Máster Título Propio

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

Aval/Membresía

tech global university

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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **90 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-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 Objetivos docentes — pág. 30

05 Salidas profesionales — pág. 36

06 Licencias de software incluidas — pág. 40

07 Metodología de estudio — pág. 44

08 Cuadro docente — pág. 54

09 Titulación — pág. 78

01

Presentación del programa

La Dirección de Ciberseguridad es un rol se ha consolidado como una figura clave dentro de las organizaciones, liderando estrategias que protegen infraestructuras críticas y gestionan riesgos tecnológicos. De acuerdo con un informe de la Agencia de la Unión Europea para la Ciberseguridad, más del 60 % de las organizaciones han reportado más de 52% de incidentes de seguridad significativo en el último año. Frente a esta realidad, los informáticos tienen la responsabilidad de manejar las estrategias más modernas para fortalecer la resiliencia operativa frente a incidentes digitales. Con el objetivo de apoyarlos con esta labor, TECH lanza un vanguardista programa universitario centrado en las técnicas de Ciberseguridad innovadoras. Además, se imparte bajo una cómoda modalidad totalmente online.

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

En un entorno digital cada vez más complejo y expuesto a amenazas constantes, la protección de los activos informáticos se ha convertido en una prioridad estratégica para cualquier organización. En este contexto, los profesionales necesitan mantenerse a la vanguardia de las técnicas más avanzadas de seguridad con el objetivo de gestionar arquitecturas robustas y prever incidentes como suplantaciones de identidad. Asimismo, los especialistas requieren disponer de una comprensión profunda de los sistemas críticos y de los vectores de ataque sofisticados.

En este marco, TECH presenta un revolucionario MBA en Dirección de Ciberseguridad (CISO, *Chief Information Security Officer*). Los materiales didácticos ahondarán en cuestiones que van desde el análisis avanzado de amenazas digitales o la auditoría de sistemas hasta el cumplimiento normativo con estándares internacionales. En este sentido, el temario proporcionará herramientas modernas para para identificar vulnerabilidades, evaluar riesgos y establecer mecanismos de protección proactiva en infraestructuras críticas. Gracias a esto, los alumnos desarrollarán habilidades avanzadas para diseñar arquitecturas digitales seguras y resilientes.

Por otro lado, TECH emplea su revolucionario método del *Relearning*, que potencia los conceptos esenciales mediante la reiteración inteligente y progresiva. De este modo, los informáticos no tendrán que invertir largas horas al estudio. Solo necesitarán un dispositivo con conexión a internet para acceder al Campus Virtual. Además, unos reconocidos Directores Invitados Internacionales impartirán unas rigurosas *Masterclasses*.

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.

Este **MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Dirección de Ciberseguridad
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras en la protección de los activos informáticos
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Unos prestigiosos Directores Invitados Internacionales ofrecerán unas intensivas Masterclasses sobre las últimas tendencias en la Dirección de Ciberseguridad"

Dominarás sofisticadas metodologías ofensivas y defensivas que permiten reforzar la seguridad de redes, software e incluso dispositivos"

Manejarás los métodos más sofisticados de seguridad para fortalecer la protección frente a amenazas digitales.

Aprovecha todos los beneficios de la metodología Relearning, la cual te permitirá organizar tu tiempo y ritmo de estudio.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la Dirección de Ciberseguridad, que vierten en este programa la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextual, es decir, un entorno simulado que proporcionará un estudio inmersivo programado para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el alumno deberá tratar de resolver las distintas situaciones de práctica profesional que se le planteen a lo largo del curso académico. Para ello, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.

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.

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».

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.

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.

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.

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 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

Este itinerario académico profundizará en áreas clave de la Dirección de Ciberseguridad, esenciales para el desarrollo profesional en sectores tecnológicos avanzados. Por lo tanto, se abordarán técnicas especializadas en seguridad para *smartphones*, permitiendo identificar brechas y reforzar dispositivos frente a amenazas persistentes. A lo largo del programa universitario, se integrará el análisis del *hacking* ético como herramienta para anticipar comportamientos ofensivos y evaluar entornos desde una perspectiva defensiva. Finalmente, se ahondará en la ingeniería inversa, indispensable para que el alumnado logre descomponer software malicioso y comprender su lógica interna.

Evaluarás las vulnerabilidades de los sistemas a través de auditorías, pentesting y simulaciones de ciberataques de última generación"

Módulo 1. Ciberinteligencia y Ciberseguridad

1.1. Ciberinteligencia
- 1.1.1. Ciberinteligencia
  - 1.1.1.1. La inteligencia
    - 1.1.1.1.1. Ciclo de inteligencia
  - 1.1.1.2. Ciberinteligencia
  - 1.1.1.3. Ciberinteligencia y Ciberseguridad
- 1.1.2. El analista de inteligencia
  - 1.1.2.1. El rol del analista de inteligencia
  - 1.1.2.2. Los sesgos del analista de inteligencia en la actividad evaluativa

1.2. Ciberseguridad
- 1.2.1. Las capas de seguridad
- 1.2.2. Identificación de las ciberamenazas
  - 1.2.2.1. Amenazas externas
  - 1.2.2.2. Amenazas internas
- 1.2.3. Acciones adversas
  - 1.2.3.1. Ingeniería social
  - 1.2.3.2. Métodos comúnmente usados

1.3. Técnicas y herramientas de inteligencias
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. Humit
- 1.3.4. Distribuciones de Linux y herramientas
- 1.3.5. OWISAM
- 1.3.6. OWASP
- 1.3.7. PTES
- 1.3.8. OSSTMM

1.4. Metodologías de evaluación
- 1.4.1. El análisis de inteligencia
- 1.4.2. Técnicas de organización de la información adquirida
- 1.4.3. Fiabilidad y credibilidad de las fuentes de información
- 1.4.4. Metodologías de análisis
- 1.4.5. Presentación de los resultados de la inteligencia

1.5. Auditorías y documentación
- 1.5.1. La auditoría en seguridad informática
- 1.5.2. Documentación y permisos para auditoría
- 1.5.3. Tipos de auditoría
- 1.5.4. Entregables
  - 1.5.4.1. Informe técnico
  - 1.5.4.2. Informe ejecutivo

1.6. Anonimato en la red
- 1.6.1. Uso de anonimato
- 1.6.2. Técnicas de anonimato (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Amenazas y tipos de seguridad
- 1.7.1. Tipos de amenazas
- 1.7.2. Seguridad física
- 1.7.3. Seguridad en redes
- 1.7.4. Seguridad lógica
- 1.7.5. Seguridad en aplicaciones web
- 1.7.6. Seguridad en dispositivos móviles

1.8. Normativa y *compliance*
- 1.8.1. RGPD
- 1.8.2. La estrategia nacional de Ciberseguridad 2019
- 1.8.3. Familia ISO 27000
- 1.8.4. Marco de Ciberseguridad NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas *cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análisis de riesgos y métricas
- 1.9.1. Alcance de riesgos
- 1.9.2. Los activos
- 1.9.3. Las amenazas
- 1.9.4. Las vulnerabilidades
- 1.9.5. Evaluación del riesgo
- 1.9.6. Tratamiento del riesgo

1.10. Organismos importantes en materia de Ciberseguridad
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR PROSUR

Módulo 2. Seguridad en *host*

2.1. Copias de seguridad
- 2.1.1. Estrategias para las copias de seguridad
- 2.1.2. Herramientas para Windows
- 2.1.3. Herramientas para Linux
- 2.1.4. Herramientas para MacOS

2.2. Antivirus de usuario
- 2.2.1. Tipos de antivirus
- 2.2.2. Antivirus para Windows
- 2.2.3. Antivirus para Linux
- 2.2.4. Antivirus para MacOS
- 2.2.5. Antivirus para *smartphones*

2.3. Detectores de intrusos HIDS
- 2.3.1. Métodos de detección de intrusos
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. *Firewall* local
- 2.4.1. *Firewalls* para Windows
- 2.4.2. *Firewalls* para Linux
- 2.4.3. *Firewalls* para MacOS

2.5. Gestores de contraseñas
- 2.5.1. *Password*
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. *Sticky password*
- 2.5.5. RoboForm

2.6. Detectores de *phishing*
- 2.6.1. Detección del *phishing* de forma manual
- 2.6.2. Herramientas *antiphishing*

2.7. *Spyware*
- 2.7.1. Mecanismos de evitación
- 2.7.2. Herramientas *antispyware*

2.8. Rastreadores
- 2.8.1. Medidas para proteger el sistema
- 2.8.2. Herramientas anti - rastreadores

2.9. EDR - *end point detection and response*
- 2.9.1. Comportamiento del sistema EDR
- 2.9.2. Diferencias entre EDR y antivirus
- 2.9.3. El futuro de los sistemas EDR

