 - 19.7.1.2. *Cloud* como objeto
 - 19.7.1.3. *Cloud* como herramienta
- 19.7.2. Retos del análisis forense en *cloud*
- 19.7.3. Investigación de los servicios de almacenamiento el *cloud*
- 19.7.4. Herramientas de análisis forense para *cloud*

19.8. Investigación de crímenes de correo electrónico

- 19.8.1. Sistemas de correo
 - 19.8.1.1. Clientes de correo
 - 19.8.1.2. Servidor de correo
 - 19.8.1.3. Servidor SMTP
 - 19.8.1.4. Servidor POP3
 - 19.8.1.5. Servidor IMAP4
- 19.8.2. Crímenes de correo
- 19.8.3. Mensaje de correo
 - 19.8.3.1. Cabeceras estándar
 - 19.8.3.2. Cabeceras extendidas

- 19.8.4. Pasos para la investigación de estos crímenes
- 19.8.5. Herramientas forenses para correo electrónico

19.9. Análisis forense de móviles

- 19.9.1. Redes celulares
 - 19.9.1.1. Tipos de redes
 - 19.9.1.2. Contenidos del CDR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Adquisición lógica
- 19.9.4. Adquisición física
- 19.9.5. Adquisición del sistema de ficheros

19.10. Redacción y presentación de informes forenses

- 19.10.1. Aspectos importantes de un informe forense
- 19.10.2. Clasificación y tipos de informes
- 19.10.3. Guía para escribir un informe
- 19.10.4. Presentación del informe
 - 19.10.4.1. Preparación previa para testificar
 - 19.10.4.2. Deposition
 - 19.10.4.3. Trato con los medios

Asignatura 20**Retos Actuales y Futuros en Seguridad Informática****20.1. Tecnología *blockchain***

- 20.1.1. Ámbitos de aplicación
- 20.1.2. Garantía de confidencialidad
- 20.1.3. Garantía de no - repudio

20.2. Dinero digital

- 20.2.1. Bitcoins
- 20.2.2. Criptomonedas
- 20.2.3. Minería de criptomonedas
- 20.2.4. Estafas piramidales
- 20.2.5. Otros potenciales delitos y problemas

20.3. Deepfake

- 20.3.1. Impacto en los medios
- 20.3.2. Peligros para la sociedad
- 20.3.3. Mecanismos de detección

20.4. El futuro de la Inteligencia Artificial

- 20.4.1. Inteligencia artificial y computación cognitiva
- 20.4.2. Usos para simplificar el servicio a clientes

20.5. Privacidad digital

- 20.5.1. Valor de los datos en la red
- 20.5.2. Uso de los datos en la red
- 20.5.3. Gestión de la privacidad e identidad digital

20.6. Cyberconflictos, cibercriminales y ciberataques

- 20.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 20.6.2. Consecuencias de ciberataques en la población general
- 20.6.3. Tipos de cibercriminales. Medidas de protección

20.7. Teletrabajo

- 20.7.1. Revolución del teletrabajo durante y post Covid19
- 20.7.2. Cuellos de botella en el acceso
- 20.7.3. Variación de la superficie de ataque
- 20.7.4. Necesidades de los trabajadores

20.8. Tecnologías *wireless* emergentes

- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Ondas milimétricas
- 20.8.4. Tendencia en *Get Smart* en vez de *Get More*

20.9. Direccionamiento futuro en redes

- 20.9.1. Problemas actuales con el direccionamiento IP
- 20.9.2. IPv6
- 20.9.3. IPv4+
- 20.9.4. Ventajas de IPv4+ sobre IPv4
- 20.9.5. Ventajas de IPv6 sobre IPv4

20.10. El reto de la concienciación de la formación temprana y continua de la población

- 20.10.1. Estrategias actuales de los gobiernos
- 20.10.2. Resistencia de la población al aprendizaje
- 20.10.3. Planes de formación que deben adoptar las empresas

Asignatura 21**Ciberseguridad y análisis de amenazas modernas con ChatGPT****21.1. Introducción a la Ciberseguridad: amenazas actuales y el rol de la Inteligencia Artificial**

- 21.1.1. Definición y conceptos básicos de Ciberseguridad
- 21.1.2. Tipos de amenazas cibernéticas modernas
- 21.1.3. Papel de la Inteligencia Artificial en la evolución de la Ciberseguridad

21.2. Confidencialidad, integridad y disponibilidad (CIA) en la era de la Inteligencia Artificial

- 21.2.1. Fundamentos del modelo CIA en Ciberseguridad
- 21.2.2. Principios de seguridad aplicados en el contexto de Inteligencia Artificial
- 21.2.3. Retos y consideraciones del CIA en sistemas impulsados por Inteligencia Artificial

21.3. Uso de ChatGPT para análisis de riesgos y escenarios de amenaza

- 21.3.1. Fundamentos de análisis de riesgos en Ciberseguridad
- 21.3.2. Capacidad de ChatGPT para identificar y evaluar escenarios de amenaza
- 21.3.3. Beneficios y limitaciones del análisis de riesgos con Inteligencia Artificial

21.4. ChatGPT en la detección de vulnerabilidades críticas

- 21.4.1. Principios de detección de vulnerabilidades en sistemas de información
- 21.4.2. Funcionalidades de ChatGPT para apoyar en la detección de vulnerabilidades
- 21.4.3. Consideraciones éticas y de seguridad al usar Inteligencia Artificial en detección de fallos

21.5. Análisis de *malware* y *ransomware* asistido por Inteligencia Artificial

- 21.5.1. Principios básicos del análisis de *malware* y *ransomware*
- 21.5.2. Técnicas de Inteligencia Artificial aplicadas en la identificación de código malicioso
- 21.5.3. Desafíos técnicos y operacionales en el análisis de *malware* asistido por Inteligencia Artificial

21.6. Identificación de ataques comunes con Inteligencia Artificial: *phishing*, ingeniería social y explotación

- 21.6.1. Clasificación de ataques: *phishing*, ingeniería social y explotación

- 21.6.2. Técnicas de Inteligencia Artificial para la identificación y análisis de ataques comunes
- 21.6.3. Dificultades y limitaciones de los modelos de Inteligencia Artificial en detección de ataques

21.7. ChatGPT en la capacitación y simulación de amenazas cibernéticas

- 21.7.1. Fundamentos de la simulación de amenazas para formación en Ciberseguridad
- 21.7.2. Capacidades de ChatGPT para diseñar escenarios de simulación
- 21.7.3. Beneficios de la simulación de amenazas como herramienta de capacitación

21.8. Políticas de seguridad cibernética con recomendaciones de Inteligencia Artificial

- 21.8.1. Principios para la formulación de políticas de seguridad cibernética
- 21.8.2. Rol de la Inteligencia Artificial en la generación de recomendaciones de seguridad
- 21.8.3. Componentes clave en políticas de seguridad orientadas a Inteligencia Artificial

21.9. Seguridad en dispositivos IoT y el papel de la Inteligencia Artificial

- 21.9.1. Fundamentos de la seguridad en el Internet de las Cosas (IoT)
- 21.9.2. Capacidades de la Inteligencia Artificial para mitigar vulnerabilidades en dispositivos IoT
- 21.9.3. Desafíos y consideraciones específicas de Inteligencia Artificial para la seguridad de IoT

21.10. Evaluación de amenazas y respuestas asistidas por herramientas de Inteligencia Artificial

- 21.10.1. Principios de evaluación de amenazas en Ciberseguridad
- 21.10.2. Características de las respuestas automatizadas mediante Inteligencia Artificial
- 21.10.3. Factores críticos en la efectividad de respuestas cibernéticas con Inteligencia Artificial

Asignatura 22

Detección y prevención de intrusiones usando modelos de Inteligencia Artificial Generativa

22.1. Fundamentos de sistemas IDS/IPS y el papel de la Inteligencia Artificial

- 22.1.1. Definición y principios básicos de los sistemas IDS e IPS
- 22.1.2. Principales tipos y configuraciones de IDS/IPS
- 22.1.3. Contribución de la Inteligencia Artificial en la evolución de los sistemas de detección y prevención

22.2. Uso de Gemini para detección de anomalías en redes

- 22.2.1. Conceptos y tipos de anomalías en el tráfico de red
- 22.2.2. Características de Gemini para el análisis de datos de red
- 22.2.3. Beneficios de la detección de anomalías en la prevención de intrusiones

22.3. Gemini y la identificación de patrones de intrusión

- 22.3.1. Principios de identificación y clasificación de patrones de intrusión
- 22.3.2. Técnicas de Inteligencia Artificial aplicadas en la detección de patrones de amenazas
- 22.3.3. Tipos de patrones y comportamiento anómalo en seguridad de redes

22.4. Aplicación de modelos generativos en la simulación de ataques

- 22.4.1. Fundamentos de los modelos generativos en Inteligencia Artificial
- 22.4.2. Uso de modelos generativos para recrear escenarios de ataque
- 22.4.3. Ventajas y limitaciones en la simulación de ataques mediante Inteligencia Artificial generativa

22.5. Clustering y clasificación de eventos usando Inteligencia Artificial

- 22.5.1. Fundamentos del *clustering* y clasificación en la detección de intrusiones
- 22.5.2. Algoritmos comunes de *clustering* aplicados en Ciberseguridad
- 22.5.3. Papel de la Inteligencia Artificial en la mejora de los métodos de clasificación de eventos

22.6. Gemini en la generación de perfiles de comportamiento

- 22.6.1. Conceptos de perfilamiento de usuarios y dispositivos
- 22.6.2. Aplicación de modelos generativos en la creación de perfiles
- 22.6.3. Ventajas de los perfiles de comportamiento en la detección de amenazas

22.7. Análisis de Big Data para la prevención de intrusiones

- 22.7.1. Importancia del *Big Data* en la detección de patrones de seguridad
- 22.7.2. Métodos de procesamiento de grandes volúmenes de datos en Ciberseguridad
- 22.7.3. Aplicaciones de Inteligencia Artificial en el análisis y prevención basados en *Big Data*

22.8. Reducción de datos y selección de características relevantes con Inteligencia Artificial

- 22.8.1. Principios de reducción de dimensionalidad en grandes volúmenes de datos
- 22.8.2. Selección de características para mejorar la eficiencia de análisis de Inteligencia Artificial
- 22.8.3. Técnicas de reducción de datos aplicadas en Ciberseguridad

22.9. Evaluación de modelos de Inteligencia Artificial en detección de intrusos

- 22.9.1. Criterios de evaluación de modelos de Inteligencia Artificial en Ciberseguridad
- 22.9.2. Indicadores de rendimiento y precisión de los modelos
- 22.9.3. Importancia de la validación y evaluación constante en la Inteligencia Artificial

22.10. Implementación de un sistema de detección de intrusos potenciado con Inteligencia Artificial generativa

- 22.10.1. Conceptos básicos de implementación de sistemas de detección de intrusos

- 22.10.2. Integración de Inteligencia Artificial generativa en los sistemas IDS/IPS
- 22.10.3. Aspectos clave para la configuración y mantenimiento de sistemas basados en Inteligencia Artificial

