Máster Título Propio

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

tech universidad tecnológica

tech universidad tecnológica

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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-direccion-ciberseguridad-ciso-chief-information-security-officer**

Índice

01

Presentación

A la vez que avanza la tecnología, también lo hacen las amenazas, perfeccionando sus técnicas de ataque. Es decir, crecen las posibilidades y vías que tienen los ciberdelincuentes para conseguir sus objetivos. Es bajo este contexto que TECH presenta una titulación con la que los profesionales podrán ponerse al día, aprendiendo de manera exhaustiva a proteger y asegurar diversos entornos digitales. Todo ello, mediante una metodología revolucionaria, el relearning; y en un cómodo formato totalmente online, que permitirá al egresado adquirir habilidades y destrezas sin un timing prestablecido. Así, al finalizar esta titulación, el profesional obtendrá unas capacidades y competencias necesarias para ejercer con gran eficiencia Chief Information Security Officer, un cargo de alta dirección y con gran prestigio, así como con altas perspectivas de crecimiento y expansión.

Al tiempo que la tecnología y la conectividad avanzan, también crecen el número y la forma de las amenazas posibles. Por eso, es crucial que los futuros Chief Information Security Officer actualicen sus conocimientos para ofrecer soluciones más adaptadas a la idiosincrasia de la empresa"

Para nadie es un secreto que estamos en plena era de la información y comunicación, pues todos estamos conectados tanto en el entorno doméstico como en los entornos corporativos. Así, tenemos acceso a multitud de información con un solo clic, con una única búsqueda en cualquiera de los motores que tenemos a nuestra disposición, ya sea desde un Smartphone, ordenador personal o del trabajo.

Al igual que avanza la tecnología para el ciudadano y empleado medio, también lo hacen las amenazas y las técnicas de ataque. Cuantas más nuevas funcionalidades existen y más comunicados estamos, más aumenta la superficie de ataque. Ante este preocupante contexto, TECH lanza este MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer), el cual ha sido desarrollado por un equipo con diferentes perfiles profesionales especializados en los diferentes sectores que combinan experiencia profesional internacional en el ámbito privado en I+D+i y amplia experiencia docente.

Asimismo, este Máster Título Propio le aporta al alumno unas excelentes y completas lecciones extras, impartidas por un especialista en Inteligencia, Ciberseguridad y Tecnologías Disruptivas de prestigio internacional. Este contenido innovador será accesible con el formato de 10 *Masterclasses* exclusivas, las cuales le permitirán al egresado actualizarse en Ciberseguridad y dirigir los departamentos encargados de estas tareas en las más importantes empresas del sector tecnológico.

El programa engloba las diferentes materias troncales del área de la ciberseguridad, seleccionadas cuidadosamente para cubrir, de forma rigurosa, un amplio espectro de las tecnologías aplicables en los diferentes ámbitos laborales. Pero también tratará otra rama de materias que suelen escasear en el catálogo académico de otras instituciones y que nutrirán de manera profunda el currículo del profesional. De esta forma, y gracias a los conocimientos trasversales que ofrece TECH con este programa, el egresado adquirirá las competencias para ejercer como directivo en el área de la ciberseguridad (Chief Information Security Officer) aumentando así sus perspectivas de crecimiento personal y profesional.

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

- El desarrollo de casos prácticos presentados por expertos en ciberseguridad
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido 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
- 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

¡Prepárate con los mejores profesionales! Aprovecha las 10 Masterclasses impartidas por un docente de renombre internacional"

Destaca en un sector en auge y conviértete en todo un experto en ciberseguridad con este MBA de TECH. Es el más completo del mercado”

Las formas en las que las personas intercambian información evolucionan de manera vertiginosa. Esto exige a los profesionales nuevas formas de protección cibernética.

Un programa 100% online y con un enfoque eminentemente práctico que sentará las bases de tu crecimiento profesional.

El programa incluye en su cuadro docente a profesionales del sector que vierten en esta capacitación 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 una capacitación inmersiva programada para entrenarse ante situaciones reales.

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

02

Objetivos

Siendo plenamente conscientes de la relevancia que tiene la ciberseguridad para empresas y personas, TECH ha desarrollado este MBA que tiene como objetivo nutrir y actualizar los conocimientos de los profesionales en materia de detección, protección y prevención de delitos informáticos. De esta manera, el futuro egresado se convertirá en una pieza clave en el cuidado de los datos y la información, minimizando la posibilidad de que los delincuentes se beneficien de posibles brechas de seguridad existente. Una competencia profesionalmente que en TECH, en tan solo 12 meses, el profesional podrá adquirir.

Estás ante una ocasión única de hacer realidad tus sueños y metas y convertirte en todo un experto en ciberseguridad”

Objetivos generales

- Analizar el rol del Analista en Ciberseguridad
- Profundizar en la Ingeniería Social y sus métodos
- Examinar las metodologías OSINT, HUMINT, OWASP, PTEC. OSSTM, OWISAM
- Realizar un análisis de riesgo y conocer las métricas de riesgo
- Determinar el adecuado uso de anonimato y uso de redes como TOR, I2P y Freenet
- Compilar las normativas vigentes en materia de ciberseguridad
- Generar conocimiento especializado para realizar una Auditoría de Seguridad
- Desarrollar políticas de uso apropiadas
- Examinar los Sistemas de detección y prevención de las amenazas más importantes
- Evaluar nuevos sistemas de detección de amenazas, así como su evolución respecto a soluciones más tradicionales
- Analizar las principales plataformas móviles actuales, características y uso de las mismas
- Identificar, Analizar y evaluar riesgos de seguridad de las partes del proyecto IoT
- Evaluar la información obtenida y desarrollar mecanismos de prevención y hacking
- Aplicar la Ingeniería Inversa al entorno de la ciberseguridad
- Concretar las pruebas que hay que realizar al software desarrollado
- Recopilar todas las pruebas y datos existentes para llevar a cabo un Informe forense
- Presentar debidamente el informe forense
- Analizar el estado actual y futuro de la seguridad informática
- Examinar los riesgos de las nuevas tecnologías emergentes
- Compilar las distintas tecnologías en relación a la seguridad informática

