Máster Título Propio

MBA en Dirección de Ciberseguridad Avanzada (CISO)

tech universidad tecnológica

tech universidad tecnológica

Máster Título Propio
MBA en Dirección de Ciberseguridad Avanzada (CISO)

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

Acceso web: **www.techtitute.com/informatica/master/master-mba-direccion-ciberseguridad-avanzada-ciso**

Índice

01

Presentación

El mundo actual avanza hacia la completa digitalización. Cada vez más procesos, operaciones y tareas básicas de todo tipo se realizan a través de un dispositivo electrónico. Pero este progreso tiene también ciertos riesgos, ya que ordenadores, *smartphones*, *tablets* y todo tipo de aplicaciones digitales pueden ser susceptibles de recibir ataques informáticos. Por esa razón, numerosas compañías buscan expertos que puedan dirigir y gestionar eficazmente la ciberseguridad de sus servicios. Así, este nuevo perfil profesional tiene una gran demanda, por lo que se ha diseñado este programa para aportar los conocimientos y técnicas más novedosas al informático, que estará preparado para ser el director de ciberseguridad en cualquier empresa que lo requiera.

Este programa te preparará de forma intensiva para que te especialices en dirección de ciberseguridad, el perfil profesional más demandado en la actualidad en el ámbito de la informática"

En los últimos años el proceso de digitalización se ha acelerado, impulsado por los continuos avances que experimenta la informática. Así, no sólo la tecnología ha disfrutado de grandes mejoras, sino también las propias herramientas digitales con las que se realizan numerosas tareas en la actualidad. Por ejemplo, estos progresos han hecho posible que muchas operaciones bancarias puedan realizarse desde una aplicación móvil. También ha habido novedades en el ámbito sanitario, en sistemas de cita previa o en el acceso a historiales clínicos. Además, gracias a estas tecnologías, es posible consultar facturas o solicitar servicios de empresas de ámbitos como la telefonía.

Pero esos avances han conllevado también el aumento de vulnerabilidades informáticas. Así, aunque las opciones para realizar diversas actividades y tareas se han ampliado, los ataques a la seguridad de dispositivos, aplicaciones y webs se han incrementado proporcionalmente. Por eso, cada vez más compañías buscan profesionales especializados en ciberseguridad que sean capaces de proporcionarles la protección adecuada contra todo tipo de ataques informáticos.

De esta manera, el perfil de Director de Ciberseguridad es uno de los más solicitados por empresas que operan en internet o que tienen servicios en el entorno digital. Y para responder a esa demanda, TECH ha diseñado este MBA en Dirección de Ciberseguridad Avanzada (CISO), que proporcionará al informático todas las herramientas necesarias para ejercer ese puesto de forma eficaz y atendiendo a las últimas novedades en protección y vulnerabilidades en este ámbito tecnológico.

En este programa podrá profundizar, por tanto, en aspectos como la seguridad en el desarrollo y diseño de sistemas, las mejores técnicas criptográficas o la seguridad en entornos cloud computing. Y lo hará a partir de una metodología 100% online con la que podrá compaginar su labor profesional con los estudios, sin rígidos horarios ni incómodos desplazamientos a un centro académico. Y, además, disfrutará de numerosos recursos didácticos multimedia, impartidos por el profesorado más prestigioso y especializado en el área de la ciberseguridad.

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

- El desarrollo de casos prácticos presentados por expertos en Informática y 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

Conoce, de primera mano, las mejores técnicas de seguridad aplicada a entornos Cloud Computing o a la tecnología Blockchain"

Disfrutarás de numerosos contenidos multimedia para agilizar tu proceso de aprendizaje, al tiempo que recibes el acompañamiento de un profesorado de gran prestigio en el ámbito de la ciberseguridad”

La metodología online de TECH te permitirá escoger el momento y el lugar para estudiar, sin entorpecer su labor profesional.

Podrás convertirte en el Director de Ciberseguridad de las mejores compañías de tu entorno.

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

El rápido desarrollo de las tecnologías informáticas ha traído consigo grandes avances, proporcionando numerosos servicios al conjunto de la población. Sin embargo, también se ha aumentado la cantidad de vulnerabilidades y ciberataques, por lo que el objetivo principal de este programa es convertir al informático en un auténtico especialista en dirección de ciberseguridad, garantizándole un enorme e inmediato progreso profesional. Así, sus nuevos conocimientos le proporcionarán la oportunidad de acceder a grandes empresas que operen digitalmente en diversos sectores.

El objetivo de este programa es convertirte en un profesional preparado para dirigir el departamento de ciberseguridad de una gran empresa"

Objetivos generales

- Generar conocimiento especializado sobre un sistema de información, tipos y aspectos de seguridad que deben ser tenidos en cuenta
- Identificar las vulnerabilidades de un sistema de información
- Desarrollar la normativa legal y tipificación del delito atacando a un sistema de información
- Evaluar los diferentes modelos de arquitectura de seguridad para establecer el modelo más adecuado a la organización
- Identificar los marcos normativos de aplicación y las bases reguladoras de los mismos
- Analizar la estructura organizativa y funcional de un área de seguridad de la información (la oficina del CISO)
- Analizar y desarrollar el concepto de riesgo, incertidumbre dentro del entorno en que vivimos
- Examinar el Modelo de Gestión de Riesgos basado en la ISO 31.000
- Examinar la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Examinar los certificados digitales
- Examinar la Infraestructura de Clave Pública (PKI)
- Desarrollar el concepto de gestión de identidades
- Identificar los métodos de autenticación
- Generar conocimiento especializado sobre el ecosistema de seguridad informática
- Evaluar el conocimiento en término de ciberseguridad
- Identificar los ámbitos de seguridad en *Cloud*
- Analizar los servicios y herramientas en cada uno de los ámbitos de seguridad
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN

Tus objetivos profesionales estarán ahora a tu alcance gracias a este Máster Título Propio, que dispone de los conocimientos más avanzados en ciberseguridad”

Objetivos específicos

Módulo 1. Seguridad en el diseño y desarrollo de sistemas

- Evaluar la seguridad de un sistema de información en todos sus componentes y capas
- Identificar los tipos de amenazas de seguridad actuales y su tendencia
- Establecer directrices de seguridad definiendo políticas y planes de seguridad y contingencia
- Analizar estrategias y herramientas para asegurar la integridad y seguridad de los sistemas de información
- Aplicar las técnicas y herramientas específicas para cada tipo de ataque o vulnerabilidad de seguridad
- Proteger la información sensible almacenada en el sistema de información
- Disponer del marco legal y tipificación del delito, completando la visión con la tipificación del delincuente y su víctima

Módulo 2. Arquitecturas y modelos de seguridad de la información

- Alinear el Plan Director de Seguridad con los objetivos estratégicos de la organización
- Establecer un marco continuo de gestión de riesgos como parte integral del Plan Director de Seguridad
- Determinar los indicadores adecuados para el seguimiento de la implantación del SGSI
- Establecer una estrategia de seguridad basada en políticas
- Analizar los objetivos y procedimientos asociados al plan de concienciación de empleados, proveedores y socios
- Identificar, dentro del marco normativo, las normativas, certificaciones y leyes de aplicación en cada organización
- Desarrollar los elementos fundamentales requeridos por la norma ISO 27001:2013
- Implantar un modelo de gestión de privacidad en línea con la regulación europea GDPR/RGPD

Módulo 3. Gestión de la seguridad IT

- Identificar las diferentes estructuras que puede tener un área de seguridad de la información
- Desarrollar un modelo de seguridad basado en tres líneas de defensa
- Presentar los diferentes comités periódicos y extraordinarios en los que interviene el área de ciberseguridad
- Concretar las herramientas tecnológicas que dan soporte a las principales funciones del equipo de operaciones de seguridad (SOC)
- Evaluar las medidas de control de vulnerabilidades adecuadas a cada escenario
- Desarrollar el marco de trabajo de operaciones de seguridad basado en NIST CSF
- Concretar el alcance de los diferentes tipos de auditorías (*Red Team*, *Pentesting*, *Bug Bounty*, etc.)
- Proponer las actividades a realizar después de un incidente de seguridad
- Configurar un centro de mando de seguridad de la información que englobe a todos los actores relevantes (autoridades, clientes, proveedores, etc.)