2.10. Control sobre la instalación de *software*
- 2.10.1. Repositorios y tiendas de *software*
- 2.10.2. Listas de *software* permitido o prohibido
- 2.10.3. Criterios de actualizaciones
- 2.10.4. Privilegios para instalar *software*

Módulo 3. Seguridad en red (perimetral)

3.1. Sistemas de detección y prevención de amenazas
- 3.1.1. Marco general de los incidentes de seguridad
- 3.1.2. Sistemas de defensa actuales: *defense in depth* y SOC
- 3.1.3. Arquitecturas de redes actuales
- 3.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 3.1.4.1. Sistemas basados en red
  - 3.1.4.2. Sistemas basados en *host*
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicación y detección de instancias/*hosts*, contenedores y *serverless*

3.2. *Firewall*
- 3.2.1. Tipos de *firewalls*
- 3.2.2. Ataques y mitigación
- 3.2.3. *Firewalls* comunes en Kernel Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. Nftables e iptables
  - 3.2.3.3. Firewalld
- 3.2.4. Sistemas de detección basados en *logs* del sistema
  - 3.2.4.1. TCP *wrappers*
  - 3.2.4.2. BlockHosts y DenyHosts
  - 3.2.4.3. Fail2Ban

3.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 3.3.1. Ataques sobre IDS/IPS
- 3.3.2. Sistemas de IDS/IPS
  - 3.3.2.1. *Snort*
  - 3.3.2.2. Suricata

3.4. *Firewalls* de siguiente generación (NGFW)
- 3.4.1. Diferencias entre NGFW y *firewall* tradicional
- 3.4.2. Capacidades principales
- 3.4.3. Soluciones comerciales
- 3.4.4. *Firewalls* para servicios de *cloud*
  - 3.4.4.1. Arquirtectura *cloud* VPC
  - 3.4.4.2. *Cloud* ACLs
  - 3.4.4.3. *Security group*

3.5. *Proxy*
- 3.5.1. Tipos de *proxy*
- 3.5.2. Uso de *proxy*. Ventajas e inconvenientes

3.6. Motores de antivirus
- 3.6.1. Contexto general del *malware* e IOCs
- 3.6.2. Problemas de los motores de antivirus

3.7. Sistemas de protección de correo
- 3.7.1. Antispam
  - 3.7.1.1. Listas blancas y negras
  - 3.7.1.2. Filtros bayesianos
- 3.7.2. *Mail gateway* (MGW)

3.8. SIEM
- 3.8.1. Componentes y arquitectura
- 3.8.2. Reglas de correlación y casos de uso
- 3.8.3. Retos actuales de los sistemas SIEM

3.9. SOAR
- 3.9.1. SOAR y SIEM: enemigos o aliados
- 3.9.2. El futuro de los sistemas SOAR

3.10. Otros Sistemas basados en red
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. Honeypots y honeynets
- 3.10.4. CASB

Módulo 4. Seguridad en *smartphones*

4.1. El mundo del dispositivo móvil
- 4.1.1. Tipos de plataformas móviles
- 4.1.2. Dispositivos iOS
- 4.1.3. Dispositivos Android

4.2. Gestión de la seguridad móvil
- 4.2.1. Proyecto de seguridad móvil OWASP
  - 4.2.1.1. Top 10 vulnerabilidades
- 4.2.2. Comunicaciones, redes y modos de conexión

4.3. El dispositivo móvil en el entorno empresarial
- 4.3.1. Riesgos
- 4.3.2. Políticas de seguridad
- 4.3.3. Monitorización de dispositivos
- 4.3.4. Gestión de dispositivos móviles (MDM)

4.4. Privacidad del usuario y seguridad de los datos
- 4.4.1. Estados de la información
- 4.4.2. Protección y confidencialidad de los datos
  - 4.4.2.1. Permisos
  - 4.4.2.2. Encriptación
- 4.4.3. Almacenamiento seguro de los datos
  - 4.4.3.1. Almacenamiento seguro en iOS
  - 4.4.3.2. Almacenamiento seguro en Android
- 4.4.4. Buenas prácticas en el desarrollo de aplicaciones

4.5. Vulnerabilidades y vectores de ataque
- 4.5.1. Vulnerabilidades
- 4.5.2. Vectores de ataque
  - 4.5.2.1. *Malware*
  - 4.5.2.2. Exfiltración de datos
  - 4.5.2.3. Manipulación de los datos

4.6. Principales amenazas
- 4.6.1. Usuario no formado
- 4.6.2. *Malware*
  - 4.6.2.1. Tipos de *malware*
- 4.6.3. Ingeniería social
- 4.6.4. Fuga de datos
- 4.6.5. Robo de información
- 4.6.6. Redes wifi no seguras
- 4.6.7. Software desactualizado
- 4.6.8. Aplicaciones maliciosas
- 4.6.9. Contraseñas poco seguras
- 4.6.10. Configuración débil o inexistente de seguridad
- 4.6.11. Acceso físico
- 4.6.12. Pérdida o robo del dispositivo
- 4.6.13. Suplantación de identidad (integridad)
- 4.6.14. Criptografía débil o rota
- 4.6.15. Denegación de servicio (DoS)

4.7. Principales ataques
- 4.7.1. Ataques de *phishing*
- 4.7.2. Ataques relacionados con los modos de comunicación
- 4.7.3. Ataques de *smishing*
- 4.7.4. Ataques de *criptojacking*
- 4.7.5. *Man in the middle*

4.8. *Hacking*
- 4.8.1. *Rooting* y *jailbreaking*
- 4.8.2. Anatomía de un ataque móvil
  - 4.8.2.1. Propagación de la amenaza
  - 4.8.2.2. Instalación de *malware* en el dispositivo
  - 4.8.2.3. Persistencia
  - 4.8.2.4. Ejecución del *payload* y extracción de la información
- 4.8.3. *Hacking* en dispositivos iOS: mecanismos y herramientas
- 4.8.4. *Hacking* en dispositivos Android: mecanismos y herramientas

4.9. Pruebas de penetración
- 4.9.1. iOS *pentesting*
- 4.9.2. Android *pentesting*
- 4.9.3. Herramientas

4.10. Protección y seguridad
- 4.10.1. Configuración de seguridad
  - 4.10.1.1. En dispositivos iOS
  - 4.10.1.2. En dispositvos Android
- 4.10.2. Medidas de seguridad
- 4.10.3. Herramientas de protección

Módulo 5. Seguridad en IoT

5.1. Dispositivos
- 5.1.1. Tipos de dispositivos
- 5.1.2. Arquitecturas estandarizadas
  - 5.1.2.1. OneM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Protocolos de aplicación
- 5.1.4. Tecnologías de conectividad

5.2. Dispositivos IoT. Áreas de aplicación
- 5.2.1. *SmartHome*
- 5.2.2. *SmartCity*
- 5.2.3. Transportes
- 5.2.4. *Wearables*
- 5.2.5. Sector salud
- 5.2.6. IIoT

5.3. Protocolos de comunicación
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Electrodomésticos
- 5.4.4. Vigilancia y seguridad

5.5. *SmartCity*
- 5.5.1. Iluminación
- 5.5.2. Meteorología
- 5.5.3. Seguridad

5.6. Transportes
- 5.6.1. Localización
- 5.6.2. Realización de pagos y obtención de servicios
- 5.6.3. Conectividad

5.7. *Wearables*
- 5.7.1. Ropa inteligente
- 5.7.2. Joyas inteligentes
- 5.7.3. Relojes inteligentes

5.8. Sector salud
- 5.8.1. Monitorización de ejercicio/ritmo cardíaco
- 5.8.2. Monitorización de pacientes y personas mayores
- 5.8.3. Implantables
- 5.8.4. Robots quirúrgicos

5.9. Conectividad
- 5.9.1. Wi-Fi/*gateway*
- 5.9.2. Bluetooth
- 5.9.3. Conectividad incorporada

5.10. Securización
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de contraseñas
- 5.10.3. Uso de protocolos cifrados
- 5.10.4. Consejos de uso

Módulo 6. *Hacking* ético

6.1. Entorno de trabajo
- 6.1.1. Distribuciones Linux
  - 6.1.1.1. Kali Linux - *offensive security*
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemas de virtualización
- 6.1.3. Sandbox
- 6.1.4. Despliegue de laboratorios

6.2. Metodologías
- 6.2.1. OSSTMM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Inteligencia de fuentes abiertas (OSINT)
- 6.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 6.3.3. Uso de herramientas pasivas

6.4. Escaneo de redes
- 6.4.1. Herramientas de escaneo
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Otras herramientas de escaneo
- 6.4.2. Técnicas de escaneo
- 6.4.3. Técnicas de evasión de *firewall* e IDS
- 6.4.4. *Banner grabbing*
- 6.4.5. Diagramas de red