Objetivos específicos

Módulo 1. Ciberinteligencia y ciberseguridad

- Desarrollar las metodologías usadas en materia de ciberseguridad
- Examinar el ciclo de inteligencia y establecer su aplicación en la Ciberinteligencia
- Determinar el papel del analista de inteligencia y los obstáculos de actividad evacuativa
- Analizar las metodologías OSINT, OWISAM, OSSTM, PTES, OWASP
- Establecer las herramientas más comunes para la producción de inteligencia
- Llevar a cabo un análisis de riesgos y conocer las métricas usadas
- Concretar las opciones de anonimato y el uso de redes como TOR, I2P, FreeNet
- Detallar las Normativas vigentes en Ciberseguridad

Módulo 2. Seguridad en host

- Concretar las políticas de *backup* de los datos de personales y profesionales
- Valorar las diferentes herramientas para dar soluciones a problemas específicos de seguridad
- Establecer mecanismos para tener un sistema actualizado
- Analizar el equipo para detectar intrusos
- Determinar las reglas de acceso al sistema
- Examinar y clasificar los correos para evitar fraudes
- Generar listas de software permitido

Módulo 3. Seguridad en red (perimetral)

- Analizar las arquitecturas actuales de red para identificar el perímetro que debemos proteger
- Desarrollar las configuraciones concretas de firewall y en Linux para mitigar los ataques más comunes
- Compilar las soluciones más usadas como Snort y Suricata, así como su configuración
- Examinar las diferentes capas adicionales que proporcionan los *firewalls* de nueva generación y funcionalidades de red en entornos Cloud
- Determinar las herramientas para la protección de la red y demostrar por qué son fundamentales para una defensa multicapa

Módulo 4. Seguridad en smartphones

- Examinar los distintos vectores de ataque para evitar convertirse en un blanco fácil
- Determinar los principales ataques y tipos de Malware a los que se exponen los usuarios de dispositivos móviles
- Analizar los dispositivos más actuales para establecer una mayor seguridad en la configuración
- Concretar los pasos principales para realizar una prueba de penetración tanto en plataformas iOS como en plataformas Android
- Desarrollar conocimiento especializado sobre las diferentes herramientas de protección y seguridad
- Establecer buenas prácticas en programación orientadas a dispositivos móviles

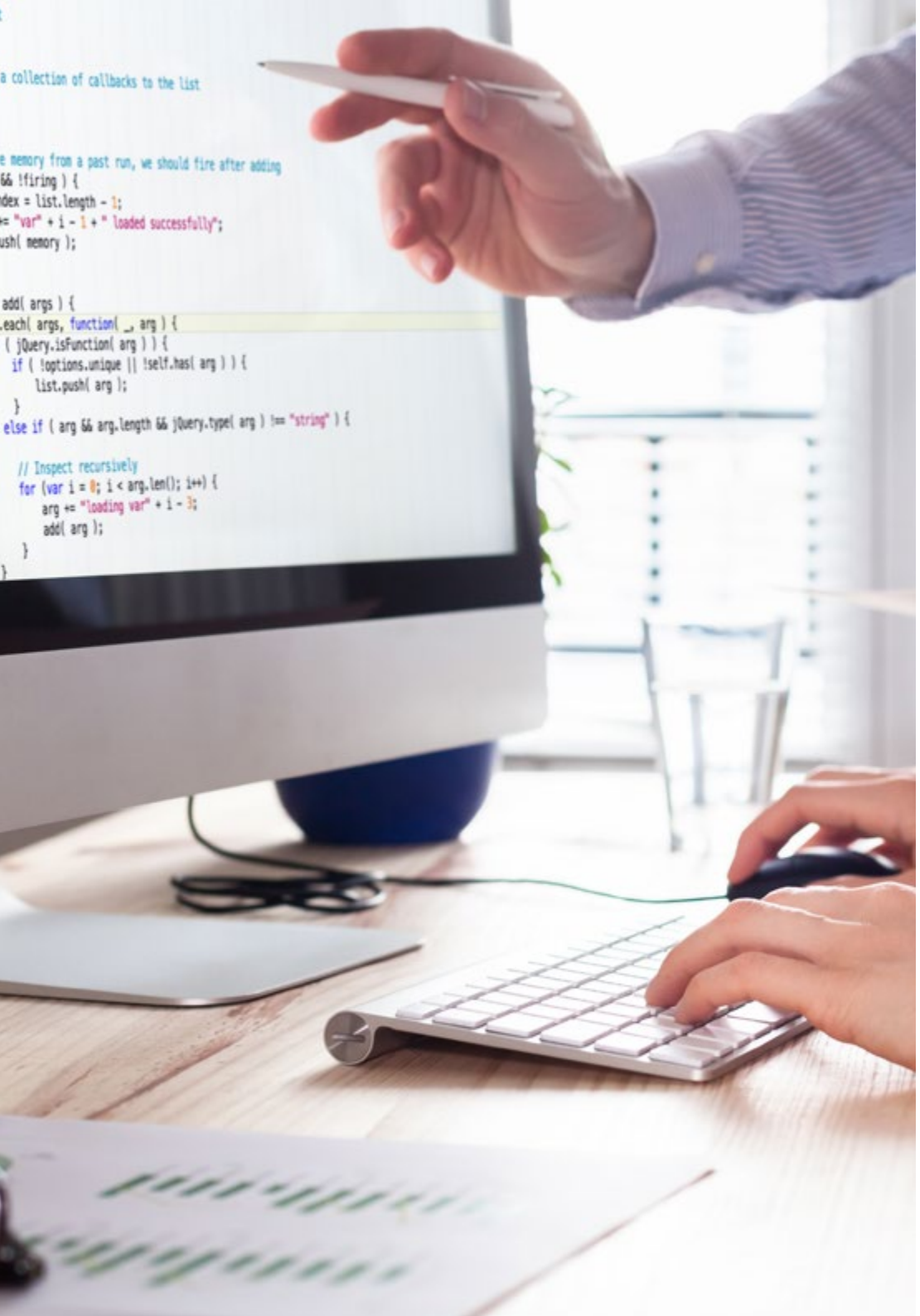
Módulo 5. Seguridad en IoT
- Analizar las principales arquitecturas de IoT
- Examinar las tecnologías de conectividad
- Desarrollar los protocolos de aplicación principales
- Concretar los diferentes tipos de dispositivos existentes
- Evaluar los niveles de riesgo y vulnerabilidades conocidas
- Desarrollar políticas de uso seguras
- Establecer las condiciones de uso apropiadas para estos dispositivos