Asignatura 23

Criptografía moderna con asistencia de ChatGPT en la protección de datos

23.1. Principios básicos de criptografía con aplicaciones de Inteligencia Artificial

- 23.1.1. Conceptos fundamentales de criptografía: confidencialidad y autenticidad
- 23.1.2. Principales algoritmos criptográficos y su relevancia actual
- 23.1.3. Papel de la Inteligencia Artificial en la modernización de la criptografía

23.2. ChatGPT en la enseñanza y práctica de criptografía simétrica y asimétrica

- 23.2.1. Introducción a la criptografía simétrica y asimétrica
- 23.2.2. Comparación entre cifrado simétrico y asimétrico
- 23.2.3. Uso de ChatGPT en el aprendizaje de métodos criptográficos

23.3. Encriptación avanzada (AES, RSA) y recomendaciones generadas por Inteligencia Artificial

- 23.3.1. Fundamentos de los algoritmos AES y RSA en la encriptación de datos
- 23.3.2. Fortalezas y debilidades de estos algoritmos en el contexto actual
- 23.3.3. Generación de recomendaciones de seguridad en criptografía avanzada con Inteligencia Artificial

23.4. Inteligencia Artificial en la gestión y autenticación de claves

- 23.4.1. Principios de gestión de claves criptográficas
- 23.4.2. Importancia de la autenticación segura de claves
- 23.4.3. Aplicación de Inteligencia Artificial para optimizar procesos de gestión y autenticación

23.5. Algoritmos de hashing y ChatGPT en la evaluación de integridad

- 23.5.1. Conceptos básicos y aplicaciones de los algoritmos de *hashing*
- 23.5.2. Funciones de hash en la verificación de integridad de datos
- 23.5.3. Análisis y verificación de integridad de datos con ayuda de ChatGPT

23.6. ChatGPT en la detección de patrones de cifrado anómalos

- 23.6.1. Introducción a la detección de patrones anómalos en criptografía
- 23.6.2. Capacidad de ChatGPT para identificar irregularidades en datos cifrados
- 23.6.3. Limitaciones de los modelos de lenguaje en la detección de cifrado anómalo

23.7. Introducción a la criptografía postcuántica con simulaciones de Inteligencia Artificial

- 23.7.1. Fundamentos de la criptografía postcuántica y su importancia
- 23.7.2. Principales algoritmos postcuánticos en investigación
- 23.7.3. Uso de Inteligencia Artificial en simulaciones para el estudio de criptografía postcuántica

23.8. Blockchain y ChatGPT en la verificación de transacciones seguras

- 23.8.1. Conceptos básicos de *blockchain* y su estructura de seguridad
- 23.8.2. Rol de la criptografía en la integridad de *blockchain*
- 23.8.3. Aplicación de ChatGPT para explicar y analizar transacciones seguras

23.9. Protección de privacidad y aprendizaje federado

- 23.9.1. Definición y principios del aprendizaje federado
- 23.9.2. Importancia de la privacidad en el aprendizaje descentralizado
- 23.9.3. Beneficios y desafíos del aprendizaje federado para la seguridad de datos

23.10. Desarrollo de un sistema de encriptación basado en Inteligencia Artificial generativa

- 23.10.1. Principios básicos en la creación de sistemas de encriptación
- 23.10.2. Ventajas de la Inteligencia Artificial generativa en el diseño de sistemas de cifrado
- 23.10.3. Componentes y requisitos de un sistema de encriptación asistido por Inteligencia Artificial

Asignatura 24

Análisis forense digital y respuesta a incidentes asistida por Inteligencia Artificial

24.1. Procesos forenses con ChatGPT para la identificación de evidencias

- 24.1.1. Conceptos básicos de análisis forense en entornos digitales
- 24.1.2. Etapas de identificación y recopilación de evidencias
- 24.1.3. Rol de ChatGPT en el apoyo a la identificación forense

24.2. Gemini y ChatGPT en la identificación y extracción de datos

- 24.2.1. Fundamentos de extracción de datos para análisis forense
- 24.2.2. Técnicas de identificación de datos relevantes
- 24.2.3. Contribución de la Inteligencia Artificial en la automatización del proceso de extracción

24.3. Análisis de logs y correlación de eventos con Inteligencia Artificial

- 24.3.1. Importancia de los logs en el análisis de incidentes
- 24.3.2. Técnicas de correlación de eventos para reconstruir incidentes
- 24.3.3. Uso de Inteligencia Artificial para identificar patrones en la correlación de logs

24.4. Recuperación de datos y restauración de sistemas usando Inteligencia Artificial

- 24.4.1. Principios de recuperación de datos y su importancia en forense digital
- 24.4.2. Técnicas de restauración de sistemas comprometidos
- 24.4.3. Aplicación de Inteligencia Artificial para mejorar los procesos de recuperación y restauración

24.5. Machine Learning para detección y reconstrucción de incidentes

- 24.5.1. Introducción a *Machine Learning* en la detección de incidentes
- 24.5.2. Técnicas de reconstrucción de incidentes con modelos de Inteligencia Artificial
- 24.5.3. Consideraciones éticas y prácticas en la detección de eventos

24.6. Reconstrucción de incidentes y simulación con ChatGPT

- 24.6.1. Fundamentos de la reconstrucción de incidentes en análisis forense
- 24.6.2. Capacidad de ChatGPT para crear simulaciones de incidentes
- 24.6.3. Limitaciones y desafíos en la simulación de incidentes complejos

24.7. Detección de actividades maliciosas en dispositivos móviles

- 24.7.1. Características y desafíos en el análisis forense de dispositivos móviles
- 24.7.2. Principales actividades maliciosas en entornos móviles
- 24.7.3. Aplicación de Inteligencia Artificial para identificar amenazas en dispositivos móviles

24.8. Respuesta automatizada a incidentes con flujos de trabajo Inteligencia Artificial

- 24.8.1. Principios de respuesta a incidentes en Ciberseguridad
- 24.8.2. Importancia de la automatización en la respuesta rápida a incidentes
- 24.8.3. Beneficios de los flujos de trabajo asistidos por Inteligencia Artificial en la mitigación

24.9. Ética y transparencia en el análisis forense con Inteligencia Artificial generativa

- 24.9.1. Principios éticos en el uso de Inteligencia Artificial en análisis forense
- 24.9.2. Transparencia y explicabilidad de modelos generativos en forense
- 24.9.3. Consideraciones sobre privacidad y responsabilidad en el análisis

24.10. Laboratorio de análisis forense y recreación de incidentes con ChatGPT y Gemini

- 24.10.1. Estructura y objetivos de un laboratorio de análisis forense
- 24.10.2. Beneficios de los entornos controlados para la práctica forense
- 24.10.3. Componentes clave para la creación de un laboratorio de simulación

Asignatura 25

Modelos predictivos de defensa proactiva en Ciberseguridad usando ChatGPT

25.1. Análisis predictivo en Ciberseguridad: técnicas y aplicaciones con Inteligencia Artificial

- 25.1.1. Conceptos básicos de análisis predictivo en seguridad
- 25.1.2. Técnicas de predicción en el ámbito de Ciberseguridad
- 25.1.3. Aplicación de Inteligencia Artificial en la anticipación de ciberamenazas

25.2. Modelos de regresión y clasificación con soporte de ChatGPT

- 25.2.1. Principios de regresión y clasificación en predicción de amenazas
- 25.2.2. Tipos de modelos de clasificación en Ciberseguridad
- 25.2.3. Asistencia de ChatGPT en la interpretación de modelos predictivos

25.3. Identificación de amenazas emergentes con predicciones de ChatGPT

- 25.3.1. Conceptos de detección de amenazas emergentes
- 25.3.2. Técnicas de identificación de nuevos patrones de ataque
- 25.3.3. Limitaciones y precauciones en la predicción de nuevas amenazas



25.4. Redes neuronales para anticipación de ataques cibernéticos

- 25.4.1. Fundamentos de redes neuronales aplicadas en Ciberseguridad
- 25.4.2. Arquitecturas comunes para detección y predicción de ataques
- 25.4.3. Desafíos en la implementación de redes neuronales en defensa cibernética

25.5. Uso de ChatGPT para simulaciones de escenarios de amenaza

- 25.5.1. Conceptos básicos de simulación de amenazas en Ciberseguridad
- 25.5.2. Capacidades de ChatGPT para desarrollar simulaciones predictivas
- 25.5.3. Factores a considerar en el diseño de escenarios simulados

25.6. Algoritmos de aprendizaje por refuerzo para optimización de defensas

- 25.6.1. Introducción al aprendizaje por refuerzo en Ciberseguridad
- 25.6.2. Algoritmos de refuerzo aplicados a estrategias de defensa
- 25.6.3. Beneficios y retos del aprendizaje por refuerzo en entornos de Ciberseguridad

25.7. Simulación de amenazas y respuestas con ChatGPT

- 25.7.1. Principios de simulación de amenazas y su relevancia en ciberdefensa
- 25.7.2. Respuestas automatizadas y optimizadas ante ataques simulados
- 25.7.3. Beneficios de la simulación para mejorar la preparación cibernética

25.8. Evaluación de precisión y efectividad en modelos predictivos de Inteligencia Artificial

- 25.8.1. Indicadores clave para la evaluación de modelos predictivos
- 25.8.2. Metodologías de evaluación de precisión en modelos de Ciberseguridad
- 25.8.3. Factores críticos en la efectividad de los modelos de Inteligencia Artificial en Ciberseguridad

25.9. Inteligencia Artificial en la gestión de incidentes y respuestas automatizadas

- 25.9.1. Fundamentos de la gestión de incidentes en Ciberseguridad
- 25.9.2. Rol de la Inteligencia Artificial en la toma de decisiones en tiempo real
- 25.9.3. Desafíos y oportunidades en la automatización de respuestas

25.10. Creación de un sistema de defensa predictivo con soporte de ChatGPT

- 25.10.1. Principios de diseño de sistemas de defensa proactiva
- 25.10.2. Integración de modelos predictivos en entornos de Ciberseguridad
- 25.10.3. Componentes clave para un sistema de defensa predictivo basado en Inteligencia Artificial

04

Convalidación de asignaturas

Si el candidato a estudiante ha cursado otra titulación universitaria de la misma rama de conocimiento o un programa equivalente al presente, incluso si solo lo cursó parcialmente y no lo finalizó, TECH le facilitará la realización de un **Estudio de Convalidaciones** que le permitirá no tener que examinarse de aquellas asignaturas que hubiera superado con éxito anteriormente.



“

Si tienes estudios susceptibles de convalidación, TECH te ayudará en el trámite para que sea rápido y sencillo”

Cuando el candidato a estudiante desee conocer si se le valorará positivamente el estudio de convalidaciones de su caso, deberá solicitar una **Opinión Técnica de Convalidación de Asignaturas** que le permita decidir si le es de interés matricularse en el programa de Grand Master Oficial Universitario.