6.5. Enumeración
- 6.5.1. Enumeración SMTP
- 6.5.2. Enumeración DNS
- 6.5.3. Enumeración de NetBIOS y Samba
- 6.5.4. Enumeración de LDAP
- 6.5.5. Enumeración de SNMP
- 6.5.6. Otras técnicas de enumeración

6.6. Análisis de vulnerabilidades
- 6.6.1. Soluciones de análisis de vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Sistemas de puntuación de vulnerabilidades
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a redes inalámbrica
- 6.7.1. Metodología de *hacking* en redes inalámbricas
  - 6.7.1.1. Wifi *discovery*
  - 6.7.1.2. Análisis de tráfico
  - 6.7.1.3. Ataques del *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *evil twin*
  - 6.7.1.5. Ataques a WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Herramientas para la seguridad inalámbrica

6.8. Hackeo de servidores webs
- 6.8.1. *Cross site scripting*
- 6.8.2. CSRF
- 6.8.3. *Session hijacking*
- 6.8.4. *SQL injection*

6.9. Explotación de vulnerabilidades
- 6.9.1. Uso de *exploits* conocidos
- 6.9.2. Uso de *metasploit*
- 6.9.3. Uso de *malware*
  - 6.9.3.1. Definición y alcance
  - 6.9.3.2. Generación de *malware*
  - 6.9.3.3. *Bypass* de soluciones antivirus

6.10. Persistencia
- 6.10.1. Instalación de Rootkits
- 6.10.2. Uso de Ncat
- 6.10.3. Uso de tareas programadas para *backdoors*
- 6.10.4. Creación de usuarios
- 6.10.5. Detección de HIDS

Módulo 7. Ingeniería inversa

7.1. Compiladores
- 7.1.1. Tipos de códigos
- 7.1.2. Fases de un compilador
- 7.1.3. Tabla de símbolos
- 7.1.4. Gestor de errores
- 7.1.5. Compilador GCC

7.2. Tipos de análisis en compiladores
- 7.2.1. Análisis léxico
  - 7.2.1.1. Terminología
  - 7.2.1.2. Componentes léxicos
  - 7.2.1.3. Analizador léxico LEX
- 7.2.2. Análisis sintáctico
  - 7.2.2.1. Gramáticas libres de contexto
  - 7.2.2.2. Tipos de análisis sintácticos
    - 7.2.2.2.1. Análisis descendente
    - 7.2.2.2.2. Análisis ascendente
  - 7.2.2.3. Árboles sintácticos y derivaciones
  - 7.2.2.4. Tipos de analizadores sintácticos
    - 7.2.2.4.1. Analizadores LR (*left to right*)
    - 7.2.2.4.2. Analizadores LALR
- 7.2.3. Análisis semántico
  - 7.2.3.1. Gramáticas de atributos
  - 7.2.3.2. S-atribuidas
  - 7.2.3.3. L-atribuidas

7.3. Estructuras de datos en ensamblador
- 7.3.1. Variables
- 7.3.2. *Arrays*
- 7.3.3. Punteros
- 7.3.4. Estructuras
- 7.3.5. Objetos

7.4. Estructuras de código en ensamblador
- 7.4.1. Estructuras de selección
  - 7.4.1.1. *If, else if, else*
  - 7.4.1.2. *Switch*
- 7.4.2. Estructuras de iteración
  - 7.4.2.1. *For*
  - 7.4.2.2. *While*
  - 7.4.2.3. Uso del *break*
- 7.4.3. Funciones

7.5. Arquitectura *hardware* x86
- 7.5.1. Arquitectura de procesadores x86
- 7.5.2. Estructuras de datos en x86
- 7.5.3. Estructuras de código en x86
- 7.5.4. Estructuras de código en x86

7.6. Arquitectura *hardware* ARM
- 7.6.1. Arquitectura de procesadores ARM
- 7.6.2. Estructuras de datos en ARM
- 7.6.3. Estructuras de código en ARM

7.7. Análisis de código estático
- 7.7.1. Desensambladores
- 7.7.2. IDA
- 7.7.3. Reconstructores de código

7.8. Análisis de código dinámico
- 7.8.1. Análisis del comportamiento
  - 7.8.1.1. Comunicaciones
  - 7.8.1.2. Monitorización
- 7.8.2. Depuradores de código en Linux
- 7.8.3. Depuradores de código en Windows

7.9. *Sandbox*
- 7.9.1. Arquitectura de un *sandbox*
- 7.9.2. Evasión de un *sandbox*
- 7.9.3. Técnicas de detección
- 7.9.4. Técnicas de evasión
- 7.9.5. Contramedidas
- 7.9.6. Sandbox en Linux
- 7.9.7. Sandbox en Windows
- 7.9.8. Sandox en MacOS
- 7.9.9. Sandbox en Android

7.10. Análisis de *malware*
- 7.10.1. Métodos de análisis de *malware*
- 7.10.2. Técnicas de ofuscación de *malware*
  - 7.10.2.1. Ofuscación de ejecutables
  - 7.10.2.2. Restricción de entornos de ejecución
- 7.10.3. Herramientas de análisis de *malware*

Módulo 8. Desarrollo seguro

8.1. Desarrollo seguro
- 8.1.1. Calidad, funcionalidad y seguridad
- 8.1.2. Confidencialidad, integridad y disponibilidad
- 8.1.3. Ciclo de vida del desarrollo de *software*

8.2. Fase de requerimientos
- 8.2.1. Control de la autenticación
- 8.2.2. Control de roles y privilegios
- 8.2.3. Requerimientos orientados al riesgo
- 8.2.4. Aprobación de privilegios

8.3. Fases de análisis y diseño
- 8.3.1. Acceso a componentes y administración del sistema
- 8.3.2. Pistas de auditoría
- 8.3.3. Gestión de sesiones
- 8.3.4. Datos históricos
- 8.3.5. Manejo apropiado de errores
- 8.3.6. Separación de funciones

8.4. Fase de implementación y codificación
- 8.4.1. Aseguramiento del ambiente de desarrollo
- 8.4.2. Elaboración de la documentación técnica
- 8.4.3. Codificación segura
- 8.4.4. Seguridad en las comunicaciones

8.5. Buenas prácticas de codificación segura
- 8.5.1. Validación de datos de entrada
- 8.5.2. Codificación de los datos de salida
- 8.5.3. Estilo de programación
- 8.5.4. Manejo de registro de cambios
- 8.5.5. Prácticas criptográficas
- 8.5.6. Gestión de errores y logs
- 8.5.7. Gestión de archivos
- 8.5.8. Gestión de memoria
- 8.5.9. Estandarización y reutilización de funciones de seguridad

8.6. Preparación del servidor y *hardening*
- 8.6.1. Gestión de usuarios, grupos y roles en el servidor
- 8.6.2. Instalación de *software*
- 8.6.3. *Hardening* del servidor
- 8.6.4. Configuración robusta del entorno de la aplicación

8.7. Preparación de la BBDD y *hardening*
- 8.7.1. Optimización del motor de BBDD
- 8.7.2. Creación del usuario propio para la aplicación
- 8.7.3. Asignación de los privilegios precisos para el usuario
- 8.7.4. *Hardening* de la BBDD

8.8. Fase de pruebas
- 8.8.1. Control de calidad en controles de seguridad
- 8.8.2. Inspección del código por fases
- 8.8.3. Comprobación de la gestión de las configuraciones
- 8.8.4. Pruebas de caja negra

8.9. Preparación del paso a producción
- 8.9.1. Realizar el control de cambios
- 8.9.2. Realizar procedimiento de paso a producción
- 8.9.3. Realizar procedimiento de *rollback*
- 8.9.4. Pruebas en fase de preproducción

8.10. Fase de mantenimiento
- 8.10.1. Aseguramiento basado en riesgos
- 8.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 8.10.3. Pruebas de mantenimiento de seguridad de caja negra

Módulo 9. Análisis forense

9.1. Adquisición de datos y duplicación
- 9.1.1. Adquisición de datos volátiles
  - 9.1.1.1. Información del sistema
  - 9.1.1.2. Información de la red
  - 9.1.1.3. Orden de volatilidad
- 9.1.2. Adquisición de datos estáticos
  - 9.1.2.1. Creación de una imagen duplicada
  - 9.1.2.2. Preparación de un documento para la cadena de custodia
- 9.1.3. Métodos de validación de los datos adquiridos
  - 9.1.3.1. Métodos para Linux
  - 9.1.3.2. Métodos para Windows

9.2. Evaluación y derrota de técnicas antiforenses
- 9.2.1. Objetivos de las técnicas antiforenses
- 9.2.2. Borrado de datos
  - 9.2.2.1. Borrado de datos y ficheros
  - 9.2.2.2. Recuperación de archivos
  - 9.2.2.3. Recuperación de particiones borradas
- 9.2.3. Protección por contraseña
- 9.2.4. Esteganografía
- 9.2.5. Borrado seguro de dispositivos
- 9.2.6. Encriptación