Módulo 6. Hacking ético
- Examinar los métodos de IOSINT
- Recopilar la información disponible en medios públicos
- Escanear redes para obtener información de modo activo
- Desarrollar laboratorios de pruebas
- Analizar las herramientas para el desempeño del *pentesting*
- Catalogar y evaluar las diferentes vulnerabilidades de los sistemas
- Concretar las diferentes metodologías de *hacking*

Módulo 7. Ingeniería inversa
- Analizar las fases de un compilador
- Examinar la arquitectura de procesadores x86 y la arquitectura de procesadores ARM
- Determinar los diferentes tipos de análisis
- Aplicar *sandboxing* en diferentes entornos
- Desarrollar las diferentes técnicas de análisis de *malware*
- Establecer las herramientas orientadas al análisis de *malware*

Módulo 8. Desarrollo seguro
- Establecer los requisitos necesarios para el correcto funcionamiento de una aplicación de forma segura
- Examinar los archivos de *logs* para entender los mensajes de error
- Analizar los diferentes eventos y decidir qué mostrar al usuario y qué guardar en los *logs*
- Generar un Código Sanitizado, fácilmente verificable y de calidad
- Evaluar la documentación adecuada para cada fase del desarrollo
- Concretar el comportamiento del servidor para optimizar el sistema
- Desarrollar Código Modular, reusable y mantenible

Módulo 9. Análisis forense
- Identificar los diferentes elementos que ponen en evidencia un delito
- Generar conocimiento especializado para Obtener los datos de los diferentes medios antes de que se pierdan
- Recuperar los datos que hayan sido borrados intencionadamente
- Analizar los registros y los logs de los sistemas
- Determinar cómo se Duplican los datos para no alterar los originales
- Fundamentar las pruebas para que sean consistentes
- Generar un informe sólido y sin fisuras
- Presentar las conclusiones de forma coherente
- Establecer cómo Defender el informe ante la autoridad competente
- Concretar estrategias para que el teletrabajo sea seguro



Módulo 10. Retos actuales y futuros en seguridad informática

- Examinar el uso de las Criptomonedas, el impacto en la economía y la seguridad
- Analizar la situación de los usuarios y el grado de analfabetismo digital
- Determinar el ámbito de uso de *Blockchain*
- Presentar alternativas a IPv4 en el Direccionamiento de Redes
- Desarrollar estrategias para formar a la población en el uso correcto de las tecnologías
- Generar conocimiento especializado para hacer frente a los nuevos retos de seguridad y evitar la suplantación de identidad
- Concretar estrategias para que el teletrabajo sea seguro

Un programa único e ideal si estás buscando aumentar tus conocimientos en ciberseguridad"