La Comisión Académica de TECH valorará cada solicitud y emitirá una resolución inmediata para facilitar la decisión de la matriculación. Tras la matrícula, el estudio de convalidaciones facilitará que el estudiante consolide sus asignaturas ya cursadas en otros programas universitarios oficiales en su expediente académico sin tener que evaluarse de nuevo de ninguna de ellas, obteniendo en menor tiempo, los títulos que componen este programa de Grand Master Oficial Universitario.

TECH le facilita a continuación toda la información relativa a este procedimiento:



Convalida tus estudios realizados y no tendrás que evaluarte de las asignaturas superadas”



¿Qué es la convalidación de estudios?

La convalidación de estudios es el trámite por el cual la Comisión Académica de TECH equipara estudios realizados de forma previa, a las asignaturas del programa tras la realización de un análisis académico de comparación. Serán susceptibles de convalidación aquellos contenidos cursados en un plan o programa de estudio oficial universitario o de nivel superior, y que sean equiparables con asignaturas del plan de estudios de este Grand Master Oficial Universitario de TECH. Las asignaturas indicadas en el documento de Opinión Técnica de Convalidación de Asignaturas quedarán consolidadas en el expediente del estudiante con la leyenda “EQ” en el lugar de la calificación, por lo que no tendrá que cursarlas de nuevo.



¿Qué es la Opinión Técnica de Convalidación de Asignaturas?

La Opinión Técnica de Convalidación de Asignaturas es el documento emitido por la Comisión Académica tras el análisis de equiparación de los estudios presentados; en este, se dictamina el reconocimiento de los estudios anteriores realizados, indicando qué plan de estudios le corresponde, así como las asignaturas y calificaciones obtenidas, como resultado del análisis del expediente del alumno. La Opinión Técnica de Convalidación de Asignaturas será vinculante en el momento en que el candidato se matricule en el programa, causando efecto en su expediente académico las convalidaciones que en ella se resuelvan. El dictamen de la Opinión Técnica de Convalidación de Asignaturas será inapelable.



¿Cómo se solicita la Opinión Técnica de Convalidación de Asignaturas?

El candidato deberá enviar una solicitud a la dirección de correo electrónico convalidaciones@techtitute.com adjuntando toda la documentación necesaria para la realización del estudio de convalidaciones y emisión de la opinión técnica. Asimismo, tendrá que abonar el importe correspondiente a la solicitud indicado en el apartado de Preguntas Frecuentes del portal web de TECH. En caso de que el alumno se matricule en el Grand Master Oficial Universitario, este pago se le descontará del importe de la matrícula y por tanto el estudio de opinión técnica para la convalidación de estudios será gratuito para el alumno.



¿Qué documentación necesitará incluir en la solicitud?

La documentación que tendrá que recopilar y presentar será la siguiente:

- Documento de identificación oficial
- Certificado de estudios, o documento equivalente que ampare los estudios realizados. Este deberá incluir, entre otros puntos, los periodos en que se cursaron los estudios, las asignaturas, las calificaciones de las mismas y, en su caso, los créditos. En caso de que los documentos que posea el interesado y que, por la naturaleza del país, los estudios realizados carezcan de listado de asignaturas, calificaciones y créditos, deberán acompañarse de cualquier documento oficial sobre los conocimientos adquiridos, emitido por la institución donde se realizaron, que permita la comparabilidad de estudios correspondiente



¿En qué plazo se resolverá la solicitud?

La opinión técnica se llevará a cabo en un plazo máximo de 48h desde que el interesado abone el importe del estudio y envíe la solicitud con toda la documentación requerida. En este tiempo la Comisión Académica analizará y resolverá la solicitud de estudio emitiendo una Opinión Técnica de Convalidación de Asignaturas que será informada al interesado mediante correo electrónico. Este proceso será rápido para que el estudiante pueda conocer las posibilidades de convalidación que permita el marco normativo para poder tomar una decisión sobre la matriculación en el programa.



¿Será necesario realizar alguna otra acción para que la Opinión Técnica se haga efectiva?

Una vez realizada la matrícula, deberá cargar en el campus virtual el informe de opinión técnica y el departamento de Secretaría Académica consolidará las convalidaciones en su expediente académico. En cuanto las asignaturas le queden convalidadas en el expediente, el estudiante quedará eximido de realizar la evaluación de estas, pudiendo consultar los contenidos con libertad sin necesidad de hacer los exámenes.

Procedimiento paso a paso





Convalida tus estudios realizados y no tendrás que evaluarte de las asignaturas superadas.

05

Objetivos docentes

El objetivo docente de este programa es brindar a los profesionales un conjunto integral de competencias que les permita comprender, gestionar y anticipar riesgos en entornos digitales altamente complejos. Por ello, integra conocimientos estratégicos, técnicos y de gestión para respaldar decisiones precisas y fundamentadas. Asimismo, potencia el pensamiento crítico, la ética profesional y el liderazgo, de modo que los participantes puedan diseñar e implementar soluciones efectivas en ciberseguridad. De esta manera, se contribuye a formar perfiles con visión global y capacidad directiva en contextos de elevada exposición al riesgo.

*Living
SUCCESS*





“

Los objetivos académicos de este programa de TECH te ayudarán a convertirte en un directivo empresarial de primer nivel”



Objetivos

Así, el Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) sostiene los siguientes objetivos:

- ♦ Diseñar marcos éticos que orienten la toma de decisiones en entornos digitales complejos
- ♦ Liderar equipos multidisciplinarios con responsabilidad social y sostenibilidad organizacional
- ♦ Formular estrategias corporativas que integren la ciberseguridad como ventaja competitiva
- ♦ Alinear recursos y procesos clave con los objetivos de seguridad y negocio
- ♦ Desarrollar políticas de atracción, retención y capacitación de talento especializado en ciberseguridad
- ♦ Fomentar culturas organizacionales orientadas a la concienciación y responsabilidad digital
- ♦ Evaluar inversiones en ciberseguridad bajo criterios de rentabilidad y control de riesgos
- ♦ Optimizar presupuestos de TI con enfoque en prevención y continuidad operativa
- ♦ Garantizar la seguridad digital en cadenas de suministro conectadas
- ♦ Implementar controles operativos que minimicen vectores de ataque externos
- ♦ Integrar arquitecturas de seguridad en el ciclo de vida de los sistemas de información
- ♦ Gobernar plataformas críticas con enfoque en disponibilidad, integridad y confidencialidad
- ♦ Comunicar el valor de la ciberseguridad como diferencial de marca y confianza
- ♦ Gestionar crisis digitales con estrategias de comunicación institucional efectivas
- ♦ Liderar proyectos de innovación con enfoque ágil y seguro desde su concepción
- ♦ Aplicar metodologías de gestión de riesgos en entornos de alta incertidumbre tecnológica
- ♦ Tomar decisiones estratégicas con visión integral de riesgo, tecnología y negocio
- ♦ Representar la función de seguridad ante consejos directivos y stakeholders clave
- ♦ Resolver un reto real de ciberseguridad con metodología científica y enfoque directivo
- ♦ Demostrar la capacidad de integrar conocimientos técnicos y gerenciales en un proyecto aplicado
- ♦ Desarrollar capacidades de análisis y anticipación de amenazas digitales
- ♦ Aplicar técnicas de inteligencia para la toma de decisiones proactivas en ciberdefensa
- ♦ Asegurar estaciones y servidores frente a malware, exploits y configuraciones vulnerables
- ♦ Implementar políticas de control de acceso y auditoría en sistemas operativos
- ♦ Diseñar arquitecturas de red con controles de seguridad efectivos y resilientes
- ♦ Detectar y mitigar intrusiones en tiempo real en entornos perimetrales
- ♦ Evaluar riesgos en dispositivos móviles y aplicaciones corporativas
- ♦ Aplicar controles de seguridad móvil en entornos BYOD y corporativos
- ♦ Garantizar la protección de dispositivos conectados en ecosistemas críticos
- ♦ Implementar estándares de seguridad en entornos de infraestructura inteligente
- ♦ Identificar vulnerabilidades en sistemas con enfoque ofensivo y legal



- ♦ Proponer contramedidas efectivas a partir de pruebas de penetración controladas
- ♦ Analizar malware y software sospechoso para comprender su comportamiento
- ♦ Desarrollar contramedidas y firmas de detección a partir del análisis de código
- ♦ Aplicar principios de seguridad en el ciclo de desarrollo de software
- ♦ Evaluar código y arquitecturas con enfoque en prevención de vulnerabilidades
- ♦ Recopilar y preservar evidencias digitales con validez legal
- ♦ Reconstruir ataques y establecer líneas de tiempo para respuesta jurídica
- ♦ Analizar tendencias emergentes en ciberamenazas y tecnologías de defensa
- ♦ Proponer estrategias de adaptación ante escenarios de riesgo en evolución
- ♦ Aplicar modelos de lenguaje para el análisis automatizado de amenazas
- ♦ Generar inteligencia accionable a partir de fuentes abiertas y técnicas
- ♦ Desarrollar sistemas de detección de anomalías con IA generativa
- ♦ Reducir falsos positivos y mejorar tiempos de respuesta en seguridad
- ♦ Diseñar esquemas criptográficos robustos con apoyo de IA
- ♦ Evaluar la resistencia de algoritmos ante ataques cuánticos y avanzados
- ♦ Automatizar análisis de evidencias digitales con herramientas de IA
- ♦ Reducir tiempos de investigación y aumentar la precisión forense
- ♦ Construir modelos predictivos de ataques con apoyo de IA generativa
- ♦ Anticipar campañas de amenazas y diseñar contramedidas preventivas

06

Salidas profesionales

Este programa prepara profesionales para responder a la creciente demanda de expertos en la gestión y protección de sistemas de información en entornos digitales complejos. En consecuencia, los egresados pueden asumir roles estratégicos como CISO, consultor en ciberseguridad, analista de riesgos o gestor de proyectos tecnológicos. Además, se integran en organizaciones públicas y privadas que requieren liderazgo en seguridad, cumplimiento normativo y protección de infraestructuras críticas, aportando una visión global y capacidad de decisión.

Upgrading...



“

Estarás preparado para asumir roles ejecutivos como CISO más exigentes del mercado laboral”

Perfil del egresado

Este triple postgrado con especialización en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) prepara a los profesionales de informática para liderar la seguridad de la información en organizaciones de todos los sectores, convirtiéndolos en actores clave frente a las crecientes amenazas cibernéticas. Con un enfoque en estrategias avanzadas, cumplimiento normativo y herramientas como OSINT, desarrollan habilidades para proteger activos digitales, garantizar la resiliencia organizacional y acceder a roles estratégicos como CISO, Director de Seguridad, Consultor en Ciberseguridad o Auditor de Seguridad.

Diseñarás e implementarás infraestructuras de seguridad robustas que protejan los datos y sistemas de las organizaciones.