9.3. Análisis forense del sistema operativo
- 9.3.1. Análisis forense de Windows
- 9.3.2. Análisis forense de Linux
- 9.3.3. Análisis forense de Mac

9.4. Análisis forense de la red
- 9.4.1. Análisis de los logs
- 9.4.2. Correlación de datos
- 9.4.3. Investigación de la red
- 9.4.4. Pasos a seguir en el análisis forense de la red

9.5. Análisis forense web
- 9.5.1. Investigación de los ataques webs
- 9.5.2. Detección de ataques
- 9.5.3. Localización de direcciones IPs

9.6. Análisis forense de bases de datos
- 9.6.1. Análisis forense en MSSQL
- 9.6.2. Análisis forense en MySQL
- 9.6.3. Análisis forense en PostgreSQL
- 9.6.4. Análisis forense en MongoDB

9.7. Análisis forense en *cloud*
- 9.7.1. Tipos de crímenes en *cloud*
  - 9.7.1.1. Cloud como sujeto
  - 9.7.1.2. Cloud como objeto
  - 9.7.1.3. Cloud como herramienta
- 9.7.2. Retos del análisis forense en *cloud*
- 9.7.3. Investigación de los servicios de almacenamiento en *cloud*
- 9.7.4. Herramientas de análisis forense para *cloud*

9.8. Investigación de crímenes de correo electrónico
- 9.8.1. Sistemas de correo
  - 9.8.1.1. Clientes de correo
  - 9.8.1.2. Servidor de correo
  - 9.8.1.3. Servidor SMTP
  - 9.8.1.4. Servidor POP3
  - 9.8.1.5. Servidor IMAP4
- 9.8.2. Crímenes de correo
- 9.8.3. Mensaje de correo
  - 9.8.3.1. Cabeceras estándar
  - 9.8.3.2. Cabeceras extendidas
- 9.8.4. Pasos para la investigación de estos crímenes
- 9.8.5. Herramientas forenses para correo electrónico

9.9. Análisis forense de móviles
- 9.9.1. Redes celulares
  - 9.9.1.1. Tipos de redes
  - 9.9.1.2. Contenidos del CDR
- 9.9.2. *Subscriber identity module* (SIM)
- 9.9.3. Adquisición lógica
- 9.9.4. Adquisición física
- 9.9.5. Adquisición del sistema de ficheros

9.10. Redacción y presentación de informes forenses
- 9.10.1. Aspectos importantes de un informe forense
- 9.10.2. Clasificación y tipos de informes
- 9.10.3. Guía para escribir un informe
- 9.10.4. Presentación del informe
  - 9.10.4.1. Preparación previa para testificar
  - 9.10.4.2. Deposición
  - 9.10.4.3. Trato con los medios

Módulo 10. Retos actuales y futuros en seguridad Informática

10.1. Tecnología *blockchain*
- 10.1.2. Ámbitos de aplicación
- 10.1.3. Garantía de confidencialidad
- 10.1.4. Garantía de no - repudio

10.2. Dinero digital
- 10.2.1. Bitcoins
- 10.2.2. Critpomonedas
- 10.2.3. Minería de criptomonedas
- 10.2.4. Estafas piramidales
- 10.2.5. Otros potenciales delitos y problemas

10.3. *Deepfake*
- 10.3.2. Impacto en los medios
- 10.3.3. Peligros para la sociedad
- 10.3.4. Mecanismos de detección

10.4. El futuro de la inteligencia artificial
- 10.4.1. Inteligencia artificial y computación cognitiva
- 10.4.2. Usos para simplificar el servicio a clientes

10.5. Privacidad digital
- 10.5.1. Valor de los datos en la red
- 10.5.2. Uso de los datos en la red
- 10.5.3. Gestión de la privacidad e identidad digital

10.6. Ciberconflictos, cibercriminales y ciberataques
- 10.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 10.6.2. Consecuencias de ciberataques en la población general
- 10.6.3. Tipos de cibercriminales. Medidas de protección

10.7. Teletrabajo
- 10.7.1. Revolución del teletrabajo durante y pos-COVID-19
- 10.7.2. Cuellos de botella en el acceso
- 10.7.3. Variación de la superficie de ataque
- 10.7.4. Necesidades de los trabajadores

10.8. Tecnologías *wireless* emergentes
- 10.8.1. WPA3
- 10.8.2. 5G
- 10.8.3. Ondas milimétricas
- 10.8.4. Tendencia en *get smart* en vez de *get more*

10.9. Direccionamiento futuro en redes
- 10.9.1. Problemas actuales con el direccionamiento IP
- 10.9.2. IPv6
- 10.9.3. IPv4+
- 10.9.4. Ventajas de IPv4+ sobre IPv4
- 10.9.5. Ventajas de IPv6 sobre IPv4

10.10. El reto de la concienciación de la formación temprana y continua de la población
- 10.10.1. Estrategias actuales de los gobiernos
- 10.10.2. Resistencia de la población al aprendizaje
- 10.10.3. Planes de formación que deben adoptar las empresas

Módulo 11. Liderazgo, ética y responsabilidad social de las empresas

11.1. Globalización y gobernanza
- 11.1.1. Gobernanza y gobierno corporativo
- 11.1.2. Fundamentos del gobierno corporativo en las empresas
- 11.1.3. El rol del consejo de administración en el marco del gobierno corporativo

11.2. Liderazgo
- 11.2.1. Liderazgo. Una aproximación conceptual
- 11.2.2. Liderazgo en las empresas
- 11.2.3. La importancia del líder en la dirección de empresas

11.3. *Cross cultural management*
- 11.3.1. Concepto de *cross cultural management*
- 11.3.2. Aportaciones al conocimiento de culturas nacionales
- 11.3.3. Gestión de la diversidad

11.4. Desarrollo directivo y liderazgo
- 11.4.1. Concepto de desarrollo directivo
- 11.4.2. Concepto de liderazgo
- 11.4.3. Teorías del liderazgo
- 11.4.4. Estilos de liderazgo
- 11.4.5. La inteligencia en el liderazgo
- 11.4.6. Los desafíos del líder en la actualidad

11.5. Ética empresarial
- 11.5.1. Ética y moral
- 11.5.2. Ética empresarial
- 11.5.3. Liderazgo y ética en las empresas

11.6. Sostenibilidad
- 11.6.1. Sostenibilidad y desarrollo sostenible
- 11.6.2. Agenda 2030
- 11.6.3. Las empresas sostenibles

11.7. Responsabilidad social de la empresa
- 11.7.1. Dimensión internacional de la responsabilidad social de las empresas
- 11.7.2. Implementación de la responsabilidad social de la empresa
- 11.7.3. Impacto y medición de la responsabilidad social de la empresa

11.8. Sistemas y herramientas de gestión responsable
- 11.8.1. RSC: La responsabilidad social corporativa
- 11.8.2. Aspectos esenciales para implantar una estrategia de gestión responsable
- 11.8.3. Pasos para la implantación de un sistema de gestión de responsabilidad social corporativa
- 11.8.4. Herramientas y estándares de la RSC

11.9. Multinacionales y derechos humanos
- 11.9.1. Globalización, empresas multinacionales y derechos humanos
- 11.9.2. Empresas multinacionales frente al derecho internacional
- 11.9.3. Instrumentos jurídicos para multinacionales en materia de derechos humanos

11.10. Entorno legal y *corporate governance*
- 11.10.1. Normas internacionales de importación y exportación
- 11.10.2. Propiedad intelectual e industrial
- 11.10.3. Derecho internacional del trabajo

Módulo 12. Dirección de personas y gestión del talento

12.1. Dirección estratégica de personas
- 12.1.1. Dirección estratégica y recursos humanos
- 12.1.2. Dirección estratégica de personas

12.2. Gestión de recursos humanos por competencias
- 12.2.1. Análisis del potencial
- 12.2.2. Política de retribución
- 12.2.3. Planes de carrera/sucesión

12.3. Evaluación del rendimiento y gestión del desempeño
- 12.3.1. La gestión del rendimiento
- 12.3.2. Gestión del desempeño: objetivos y proceso

12.4. Innovación en gestión del talento y las personas
- 12.4.1. Modelos de gestión el talento estratégico
- 12.4.2. Identificación, formación y desarrollo del talento
- 12.4.3. Fidelización y retención
- 12.4.4. Proactividad e innovación

12.5. Motivación
- 12.5.1. La naturaleza de la motivación
- 12.5.2. La teoría de las expectativas
- 12.5.3. Teorías de las necesidades
- 12.5.4. Motivación y compensación económica

12.6. Desarrollo de equipos de alto desempeño
- 12.6.1. Los equipos de alto desempeño: los equipos autogestionados
- 12.6.2. Metodologías de gestión de equipos autogestionados de alto desempeño

12.7. Gestión del cambio
- 12.7.1. Gestión del cambio
- 12.7.2. Tipo de procesos de gestión del cambio
- 12.7.3. Etapas o fases en la gestión del cambio