03

Competencias

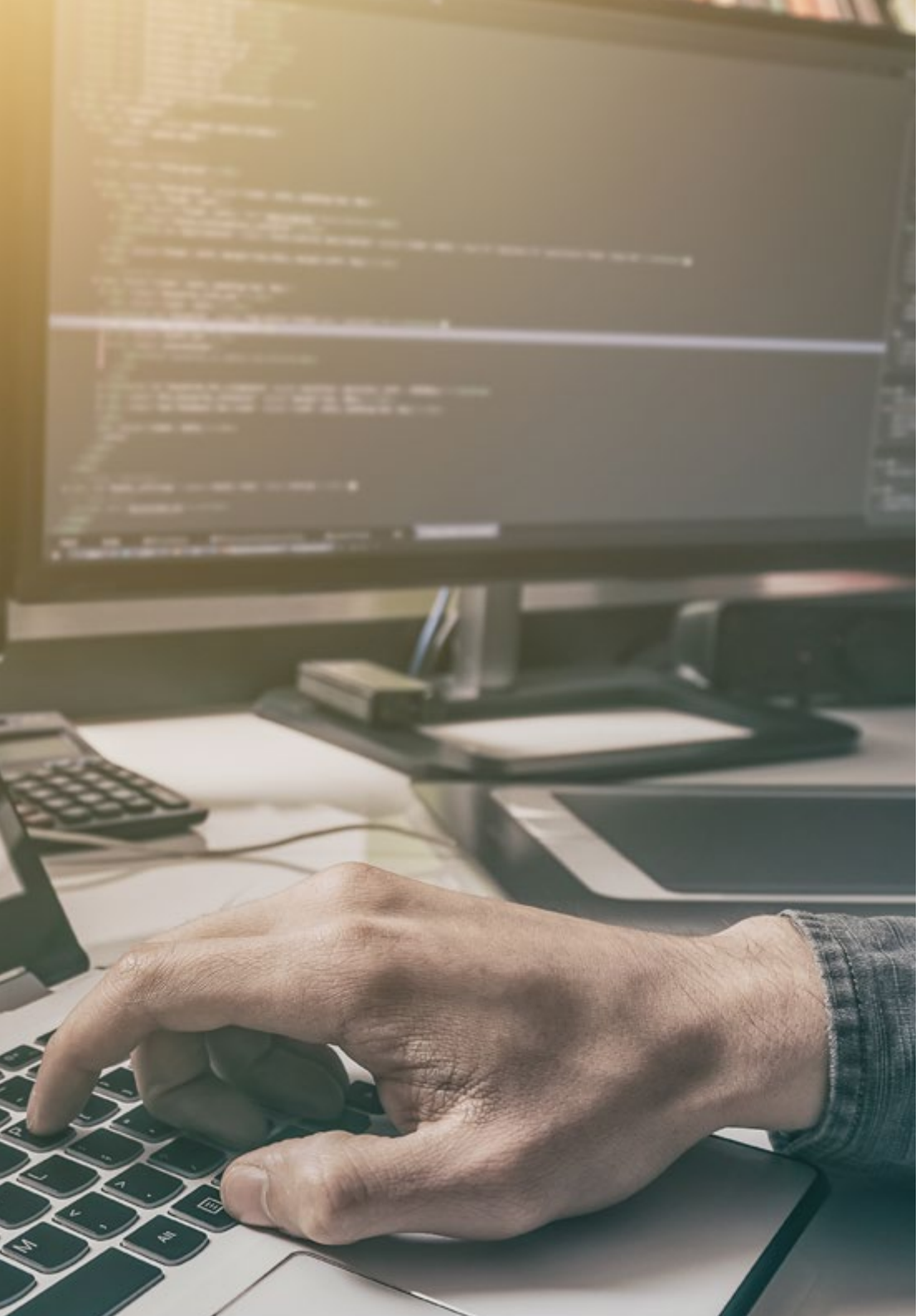
Tras finalizar el proceso de evaluación de este Máster, el profesional habrá adquirido una serie de conocimientos, herramientas y competencias que le permitirán ejercer en este sector con mayores garantías de éxito. De esta manera, el alumno no solo se convertirá en todo un experto en ciberseguridad, sino que también contribuirá positivamente a la disminución de los delitos informáticos a través del forjamiento de una red más segura y fortalecida para todos. Alcanzando puestos de alta dirección como Chief Information Security Officer.

El sector de la ciberseguridad requiere una actualización constante de los conocimientos. Con programas como este, el profesional lo consigue de manera rápida y efectiva"

Competencias generales

- Conocer las metodologías usadas en materia de ciberseguridad
- Saber evaluar cada tipo de amenaza para ofrecer una solución óptima en cada caso
- Ser capaz de generar soluciones inteligentes completas para automatizar comportamientos ante incidentes
- Saber cómo evaluar los riesgos asociados a las vulnerabilidades tanto fuera como dentro de la empresa
- Conocer la evolución y el impacto del IoT a lo largo del tiempo
- Ser capaz de demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas
- Saber aplicar *sandboxing* en diferentes entornos
- Conocer las directrices que debe seguir un buen desarrollador para cumplir con la Seguridad necesaria

Mejorar tus competencias en un servicio para todos impulsará tu trayectoria profesional y tu carrera personal”



Competencias específicas

- Saber realizar operaciones de seguridad defensiva
- Tener una percepción profunda y especializada sobre la seguridad informática
- Ostentar conocimiento especializado en el ámbito de la Ciberseguridad y Ciberinteligencia
- Tener conocimientos profundos sobre aspectos fundamentales como el Ciclo de inteligencia, fuentes de inteligencia, ingeniería social, metodología OSINT, HUMINT, *Anonimización*, análisis de riesgos, metodologías existentes (OWASP, OWISAM, OSSTM, PTES) y normativas vigentes en materia de ciberseguridad
- Entender la importancia de idear una defensa multicapa, también conocida como "*Defense in Depth*", que cubra todos los aspectos de una red corporativa donde algunos de los conceptos y sistemas que veremos podrán ser utilizados y aplicados también en un ambiente doméstico
- Saber aplicar procesos de seguridad para smartphones y dispositivos portátiles
- Conocer los medios para realizar el llamado hacking ético y proteger una empresa de un ciberataque
- Ser capaz de investigar un incidente de ciberseguridad
- Conocer las diferentes técnicas de ataque y defensa existentes
- Analizar el rol del Analista en Ciberseguridad
- Conocer el funcionamiento de la Ingeniería Social y sus métodos

04

Dirección del curso

El MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) ha sido desarrollado por un equipo de personas con diferentes perfiles profesionales especializados en los diferentes sectores que combinan experiencia profesional internacional en el ámbito privado en I+D+i y amplia experiencia docente. Por tanto, no sólo están al día en cada una de las tecnologías, sino que poseen perspectiva hacia las futuras necesidades del sector y las exponen de forma didáctica. Así, el profesional se asegura aprender de la mano de los mejores del sector, con la garantía de ostentar los conocimientos más actualizados.

