Máster Título Propio

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

tech global university

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: **60 ECTS**
- 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 **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

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
- Estructurar estrategias para la implementación y mejora de la sostenibilidad y la responsabilidad social en las empresas

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
- Proponer soluciones efectivas para la gestión del cambio y la resolución de conflictos en las organizaciones

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
- Diferenciar decisiones financieras clave y la gestión de riesgos en la dirección financiera
- 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
- Determinar las etapas del proceso de planificación estratégica de marketing
- 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 dirección de empresas
- Evaluar las funciones y responsabilidades del directivo en la cultura organizacional
- 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

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"

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, 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

TECH cuenta con un distinguido y especializado grupo de Directores Invitados Internacionales, con importantes roles de liderazgo en las empresas más punteras del mercado global"

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 tecnológic**o. 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 c**omerciales 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. 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.

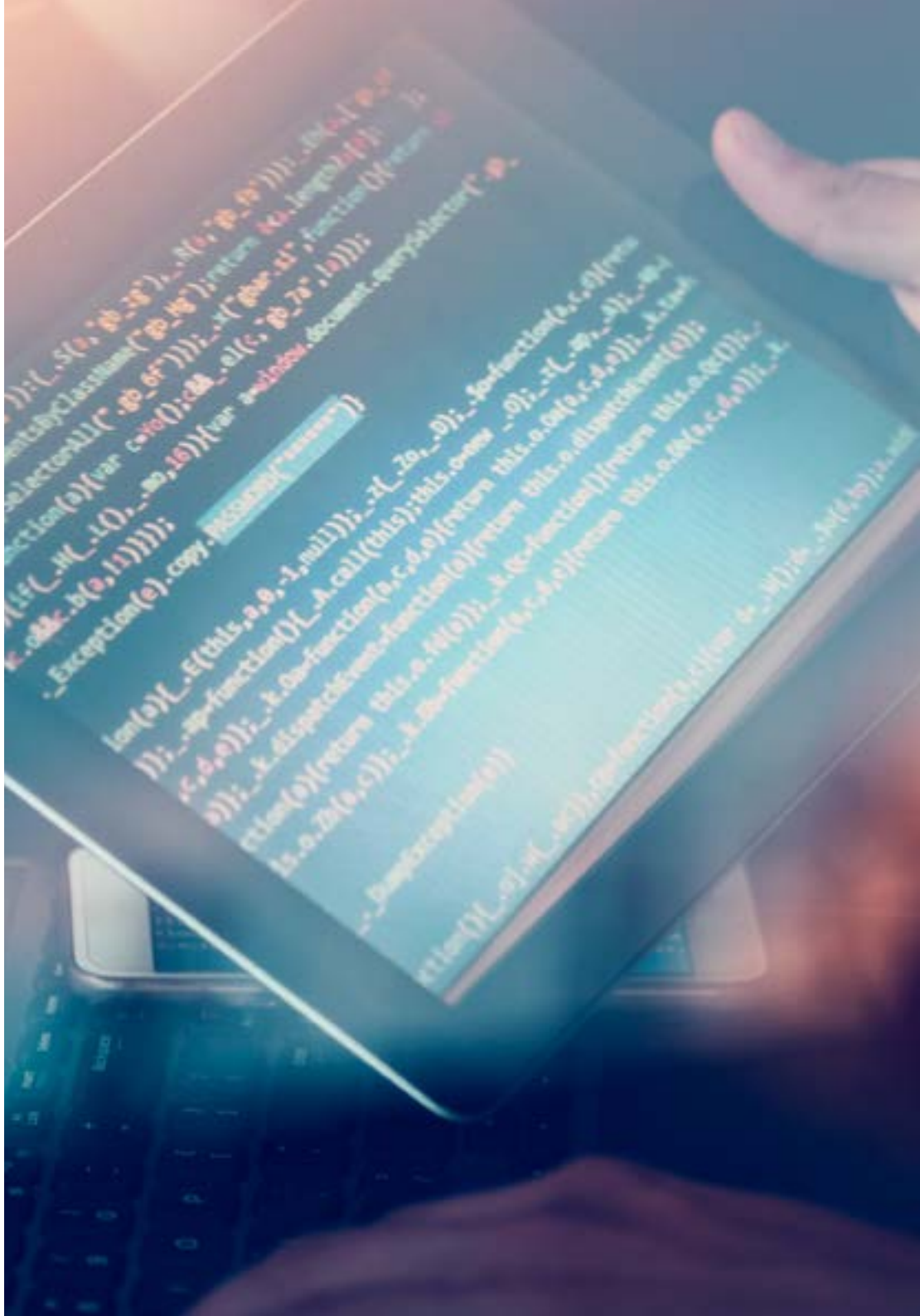
Un temario de nivel, diseñado por y para profesionales de nivel ¿vas a perder esta oportunidad?"