12.8. Negociación y gestión de conflictos
- 12.8.1. Negociación
- 12.8.2. Gestión de conflictos
- 12.8.3. Gestión de crisis

12.9. Comunicación directiva
- 12.9.1. Comunicación interna y externa en el ámbito empresarial
- 12.9.2. Departamentos de comunicación
- 12.9.3. El responsable de comunicación de la empresa. El perfil del dircom

12.10. Productividad, atracción, retención y activación del talento
- 12.10.1. La productividad
- 12.10.2. Palancas de atracción y retención de talento

Módulo 13. Dirección económico - financiera

13.1. Entorno económico
- 13.1.1. Entorno macroeconómico y el sistema financiero nacional
- 13.1.2. Instituciones financieras
- 13.1.3. Mercados financieros
- 13.1.4. Activos financieros
- 13.1.5. Otros entes del sector financiero

13.2. Contabilidad directiva
- 13.2.1. Conceptos básicos
- 13.2.2. El activo de la empresa
- 13.2.3. El pasivo de la empresa
- 13.2.4. El patrimonio neto de la empresa
- 13.2.5. La cuenta de resultados

13.3. Sistemas de información y *business intelligence*
- 13.3.1. Fundamentos y clasificación
- 13.3.2. Fases y métodos de reparto de costes
- 13.3.3. Elección de centro de costes y efecto

13.4. Presupuesto y control de gestión
- 13.4.1. El modelo presupuestario
- 13.4.2. El Presupuesto de capital
- 13.4.3. La Presupuesto de explotación
- 13.4.5. El Presupuesto de tesorería
- 13.4.6. Seguimiento del presupuesto

13.5. Dirección financiera
- 13.5.1. Las decisiones financieras de la empresa
- 13.5.2. El departamento financiero
- 13.5.3. Excedentes de tesorería
- 13.5.4. Riesgos asociados a la dirección financiera
- 13.5.5. Gestión de riesgos de la dirección financiera

13.6. Planificación financiera
- 13.6.1. Definición de la planificación financiera
- 13.6.2. Acciones a efectuar en la planificación financiera
- 13.6.3. Creación y establecimiento de la estrategia empresarial
- 13.6.4. El cuadro *cash flow*
- 13.6.5. El cuadro de circulante

13.7. Estrategia financiera corporativa
- 13.7.1. Estrategia corporativa y fuentes de financiación
- 13.7.2. Productos financieros de financiación empresarial

13.8. Financiación estratégica
- 13.8.1. La autofinanciación
- 13.8.2. Ampliación de fondos propios
- 13.8.3. Recursos híbridos
- 13.8.4. Financiación a través de intermediarios

13.9. Análisis y planificación financiera
- 13.9.1. Análisis del balance de situación
- 13.9.2. Análisis de la cuenta de resultados
- 13.9.3. Análisis de la rentabilidad

13.10. Análisis y resolución de casos/problemas
- 13.10.1. Información financiera de Industria de Diseño y Textil, S.A. (INDITEX)

Módulo 14. Dirección comercial y marketing estratégico

14.1. Dirección comercial
- 14.1.1. Marco conceptual de la dirección comercial
- 14.1.2. Estrategia y planificación comercial
- 14.1.3. El rol de los directores comerciales

14.2. Marketing
- 14.2.1. Concepto de marketing
- 14.2.2. Elementos básicos del marketing
- 14.2.3. Actividades de marketing de la empresa

14.3. Gestión estratégica del marketing
- 14.3.1. Concepto de marketing estratégico
- 14.3.2. Concepto de planificación estratégica de marketing
- 14.3.3. Etapas del proceso de planificación estratégica de marketing

14.4. Marketing digital y comercio electrónico
- 14.4.1. Objetivos del marketing digital y comercio electrónico
- 14.4.2. Marketing digital y medios que emplea
- 14.4.3. Comercio electrónico. Contexto general
- 14.4.4. Categorías del comercio electrónico
- 14.4.5. Ventajas y desventajas del *e-commerce* frente al comercio tradicional

14.5. Marketing digital para reforzar la marca
- 14.5.1. Estrategias online para mejorar la reputación de tu marca
- 14.5.2. *Branded content & storytelling*

14.6. Marketing digital para captar y fidelizar clientes
- 14.6.1. Estrategias de fidelización y vinculación a través de internet
- 14.6.2. *Visitor relationship management*
- 14.6.3. Hipersegmentación

14.7. Gestión de campañas digitales
- 14.7.1. ¿Qué es una campaña de publicidad digital?
- 14.7.2. Pasos para lanzar una campaña de marketing online
- 14.7.3. Errores de las campañas de publicidad digital

14.8. Estrategia de ventas
- 14.8.1. Estrategia de ventas
- 14.8.2. Métodos de ventas

14.9. Comunicación corporativa
- 14.9.1. Concepto
- 14.9.2. Importancia de la comunicación en la organización
- 14.9.3. Tipo de la comunicación en la organización
- 14.9.4. Funciones de la comunicación en la organización
- 14.9.5. Elementos de la comunicación
- 14.9.6. Problemas de la comunicación
- 14.9.7. Escenarios de la comunicación

14.10. Comunicación y reputación digital
- 14.10.1. Reputación online
- 14.10.2. ¿Cómo medir la reputación digital?
- 14.10.3. Herramientas de reputación online
- 14.10.4. Informe de reputación online
- 14.10.5. *Branding* online

Módulo 15. *Management* directivo

15.1. *General management*
- 15.1.1. Concepto de *general management*
- 15.1.2. La acción del *manager general*
- 15.1.3. El director general y sus funciones
- 15.1.4. Transformación del trabajo de la Dirección

15.2. El directivo y sus funciones. La cultura organizacional y sus enfoques
- 15.2.1. El directivo y sus funciones. La cultura organizacional y sus enfoques

15.3. Dirección de operaciones
- 15.3.1. Importancia de la dirección
- 15.3.2. La cadena de valor
- 15.3.3. Gestión de calidad

15.4. Oratoria y formación de portavoces
- 15.4.1. Comunicación interpersonal
- 15.4.2. Habilidades comunicativas e influencia
- 15.4.3. Barreras en la comunicación

15.5. Herramientas de. comunicaciones personales y organizacional
- 15.5.1. La comunicación interpersonal
- 15.5.2. Herramientas de la comunicación interpersonal
- 15.5.3. La comunicación en la organización
- 15.5.4. Herramientas en la organización

15.6. Comunicación en situaciones de crisis
- 15.6.1. Crisis
- 15.6.2. Fases de la crisis
- 15.6.3. Mensajes: contenidos y momentos

15.7. Preparación de un plan de crisis
- 15.7.1. Análisis de posibles problemas
- 15.7.2. Planificación
- 15.7.3. Adecuación del personal

15.8. Inteligencia emocional
- 15.8.1. Inteligencia emocional y comunicación
- 15.8.2. Asertividad, empatía y escucha activa
- 15.8.3. Autoestima y comunicación emocional

15.9. *Branding* personal
- 15.9.1. Estrategias para desarrollar la marca personal
- 15.9.2. Leyes del *branding* personal
- 15.9.3. Herramientas de la construcción de marcas personales

15.10. Liderazgo y gestión de equipos
- 15.10.1. Liderazgo y estilos de liderazgo
- 15.10.2. Capacidades y desafíos del líder
- 15.10.3. Gestión de procesos de cambio
- 15.10.4. Gestión de equipos multiculturales

Integrarás la Ciberseguridad en la gobernanza corporativa y en la cultura organizacional de cualquier institución"

04

Objetivos docentes

Esta titulación universitaria tiene como propósito resaltar la importancia estratégica de la Dirección de Ciberseguridad en contextos altamente digitalizados. A través de un enfoque integral, se impulsará al profesional en el desarrollo de competencias vinculadas a la gestión de incidentes y la coordinación de equipos especializados. De este modo, se fortalecerá la capacidad de liderar procesos de defensa tecnológica con una visión directiva, orientada tanto a la prevención como a la respuesta eficaz ante riesgos emergentes.