Módulo 4. Análisis de riesgos y entorno de seguridad IT

- Examinar, con una visión holística, el entorno en el que nos movemos
- Identificar los principales riesgos y oportunidades que pueden afectar a la consecución de nuestros objetivos
- Analizar los riesgos en base a las mejores prácticas a nuestro alcance
- Evaluar el posible impacto de dichos riesgos y oportunidades
- Desarrollar técnicas que permitan tratar los riesgos y oportunidades de manera que maximicemos un aporte de valor
- Examinar en profundidad las diferentes técnicas de transferencia de riesgos, así como de valor
- Generar valor desde el diseño de modelos propios para la gestión ágil de riesgos
- Examinar los resultados para proponer mejoras continuas en gestión de proyectos y procesos basados en modelos de gestión impulsados por el riesgo o *Risk-Driven*
- Innovar y transformar los datos generales en información relevante para la toma de decisiones basadas en el riesgo

Módulo 5. Criptografía en IT

- Compilar las operaciones fundamentales (XOR, números grandes, sustitución y transposición) y los diversos componentes (funciones One-Way, Hash, generadores de números aleatorios)
- Analizar las técnicas criptográficas
- Desarrollar los diferentes algoritmos criptográficos
- Demostrar el uso de las firmas digitales y su aplicación en los certificados digitales
- Evaluar los sistemas de manejo de claves y la importancia de la longitud de las claves criptográficas
- Examinar los algoritmos derivación de claves
- Analizar el ciclo de vida de las claves
- Evaluar los modos de cifrado de bloque y de flujo
- Determinar los generadores de números pseudoaleatorios
- Desarrollar casos reales de aplicación de criptografía, como Kerberos, PGP o tarjetas inteligentes
- Examinar asociaciones y organismos relacionados, como ISO, NIST o NCSC
- Determinar los retos en la criptografía de la computación cuántica

Módulo 6. Gestión de identidad y accesos en seguridad IT
- Desarrollar el concepto de identidad digital
- Evaluar el control de acceso físico a la información
- Fundamentar la autenticación biométrica y la autenticación MFA
- Evaluar ataques relacionados con la confidencialidad de la información
- Analizar la federación de identidades
- Establecer el control de acceso a la red

Módulo 7. Seguridad en comunicaciones y operación software
- Desarrollar conocimiento especializado en materia de seguridad física y lógica
- Demostrar el conocimiento en comunicaciones y redes
- Identificar principales ataques maliciosos
- Establecer un marco de desarrollo seguros
- Demostrar conocer las principales normativas de sistemas de gestión de la seguridad de la información
- Fundamentar el funcionamiento de un centro de operaciones en materias de ciberseguridad
- Demostrar la importancia de contar con prácticas en ciberseguridad para catástrofes organizativas

Módulo 8. Seguridad en entornos Cloud
- Identificar riesgos de un despliegue de infraestructura en *Cloud* pública
- Definir los requerimientos de seguridad
- Desarrollar un plan de seguridad para un despliegue en *Cloud*
- Identificar los servicios *Cloud* a desplegar para la ejecución de un plan de seguridad
- Determinar la operativa necesaria para los mecanismos de prevención
- Establecer las Directrices para un sistema de *Logging* y monitorización
- Proponer acciones de respuesta ante incidentes

Módulo 9. Seguridad en comunicaciones de dispositivos IoT
- Presentar la arquitectura simplificada del IoT
- Fundamentar las diferencias entre tecnologías de conectividad generalistas y tecnologías de conectividad para el IoT
- Establecer el concepto del triángulo de hierro de la conectividad del IoT
- Analizar las especificaciones de seguridad de la tecnología LoRaWAN, de la tecnología NB-IoT y de la tecnología WiSUN
- Fundamentar la elección de la tecnología IoT adecuada para cada proyecto

Módulo 10. Plan de continuidad del negocio asociado a la seguridad
- Presentar los elementos clave de cada fase y analizar las características del Plan de Continuidad de Negocio (PCN)
- Fundamentar la necesidad de un Plan de Continuidad para el Negocio
- Determinar los mapas de éxito y riesgo de cada fase del Plan de Continuidad de Negocio
- Concretar cómo se establece un Plan de Acción para la implantación
- Evaluar la completitud de un Plan de Continuidad del Negocio (PCN)
- Desarrollar el Plan de Implantación con éxito de un Plan de Continuidad para el Negocio