- ♦ **Liderazgo y gestión de equipos:** Será capaz de dirigir y motivar equipos multidisciplinarios en entornos complejos
- ♦ **Toma de decisiones estratégicas:** Analizará datos y tomar decisiones que impulsen el crecimiento organizacional
- ♦ **Visión global del negocio:** Dispondrá de conocimiento integral de las áreas clave de la empresa, desde finanzas hasta marketing
- ♦ **Adaptabilidad e innovación:** Estará preparado para enfrentar cambios y fomentar la innovación dentro de la organización
- ♦ **Comunicación efectiva:** Adquirirá un dominio holístico de las habilidades comunicativas esenciales para la negociación y la presentación de ideas

En definitiva, después de realizar este triple posgrado, los egresados podrán desempeñar sus conocimientos y habilidades en:

1. Chief Executive Officer (CEO): líder de la estrategia global de ciberseguridad para alinear los objetivos empresariales con la protección digital y toma decisiones clave sobre la asignación de recursos.

Responsabilidades: Desarrollo de estrategias de ciberseguridad, toma de decisiones sobre inversiones en seguridad, y supervisión general de la protección digital de la empresa.

2. Chief Financial Officer (CFO): supervisor del presupuesto destinado a ciberseguridad, asegurando que las inversiones en protección de la información sean rentables.

Responsabilidades: Gestión del presupuesto de ciberseguridad, evaluación de rentabilidad de inversiones en seguridad, y asignación de recursos financieros.

3. Chief Information Security Officer (CISO): encargado de diseñar y ejecutar la estrategia de seguridad de la información para proteger los activos empresariales de amenazas cibernéticas.

Responsabilidades: Desarrollo de políticas de seguridad, gestión de riesgos cibernéticos, y protección de los activos informáticos.

4. Director de Operaciones: coordinador en la implementación de políticas y procedimientos de ciberseguridad en las operaciones diarias para asegurar la protección continua.

Responsabilidades: Supervisión de la aplicación de medidas de seguridad, integración de prácticas de ciberseguridad en las operaciones, y garantía de protección diaria.

5. Director de Marketing: responsable de manejar la comunicación y percepción de la ciberseguridad de la empresa en el mercado, promoviendo prácticas seguras y fomentando la confianza del cliente.

Responsabilidades: Gestión de la imagen de seguridad, comunicación de políticas de protección al público, y promoción de la confianza del cliente en las prácticas de ciberseguridad.

- 6. Director de Recursos Humanos:** encargado de la formación y sensibilización en ciberseguridad del personal, garantizando que se cumplan las políticas de seguridad.
Responsabilidades: Formación en seguridad para empleados, supervisión del cumplimiento de políticas de ciberseguridad, y gestión de la sensibilización en protección digital.
- 7. Incident Manager:** coordinador de la respuesta a incidentes de seguridad, gestionando la identificación, contención, erradicación y recuperación de ataques cibernéticos.
Responsabilidades: Gestión de incidentes de seguridad, coordinación de la respuesta a ataques, y recuperación de sistemas afectados.
- 8. Compliance Officer:** encargado de asegurar que las prácticas de ciberseguridad cumplan con las normativas y regulaciones legales y de la industria aplicables.
Responsabilidades: Verificación del cumplimiento normativo en ciberseguridad, desarrollo de prácticas conforme a regulaciones, y auditorías de seguridad.
- 9. Analista de Ciberseguridad:** gestor de monitorear, analizar y responder a amenazas y vulnerabilidades para proteger los sistemas y datos de la organización.
Responsabilidades: Vigilancia de amenazas, análisis de vulnerabilidades, y respuesta a incidentes de seguridad.
- 10. Investigador de Ciberseguridad:** líder de realizar investigaciones detalladas sobre incidentes de seguridad y vulnerabilidades, desarrollando nuevas técnicas para mejorar la protección de la información.
Responsabilidades: Investigación de incidentes de seguridad, desarrollo de técnicas de protección, y análisis de vulnerabilidades avanzadas.

Salidas académicas y de investigación

Además de todos los puestos laborales para los que serás apto mediante el estudio de este Grand Master Oficial Universitario de TECH, también podrás continuar con una sólida trayectoria académica e investigativa. Tras completar este programa universitario, estarás listo para continuar con tus estudios desarrollando un Doctorado asociado a esta área de conocimiento y así, progresivamente, alcanzar otros méritos científicos.



Esta es la oportunidad académica que estabas esperando para impulsar tu carrera profesional”

07

Idiomas gratuitos

Convencidos de que la formación en idiomas es fundamental en cualquier profesional para lograr una comunicación potente y eficaz, TECH ofrece un itinerario complementario al plan de estudios curricular, en el que el alumno, además de adquirir las competencias de este triple posgrado podrá aprender idiomas de un modo sencillo y práctico.

*Acredita tu
competencia
lingüística*



“

TECH te incluye el estudio de idiomas en este triple posgrado de forma ilimitada y gratuita”

En el mundo competitivo actual, hablar otros idiomas forma parte clave de nuestra cultura moderna. Hoy en día, resulta imprescindible disponer de la capacidad de hablar y comprender otros idiomas, además de lograr un título oficial que acredite y reconozca las competencias lingüísticas adquiridas. De hecho, ya son muchos los colegios, las universidades y las empresas que solo aceptan a candidatos que certifican su nivel mediante un título oficial en base al Marco Común Europeo de Referencia para las Lenguas (MCER).

El Marco Común Europeo de Referencia para las Lenguas es el máximo sistema oficial de reconocimiento y acreditación del nivel del alumno. Aunque existen otros sistemas de validación, estos proceden de instituciones privadas y, por tanto, no tienen validez oficial. El MCER establece un criterio único para determinar los distintos niveles de dificultad de los cursos y otorga los títulos reconocidos sobre el nivel de idioma que se posee.

En TECH se ofrecen los únicos cursos intensivos de preparación para la obtención de certificaciones oficiales de nivel de idiomas, basados 100% en el MCER. Los 48 Cursos de Preparación de Nivel Idiomático que tiene la Escuela de Idiomas de TECH están desarrollados con base en las últimas tendencias metodológicas de aprendizaje en línea, el enfoque orientado a la acción y el enfoque de adquisición de competencia lingüística, con la finalidad de preparar los exámenes oficiales de certificación de nivel.

El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

“

Solo el coste de los Cursos de Preparación de idiomas y los exámenes de certificación, que puedes llegar a hacer gratis, valen más de 3 veces el precio total de este itinerario académico”

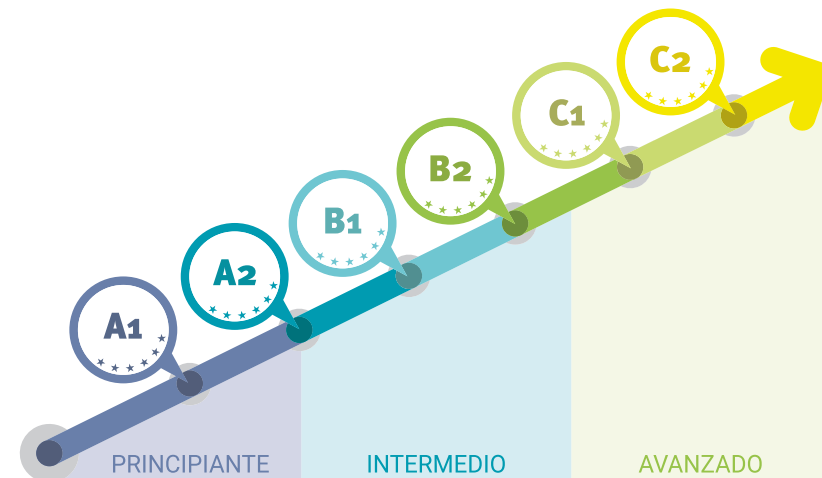




TECH incorpora, como contenido extracurricular al plan de estudios oficial, la posibilidad de que el alumno estudie idiomas, seleccionando aquellos que más le interesen de entre la gran oferta disponible:

- Podrá elegir los Cursos de Preparación de Nivel de los idiomas y nivel que desee, de entre los disponibles en la Escuela de Idiomas de TECH, mientras estudie el Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer), para poder prepararse el examen de certificación de nivel
- En cada programa de idiomas tendrá acceso a todos los niveles MCER, desde el nivel A1 hasta el nivel C2
- Cada año podrá presentarse a un examen telepresencial de certificación de nivel, con un profesor nativo experto. Al terminar el examen, TECH le expedirá un certificado de nivel de idioma
- Estudiar idiomas NO aumentará el coste del programa. El estudio ilimitado y la certificación anual de cualquier idioma están incluidas en este triple posgrado

“ 48 Cursos de Preparación de Nivel para la certificación oficial de 8 idiomas en los niveles MCER A1, A2, B1, B2, C1 y C2”



08

Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los **case studies** con el **Relearning**, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

*Excelencia.
Flexibilidad.
Vanguardia.*



“

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera”

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

“

*En TECH NO tendrás clases en directo
(a las que luego nunca puedes asistir)”*



Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

“

El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”

Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.



Método Relearning

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

El Relearning te permitirá aprender con menos esfuerzo y más rendimiento, implicándote más en tu especialización, desarrollando el espíritu crítico, la defensa de argumentos y el contraste de opiniones: una ecuación directa al éxito.



Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.



La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios”

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos según el índice global score, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.



Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:



Material de estudio

Todos los contenidos didácticos son creados por los especialistas que van a impartir el curso, específicamente para él, de manera que el desarrollo didáctico sea realmente específico y concreto.

Estos contenidos son aplicados después al formato audiovisual que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.



Prácticas de habilidades y competencias

Realizarás actividades de desarrollo de competencias y habilidades específicas en cada área temática. Prácticas y dinámicas para adquirir y desarrollar las destrezas y habilidades que un especialista precisa desarrollar en el marco de la globalización que vivimos.