Durante el MBA te acompañarán una serie de profesionales expertos que harán de tu experiencia educativa un hecho único”

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"

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. 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

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

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

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

05

Estructura y contenido

Para asegurar que el alumno adquiere los conocimientos más rigurosos y novedosos en materia de ciberseguridad, TECH ha diseñado una serie de materiales que reúnen las últimas actualizaciones de la profesión. Estos contenidos han sido diseñados por un grupo de experto en la materia, por lo que están adaptados a las necesidades actuales de los puestos ofertados en el sector. Una ocasión única y eminentemente profesionalizante que catapultará al alumno al éxito en su desarrollo profesional.

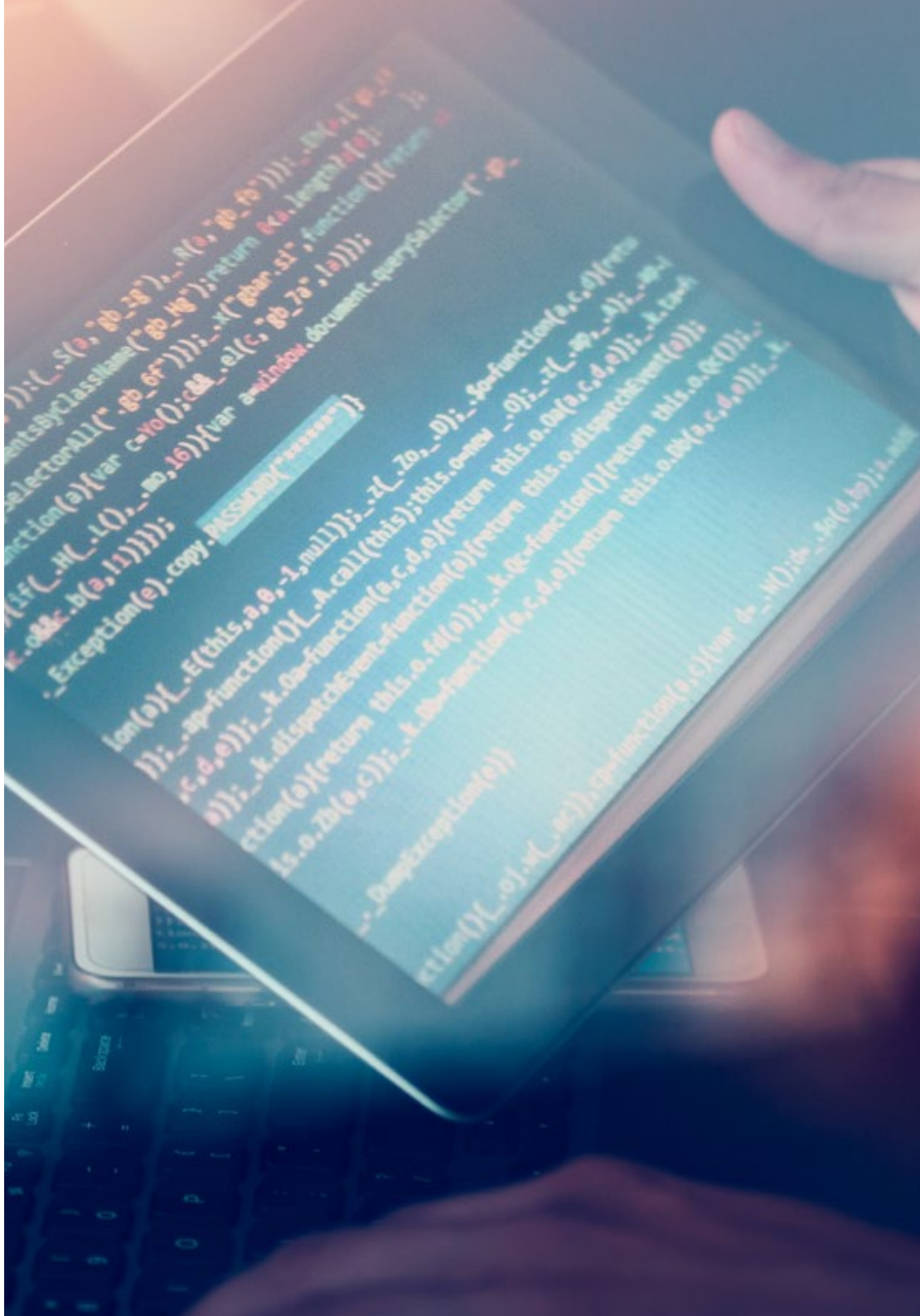
Un temario de nivel, diseñado por y para profesionales de nivel ¿vas a perder esta oportunidad? "

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. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM



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. StickyPassword
- 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 red 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. Fai2ban

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. Arquitectura 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 forzado
- 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 Wi-Fi 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 dispositivos 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 Cardiaco
- 5.8.2. Monitorización de pacientes y personas mayores
- 5.8.3. Implantadles
- 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. OSSTM
- 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. Wi-Fi *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. *SQLinjection*
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
- 7.5.3. 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. Sandbox 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 el 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*
- 10.1.1. Ámbitos de aplicación
- 10.1.2. Garantía de confidencialidad
- 10.1.3. 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*
- 10.3.1. Impacto en los medios
- 10.3.2. Peligros para la sociedad
- 10.3.3. 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 post Covid19
- 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

06

Metodología

Este programa de capacitación ofrece una forma diferente de aprender. Nuestra metodología se desarrolla a través de un modo de aprendizaje de forma cíclica: ***el Relearning***.

Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

Descubre el Relearning, un sistema que abandona el aprendizaje lineal convencional para llevarte a través de sistemas cíclicos de enseñanza: una forma de aprender que ha demostrado su enorme eficacia, especialmente en las materias que requieren memorización"

Estudio de Caso para contextualizar todo el contenido

Nuestro programa ofrece un método revolucionario de desarrollo de habilidades y conocimientos. Nuestro objetivo es afianzar competencias en un contexto cambiante, competitivo y de alta exigencia.

Con TECH podrás experimentar una forma de aprender que está moviendo los cimientos de las universidades tradicionales de todo el mundo"

Accederás a un sistema de aprendizaje basado en la reiteración, con una enseñanza natural y progresiva a lo largo de todo el temario.

El alumno aprenderá, mediante actividades colaborativas y casos reales, la resolución de situaciones complejas en entornos empresariales reales.

Un método de aprendizaje innovador y diferente

El presente programa de TECH es una enseñanza intensiva, creada desde 0, que propone los retos y decisiones más exigentes en este campo, ya sea en el ámbito nacional o internacional. Gracias a esta metodología se impulsa el crecimiento personal y profesional, dando un paso decisivo para conseguir el éxito. El método del caso, técnica que sienta las bases de este contenido, garantiza que se sigue la realidad económica, social y profesional más vigente.

> *Nuestro programa te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"*

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de Informática del mundo desde que éstas existen. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, el método del caso consistió en presentarles situaciones complejas reales para que tomasen decisiones y emitiesen juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Ante una determinada situación, ¿qué debería hacer un profesional? Esta es la pregunta a la que te enfrentamos en el método del caso, un método de aprendizaje orientado a la acción. A lo largo del curso, los estudiantes se enfrentarán a múltiples casos reales. Deberán integrar todos sus conocimientos, investigar, argumentar y defender sus ideas y decisiones.

Relearning Methodology

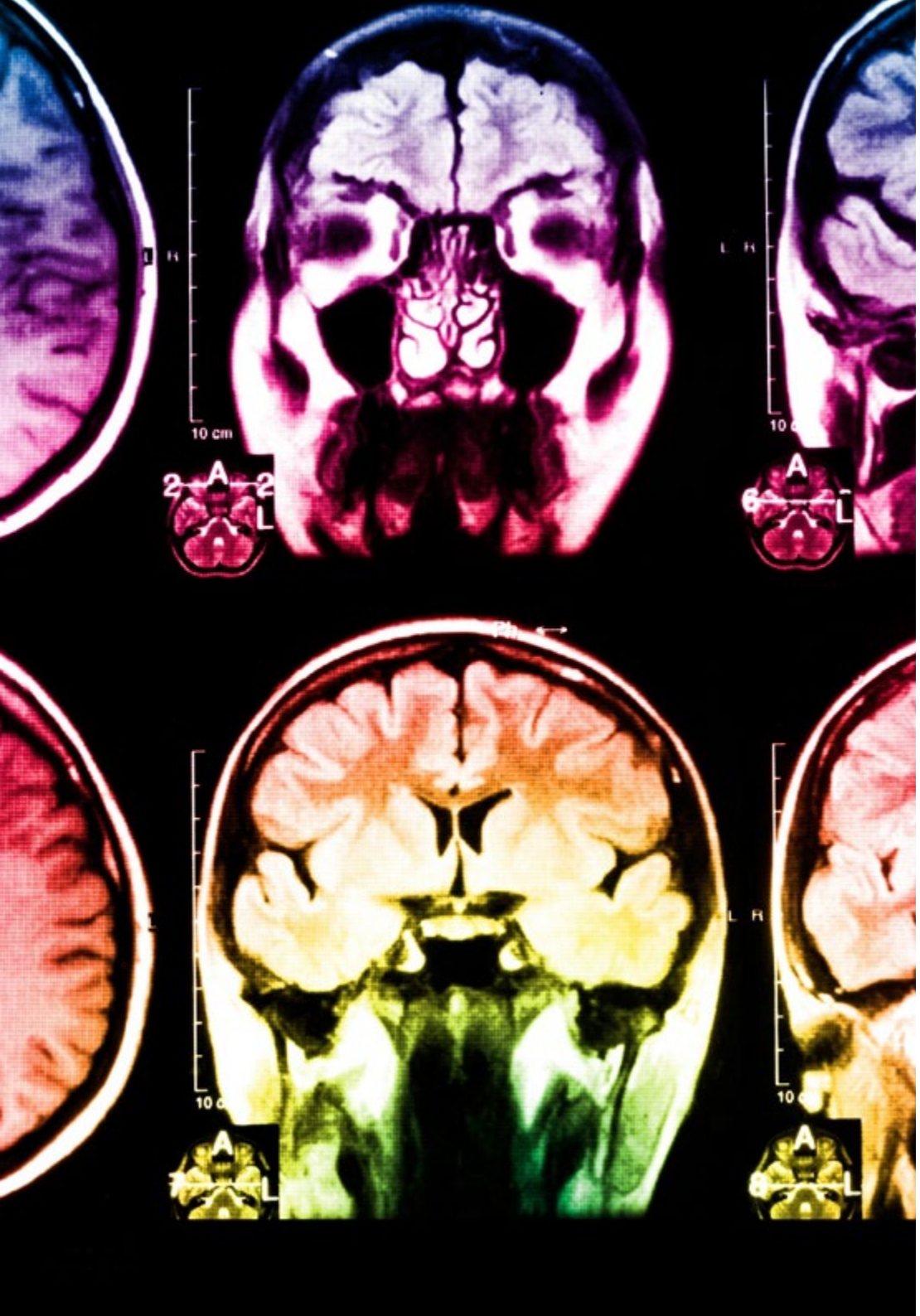
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

En 2019 obtuvimos los mejores resultados de aprendizaje de todas las universidades online en español en el mundo.