03

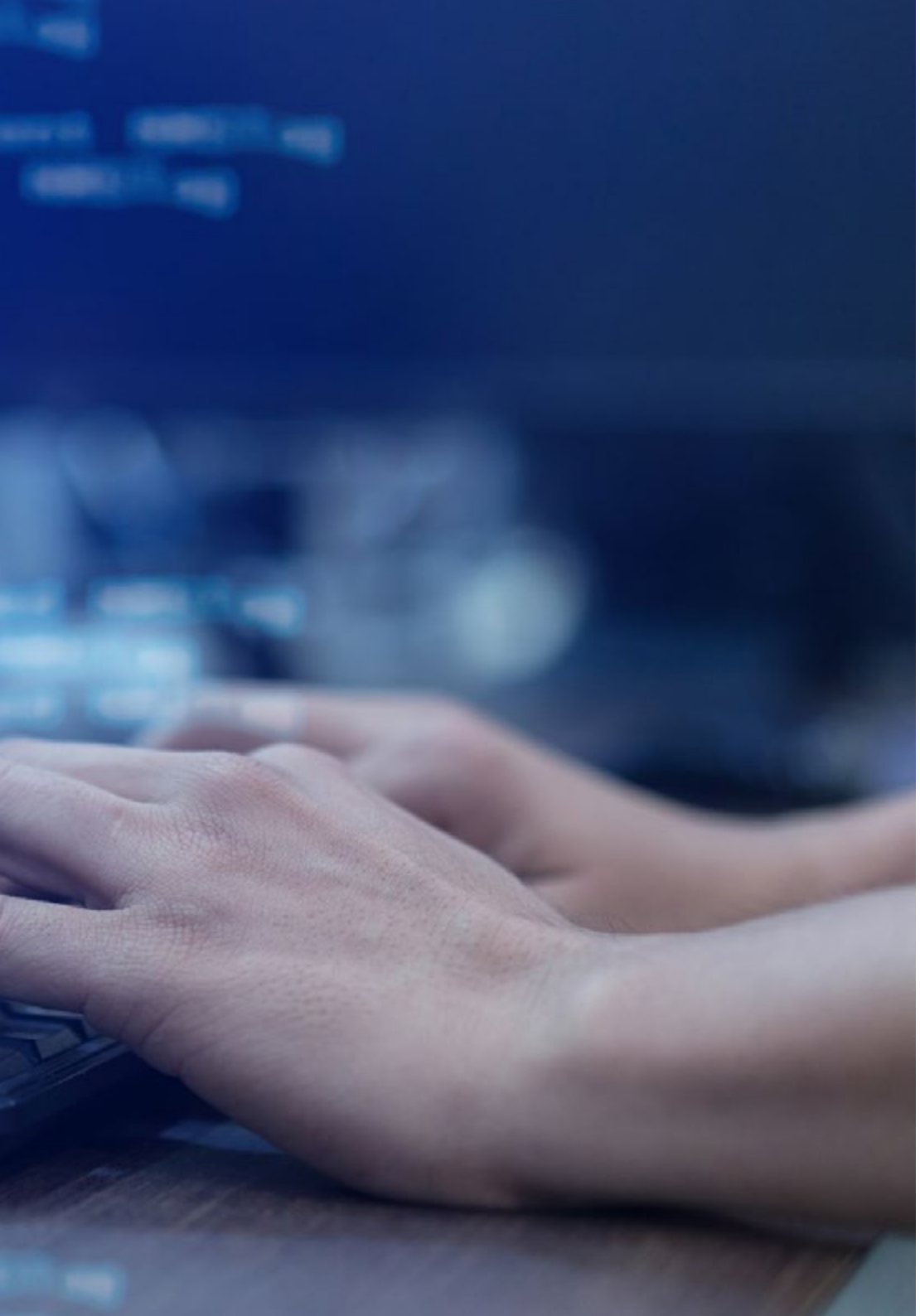
Competencias

Gracias a este Máster Título Propio el profesional adquirirá numerosas nuevas competencias en el ámbito de la ciberseguridad. La irrupción en los últimos años de tecnologías como el *Blockchain*, el *Cloud Computing* o la inteligencia artificial ha propiciado el desarrollo de nuevas áreas de la ciberseguridad. Por esa razón, este programa ha sido especialmente diseñado para proporcionarle al profesional todas las habilidades necesarias para adaptarse a estas tecnologías en auge.

Las competencias que te proporcionará este programa te permitirán actualizarte y adaptarte al nuevo entorno informático, donde han irrumpido con fuerza tecnologías como el Blockchain o la inteligencia artificial"

Competencias generales

- Aplicar las medidas de seguridad más adecuadas dependiendo de las amenazas
- Determinar la política y plan de seguridad en el sistema de información de una compañía, completando el diseño y puesta en marcha del Plan de Contingencia
- Establecer un programa de auditorías que cubra las necesidades de autoevaluación de la organización en materia de ciberseguridad
- Desarrollar un programa de análisis y control de vulnerabilidades y un plan de respuesta a incidentes de ciberseguridad
- Maximizar las oportunidades que se presenten y eliminar la exposición a todos los posibles riesgos desde el propio diseño
- Compilar los sistemas de gestión de claves
- Evaluar la seguridad de la información de una compañía
- Analizar los sistemas de acceso a la información
- Desarrollar las mejores prácticas en el desarrollo seguro
- Presentar los riesgos que supone a las compañías no tener un entorno de seguridad informática



Competencias específicas

- Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Aplicar la metodología MAGERIT para evolucionar el modelo y llevarlo un paso más allá
- Diseñar nuevas metodologías de gestión de riesgos propias, basadas en el concepto *agile Risk Management*
- Identificar, analizar, evaluar y tratar los riesgos a los que se enfrenta el profesional desde una nueva perspectiva empresarial basada en un modelo *Risk-Driven* o impulsado por el riesgo que permita no sólo sobrevivir en propio entorno, sino impulsar el aporte de valor propio
- Examinar el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en *Cloud*
- Evaluar las diferencias en las implementaciones concretas de diferentes vendedores de *Cloud* pública
- Evaluar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN
- Presentar las especificaciones básicas de las principales tecnologías LPWAN para el IoT

04

Dirección del curso

La enorme complejidad de la ciberseguridad actual exige un aprendizaje completo y detallado. Por esa razón, TECH se ha encargado de reunir al mejor profesorado especializado en esta área. Así, el profesional disfrutará del acompañamiento y supervisión de un cuadro docente que está al tanto de los últimos avances en esta área, de modo que podrá incorporar a su trabajo diario las mejores técnicas de ciberseguridad, al tiempo que adquiere las habilidades necesarias de dirección en esta área.

Tendrás a tu disposición a auténticos especialistas en ciberseguridad. Esta es la oportunidad que estabas buscando”

Dirección

D. Olalla Bonal, Martín

- Gerente Senior de Práctica de Blockchain en EY
- Especialista Técnico Cliente Blockchain para IBM
- Director de Arquitectura para Blocknitive
- Coordinador de Equipo en Bases de Datos Distribuidas no Relacionales para WedoIT, Subsidiaria de IBM
- Arquitecto de Infraestructuras en Bankia
- Responsable del Departamento de Maquetación en T-Systems
- Coordinador de Departamento para Bing Data España SL

Profesores

Dr. Nogales Ávila, Javier

- Enterprise Cloud and sourcing senior consultant. Quint
- Cloud and Technology Consultant. Indra
- Associate Technology Consultant. Accenture
- Graduado por la Universidad de Jaén y University of Technology and Economics of Budapest (BME)
- Grado en Ingeniería de Organización Industrial

D. Rodrigo Estébanez, Juan Manuel

- Cofundador de Ismet Tech
- Gerente de Seguridad de la Información en Ecix Group
- *Operational Security Officer* en Atos IT Solutions and Services A/S
- Docente de Gestión de Ciberseguridad en estudios universitarios
- Graduado en Ingeniería por la Universidad de Valladolid
- Máster en Sistemas de Gestión Integrados por la Universidad CEU San Pablo

Profesores

Dr. Gómez Rodríguez, Antonio

- Ingeniero Principal de Soluciones Cloud para Oracle
- Coorganizador de Málaga Developer Meetup
- Consultor Especialista para Sopra Group y Everis
- Líder de equipos en System Dynamics
- Desarrollador de Softwares en SGO Software
- Máster en E-Business por la Escuela de Negocios de La Salle
- Postgrado en Tecnologías y Sistemas de Información por el Instituto Catalán de Tecnología
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña

Dr. del Valle Arias, Jorge

- Smart City Solutions & Software Business Development Manager España. Itron, Inc Consultor IoT
- Director de Negocios Interino de IoT. TCOMET
- Responsable de la Unidad de Negocio IoT, Industria 4.0. Diode España
- Gerente de Área de Ventas de IoT y Telecomunicaciones. Aicox Soluciones
- Director Técnico (CTO) y Gerente de Desarrollo de Negocios. Consultoría TELYC
- Fundador y CEO de Sensor Intelligence
- Jefe de Operaciones y Proyectos. Codio
- Director de Operaciones en Codium Networks
- Ingeniero jefe de diseño de hardware y firmware. AITEMIN
- Jefe Regional de Planificación y Optimización RF - Red LMDS 3,5 GHz. Clearwire
- Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid
- Executive MBA por la International Graduate School de La Salle de Madrid
- Máster en Energías Renovables. CEPYME

D. Gonzalo Alonso, Félix

- Director General y Fundador en Smart REM Solutions
- Socio Fundador y Responsable de Ingeniería de Riesgos e Innovación. Dynargy
- Gerente y Socio Fundador. Risknova (Gabinete Pericial Especializado en Tecnología)
- Licenciado en Ingeniería de Organización Industrial por la Universidad Pontificia de Comillas ICAI
- Graduado en Ingeniería técnica Industrial especialidad Electrónica Industrial por la Universidad Pontificia de Comillas ICAI
- Máster en Dirección Aseguradora por ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