Resúmenes interactivos

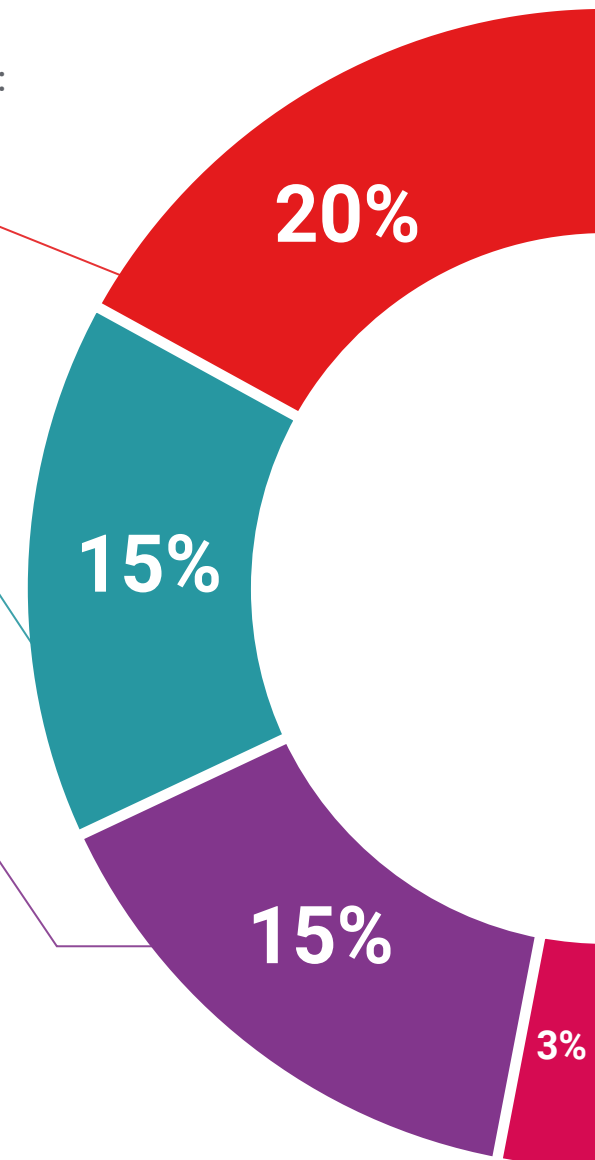
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

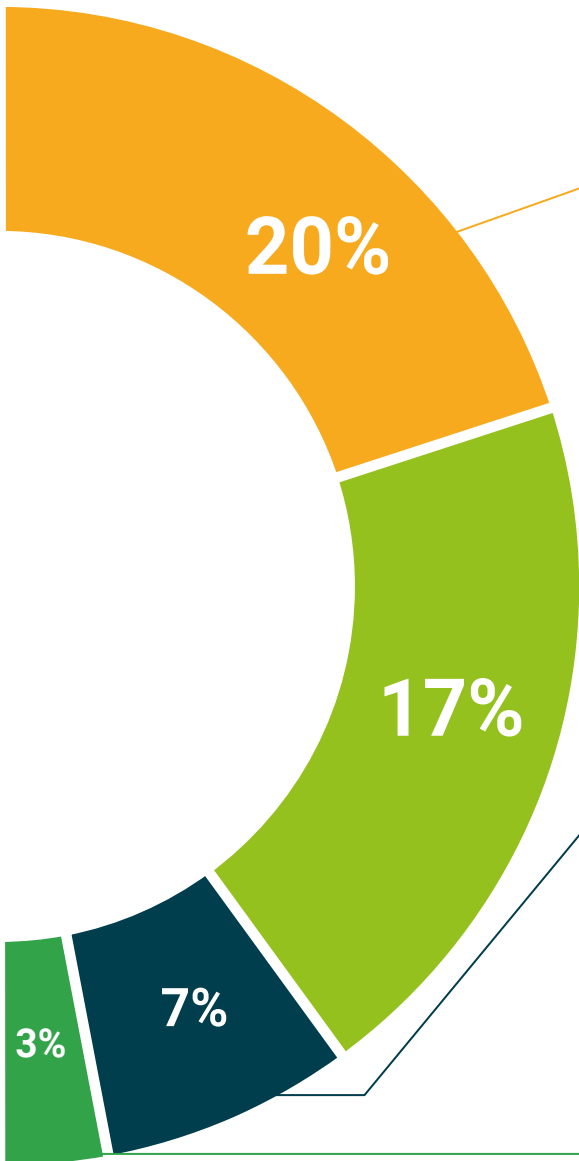
Este sistema exclusivo educativo para la presentación de contenidos multimedia fue premiado por Microsoft como "Caso de éxito en Europa".



Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.



Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.



Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos. El denominado *Learning from an expert* afianza el conocimiento y el recuerdo, y genera seguridad en nuestras futuras decisiones difíciles.



Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.



Modelo asincrónico

El modelo metodológico de TECH se estructura sobre una dinámica asíncrona que permite a los estudiantes marcar su propio ritmo de aprendizaje. Desde el inicio de su matrícula, cada estudiante dispone de todos los recursos necesarios para abordar los contenidos y alcanzar los objetivos de cada asignatura, sin depender de clases magistrales. A través de materiales pedagógicos interactivos, actividades prácticas y un seguimiento personalizado, se favorece un estudio autónomo riguroso que se adapta a las necesidades individuales y promueve un aprendizaje profundo, sostenido por tutorías flexibles y una evaluación continua.

Los estudiantes dispondrán de sesiones sincrónicas estratégicas que les permitirán interactuar directamente con el personal docente. Estas sesiones, están orientadas a resolver dudas, guiar procesos formativos, retroalimentar actividades de desarrollo práctico y acompañar la realización de prácticas externas y la elaboración de trabajos finales de titulación. Tanto las tutorías sincrónicas como asincrónicas se desarrollan en entornos virtuales, lo que permite un acompañamiento cercano sin perder la flexibilidad que caracteriza al modelo.

Competencias de trabajo colaborativo

El desarrollo de competencias profesionales en los estudiantes se refuerza a través de dinámicas de trabajo colaborativo. El modelo de TECH promueve el trabajo en equipo mediante actividades orientadas al desarrollo de habilidades comunicativas, de liderazgo y de resolución conjunta de problemas, todas ellas esenciales en los entornos laborales actuales. La participación en espacios de colaboración ya sea en foros virtuales, desarrollo de proyectos o actividades de desarrollo práctico, permite generar experiencias de aprendizaje que enriquecen la formación individual y complementan el estudio autónomo con perspectivas diversas.





Secuencia cronológica y progresiva

La estructura del plan de estudios se basa en un diseño secuencial y progresivo, en el que cada asignatura se cursa de forma individual y consecutiva. Este enfoque permite al estudiante enfocarse en una asignatura a la vez, facilitando una comprensión profunda de los contenidos y una dedicación completa a las actividades formativas relacionadas. Además, el sistema de matriculación continua ofrece la posibilidad de iniciar los estudios en cualquier momento del año, con un calendario académico personalizado, lo que asegura una progresión ordenada y coherente sin perder la flexibilidad ni la adaptabilidad que caracterizan al modelo.

La evaluación de cada asignatura se llevará a cabo a través de trabajos, actividades, ejercicios y exámenes. Cada asignatura tendrá un examen final que se realizará 100% online, bajo la supervisión de un programa de *proctoring* que monitorizará el dispositivo que emplee el estudiante para garantizar que no hay fraude académico.

Asignaturas impartidas en inglés

El plan de estudios incorpora una dimensión internacional mediante la oferta de asignaturas impartidas íntegramente en lengua inglesa, lo que permite a los estudiantes desarrollar competencias lingüísticas avanzadas y familiarizarse con la terminología específica de su área en un contexto académico bilingüe. Para cursarlas, es necesario dominar el idioma inglés a un nivel mínimo de B1 del marco europeo de referencia de las lenguas, lo que garantiza que los estudiantes puedan seguir el contenido y desarrollar su aprendizaje a nivel académico de forma adecuada. Esta formación multilingüe constituye un valor estratégico que amplía las oportunidades profesionales y fortalece la proyección internacional del título.

En caso de que el estudiante no disponga de un nivel de inglés B1, TECH Universidad le ofrecerá clases particulares y cursos de inglés para perfeccionar el idioma y poder abordar los contenidos con soltura.

09

Cuadro docente

El equipo docente del Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) está compuesto por profesionales altamente cualificados en estos ámbitos. Gracias a su experiencia, han desarrollado materiales didácticos de elevada calidad, totalmente alineados con las exigencias del mercado laboral actual. De este modo, los profesionales de informática se sumergirán en una experiencia formativa intensiva que les permitirá alcanzar un progreso significativo y tangible en sus trayectorias profesionales.



“

Un equipo docente conformado por expertos en Dirección de Ciberseguridad te guiará durante todo el itinerario académico”

Director Invitado Internacional

El Doctor Frederic Lemieux es reconocido a nivel internacional como experto innovador y líder inspirador en los campos de la **Inteligencia, Seguridad Nacional, Seguridad Interna, Ciberseguridad y Tecnologías Disruptivas**. Y es que su constante dedicación y relevantes aportaciones en Investigación y Educación, le posicionan como una figura clave en la **promoción de la seguridad** y el **entendimiento de las tecnologías emergentes** en la actualidad. Durante su trayectoria profesional, ha conceptualizado y dirigido programas académicos de vanguardia en diversas instituciones de renombre, como la **Universidad de Montreal, la Universidad George Washington** y la **Universidad de Georgetown**.

A lo largo de su extenso bagaje, ha publicado múltiples libros de gran relevancia, todos ellos relacionados con la **inteligencia criminal, la labor policial, las amenazas cibernéticas** y la **seguridad internacional**. Asimismo, ha contribuido de manera significativa al campo de la **Ciberseguridad** con la publicación de numerosos artículos en revistas académicas, las cuales examinan el control del crimen durante desastres importantes, la lucha contra el terrorismo, las agencias de inteligencia y la cooperación policial. Además, ha sido panelista y ponente principal en diversas conferencias nacionales e internacionales, consolidándose como un referente en el ámbito académico y profesional.

El Doctor Lemieux ha desempeñado roles editoriales y evaluativos en diferentes organizaciones académicas, privadas y gubernamentales, reflejando su influencia y compromiso con la excelencia en su campo de especialización. De esta forma, su prestigiosa carrera académica lo ha llevado a desempeñarse como Profesor de Prácticas y Director de Facultad de los programas MPS en **Inteligencia Aplicada, Gestión de Riesgos en Ciberseguridad, Gestión Tecnológica** y **Gestión de Tecnologías de la Información** en la **Universidad de Georgetown**.



Dr. Lemieux, Frederic

- Director del Máster en Cybersecurity Risk Management en Georgetown, Washington, Estados Unidos
- Director del Máster en Technology Management en la Universidad de Georgetown
- Director del Máster en Applied Intelligence en la Universidad de Georgetown
- Profesor de Prácticas en la Universidad de Georgetown
- Doctor en Criminología por la School of Criminology en la Universidad de Montreal
- Licenciado en Sociología y Minor Degree en Psicología por la Universidad de Laval
- Miembro de New Program Roundtable Committee, Universidad de Georgetown

“

Gracias a TECH podrás aprender con los mejores profesionales del mundo”

Directora Invitada Internacional

Con más de 20 años de experiencia en el diseño y la dirección de equipos globales de **adquisición de talento**, Jennifer Dove es experta en **contratación** y **estrategia tecnológica**. A lo largo de su experiencia profesional ha ocupado puestos directivos en varias organizaciones tecnológicas dentro de empresas de la lista **Fortune 50**, como **NBCUniversal** y **Comcast**. Su trayectoria le ha permitido destacar en entornos competitivos y de alto crecimiento.

Como **Vicepresidenta de Adquisición de Talento** en **Mastercard**, se encarga de supervisar la estrategia y la ejecución de la incorporación de talento, colaborando con los líderes empresariales y los responsables de **Recursos Humanos** para cumplir los objetivos operativos y estratégicos de contratación. En especial, su finalidad es **crear equipos diversos, inclusivos y de alto rendimiento** que impulsen la innovación y el crecimiento de los productos y servicios de la empresa. Además, es experta en el uso de herramientas para atraer y retener a los mejores profesionales de todo el mundo. También se encarga de **amplificar la marca de empleador** y la propuesta de valor de **Mastercard** a través de publicaciones, eventos y redes sociales.