Garantizarás la evaluación continua de amenazas persistentes y su adecuada gestión en entornos digitales altamente expuestos”

Objetivos generales

- Comprender en profundidad los principios fundamentales de la ciberseguridad y su aplicación estratégica en el entorno empresarial
- Ahondar en las configuraciones esenciales para garantizar la seguridad en *host* frente a vulnerabilidades internas y externas
- Integrar mecanismos de protección perimetral en redes corporativas, reforzando la defensa ante accesos no autorizados
- Ahondar en la seguridad móvil, evaluando riesgos y aplicando soluciones efectivas en dispositivos inteligentes
- Reconocer los desafíos de la seguridad en IoT y aplicar protocolos para minimizar riesgos en sistemas interconectados
- Emplear técnicas de *hacking* ético para evaluar la robustez de sistemas y proponer mejoras de seguridad
- Aplicar conocimientos de ingeniería inversa para descomponer software malicioso y detectar su funcionamiento interno
- Incorporar prácticas de desarrollo seguro en el diseño de aplicaciones y sistemas tecnológicos
- Utilizar herramientas de análisis forense para investigar incidentes y preservar evidencia digital
- Evaluar retos emergentes en ciberseguridad, proyectando escenarios futuros con un enfoque de liderazgo ético

Objetivos específicos

Módulo 1. Ciberinteligencia y Ciberseguridad

- Examinar el ciclo de inteligencia como base operativa para la recolección y análisis de datos relevantes en Ciberseguridad
- Distinguir el rol del analista de inteligencia, considerando los sesgos que pueden afectar su juicio evaluativo
- Identificar técnicas de ingeniería social utilizadas comúnmente en escenarios de ataque digital
- Integrar metodologías de análisis y evaluación para validar la fiabilidad de las fuentes de información

Módulo 2. Seguridad en *host*

- Establecer estrategias efectivas de respaldo en diferentes sistemas operativos, garantizando la integridad de los datos ante posibles incidentes
- Evaluar las capacidades de los principales antivirus y herramientas HIDS, según el entorno operativo
- Emplear técnicas de detección y mitigación frente a amenazas como *phishing*, *spyware* o rastreadores, a través de soluciones especializadas
- Implementar controles sobre la instalación de *software*, considerando criterios de seguridad, permisos y políticas de actualización

Módulo 3. Seguridad en red (perimetral)

- Diferenciar los tipos de arquitecturas perimetrales, así como sus sistemas de detección y prevención, valorando su impacto en la protección de redes
- Configurar soluciones antispam y *mail gateway* para reducir vulnerabilidades en la comunicación por correo electrónico
- Examinar la utilidad de plataformas SIEM y SOAR en la gestión automatizada de incidentes y en la toma de decisiones basada en eventos

Módulo 4. Seguridad en *smartphones*

- Reconocer las principales plataformas móviles y sus implicaciones en la seguridad del dispositivo
- Interpretar las vulnerabilidades más frecuentes en entornos móviles según el proyecto OWASP
- Establecer políticas de seguridad efectivas para el uso empresarial de dispositivos móviles
- Aplicar medidas de protección de datos personales, como cifrado, permisos y almacenamiento seguro
- Ejecutar pruebas de penetración en sistemas iOS y Android utilizando herramientas especializadas

Módulo 5. Seguridad en IoT

- Clasificar los dispositivos IoT según su arquitectura, conectividad y área de aplicación
- Examinar los principales protocolos de comunicación utilizados en entornos IoT
- Determinar los riesgos asociados a la implementación de soluciones IoT en sectores como salud, transporte y *SmartCity*
- Integrar mecanismos de securización en redes IoT mediante cifrado, autenticación y buenas prácticas

Módulo 6. *Hacking* ético

- Reconocer las principales metodologías de *pentesting* empleadas en entornos profesionales
- Aplicar técnicas de *footprinting* y escaneo para detectar vulnerabilidades en sistemas y redes
- Utilizar herramientas de análisis de vulnerabilidades y sistemas de puntuación para priorizar riesgos

- Ejecutar ataques simulados en redes inalámbricas y servidores web con fines de auditoría ética
- Implementar técnicas de explotación y persistencia para evaluar el impacto de brechas de seguridad

Módulo 7. Ingeniería inversa

- Comprender la estructura interna de un compilador y sus fases fundamentales en el proceso de traducción de código
- Emplear herramientas de desensamblado y depuración para el análisis estático y dinámico de binarios
- Investigar el comportamiento de *malware* mediante métodos de análisis y técnicas de contramedida frente a la ofuscación

Módulo 8. Desarrollo seguro

- Integrar medidas de seguridad en cada etapa del ciclo de vida del desarrollo de *software*, desde los requerimientos hasta el mantenimiento
- Diseñar sistemas con controles robustos de autenticación, gestión de sesiones y manejo de errores orientados a minimizar riesgos
- Aplicar buenas prácticas de codificación segura, incluyendo la validación de datos, el uso adecuado de criptografía y el control de la memoria

Módulo 9. Análisis forense

- Realizar la adquisición y validación de datos forenses, asegurando su integridad y cadena de custodia
- Identificar y mitigar técnicas antiforenses utilizadas para ocultar, modificar o eliminar evidencia digital
- Aplicar metodologías de análisis forense en sistemas operativos, redes, aplicaciones web y bases de datos
- Profundizar en los principales incidentes de seguridad en entornos *cloud*, considerando sus particularidades y desafíos

Módulo 10. Retos actuales y futuros en seguridad Informática

- Identificar los ámbitos de aplicación de la tecnología *blockchain* y su papel en la seguridad Informática
- Examinar el impacto de los *deepfakes* en los medios y la sociedad, junto con sus mecanismos de detección
- Analizar la evolución de la ciberseguridad ante el crecimiento del teletrabajo y las tecnologías emergentes

Módulo 11. Liderazgo, ética y responsabilidad social de las empresas

- Analizar el impacto de la globalización en la gobernanza y el gobierno corporativo
- Evaluar la importancia del liderazgo efectivo en la dirección y éxito de las empresas
- Definir las estrategias de gestión intercultural y su relevancia en entornos empresariales diversos
- Desarrollar habilidades de liderazgo y entender los desafíos actuales que enfrentan los líderes
- Determinar los principios y prácticas de la ética empresarial y su aplicación en la toma de decisiones corporativas

Módulo 12. Dirección de personas y gestión del talento

- Determinar la relación entre la dirección estratégica y la gestión de recursos humanos
- Profundizar las competencias necesarias para la gestión eficaz de recursos humanos por competencias
- Ahondar en las metodologías para la evaluación del rendimiento y la gestión del desempeño

- Integrar las innovaciones en la gestión del talento y su impacto en la retención y fidelización del personal
- Desarrollar estrategias para la motivación y el desarrollo de equipos de alto desempeño

Módulo 13. Dirección económico - financiera

- Analizar el entorno macroeconómico y su influencia en el sistema financiero nacional e internacional
- Definir los sistemas de información y *business intelligence* para la toma de decisiones financieras
- Valorar estrategias para la planificación financiera y la obtención de financiación empresarial

Módulo 14. Dirección comercial y marketing estratégico

- Estructurar el marco conceptual y la importancia de la Dirección comercial en las empresas
- Ahondar en los elementos y actividades fundamentales del marketing y su impacto en la organización
- Evaluar estrategias para mejorar la comunicación corporativa y la reputación digital de la empresa

Módulo 15. *Management* directivo

- Definir el concepto de general *management* y su relevancia en la gestión de empresas
- Analizar la importancia de la dirección de operaciones y la gestión de la calidad en la cadena de valor
- Desarrollar habilidades de comunicación interpersonal y oratoria para la formación de portavoces

05

Salidas profesionales

Este Máster Título Propio de TECH constituye una opción académica de referencia para profesionales de la informática que buscan dominar los entornos críticos de la seguridad digital. Asimismo, los egresados manejarán las herramientas más modernas para la realización de auditorías, análisis de vulnerabilidades y gestión de riesgos.
De igual modo, los alumnos obtendrán un enfoque integral sobre la Ciberinteligencia fundamentado en el cumplimiento normativo y la protección de infraestructuras. Sin duda, una experiencia rigurosa y actualizada que les permitirá liderar la Ciberseguridad en entornos organizacionales complejos.

¿Quieres desempeñarte como Asesor en Políticas de Seguridad Digital? Este programa universitario te otorgará las claves para lograrlo en solo 7 meses"

Perfil del egresado

El egresado de este contará con un perfil altamente especializado para intervenir en escenarios críticos vinculados a la seguridad informática. Por lo tanto, dominará procesos de autenticación, técnicas de encriptación avanzada y mecanismos de protección frente a intrusiones. Asimismo, adquirirá competencias para analizar comportamientos sospechosos en infraestructuras digitales, coordinar protocolos de respuesta ante incidentes y optimizar la privacidad de la información. En paralelo, desarrollará habilidades para liderar equipos multidisciplinares, impulsar mejoras continuas en entornos corporativos y adaptarse con agilidad a los cambios tecnológicos que transforman el panorama de los riesgos digitales.

Guiarás a las instituciones en la implementación de marcos normativos, políticas de acceso y planes de concienciación en seguridad Informática.