Dr. Entrenas, Alejandro

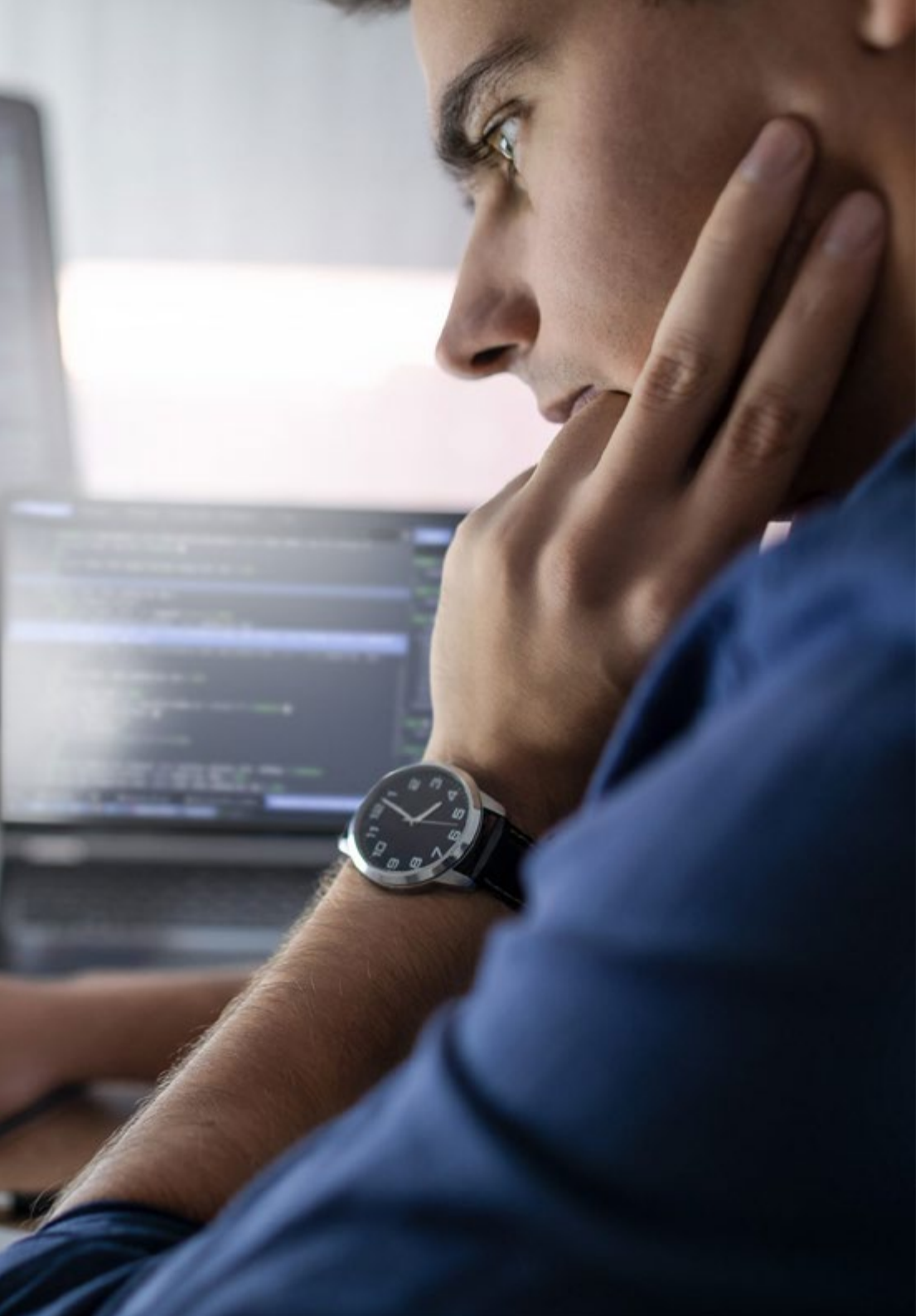
- Jefe de Proyecto en Ciberseguridad. Entelgy Innotec Security
- Consultor de Ciberseguridad. Entelgy
- Analista de Seguridad de la Información. Innovery España
- Analista en Seguridad de la Información. Atos
- Licenciado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Córdoba
- Máster en Dirección y Gestión de la Seguridad de la Información en la Universidad Politécnica de Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

D. Ortega, Octavio

- Especialista en Marketing y Desarrollo Web
- Programador de Aplicaciones Informáticas y Desarrollador Web *Freelance*
- *Chief Operating* Officer en Smallsquid SL
- Administrador e-commerce de Ortega y Serrano
- Docente en cursos de Certificados de Profesionalidad en Informática y Comunicaciones
- Docente de cursos de Seguridad Informática
- Licenciado en Psicología por la Universidad Abierta de Cataluña
- Técnico Superior Universitario en Análisis, Diseño y Soluciones de *Software*
- Técnico Superior Universitario en Programación Avanzada

D. Embid Ruiz, Mario

- Abogado Experto en TIC y Protección de Datos en Martínez-Echevarría Abogados
- Responsable legal de Branddocs SL
- Analista de Riesgo en el Segmento Pymes de BBVA
- Docente en estudios de posgrado universitario relacionados con el Derecho
- Licenciatura en Derecho por la Universidad Rey Juan Carlos
- Licenciado en Administración y Dirección de Empresas por la Universidad Rey Juan Carlos
- Máster en Derecho de las Nuevas Tecnologías, Internet y Audiovisual por el Centro de Estudios Universitarios Villanueva



Dr. Gozalo Fernández, Juan Luis

- Gerente de Productos basados en Blockchain para Open Canarias
- Director Blockchain DevOps en Alastria
- Director de Tecnología Nivel de Servicio en Santander España
- Director Desarrollo Aplicación Móvil Tinkerlink en Cronos Telecom
- Director Tecnología Gestión de Servicio IT en Barclays Bank España
- Licenciado en Ingeniería Superior de Informática en la UNED
- Especialización en *Deep Learning* en DeepLearning.ai

Dra. Jurado Jabonero, Lorena

- Responsable de Seguridad de la Información (CISO) en el Grupo Pascual
- Cybersecurity Manager en KPMG. España
- Consultor de Procesos TI y Control y Gestión de Proyectos de Infraestructura en Bankia
- Ingeniero de Herramientas de Explotación en Dalkia
- Desarrollador en el Grupo Banco Popular
- Desarrollador de Aplicaciones por la Universidad Politécnica de Madrid
- Graduada en Ingeniería Informática por la Universidad Alfonso X el Sabio
- Ingeniero Técnico en Informática de Gestión por la Universidad Politécnica de Madrid
  Certified Data Privacy Solutions Engineer (CDPSE) por ISACA

05

Estructura y contenido

Este MBA en Dirección de Ciberseguridad Avanzada (CISO) está estructurado en 10 módulos especializados que permitirán al profesional profundizar en aspectos como la identificación digital, los sistemas de control de acceso, la arquitectura de seguridad de la información, la estructura del área de seguridad, los sistemas de gestión de la seguridad de la información en comunicaciones y operación software o el desarrollo del plan de continuidad del negocio asociado a la seguridad. Con ello, el informático podrá conocer de forma completa todas las cuestiones relevantes de la ciberseguridad actual.