Jennifer Dove ha demostrado su compromiso con el desarrollo profesional continuo, participando activamente en redes de profesionales de **Recursos Humanos** y contribuyendo a la incorporación de numerosos trabajadores a diferentes empresas. Tras obtener su licenciatura en **Comunicación Organizacional** por la Universidad de **Miami**, ha ocupado cargos directivos de selección de personal en empresas de diversas áreas.

Por otra parte, ha sido reconocida por su habilidad para liderar transformaciones organizacionales, **integrar tecnologías** en los **procesos de reclutamiento** y desarrollar programas de liderazgo que preparan a las instituciones para los desafíos futuros. También ha implementado con éxito programas de **bienestar laboral** que han aumentado significativamente la satisfacción y retención de empleados.



Dña. Dove, Jennifer

- Vicepresidenta de Adquisición de Talentos en Mastercard, Nueva York, Estados Unidos
- Directora de Adquisición de Talentos en NBCUniversal Media, Nueva York, Estados Unidos
- Responsable de Selección de Personal Comcast
- Directora de Selección de Personal en Rite Hire Advisory
- Vicepresidenta Ejecutiva de la División de Ventas en Ardor NY Real Estate
- Directora de Selección de Personal en Valerie August & Associates
- Ejecutiva de Cuentas en BNC
- Ejecutiva de Cuentas en Vault
- Graduada en Comunicación Organizacional por la Universidad de Miami



Expertos de prestigio internacional te brindarán una revisión holística de las innovaciones más importantes a día de hoy en el mundo directivo y de los negocios”

Director Invitado Internacional

Líder tecnológico con décadas de experiencia en las principales multinacionales tecnológicas, Rick Gauthier se ha desarrollado de forma prominente en el campo de los servicios en la nube y mejora de procesos de extremo a extremo. Ha sido reconocido como un líder y responsable de equipos con gran eficiencia, mostrando un talento natural para garantizar un alto nivel de compromiso entre sus trabajadores.

Posee dotes innatas en la estrategia e innovación ejecutiva, desarrollando nuevas ideas y respaldando su éxito con datos de calidad. Su trayectoria en **Amazon** le ha permitido administrar e integrar los servicios informáticos de la compañía en Estados Unidos. En **Microsoft** ha liderado un equipo de 104 personas, encargadas de proporcionar infraestructura informática a nivel corporativo y apoyar a departamentos de ingeniería de productos en toda la compañía.

Esta experiencia le ha permitido destacarse como un directivo de alto impacto, con habilidades notables para aumentar la eficiencia, productividad y satisfacción general del cliente.



D. Gauthier, Rick

- Director regional de IT en Amazon, Seattle, Estados Unidos
- Jefe de programas sénior en Amazon
- Vicepresidente de Wimmer Solutions
- Director sénior de servicios de ingeniería productiva en Microsoft
- Titulado en Ciberseguridad por Western Governors University
- Certificado Técnico en *Commercial Diving* por Divers Institute of Technology
- Titulado en Estudios Ambientales por The Evergreen State College

“

Aprovecha la oportunidad para conocer los últimos avances en esta materia para aplicarla a tu práctica diaria”

Director Invitado Internacional

Romi Arman es un reputado experto internacional con más de dos décadas de experiencia en **Transformación Digital, Marketing, Estrategia y Consultoría**. A través de esa extendida trayectoria, ha asumido diferentes riesgos y es un permanente **defensor** de la **innovación** y el **cambio** en la coyuntura empresarial. Con esa experticia, ha colaborado con directores generales y organizaciones corporativas de todas partes del mundo, empujándoles a dejar de lado los modelos tradicionales de negocios. Así, ha contribuido a que compañías como la energética Shell se conviertan en **verdaderos líderes del mercado**, centradas en sus **clientes** y el **mundo digital**.

Las estrategias diseñadas por Arman tienen un impacto latente, ya que han permitido a varias corporaciones **mejorar las experiencias de los consumidores, el personal y los accionistas** por igual. El éxito de este experto es cuantificable a través de métricas tangibles como el **CSAT**, el **compromiso de los empleados** en las instituciones donde ha ejercido y el crecimiento del **indicador financiero EBITDA** en cada una de ellas.

También, en su recorrido profesional ha nutrido y **liderado equipos de alto rendimiento** que, incluso, han recibido galardones por su **potencial transformador**. Con Shell, específicamente, el ejecutivo se ha propuesto siempre superar tres retos: **satisfacer** las complejas **demandas de descarbonización** de los clientes, **apoyar** una “**descarbonización rentable**” y **revisar** un panorama fragmentado de **datos, digital y tecnológico**. Así, sus esfuerzos han evidenciado que para lograr un éxito sostenible es fundamental partir de las necesidades de los consumidores y sentar las bases de la transformación de los procesos, los datos, la tecnología y la cultura.

Por otro lado, el directivo destaca por su dominio de las **aplicaciones empresariales** de la **Inteligencia Artificial**, temática en la que cuenta con un posgrado de la Escuela de Negocios de Londres. Al mismo tiempo, ha acumulado experiencias en **IoT** y el **Salesforce**.



D. Arman, Romi

- Director de Transformación Digital (CDO) en la Corporación Energética Shell, Londres, Reino Unido
- Director Global de Comercio Electrónico y Atención al Cliente en la Corporación Energética Shell
- Gestor Nacional de Cuentas Clave (fabricantes de equipos originales y minoristas de automoción) para Shell en Kuala Lumpur, Malasia
- Consultor Sénior de Gestión (Sector Servicios Financieros) para Accenture desde Singapur
- Licenciado en la Universidad de Leeds
- Posgrado en Aplicaciones Empresariales de la IA para Altos Ejecutivos de la Escuela de Negocios de Londres
- Certificación Profesional en Experiencia del Cliente CCXP
- Curso de Transformación Digital Ejecutiva por IMD



¿Deseas actualizar tus conocimientos con la más alta calidad educativa? TECH te ofrece el contenido más actualizado del mercado académico, diseñado por auténticos expertos de prestigio internacional”

Director Invitado Internacional

Manuel Arens es un **experimentado profesional** en el manejo de datos y líder de un equipo altamente cualificado. De hecho, Arens ocupa el cargo de **gerente global de compras** en la división de Infraestructura Técnica y Centros de Datos de Google, empresa en la que ha desarrollado la mayor parte de su carrera profesional. Con base en Mountain View, California, ha proporcionado soluciones para los desafíos operativos del gigante tecnológico, tales como la **integridad de los datos maestros**, las **actualizaciones de datos de proveedores** y la **priorización** de los mismos. Ha liderado la planificación de la cadena de suministro de centros de datos y la evaluación de riesgos del proveedor, generando mejoras en el proceso y la gestión de flujos de trabajo que han resultado en ahorros de costos significativos.

Con más de una década de trabajo proporcionando soluciones digitales y liderazgo para empresas en diversas industrias, tiene una amplia experiencia en todos los aspectos de la prestación de soluciones estratégicas, incluyendo **Marketing**, **análisis de medios**, **medición** y **atribución**. De hecho, ha recibido varios reconocimientos por su labor, entre ellos el **Premio al Liderazgo BIM**, el **Premio a la Liderazgo Search**, **Premio al Programa de Generación de Leads de Exportación** y el **Premio al Mejor Modelo de Ventas de EMEA**.

Asimismo, Arens se desempeñó como **Gerente de Ventas** en Dublín, Irlanda. En este puesto, construyó un equipo de 4 a 14 miembros en tres años y lideró al equipo de ventas para lograr resultados y colaborar bien entre sí y con equipos interfuncionales. También ejerció como **Analista Sénior** de Industria, en Hamburgo, Alemania, creando storylines para más de 150 clientes utilizando herramientas internas y de terceros para apoyar el análisis. Desarrolló y redactó informes en profundidad para demostrar su dominio del tema, incluyendo la comprensión de los **factores macroeconómicos** y **políticos/regulatorios** que afectan la adopción y difusión de la tecnología.

También ha liderado equipos en empresas como **Eaton**, **Airbus** y **Siemens**, en los que adquirió valiosa experiencia en gestión de cuentas y cadena de suministro. Destaca especialmente su labor para superar continuamente las expectativas mediante la **construcción de valiosas relaciones con los clientes** y **trabajar de forma fluida con personas en todos los niveles de una organización**, incluyendo stakeholders, gestión, miembros del equipo y clientes. Su enfoque impulsado por los datos y su capacidad para desarrollar soluciones innovadoras y escalables para los desafíos de la industria lo han convertido en un líder prominente en su campo.



D. Arens, Manuel

- Gerente Global de Compras en Google, Mountain View, Estados Unidos
- Responsable principal de Análisis y Tecnología B2B en Google, Estados Unidos
- Director de ventas en Google, Irlanda
- Analista Industrial Sénior en Google, Alemania
- Gestor de cuentas en Google, Irlanda
- Accounts Payable en Eaton, Reino Unido
- Gestor de Cadena de Suministro en Airbus, Alemania

“

¡Apuesta por TECH! Podrás acceder a los mejores materiales didácticos, a la vanguardia tecnológica y educativa, implementados por reconocidos especialistas de renombre internacional en la materia”

Director Invitado Internacional

Andrea La Sala es un experimentado ejecutivo del Marketing cuyos proyectos han tenido un **significativo impacto** en el entorno de la Moda. A lo largo de su exitosa carrera ha desarrollado disímiles tareas relacionadas con **Productos, Merchandising y Comunicación**. Todo ello, ligado a marcas de prestigio como **Giorgio Armani, Dolce&Gabbana, Calvin Klein**, entre otras.

Los resultados de este directivo de **alto perfil internacional** han estado vinculados a su probada capacidad para **synetizar información** en marcos claros y ejecutar **acciones concretas** alineadas a objetivos **empresariales específicos**. Además, es reconocido por su **proactividad y adaptación a ritmos acelerados** de trabajo. A todo ello, este experto adiciona una **fuerte conciencia comercial, visión de mercado** y una **auténtica pasión por los productos**.

Como **Director Global de Marca y Merchandising** en **Giorgio Armani**, ha supervisado disímiles **estrategias de Marketing para ropas y accesorios**. Asimismo, sus tácticas han estado centradas en el **ámbito minorista** y las **necesidades y el comportamiento del consumidor**. Desde este puesto, La Sala también ha sido responsable de configurar la comercialización de productos en diferentes mercados, actuando como **jefe de equipo** en los **departamentos de Diseño, Comunicación y Ventas**.

Por otro lado, en empresas como **Calvin Klein** o el **Gruppo Coin**, ha emprendido proyectos para impulsar la **estructura, el desarrollo y la comercialización de diferentes colecciones**. A su vez, ha sido encargado de crear **calendarios eficaces** para las campañas de compra y venta. Igualmente, ha tenido bajo su dirección los **términos, costes, procesos y plazos de entrega** de diferentes operaciones.

Estas experiencias han convertido a Andrea La Sala en uno de los principales y más cualificados **líderes corporativos** de la **Moda** y el **Lujo**. Una alta capacidad directiva con la que ha logrado implementar de manera eficaz el **posicionamiento positivo de diferentes marcas** y redefinir sus indicadores clave de rendimiento (KPI).