- **Pensamiento Crítico:** Capacidad para evaluar situaciones complejas desde una perspectiva analítica, cuestionando la validez de las evidencias digitales y tomando decisiones fundamentadas en datos precisos
- **Resolución de Problemas:** Aptitud que permite identificar de manera ágil de vulnerabilidades o incidentes informáticos, así como la aplicación de soluciones eficaces en contextos cambiantes y de alta presión
- **Comunicación Efectiva:** Destreza para transmitir hallazgos técnicos con claridad tanto a perfiles especializados como a equipos no técnicos, mejorando la colaboración y la toma de decisiones estratégicas
- **Adaptabilidad Tecnológica:** Los profesionales están preparados para incorporar de manera constante de nuevos recursos digitales, herramientas y entornos, imprescindible en un sector en evolución continua como la Ciberseguridad

Después de realizar el programa universitario, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Administrador de Infraestructuras Seguras:** Encargado de gestionar sistemas y redes aplicando protocolos avanzados de Ciberseguridad que garanticen la continuidad operativa y la protección ante intrusiones.
2. **Técnico en Gestión de Vulnerabilidades:** Especialista en realizar escaneos periódicos, interpretar resultados y aplicar medidas correctivas para mitigar riesgos en sistemas operativos y aplicaciones.
3. **Consultor en Arquitectura Segura de Redes:** Diseña infraestructuras resistentes a ciberataques mediante la segmentación de redes, firewalls de nueva generación y políticas de acceso granular.
4. **Asesor en Protección de Datos Empresariales:** Experto en diseñar estrategias que aseguren la confidencialidad, integridad y disponibilidad de la información en entornos corporativos.

Destacarás por tu responsabilidad en la protección de activos digitales y la privacidad de los datos confidenciales"

06

Licencias de software incluidas

TECH es referencia en el mundo universitario por combinar la última tecnología con las metodologías docentes para potencial el proceso de enseñanza-aprendizaje. Para ello, ha establecido una red de alianzas que le permite tener acceso a las herramientas de software más avanzadas del mundo profesional.

Al matricularte recibirás, de forma completamente gratuita, las credenciales de uso académico de las siguientes aplicaciones de software profesional"

TECH ha establecido una red de alianzas profesionales en la que se encuentran los principales proveedores de software aplicado a las diferentes áreas profesionales. Estas alianzas permiten a TECH tener acceso al uso de centenares de aplicaciones informáticas y licencias de software para acercarlas a sus estudiantes.

Las licencias de software para uno académico permitirán a los estudiantes utilizar las aplicaciones informáticas más avanzadas en su área profesional, de modo que podrán conocerlas y aprender su dominio sin tener que incurrir en costes. TECH se hará cargo del procedimiento de contratación para que los alumnos puedan utilizarlas de modo ilimitado durante el tiempo que estén estudiando el programa de Máster Título Propio MBA en Dirección de Ciberseguridad (CISO, *Chief Information Security Officer*), y además lo podrán hacer de forma completamente gratuita.

TECH te dará acceso gratuito al uso de las siguientes aplicaciones de software:

Google Career Launchpad

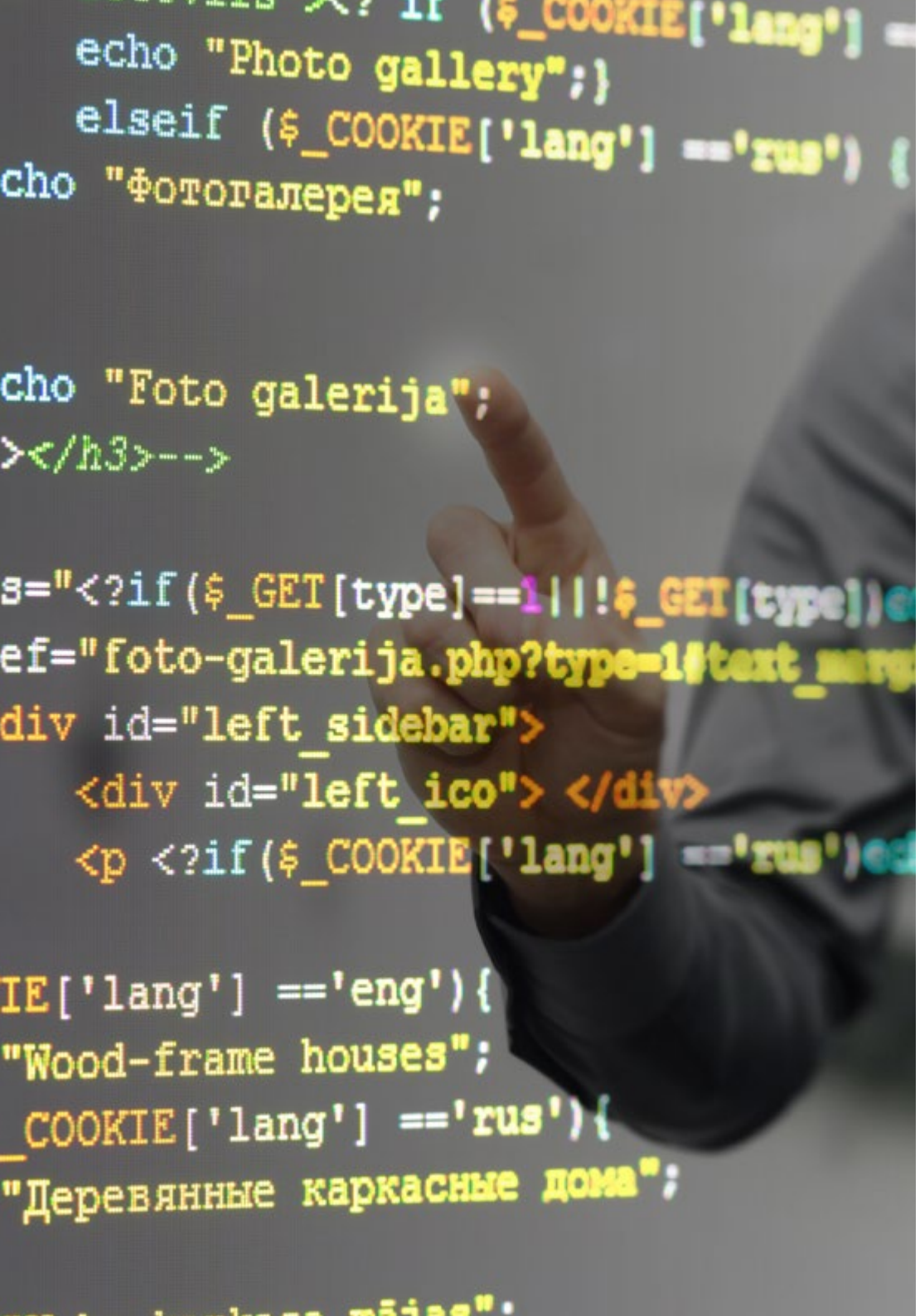
Google Career Launchpad es una solución para desarrollar habilidades digitales en tecnología y análisis de datos. Con un valor estimado de **5.000 dólares**, se incluye de forma **gratuita** en el programa universitario de TECH, brindando acceso a laboratorios interactivos y certificaciones reconocidas en el sector.

Esta plataforma combina capacitación técnica con casos prácticos, usando tecnologías como BigQuery y Google AI. Ofrece entornos simulados para experimentar con datos reales, junto a una red de expertos para orientación personalizada.

Funcionalidades destacadas:

- **Cursos especializados:** contenido actualizado en cloud computing, machine learning y análisis de datos
- **Laboratorios en vivo:** prácticas con herramientas reales de Google Cloud sin configuración adicional
- **Certificaciones integradas:** preparación para exámenes oficiales con validez internacional
- **Mentorías profesionales:** sesiones con expertos de Google y partners tecnológicos
- **Proyectos colaborativos:** retos basados en problemas reales de empresas líderes

En conclusión, **Google Career Launchpad** conecta a los usuarios con las últimas tecnologías del mercado, facilitando su inserción en áreas como inteligencia artificial y ciencia de datos con credenciales respaldadas por la industria.



Gracias a TECH podrás utilizar gratuitamente las mejores aplicaciones de software de tu área profesional”

07

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.

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.