No encontrarás unos contenidos más completos y novedosos que estos para especializarte en dirección de ciberseguridad avanzada"

Módulo 1. Seguridad en el diseño y desarrollo de sistemas

1.1. Sistemas de Información
- 1.1.1. Dominios de un sistema de información
- 1.1.2. Componentes de un sistema de información
- 1.1.3. Actividades de un sistema de información
- 1.1.4. Ciclo de vida de un sistema de información
- 1.1.5. Recursos de un sistema de información

1.2. Sistemas de información. Tipología
- 1.2.1. Tipos de sistemas de información
  - 1.2.1.1. Empresarial
  - 1.2.1.2. Estratégicos
  - 1.2.1.3. Según el ámbito de la aplicación
  - 1.2.1.4. Específicos
- 1.2.2. Sistemas de Información. Ejemplos reales
- 1.2.3. Evolución de los sistemas de información: etapas
- 1.2.4. Metodologías de los sistemas de información

1.3. Seguridad de los sistemas de información. Implicaciones legales
- 1.3.1. Acceso a datos
- 1.3.2. Amenazas de seguridad: vulnerabilidades
- 1.3.3. Implicaciones legales: delitos
- 1.3.4. Procedimientos de mantenimiento de un sistema de información

1.4. Seguridad de un sistema de información. Protocolos de seguridad
- 1.4.1. Seguridad de un sistema de información
  - 1.4.1.1. Integridad
  - 1.4.1.2. Confidencialidad
  - 1.4.1.3. Disponibilidad
  - 1.4.1.4. Autenticación
- 1.4.2. Servicios de seguridad
- 1.4.3. Protocolos de seguridad de la información. Tipología
- 1.4.4. Sensibilidad de un sistema de información

1.5. Seguridad en un sistema de información. Medidas y sistemas de control de acceso
- 1.5.1. Medidas de seguridad
- 1.5.2. Tipo de medidas de seguridad
  - 1.5.2.1. Prevención
  - 1.5.2.2. Detección
  - 1.5.2.3. Corrección
- 1.5.3. Sistemas de control de acceso. Tipología
- 1.5.4. Criptografía

1.6. Seguridad en redes e internet
- 1.6.1. Firewalls
- 1.6.2. Identificación digital
- 1.6.3. Virus y gusanos
- 1.6.4. *Hacking*
- 1.6.5. Ejemplos y casos reales

1.7. Delitos informáticos
- 1.7.1. Delito informático
- 1.7.2. Delitos informáticos. Tipología
- 1.7.3. Delito Informático. Ataque. Tipologías
- 1.7.4. El caso de la realidad virtual
- 1.7.5. Perfiles de delincuentes y víctimas. Tipificación del delito
- 1.7.6. Delitos informáticos. Ejemplos y casos reales

1.8. Plan de seguridad en un sistema de información
- 1.8.1. Plan de seguridad. Objetivos
- 1.8.2. Plan de seguridad. Planificación
- 1.8.3. Plan de riesgos. Análisis
- 1.8.4. Política de seguridad. Implementación en la organización
- 1.8.5. Plan de seguridad. Implementación en la organización
- 1.8.6. Procedimientos de seguridad. Tipos
- 1.8.7. Planes de seguridad. Ejemplos

1.9. Plan de contingencia
- 1.9.1. Plan de contingencia. Funciones
- 1.9.2. Plan de emergencia: Elementos y objetivos
- 1.9.3. Plan de contingencia en la organización. Implementación
- 1.9.4. Planes de contingencia. Ejemplos

1.10. Gobierno de la seguridad de sistemas de información
- 1.10.1. Normativa legal
- 1.10.2. Estándares
- 1.10.3. Certificaciones
- 1.10.4. Tecnologías

Módulo 2. Arquitecturas y modelos de seguridad de la información

2.1. Arquitectura de seguridad de la información
- 2.1.1. SGSI/PDS
- 2.1.2. Alineación estratégica
- 2.1.3. Gestión del riesgo
- 2.1.4. Medición del desempeño

2.2. Modelos de seguridad de la información
- 2.2.1. Basados en políticas de seguridad
- 2.2.2. Basados en herramientas de protección
- 2.2.3. Basados en equipos de trabajo

2.3. Modelo de seguridad. Componentes clave
- 2.3.1. Identificación de riesgos
- 2.3.2. Definición de controles
- 2.3.3. Evaluación continua de niveles de riesgo
- 2.3.4. Plan de concienciación de empleados, proveedores, socios, etc.

2.4. Proceso de gestión de riesgos
- 2.4.1. Identificación de activos
- 2.4.2. Identificación de amenazas
- 2.4.3. Evaluación de riesgos
- 2.4.4. Priorización de controles
- 2.4.5. Reevaluación y riesgo residual

2.5. Procesos de negocio y seguridad de la información
- 2.5.1. Procesos de negocio
- 2.5.2. Evaluación de riesgos basados en parámetros de negocio
- 2.5.3. Análisis de impacto al negocio
- 2.5.4. Las operaciones de negocio y la seguridad de la información

2.6. Proceso de mejora continua
- 2.6.1. El ciclo de Deming
  - 2.6.1.1. Planificar
  - 2.6.1.2. Hacer
  - 2.6.1.3. Verificar
  - 2.6.1.4. Actuar

2.7. Arquitecturas de seguridad
- 2.7.1. Selección y homogeneización de tecnologías
- 2.7.2. Gestión de identidades. Autenticación
- 2.7.3. Gestión de accesos. Autorización
- 2.7.4. Seguridad de infraestructura de red
- 2.7.5. Tecnologías y soluciones de cifrado
- 2.7.6. Seguridad de Equipos Terminales (EDR)

2.8. El marco normativo
- 2.8.1. Normativas sectoriales
- 2.8.2. Certificaciones
- 2.8.3. Legislaciones

2.9. La norma ISO 27001
- 2.9.1. Implementación
- 2.9.2. Certificación
- 2.9.3. Auditorías y tests de intrusión
- 2.9.4. Gestión continua del riesgo
- 2.9.5. Clasificación de la información

2.10. Legislación sobre privacidad. RGPD (GDPR)
- 2.10.1. Alcance del Reglamento General de Protección de Datos (RGPD)
- 2.10.2. Datos personales
- 2.10.3. Roles en el tratamiento de datos personales
- 2.10.4. Derechos ARCO
- 2.10.5. El DPO. Funciones

Módulo 3. Gestión de la seguridad IT

3.1. Gestión de la seguridad
- 3.1.1. Operaciones de seguridad
- 3.1.2. Aspecto legal y regulatorio
- 3.1.3. Habilitación del negocio
- 3.1.4. Gestión de riesgos
- 3.1.5. Gestión de identidades y accesos

3.2. Estructura del área de seguridad. La oficina del CISO
- 3.2.1. Estructura organizativa. Posición del CISO en la estructura
- 3.2.2. Las líneas de defensa
- 3.2.3. Organigrama de la oficina del CISO
- 3.2.4. Gestión presupuestaria

3.3. Gobierno de seguridad
- 3.3.1. Comité de seguridad
- 3.3.2. Comité de seguimiento de riesgos
- 3.3.3. Comité de auditoría
- 3.3.4. Comité de crisis

3.4. Gobierno de seguridad. Funciones
- 3.4.1. Políticas y normas
- 3.4.2. Plan director de seguridad
- 3.4.3. Cuadros de mando
- 3.4.4. Concienciación y formación
- 3.4.5. Seguridad en la cadena de suministro

3.5. Operaciones de seguridad
- 3.5.1. Gestión de identidades y accesos
- 3.5.2. Configuración de reglas de seguridad de red. *Firewalls*
- 3.5.3. Gestión de plataformas IDS/IPS
- 3.5.4. Análisis de vulnerabilidades

3.6. Marco de trabajo de ciberseguridad. NIST CSF
- 3.6.1. Metodología NIST
  - 3.6.1.1. Identificar
  - 3.6.1.2. Proteger
  - 3.6.1.3. Detectar
  - 3.6.1.4. Responder
  - 3.6.1.5. Recuperar