D. La Sala, Andrea

- ♦ Director Global de Marca y Merchandising Armani Exchange en Giorgio Armani, Milán, Italia
- ♦ Director de Merchandising en Calvin Klein
- ♦ Responsable de Marca en Gruppo Coin
- ♦ Brand Manager en Dolce&Gabbana
- ♦ Brand Manager en Sergio Tacchini S.p.A.
- ♦ Analista de Mercado en Fastweb
- ♦ Graduado de Business and Economics en la Università degli Studi del Piemonte Orientale

“

Los profesionales más cualificados y experimentados a nivel internacional te esperan en TECH para ofrecerte una enseñanza de primer nivel, actualizada y basada en la última evidencia científica. ¿A qué esperas para matricularte?”

Director Invitado Internacional

Mick Gram es sinónimo de innovación y excelencia en el campo de la **Inteligencia Empresarial** a nivel internacional. Su exitosa carrera se vincula a puestos de liderazgo en multinacionales como **Walmart** y **Red Bull**. Asimismo, este experto destaca por su visión para **identificar tecnologías emergentes** que, a largo plazo, alcanzan un impacto imperecedero en el entorno corporativo.

Por otro lado, el ejecutivo es considerado un **pionero** en el **empleo de técnicas de visualización de datos** que simplificaron conjuntos complejos, haciéndolos accesibles y facilitadores de la toma de decisiones. Esta habilidad se convirtió en el pilar de su perfil profesional, transformándolo en un deseado activo para muchas organizaciones que apostaban por **recopilar información** y **generar acciones** concretas a partir de ellos.

Uno de sus proyectos más destacados de los últimos años ha sido la **plataforma Walmart Data Cafe**, la más grande de su tipo en el mundo que está anclada en la nube destinada al **análisis de Big Data**. Además, ha desempeñado el cargo de **Director de Business Intelligence** en **Red Bull**, abarcando áreas como **Ventas, Distribución, Marketing** y **Operaciones de Cadena de Suministro**. Su equipo fue reconocido recientemente por su innovación constante en cuanto al uso de la nueva API de Walmart Luminare para **insights** de Compradores y Canales.

En cuanto a su formación, el directivo cuenta con varios **Másteres** y estudios de posgrado en centros de prestigio como la **Universidad de Berkeley**, en Estados Unidos, y la **Universidad de Copenhague**, en Dinamarca. A través de esa actualización continua, el experto ha alcanzado competencias de vanguardia. Así, ha llegado a ser considerado un **líder nato** de la **nueva economía mundial**, centrada en el impulso de los datos y sus posibilidades infinitas.



D. Gram, Mick

- ♦ Director de *Business Intelligence* y Análisis en Red Bull, Los Ángeles, Estados Unidos
- ♦ Arquitecto de soluciones de *Business Intelligence* para Walmart Data Cafe
- ♦ Consultor independiente de *Business Intelligence* y *Data Science*
- ♦ Director de *Business Intelligence* en Capgemini
- ♦ Analista Jefe en Nordea
- ♦ Consultor Jefe de *Business Intelligence* para SAS
- ♦ Executive Education en IA y Machine Learning en UC Berkeley College of Engineering
- ♦ MBA Executive en e-commerce en la Universidad de Copenhague
- ♦ Licenciatura y Máster en Matemáticas y Estadística en la Universidad de Copenhague



¡Estudia en la mejor universidad online del mundo según Forbes! En este MBA tendrás acceso a una amplia biblioteca de recursos multimedia, elaborados por reconocidos docentes de relevancia internacional”

Director Invitado Internacional

Scott Stevenson es un distinguido experto del sector del **Marketing Digital** que, por más de 19 años, ha estado ligado a una de las compañías más poderosas de la industria del entretenimiento, **Warner Bros. Discovery**. En este rol, ha tenido un papel fundamental en la **supervisión de logística y flujos de trabajos creativos** en diversas plataformas digitales, incluyendo redes sociales, búsqueda, *display* y medios lineales.

El liderazgo de este ejecutivo ha sido crucial para impulsar **estrategias de producción en medios pagados**, lo que ha resultado en una notable **mejora** en las **tasas de conversión** de su empresa. Al mismo tiempo, ha asumido otros roles, como el de Director de Servicios de Marketing y Gerente de Tráfico en la misma multinacional durante su antigua gerencia.

A su vez, Stevenson ha estado ligado a la distribución global de videojuegos y **campañas de propiedad digital**. También, fue el responsable de introducir estrategias operativas relacionadas con la formación, finalización y entrega de contenido de sonido e imagen para **comerciales de televisión y trailers**.

Por otro lado, el experto posee una Licenciatura en Telecomunicaciones de la Universidad de Florida y un Máster en Escritura Creativa de la Universidad de California, lo que demuestra su destreza en **comunicación y narración**. Además, ha participado en la Escuela de Desarrollo Profesional de la Universidad de Harvard en programas de vanguardia sobre el uso de la **Inteligencia Artificial** en los **negocios**. Así, su perfil profesional se erige como uno de los más relevantes en el campo actual del **Marketing** y los **Medios Digitales**.



D. Stevenson, Scott

- Director de Marketing Digital en Warner Bros. Discovery, Burbank, Estados Unidos
- Gerente de Tráfico en Warner Bros. Entertainment
- Máster en Escritura Creativa de la Universidad de California
- Licenciatura en Telecomunicaciones de la Universidad de Florida

“

¡Alcanza tus objetivos académicos y profesionales con los expertos mejor cualificados del mundo! Los docentes de este MBA te guiarán durante todo el proceso de aprendizaje”

Directora Invitada Internacional

Galardonada con el "*International Content Marketing Awards*" por su creatividad, liderazgo y calidad de sus contenidos informativos, Wendy Thole-Muir es una reconocida **Directora de Comunicación** altamente especializada en el campo de la **Gestión de Reputación**.

En este sentido, ha desarrollado una sólida trayectoria profesional de más de dos décadas en este ámbito, lo que le ha llevado a formar parte de prestigiosas entidades de referencia internacional como **Coca-Cola**. Su rol implica la supervisión y manejo de la comunicación corporativa, así como el control de la imagen organizacional. Entre sus principales contribuciones, destaca haber liderado la implementación de la **plataforma de interacción interna Yammer**. Gracias a esto, los empleados aumentaron su compromiso con la marca y crearon una comunidad que mejoró la transmisión de información significativamente.

Por otra parte, se ha encargado de gestionar la comunicación de las **inversiones estratégicas** de las empresas en diferentes países africanos. Una muestra de ello es que ha manejado diálogos en torno a las inversiones significativas en Kenya, demostrando el compromiso de las entidades con el desarrollo tanto económico como social del país. A su vez, ha logrado numerosos **reconocimientos** por su capacidad de gestionar la percepción sobre las firmas en todos los mercados en los que opera. De esta forma, ha logrado que las compañías mantengan una gran notoriedad y los consumidores las asocien con una elevada calidad.

Además, en su firme compromiso con la excelencia, ha participado activamente en reputados **Congresos y Simposios** a escala global con el objetivo de ayudar a los profesionales de la información a mantenerse a la vanguardia de las técnicas más sofisticadas para **desarrollar planes estratégicos de comunicación** exitosos. Así pues, ha ayudado a numerosos expertos a anticiparse a situaciones de crisis institucionales y a manejar acontecimientos adversos de manera efectiva.



Dña. Thole-Muir, Wendy

- ♦ Directora de Comunicación Estratégica y Reputación Corporativa en Coca-Cola, Sudáfrica
- ♦ Responsable de Reputación Corporativa y Comunicación en ABI at SABMiller de Lovania, Bélgica
- ♦ Consultora de Comunicaciones en ABI, Bélgica
- ♦ Consultora de Reputación y Comunicación de Third Door en Gauteng, Sudáfrica
- ♦ Máster en Estudios del Comportamiento Social por Universidad de Sudáfrica
- ♦ Máster en Artes con especialidad en Sociología y Psicología por Universidad de Sudáfrica
- ♦ Licenciatura en Ciencias Políticas y Sociología Industrial por Universidad de KwaZulu-Natal
- ♦ Licenciatura en Psicología por Universidad de Sudáfrica

“

Gracias a esta titulación universitaria, 100% online, podrás compaginar el estudio con tus obligaciones diarias, de la mano de los mayores expertos internacionales en el campo de tu interés. ¡Inscríbete ya!”

10

Triple titulación

TECH ofrece este programa con **triple titulación** que permitirá al estudiante ampliar sus perspectivas profesionales y académicas en relación al mundo de los negocios, la economía y la dirección de equipos específicos dentro de las diferentes empresas. Cursando este plan de estudios alcanzará el conocimiento y la acreditación necesarios para convertirse en un auténtico directivo especialista en redes sociales.



“

Al terminar este programa recibirás tres títulos, uno oficial y dos propios con los que dispondrás de un currículum mucho más atractivo para cualquier empresa”

El **Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** es un programa ofrecido por TECH, que es una Universidad Oficial española legalmente reconocida mediante la Ley 1/2024, de 16 de abril, de la Comunidad Autónoma de Canarias, publicada en el [Boletín Oficial del Estado \(BOE\) núm. 181, de 27 de julio de 2024 \(pág. 96.369\)](#), e integrada en el Registro de Universidades, Centros y Títulos ([RUCT](#)) del Ministerio de Ciencia, Innovación y Universidades con el código 104.

Este programa le brinda al estudiante una triple titulación, además del título de **Grand Master de Formación Permanente en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**, obtendrá el título oficial de **Máster Universitario en Dirección y Administración de Empresas (MBA)** y el título propio de **Máster de Formación Permanente MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**.

Con esta triple titulación, de alto valor curricular, el egresado podrá optar a puestos bien remunerados y de responsabilidad en el mundo laboral, así como a tener acceso a los estudios de **nivel de doctorado** con el que progresar en la carrera académica y universitaria.



Supera con éxito este programa y recibe tu titulación universitaria para ejercer con total garantía en un campo profesional exigente como la Dirección y Administración de Empresas”

TECH es miembro de **Business Graduates Association (BGA)**, la red internacional que reúne a las escuelas de negocios más prestigiosas del mundo. Esta distinción reafirma su compromiso con la excelencia en la gestión responsable y la capacitación para directivos.

Aval/Membresía



Título Propio: **Grand Master de Formación Permanente en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**

Título Oficial: **Máster Universitario en Dirección y Administración de Empresas (MBA)**

Título Propio: **Máster de Formación Permanente MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**

Modalidad: **100% online**

Duración: **2 años**

Créditos: **120 ECTS**



11

Homologación del título

Para que los títulos universitarios obtenidos, tras finalizar el **Grand Master Oficial Universitario MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**, tengan validez oficial en cualquier país, se deberá realizar un trámite específico de reconocimiento en la Administración correspondiente. TECH facilitará al egresado toda la documentación necesaria para tramitar su expediente con éxito.