En TECH aprenderás con una metodología vanguardista concebida para capacitar a los directivos del futuro. Este método, a la vanguardia pedagógica mundial, se denomina Relearning.

Nuestra universidad es la única en habla hispana licenciada para emplear este exitoso método. En 2019, conseguimos mejorar los niveles de satisfacción global de nuestros alumnos (calidad docente, calidad de los materiales, estructura del curso, objetivos…) con respecto a los indicadores de la mejor universidad online en español.



En nuestro programa, el aprendizaje no es un proceso lineal, sino que sucede en espiral (aprender, desaprender, olvidar y reaprender). Por eso, se combinan cada uno de estos elementos de forma concéntrica. Con esta metodología se han capacitado más de 650.000 graduados universitarios con un éxito sin precedentes en ámbitos tan distintos como la bioquímica, la genética, la cirugía, el derecho internacional, las habilidades directivas, las ciencias del deporte, la filosofía, el derecho, la ingeniería, el periodismo, la historia o los mercados e instrumentos financieros. Todo ello en un entorno de alta exigencia, con un alumnado universitario de un perfil socioeconómico alto y una media de edad de 43,5 años.

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

A partir de la última evidencia científica en el ámbito de la neurociencia, no solo sabemos organizar la información, las ideas, las imágenes y los recuerdos, sino que sabemos que el lugar y el contexto donde hemos aprendido algo es fundamental para que seamos capaces de recordarlo y almacenarlo en el hipocampo, para retenerlo en nuestra memoria a largo plazo.

De esta manera, y en lo que se denomina Neurocognitive context-dependent e-learning, los diferentes elementos de nuestro programa están conectados con el contexto donde el participante desarrolla su práctica profesional.

Este programa ofrece los mejores materiales educativos, preparados a conciencia para los profesionales:

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, para crear el método de trabajo online de TECH. Todo ello, con las técnicas más novedosas que ofrecen piezas de gran calidad en todos y cada uno los materiales que se ponen a disposición del alumno.

Clases magistrales

Existe evidencia científica sobre la utilidad de la observación de terceros expertos.

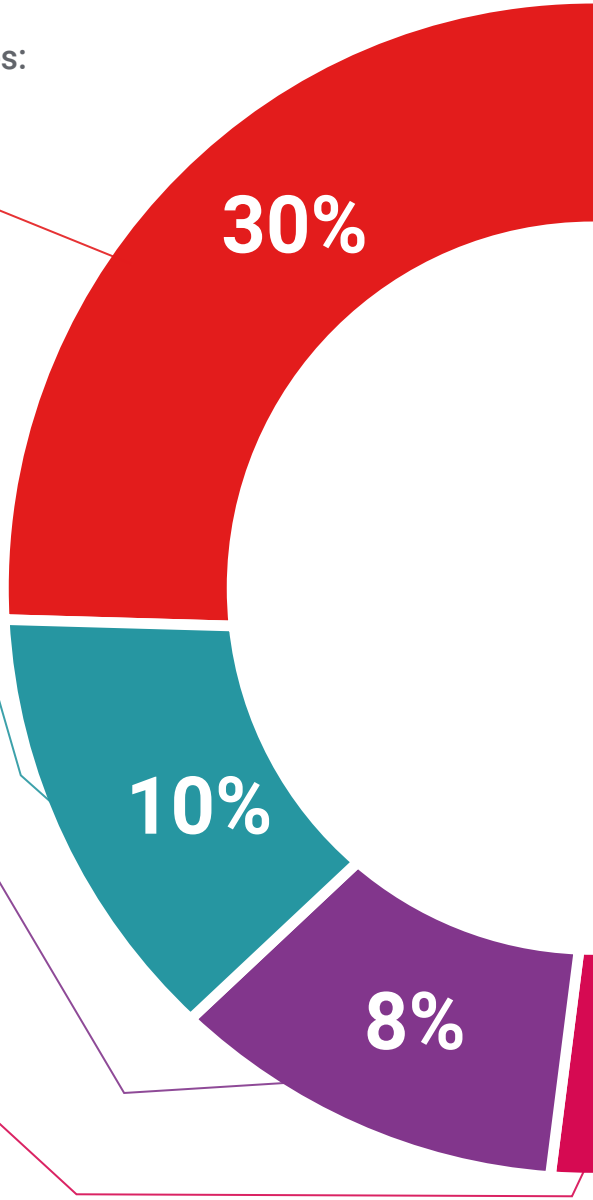
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