3.7. Centro de Operaciones de Seguridad (SOC). Funciones
- 3.7.1. Protección. *Red Team, pentesting, threat intelligence*
- 3.7.2. Detección. SIEM, *user behavior analytics, fraud prevention*
- 3.7.3. Respuesta

3.8. Auditorías de seguridad
- 3.8.1. Test de intrusión
- 3.8.2. Ejercicios de *red team*
- 3.8.3. Auditorías de código fuente. Desarrollo seguro
- 3.8.4. Seguridad de componentes (*software supply chain*)
- 3.8.5. Análisis forense

3.9. Respuesta a incidentes
- 3.9.1. Preparación
- 3.9.2. Detección, análisis y notificación
- 3.9.3. Contención, erradicación y recuperación
- 3.9.4. Actividad post incidente
  - 3.9.4.1. Retención de evidencias
  - 3.9.4.2. Análisis forense
  - 3.9.4.3. Gestión de brechas
- 3.9.5. Guías oficiales de gestión de ciberincidentes

3.10. Gestión de vulnerabilidades
- 3.10.1. Análisis de vulnerabilidades
- 3.10.2. Valoración de vulnerabilidad
- 3.10.3. Bastionado de sistemas
- 3.10.4. Vulnerabilidades de día 0. *Zero-day*

Módulo 4. Análisis de riesgos y entorno de seguridad IT

4.1. Análisis del entorno
- 4.1.1. Análisis de la situación coyuntural
  - 4.1.1.1. Entornos VUCA
    - 4.1.1.1.1. Volátil
    - 4.1.1.1.2. Incierto
    - 4.1.1.1.3. Complejo
    - 4.1.1.1.4. Ambiguo
  - 4.1.1.2. Entornos BANI
    - 4.1.1.2.1. Quebradizo
    - 4.1.1.2.2. Ansioso
    - 4.1.1.2.3. No lineal
    - 4.1.1.2.4. Incomprensible
- 4.1.2. Análisis del entorno general. PESTEL
  - 4.1.2.1. Político
  - 4.1.2.2. Económico
  - 4.1.2.3. Social
  - 4.1.2.4. Tecnológico
  - 4.1.2.5. Ecológico/Ambiental
  - 4.1.2.6. Legal
- 4.1.3. Análisis de la situación interna. DAFO
  - 4.1.3.1. Objetivos
  - 4.1.3.2. Amenazas
  - 4.1.3.3. Oportunidades
  - 4.1.3.4. Fortalezas

4.2. Riesgo e incertidumbre
- 4.2.1. Riesgo
- 4.2.2. Gerencia de riesgos
- 4.2.3. Estándares de gestión de riesgos

4.3. Directrices para la gestión de riesgos ISO 31.000:2018
- 4.3.1. Objeto
- 4.3.2. Principios
- 4.3.3. Marco de referencia
- 4.3.4. Proceso

4.4. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)
- 4.4.1. Metodología MAGERIT
  - 4.4.1.1. Objetivos
  - 4.4.1.2. Método
  - 4.4.1.3. Elementos
  - 4.4.1.4. Técnicas
  - 4.4.1.5. Herramientas disponibles (PILAR)

4.5. Transferencia del riesgo cibernético
- 4.5.1. Transferencia de riesgos
- 4.5.2. Riesgos cibernéticos. Tipología
- 4.5.3. Seguros de ciber riesgos

4.6. Metodologías ágiles para la gestión de riesgos
- 4.6.1. Metodologías ágiles
- 4.6.2. Scrum para la gestión del riesgo
- 4.6.3. *Agile risk management*

4.7. Tecnologías para la gestión del riesgo
- 4.7.1. Inteligencia artificial aplicada a la gestión de riesgos
- 4.7.2. *Blockchain* y criptografía. Métodos de preservación del valor
- 4.7.3. Computación cuántica. Oportunidad o amenaza

4.8. Elaboración de mapas de riesgos IT basados en metodologías ágiles
- 4.8.1. Representación de la probabilidad y el impacto en entornos ágiles
- 4.8.2. El riesgo como amenaza del valor
- 4.8.3. Re-evolución en la gestión de proyectos y procesos ágiles basados en KRIs

4.9. *Risk driven* en la gestión de riesgos
- 4.9.1. *Risk driven*
- 4.9.2. *Risk driven* en la gestión de riesgos
- 4.9.3. Elaboración de un modelo de gestión empresarial impulsado por el riesgo

4.10. Innovación y transformación digital en la gestión de riesgos IT
- 4.10.1. La gestión de riesgos ágiles como fuente de innovación empresarial
- 4.10.2. Transformación de datos en información útil para la toma de decisiones
- 4.10.3. Visión holística de la empresa a través del riesgo

Módulo 5. Criptografía en IT

5.1. Criptografía
- 5.1.1. Criptografía
- 5.1.2. Fundamentos matemáticos

5.2. Criptología
- 5.2.1. Criptología
- 5.2.2. Criptoanálisis
- 5.2.3. Esteganografía y estegoanálisis

5.3. Protocolos criptográficos
- 5.3.1. Bloques básicos
- 5.3.2. Protocolos básicos
- 5.3.3. Protocolos intermedios
- 5.3.4. Protocolos avanzados
- 5.3.5. Protocolos exotéricos

5.4. Técnicas criptográficas
- 5.4.1. Longitud de claves
- 5.4.2. Manejo de claves
- 5.4.3. Tipos de algoritmos
- 5.4.4. Funciones resumen. *Hash*
- 5.4.5. Generadores de números pseudoaleatorios
- 5.4.6. Uso de algoritmos

5.5. Criptografía simétrica
- 5.5.1. Cifrados de bloque
- 5.5.2. DES (*Data Encryption Standard*)
- 5.5.3. Algoritmo RC4
- 5.5.4. AES (*Advanced Encryption Standard*)
- 5.5.5. Combinación de cifrados de bloques
- 5.5.6. Derivación de claves

5.6. Criptografía asimétrica
- 5.6.1. Diffie-Hellman
- 5.6.2. DSA (*Digital Signature Algorithm*)
- 5.6.3. RSA (Rivest, Shamir y Adleman)
- 5.6.4. Curva elíptica
- 5.6.5. Criptografía asimétrica. Tipología

5.7. Certificados digitales
- 5.7.1. Firma digital
- 5.7.2. Certificados X509
- 5.7.3. Infraestructura de clave pública (PKI)

5.8. Implementaciones
- 5.8.1. Kerberos
- 5.8.2. IBM CCA
- 5.8.3. *Pretty Good Privacy* (PGP)
- 5.8.4. ISO *Authentication Framework*
- 5.8.5. SSL y TLS
- 5.8.6. Tarjetas inteligentes en medios de pago (EMV)
- 5.8.7. Protocolos de telefonía móvil
- 5.8.8. *Blockchain*

5.9. Esteganografía
- 5.9.1. Esteganografía
- 5.9.2. Estegoanálisis
- 5.9.3. Aplicaciones y usos

5.10. Criptografía cuántica
- 5.10.1. Algoritmos cuánticos
- 5.10.2. Protección de algoritmos frente a computación cuántica
- 5.10.3. Distribución de claves cuántica

Módulo 6. Gestión de identidad y accesos en seguridad IT

6.1. Gestión de identidad y accesos (IAM)
- 6.1.1. Identidad digital
- 6.1.2. Gestión de identidad
- 6.1.3. Federación de identidades

6.2. Control de acceso físico
- 6.2.1. Sistemas de protección
- 6.2.2. Seguridad de las áreas
- 6.2.3. Instalaciones de recuperación