“

Tras finalizar este programa recibirás un título académico oficial y un título propio, ambos con validez internacional”

Cualquier estudiante interesado en tramitar el reconocimiento oficial de esta titulación universitaria en un país diferente a España, necesitará la documentación académica y el título emitido con la Apostilla de La Haya, que podrá solicitar al departamento de Secretaría Académica a través de correo electrónico: homologacion@techtitute.com.

La Apostilla de La Haya otorgará validez internacional a la documentación y permitirá su uso ante los diferentes organismos oficiales en cualquier país.

Una vez el egresado reciba su documentación deberá realizar el trámite correspondiente, siguiendo las indicaciones del ente regulador de la Educación Superior en su país. Para ello, TECH facilitará en el portal web una guía que le ayudará en la preparación de la documentación y el trámite de reconocimiento en cada país.

Con TECH podrás hacer válido el título oficial que obtendrás con este Grand Master Oficial Universitario en cualquier país.





El trámite de homologación permitirá que los estudios oficiales realizados en TECH tengan validez oficial en el país de elección, considerando el título oficial obtenido del mismo modo que si el estudiante hubiera estudiado allí. Esto le confiere un valor internacional del que podrá beneficiarse el egresado una vez haya superado el programa y realice adecuadamente el trámite.

El equipo de TECH le acompañará durante todo el proceso, facilitándole toda la documentación necesaria y asesorándole en cada paso hasta que logre una resolución positiva.



El equipo de TECH te acompañará paso a paso en la realización del trámite para lograr la validez oficial internacional de la triple titulación que te proporciona este programa”

12

Requisitos de acceso

Los requisitos de acceso de este programa de posgrado se establecen de conformidad con el artículo 18 del Real Decreto 822/2021, de 28 de septiembre. En dicho documento se recogen todos los títulos, nacionales o extranjeros, que los cuales los potenciales alumnos de este programa pueden presentar para acreditar sus conocimientos y competencias.



“

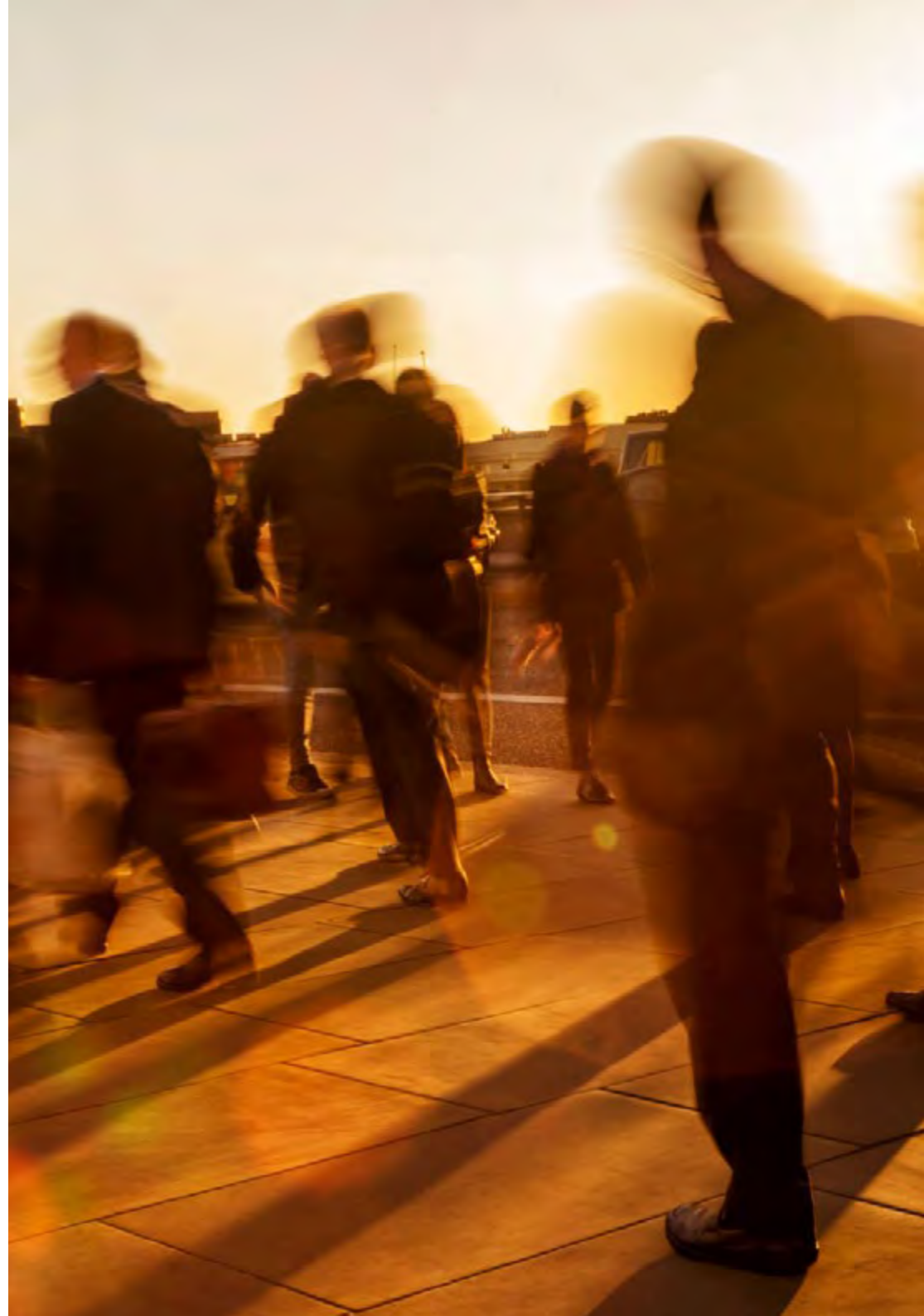
Revisa los requisitos de acceso a este triple posgrado de TECH y prepárate para iniciar este itinerario académico con el que actualizarás todas tus competencias profesionales”

Así se determina que es necesario estar en posesión de alguna de las siguientes titulaciones:

- ♦ Título universitario oficial de Graduado o Graduada español o equivalente. Además, se permitirá el acceso al Grand Master Oficial Universitario a aquellos estudiantes de Grado a los que les falte por superar el TFG y como máximo hasta 9 créditos ECTS para obtenerlo. En ningún caso podrá titularse si previamente no ha obtenido el título de grado
- ♦ Título expedido por una institución de educación superior extranjera perteneciente al Espacio Europeo de Educación Superior (EEES) que faculte, en el país de expedición, para acceder a las enseñanzas de nivel de Máster Universitario
- ♦ Título oficial expedido en un sistema educativo extranjero no perteneciente al EEES, en alguno de los siguientes supuestos:
 - » Título de educación superior extranjero homologado a un título universitario oficial español
 - » Acceso condicionado a la comprobación previa (sin homologación) de que los estudios cursados corresponden a un nivel de formación equivalente al de los títulos universitarios oficiales españoles y que capacitan para acceder a estudios de nivel Máster Universitario en el país en el que se ha expedido el título. Este trámite no implica, en ningún caso, la homologación del título previo, ni su reconocimiento para otra finalidad que no sea la de acceder a los programas de TECH

“

Consigue ya tu plaza en este Grand Master Oficial Universitario de TECH si cumples con alguno de sus requisitos de acceso”



Requisito lingüístico

Los estudiantes procedentes de países o de sistemas educativos con lengua diferente al español, deberán acreditar un conocimiento del español de nivel B2 según el marco Común Europeo de Referencia para lenguas.

En relación con la acreditación del nivel de lengua española para la admisión a un título oficial se puede optar por una de las siguientes alternativas:

- ♦ Presentación del documento que justifique el nivel de español B2
- ♦ Realización de una prueba de nivel interna de la universidad

Quedan exentos de este requisito:

- ♦ Quienes acrediten la nacionalidad española
- ♦ Los que posean una titulación extranjera equivalente a: Filología Hispánica, Traducción e Interpretación (con idioma español), Literatura y/o Lingüística española
- ♦ Quienes hayan realizado estudios previos en español

¿Cumples con los requisitos de acceso lingüísticos de este Grand Master Oficial Universitario? No dejes pasar la oportunidad y matricúlate ahora.

13

Proceso de admisión

El proceso de admisión de TECH es el más simple de todas las universidades online. Se podrá comenzar el programa sin trámites ni esperas: el alumno empezará a preparar la documentación y podrá entregarla más adelante, sin prisas ni complicaciones. Lo más importante para TECH es que los procesos administrativos sean sencillos y no ocasionen retrasos, ni incomodidades.



“

TECH ofrece el procedimiento de admisión a los estudios de Grand Master Oficial Universitario más sencillo y rápido de todas las universidades virtuales”

Para TECH lo más importante en el inicio de la relación académica con el alumno es que esté centrado en el proceso de enseñanza, sin demoras ni preocupaciones relacionadas con el trámite administrativo. Por ello, se ha creado un procedimiento más cómodo en el que podrá enfocarse desde el primer momento a su formación, contando con un plazo de tiempo para la entrega de la documentación pertinente.

Los pasos para la admisión son simples:

1. Facilitar los datos personales al asesor académico para realizar la inscripción.
2. Recibir un email en el correo electrónico en el que se accederá a la página segura de la universidad y aceptar las políticas de privacidad, las condiciones de contratación e introducir los datos de tarjeta bancaria.
3. Recibir un nuevo email de confirmación y las credenciales de acceso al campus virtual.
4. Comenzar el programa en la fecha de inicio oficial.

De esta manera, el estudiante podrá incorporarse al curso sin esperas. De forma posterior se le informará del momento en el que se podrán ir enviando los documentos, a través del campus virtual, de manera muy cómoda y rápida. Sólo se deberán subir al sistema para considerarse enviados, sin traslados ni pérdidas de tiempo.

Todos los documentos facilitados deberán ser rigurosamente válidos y estar vigentes en el momento de subirlos.

Los documentos necesarios que deberán tenerse preparados con calidad suficiente para cargarlos en el campus virtual son:

- Copia digitalizada del documento del DNI o documento de identidad oficial del alumno
- Copia digitalizada del título académico oficial de Grado o título equivalente con el que se accede al Grand Master Oficial Universitario. En caso de que el estudiante no haya terminado el Grado pero le reste por superar únicamente el TFG y hasta 9 ECTS del programa, deberá aportar un certificado oficial de notas de su universidad donde se corrobore esta situación

Para resolver cualquier duda que surja el estudiante podrá dirigirse a su asesor académico, con gusto le atenderá en todo lo que necesite. En caso de requerir más información, puede ponerse en contacto con procesodeadmission@techtitute.com.

Este procedimiento de acceso te ayudará a iniciar tu Grand Master Oficial Universitario cuanto antes, sin trámites ni demoras.

tech
universidad

Grand Master Oficial
Universitario
MBA en Dirección
de Ciberseguridad
(CISO, Chief Information
Security Officer)

Idioma: **Español**

Modalidad: **100% online**

Duración: **2 años**

Créditos: **120 ECTS**

Grand Master Oficial Universitario

MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Aval/Membresía



tech
universidad