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

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 *Ecommerce* 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

Tu futuro empieza aquí. Matricúlate hoy y sé el Chief Information Officer de empresas de gran envergadura”

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

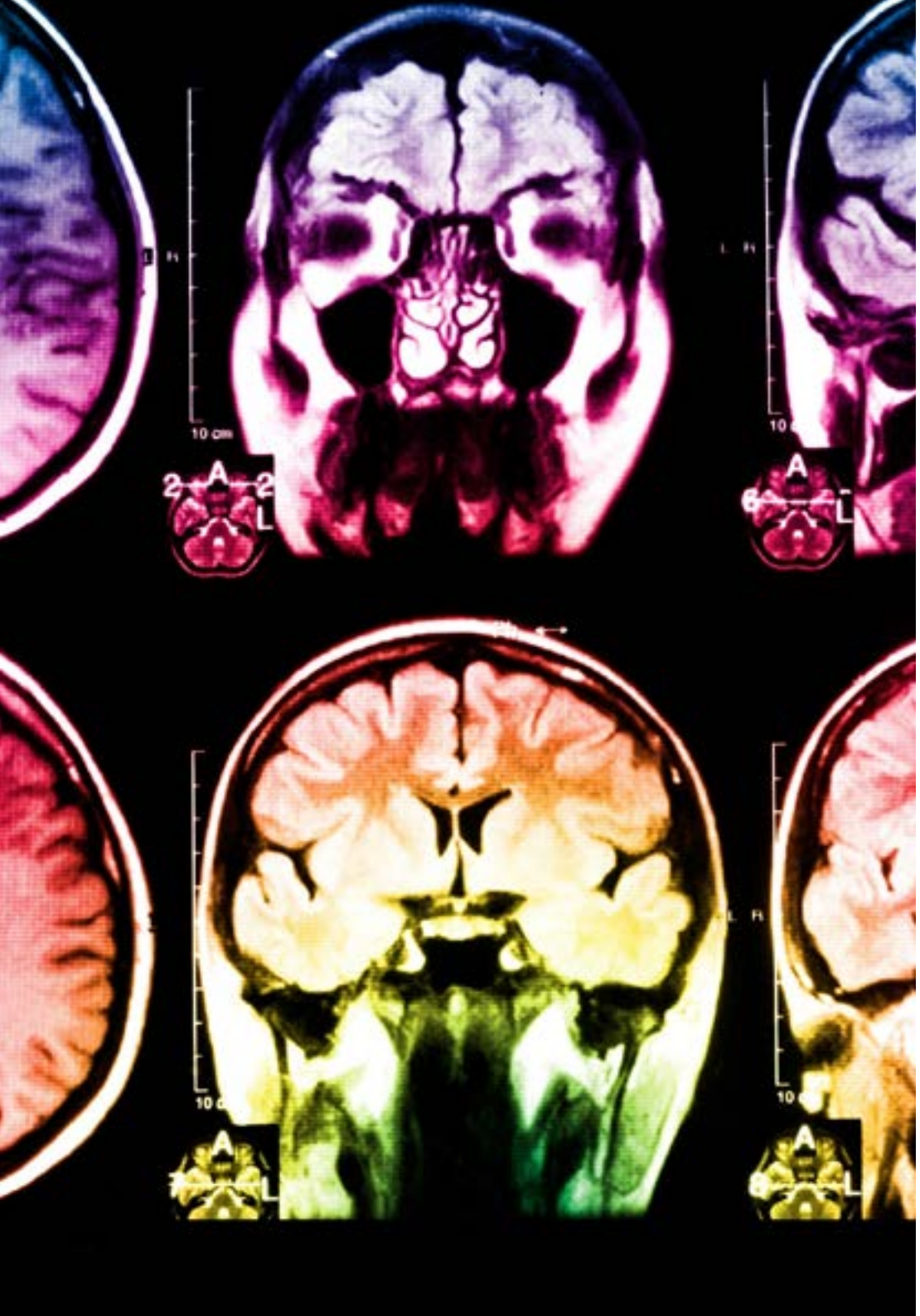
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