6.3. Control de acceso lógico
- 6.3.1. Autenticación: tipología
- 6.3.2. Protocolos de autenticación
- 6.3.3. Ataques de autenticación

6.4. Control de acceso lógico. Autenticación MFA
- 6.4.1. Control de acceso lógico. Autenticación MFA
- 6.4.2. Contraseñas. Importancia
- 6.4.3. Ataques de autenticación

6.5. Control de acceso lógico. Autenticación biométrica
- 6.5.1. Control de Acceso Lógico. Autenticación biométrica
  - 6.5.1.1. Autenticación biométrica. Requisitos
- 6.5.2. Funcionamiento
- 6.5.3. Modelos y técnicas

6.6. Sistemas de gestión de autenticación
- 6.6.1. *Single sign on*
- 6.6.2. Kerberos
- 6.6.3. Sistemas AAA

6.7. Sistemas de gestión de autenticación: Sistemas AAA
- 6.7.1. TACACS
- 6.7.2. RADIUS
- 6.7.3. DIAMETER

6.8. Servicios de control de acceso
- 6.8.1. FW-Cortafuegos
- 6.8.2. VPN-Redes Privadas Virtuales
- 6.8.3. IDS-Sistema de Detección de Intrusiones

6.9. Sistemas de control de acceso a la red
- 6.9.1. NAC
- 6.9.2. Arquitectura y elementos
- 6.9.3. Funcionamiento y estandarización

6.10. Acceso a redes inalámbricas
- 6.10.1. Tipos de redes inalámbricas
- 6.10.2. Seguridad en redes inalámbricas
- 6.10.3. Ataques en redes inalámbricas

Módulo 7. Seguridad en comunicaciones y operación software

7.1. Seguridad informática en comunicaciones y operación software
- 7.1.1. Seguridad informática
- 7.1.2. Ciberseguridad
- 7.1.3. Seguridad en la nube

7.2. Seguridad informática en comunicaciones y operación software. Tipología
- 7.2.1. Seguridad física
- 7.2.2. Seguridad lógica

7.3. Seguridad en comunicaciones
- 7.3.1. Principales elementos
- 7.3.2. Seguridad de redes
- 7.3.3. Mejores prácticas

7.4. Ciberinteligencia
- 7.4.1. Ingeniería social
- 7.4.2. *Deep web*
- 7.4.3. *Phishing*
- 7.4.4. *Malware*

7.5. Desarrollo seguro en comunicaciones y operación software
- 7.5.1. Desarrollo seguro. Protocolo HTTP
- 7.5.2. Desarrollo seguro. Ciclo de vida
- 7.5.3. Desarrollo seguro. Seguridad PHP
- 7.5.4. Desarrollo seguro. Seguridad NET
- 7.5.5. Desarrollo seguro. Mejores prácticas

7.6. Sistemas de gestión de la seguridad de la información en comunicaciones y operación software
- 7.6.1. GDPR
- 7.6.2. ISO 27021
- 7.6.3. ISO 27017/18

7.7. Tecnologías SIEM
- 7.7.1. Tecnologías SIEM
- 7.7.2. Operativa de SOC
- 7.7.3. SIEM *Vendors*

7.8. El rol de la seguridad en las organizaciones
- 7.8.1. Roles en las organizaciones
- 7.8.2. Rol de los especialistas IoT en las compañías
- 7.8.3. Certificaciones reconocidas en el mercado

7.9. Análisis forense
- 7.9.1. Análisis forense
- 7.9.2. Análisis forense. Metodología
- 7.9.3. Análisis forense. Herramientas e implantación

7.10. La ciberseguridad en la actualidad
- 7.10.1. Principales ataques informáticos
- 7.10.2. Previsiones de empleabilidad
- 7.10.3. Retos

Módulo 8. Seguridad en entornos Cloud

8.1. Seguridad en entornos *Cloud Computing*
- 8.1.1. Seguridad en entornos *Cloud Computing*
- 8.1.2. Seguridad en entornos *Cloud Computing*. Amenazas y riesgos seguridad
- 8.1.3. Seguridad en entornos *Cloud Computing*. Aspectos clave de seguridad

8.2. Tipos de infraestructura *Cloud*
- 8.2.1. Público
- 8.2.2. Privado
- 8.2.3. Híbrido

8.3. Modelo de gestión compartida
- 8.3.1. Elementos de seguridad gestionados por proveedor
- 8.3.2. Elementos gestionados por cliente
- 8.3.3. Definición de la estrategia para seguridad

8.4. Mecanismos de prevención
- 8.4.1. Sistemas de gestión de autenticación
- 8.4.2. Sistema de gestión de autorización: políticas de acceso
- 8.4.3. Sistemas de gestión de claves

8.5. Securización de sistemas
- 8.5.1. Securización de los sistemas de almacenamiento
- 8.5.2. Protección de los sistemas de base de datos
- 8.5.3. Securización de datos en tránsito

8.6. Protección de infraestructura
- 8.6.1. Diseño e implementación de red segura
- 8.6.2. Seguridad en recursos de computación
- 8.6.3. Herramientas y recursos para protección de infraestructura

8.7. Detección de las amenazas y ataques
- 8.7.1. Sistemas de auditoría, *Logging* y monitorización
- 8.7.2. Sistemas de eventos y alarmas
- 8.7.3. Sistemas SIEM

8.8. Respuesta ante incidentes
- 8.8.1. Plan de respuesta a incidentes
- 8.8.2. La Continuidad de Negocio
- 8.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

8.9. Seguridad en *Clouds* públicos
- 8.9.1. AWS (Amazon Web Services)
- 8.9.2. Microsoft Azure
- 8.9.3. Google GCP
- 8.9.4. Oracle Cloud

8.10. Normativa y cumplimiento
- 8.10.1. Cumplimiento de normativas de seguridad
- 8.10.2. Gestión de riesgos
- 8.10.3. Personas y proceso en las organizaciones

Módulo 9. Seguridad en comunicaciones de dispositivos IoT

9.1. De la telemetría al IoT
- 9.1.1. Telemetría
- 9.1.2. Conectividad M2M
- 9.1.3. Democratización de la telemetría

9.2. Modelos de referencia IoT
- 9.2.1. Modelo de referencia IoT
- 9.2.2. Arquitectura simplificada IoT

9.3. Vulnerabilidades de seguridad del IoT
- 9.3.1. Dispositivos IoT
- 9.3.2. Dispositivos IoT. Casuística de uso
- 9.3.3. Dispositivos IoT. Vulnerabilidades

9.4. Conectividad del IoT
- 9.4.1. Redes PAN, LAN, WAN
- 9.4.2. Tecnologías inalámbricas no IoT
- 9.4.3. Tecnologías inalámbricas LPWAN

9.5. Tecnologías LPWAN
- 9.5.1. El triángulo de hierro de las redes LPWAN
- 9.5.2. Bandas de frecuencia libres vs. Bandas licenciadas
- 9.5.3. Opciones de tecnologías LPWAN

9.6. Tecnología LoRaWAN
- 9.6.1. Tecnología LoRaWAN
- 9.6.2. Casos de uso LoRaWAN. Ecosistema
- 9.6.3. Seguridad en LoRaWAN

9.7. Tecnología Sigfox
- 9.7.1. Tecnología Sigfox
- 9.7.2. Casos de uso Sigfox. Ecosistema
- 9.7.3. Seguridad en Sigfox

9.8. Tecnología Celular IoT
- 9.8.1. Tecnología Celular IoT (NB-IoT y LTE-M)
- 9.8.2. Casos de uso Celular IoT. Ecosistema
- 9.8.3. Seguridad en Celular IoT