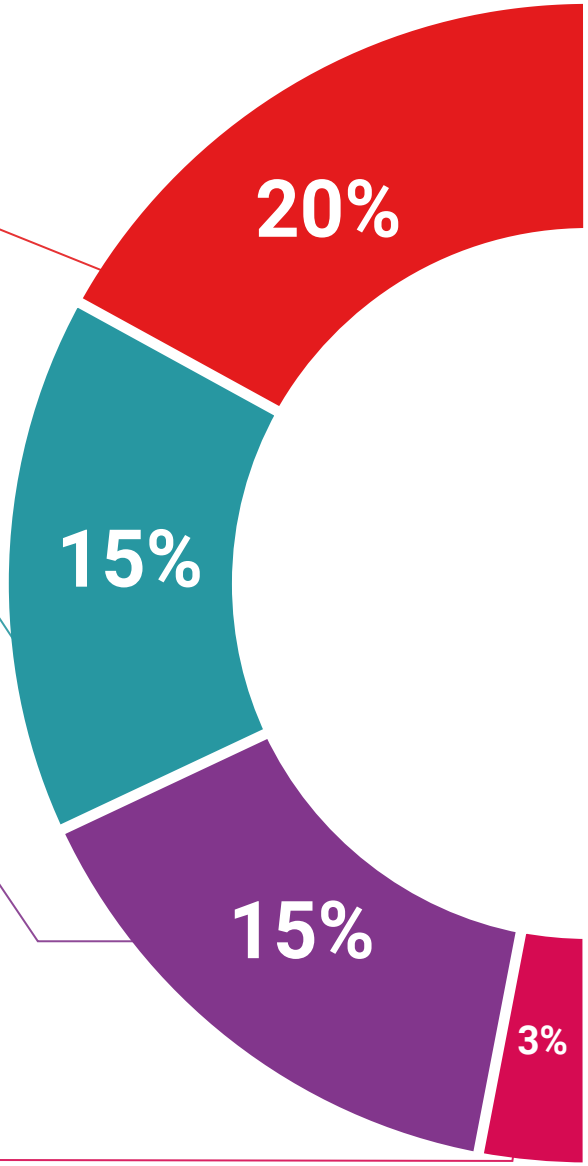
Resúmenes interactivos

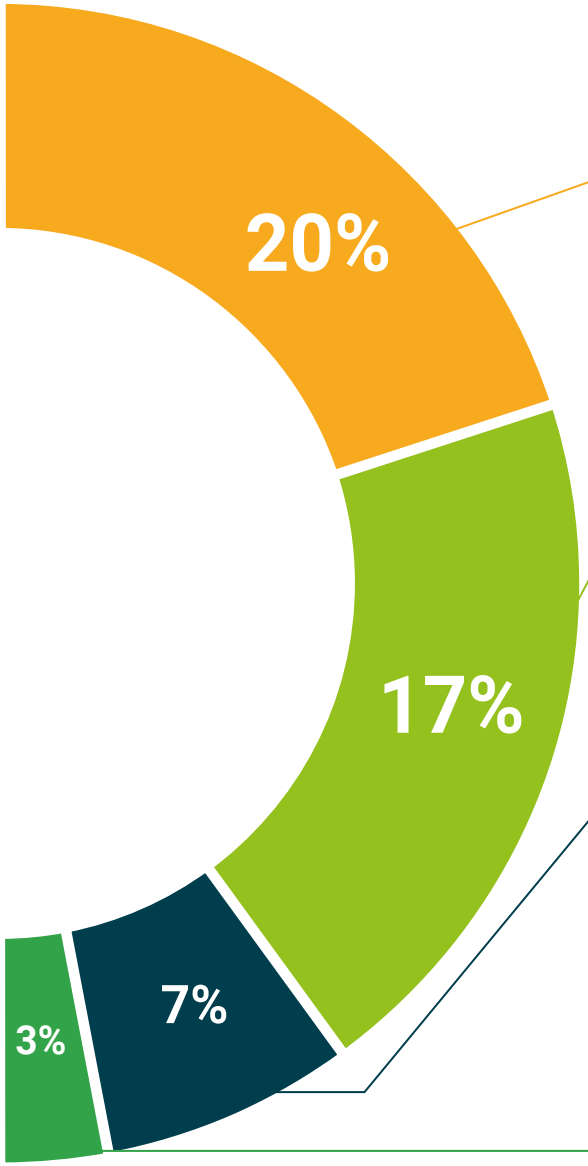
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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.

08

Cuadro docente

Este Máster Título Propio MBA en Dirección de Ciberseguridad (CISO, *Chief Information Security Officer*) ha sido diseñado por un equipo multidisciplinar con una sólida trayectoria laboral. Así pues, han formado parte de reconocidas instituciones para optimizar la protección de infraestructuras críticas, el desarrollo de normativas internacionales y la gestión de incidentes de alto impacto. Así pues, su experiencia ha permitido estructurar un itinerario académico que combina el rigor técnico con la aplicabilidad real en entornos corporativos de máxima exigencia.

Disfrutarás del asesoramiento personalizado del equipo docente, integrado por auténticas diferencias en la Dirección de Ciberseguridad”

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

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

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 **sintetizar 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 Luminate 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 *Bussiness 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!"

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (*Chief Security Officer/Senior Security Architect*) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Profesores

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la Gestión, Coordinación y Documentación del Entorno Virtualizado de Alarmas de Seguridad
- Analista Programadora de Aplicaciones Java para cajeros automáticos
- Profesional del Desarrollo de *Software* para Aplicación de Validación de Firma y Gestión Documental
- Técnico de Sistemas para la Migración de Equipos y para la Gestión, Mantenimiento y Formación de Dispositivos Móviles PDA
- Ingeniero Técnico de Informática de Sistemas por la Universidad Oberta de Cataluña
- Máster en Seguridad Informática y Hacking Ético Oficial de EC- Council y CompTIA por la Escuela Profesional de Nuevas Tecnologías CICE

D. Catalá Barba, José Francisco

- Técnico Electrónico Experto en Ciberseguridad
- Desarrollador de Aplicaciones para Dispositivos Móviles
- Técnico Electrónico en Mando Intermedio en el Ministerio de la Defensa de España
- Técnico Electrónico en Factoría Ford Sita en Valencia

D. Peralta Alonso, Jon

- Consultor Sénior de Protección de Datos y Ciberseguridad en Altia
- Abogado / Asesor jurídico en Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Asesor Jurídico / Pasante en Despacho Profesional: Óscar Padura
- Grado en Derecho por la Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos por EIS Innovative School
- Máster Universitario en Abogacía por la Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil por la Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC

D. Jiménez Ramos, Álvaro

- Analista de Ciberseguridad
- Analista de Seguridad Sénior en The Workshop
- Analista de Ciberseguridad L1 en Axians
- Analista de Ciberseguridad L2 en Axians
- Analista de Ciberseguridad en SACYR S.A.
- Grado en Ingeniería Telemática por la Universidad Politécnica de Madrid
- Máster de Ciberseguridad y Hacking Ético por CICE
- Curso Superior de Ciberseguridad por Deusto Formación

D. Redondo, Jesús Serrano

- Desarrollador Web y Técnico en Ciberseguridad
- Desarrollador Web en Roams, Palencia
- Desarrollador *FrontEnd* en Telefónica, Madrid
- Desarrollador *FrontEnd* en Best Pro Consulting SL, Madrid
- Instalador de Equipos y Servicio de Telecomunicaciones en Grupo Zener, Castilla y León
- Instalador de Equipos y Servicios de Telecomunicaciones en Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática por CFTIC Getafe, Madrid
- Técnico Superior en Sistemas Telecomunicaciones e Informáticos por IES Trinidad Arroyo, Palencia
- Técnico Superior en Instalaciones Electrotécnicas MT y BT por IES Trinidad Arroyo, Palencia
- Formación en Ingeniería Inversa, Estenografía y Cifrado por la Academia Hacker Incibe

Una experiencia de capacitación única, clave y decisiva para impulsar tu desarrollo profesional"

09

Titulación

Este MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Propio expedido por TECH Global University.

Supera con éxito este programa y recibe tu titulación universitaria sin desplazamientos ni farragosos trámites”

Este programa te permitirá obtener el título propio de **MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra ***(boletín oficial)***. Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio.El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

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

BUSINESS GRADUATES ASSOCIATION MEMBER

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

Modalidad: **online**

Duración: **12 meses**

Acreditación: **90 ECTS**

tech global university

D/Dña _____, con documento de identificación _____ ha superado con éxito y obtenido el título de:

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

Se trata de un título propio de 2.700 horas de duración equivalente a 90 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código única TECH: AFWOR23S techtitute.com/titulos

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

Distribución General del Plan de Estudios

Tipo de materia	Créditos ECTS
Obligatoria (OB)	90
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
	Total 90

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Ciberinteligencia y Ciberseguridad	6	OB
1º	Seguridad en *host*	6	OB
1º	Seguridad en red (perimetral)	6	OB
1º	Seguridad en *smartphones*	6	OB
1º	Seguridad en IoT	6	OB
1º	Hacking ético	6	OB
1º	Ingeniería inversa	6	OB
1º	Desarrollo seguro	6	OB
1º	Análisis forense	6	OB
1º	Retos actuales y futuros en seguridad Informática	6	OB
1º	Liderazgo, ética y responsabilidad social de las empresas	6	OB
1º	Dirección de personas y gestión del talento	6	OB
1º	Dirección económico-financiera	6	OB
1º	Dirección comercial y marketing estratégico	6	OB
1º	*Management* directivo	6	OB

Dr. Pedro Navarro Illana
Rector

tech global university

*Apostilla de La Haya. En caso de que el alumno solicite que su título en papel recabe la Apostilla de La Haya, TECH Global University realizará las gestiones oportunas para su obtención, con un coste adicional.

tech global university

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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Global University**
- Acreditación: **90 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio

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

Aval/Membresía