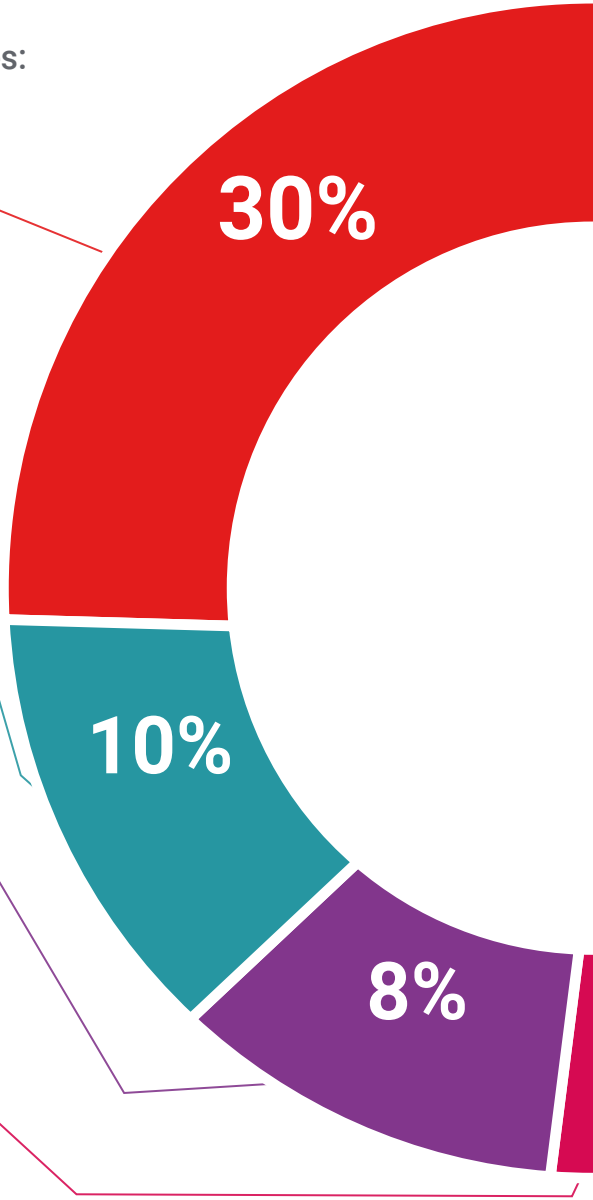
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