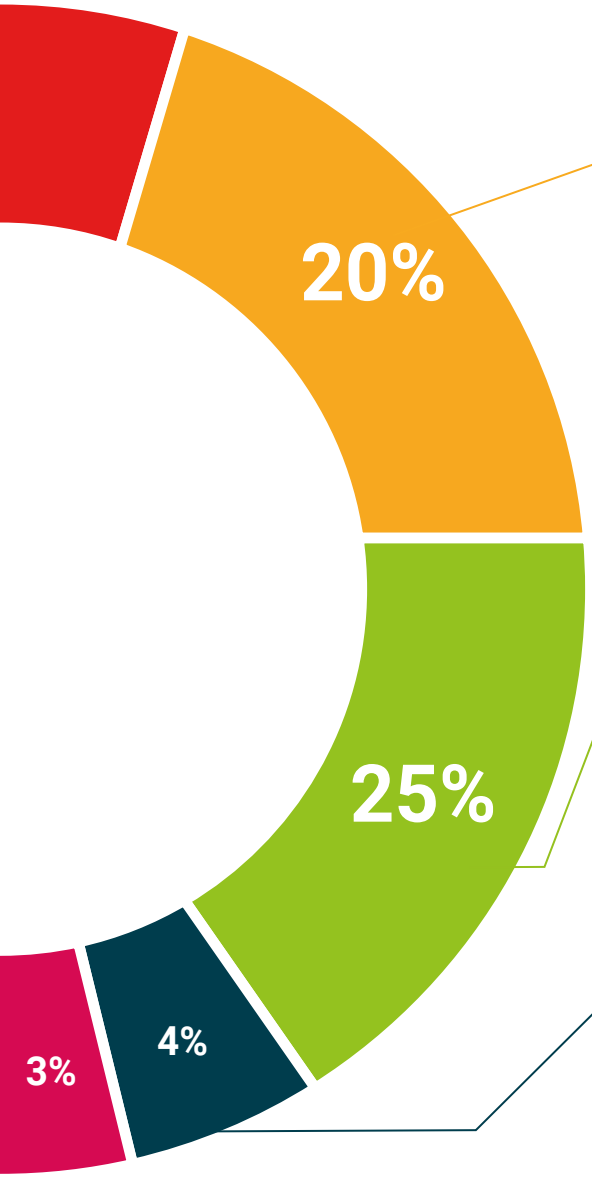
Prácticas de habilidades y competencias

Realizarán 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.

Lecturas complementarias

Artículos recientes, documentos de consenso y guías internacionales, entre otros. En la biblioteca virtual de TECH el estudiante tendrá acceso a todo lo que necesita para completar su capacitación.





Case studies

Completarán una selección de los mejores casos de estudio elegidos expresamente para esta titulación. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Resúmenes interactivos

El equipo de TECH presenta los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audios, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Testing & Retesting

Se evalúan y reevalúan periódicamente los conocimientos del alumno a lo largo del programa, mediante actividades y ejercicios evaluativos y autoevaluativos para que, de esta manera, el estudiante compruebe cómo va consiguiendo sus metas.

07

Titulación

El Máster Título Propio en 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 Universidad Tecnológica.

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

Este **Máster Título Propio en MBA en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** contiene el programa más completo y actualizado del mercado.

Tras la superación de la evaluación, el alumno recibirá por correo postal* con acuse de recibo su correspondiente título de **Máster Propio** emitido por **TECH Universidad Tecnológica.**

El título expedido por **TECH Universidad Tecnológica** expresará la calificación que haya obtenido en el Máster Título Propio, y reunirá los requisitos comúnmente exigidos por las bolsas de trabajo, oposiciones y comités evaluadores de carreras profesionales.

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

N.º Horas Oficiales: **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

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

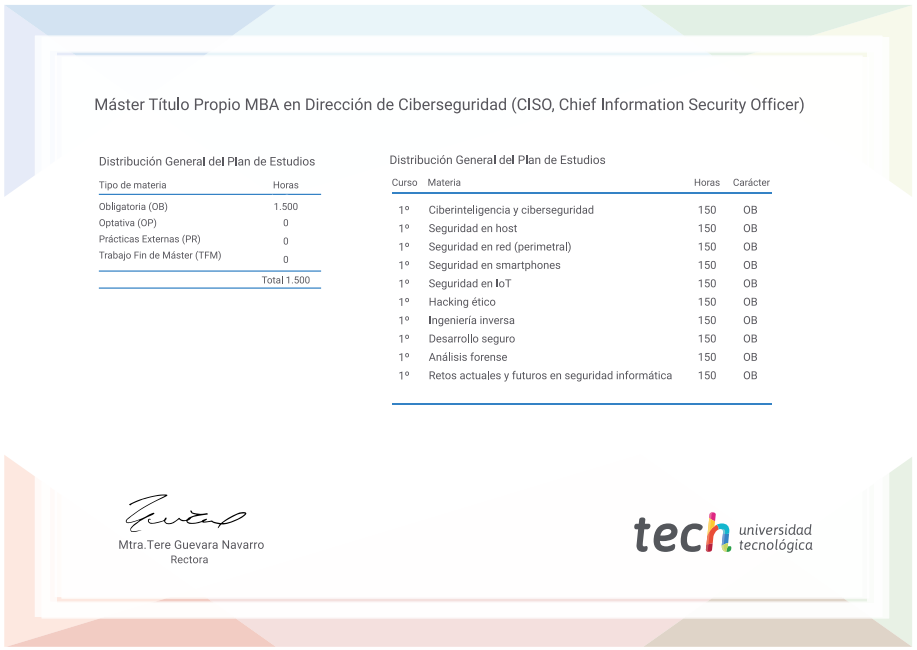
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH es una Institución Particular de Educación Superior reconocida por la Secretaría de Educación Pública a partir del 28 de junio de 2018.

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único 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	Horas
Obligatoria (OB)	1.500
Optativa (OP)	0
Prácticas Externas (PR)	0
Trabajo Fin de Máster (TFM)	0
Total	1.500

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Ciberinteligencia y ciberseguridad	150	OB
1º	Seguridad en host	150	OB
1º	Seguridad en red (perimetral)	150	OB
1º	Seguridad en smartphones	150	OB
1º	Seguridad en IoT	150	OB
1º	Hacking ético	150	OB
1º	Ingeniería inversa	150	OB
1º	Desarrollo seguro	150	OB
1º	Análisis forense	150	OB
1º	Retos actuales y futuros en seguridad informática	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

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

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio

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

tech universidad tecnológica