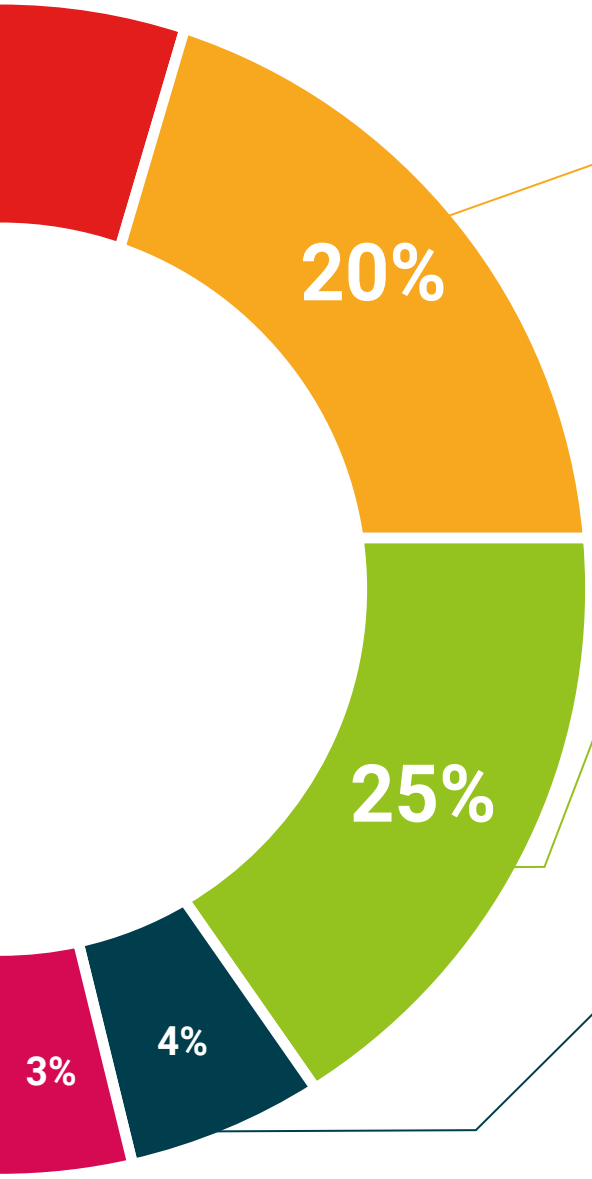
Prácticas de habilidades y competencias

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 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.

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

Modalidad: **online**

Duración: **12 meses**

Acreditación: **60 ECTS**


tech global university

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

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

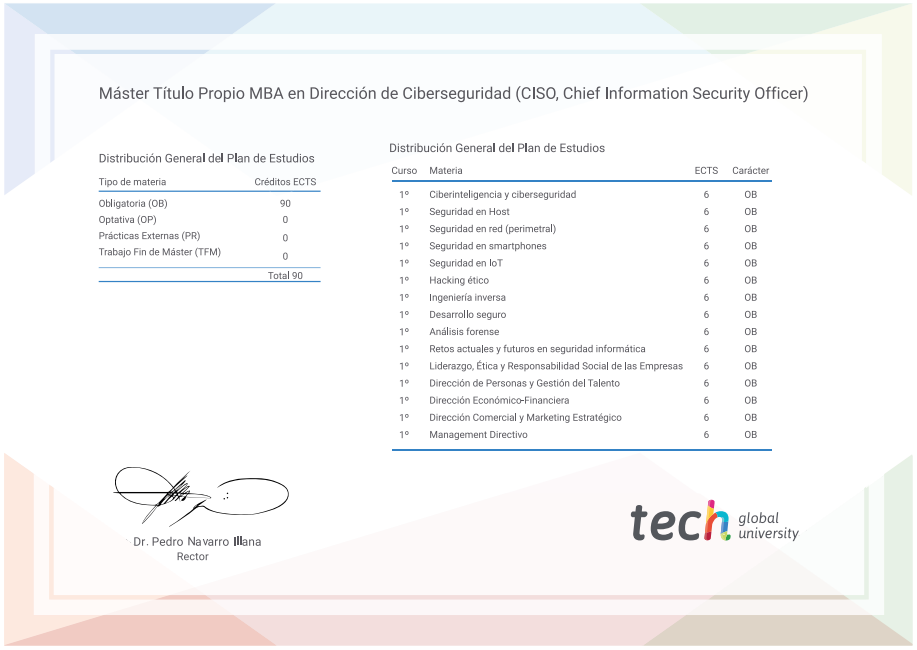
Se trata de un título propio de 2.700 horas de duración equivalente a 90 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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 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	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: **60 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio

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

tech global university