9.9. Tecnología WiSUN
- 9.9.1. Tecnología WiSUN
- 9.9.2. Casos de uso WiSUN. Ecosistema
- 9.9.3. Seguridad en WiSUN

9.10. Otras tecnologías IoT
- 9.10.1. Otras tecnologías IoT
- 9.10.2. Casos de uso y ecosistema de otras tecnologías IoT
- 9.10.3. Seguridad en otras tecnologías IoT

Módulo 10. Plan de continuidad del negocio asociado a la seguridad

10.1. Plan de Continuidad de Negocio
- 10.1.1. Los planes de Continuidad de Negocio (PCN)
- 10.1.2. Plan de Continuidad de Negocio (PCN). Aspectos clave
- 10.1.3. Plan de Continuidad de Negocio (PCN) para la valoración de la empresa

10.2. Métricas en un plan de Continuidad de Negocio (PCN)
- 10.2.1. *Recovery Time Objective* (RTO) y *Recovery Point Objective* (RPO)
- 10.2.2. Tiempo Máximo Tolerable (MTD)
- 10.2.3. Niveles Mínimos de Recuperación (ROL)
- 10.2.4. Punto de Recuperación Objetivo (RPO)

10.3. Proyectos de continuidad. Tipología
- 10.3.1. Plan de Continuidad de Negocio (PCN)
- 10.3.2. Plan de continuidad de TIC (PCTIC)
- 10.3.3. Plan de recuperación ante desastres (PRD)

10.4. Gestión de riesgos asociada al PCN
- 10.4.1. Análisis de impacto sobre el negocio
- 10.4.2. Beneficios de la implantación de un PCN
- 10.4.3. Mentalidad basada en riesgos

10.5. Ciclo de vida de un plan de Continuidad de Negocio
- 10.5.1. Fase 1: Análisis de la organización
- 10.5.2. Fase 2: Determinación de la estrategia de continuidad
- 10.5.3. Fase 3: Respuesta a la contingencia
- 10.5.4. Fase 4: Prueba, mantenimiento y revisión

10.6. Fase del análisis de la organización de un PCN
- 10.6.1. Identificación de procesos en el alcance del PCN
- 10.6.2. Identificación de áreas críticas del negocio
- 10.6.3. Identificación de dependencias entre áreas y procesos
- 10.6.4. Determinación del MTD adecuado
- 10.6.5. Entregables. Creación de un plan

10.7. Fase de determinación de la estrategia de continuidad en un PCN
- 10.7.1. Roles en la fase de determinación de la estrategia
- 10.7.2. Tareas de la fase de determinación de la estrategia
- 10.7.3. Entregables

10.8. Fase de respuesta a la contingencia en un PCN
- 10.8.1. Roles en la fase de respuesta
- 10.8.2. Tareas en esta fase
- 10.8.3. Entregables

10.9. Fase de pruebas, mantenimiento y revisión de un PCN
- 10.9.1. Roles en la fase de pruebas, mantenimiento y revisión
- 10.9.2. Tareas en la fase de pruebas, mantenimiento y revisión
- 10.9.3. Entregables

10.10. Normas ISO asociadas a los planes de Continuidad de Negocio (PCN)
- 10.10.1. ISO 22301:2019
- 10.10.2. ISO 22313:2020
- 10.10.3. Otras normas ISO e internacionales relacionadas

Al mejor profesorado y a su innovador sistema de enseñanza se le une el temario más completo y actualizado: estás ante una gran oportunidad de progresar como informático”

06

Metodología

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

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

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

Estudio de Caso para contextualizar todo el contenido

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

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

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

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

Un método de aprendizaje innovador y diferente

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

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

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

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

Relearning Methodology

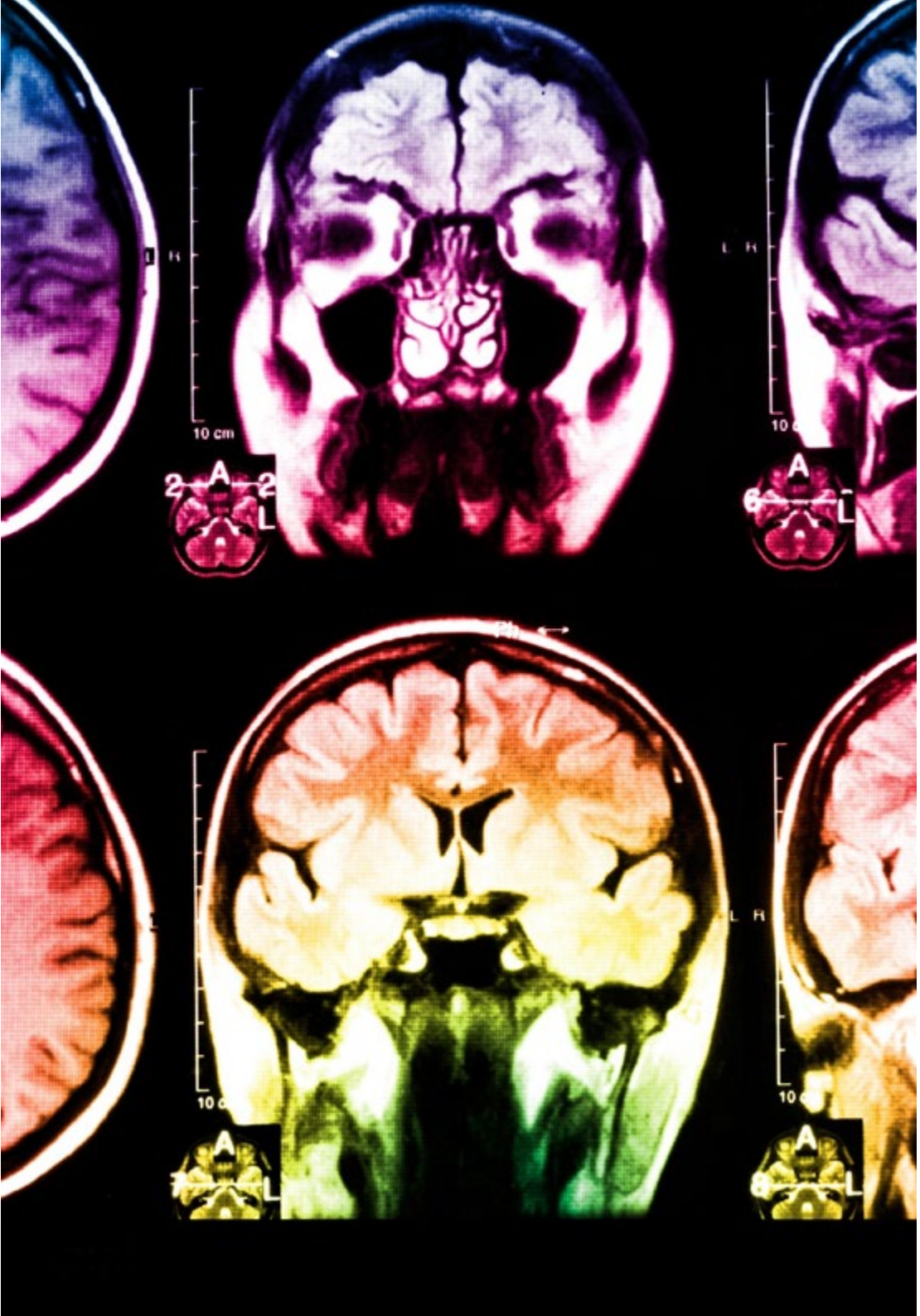
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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

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

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

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



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

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

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

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

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

Material de estudio

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

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

Clases magistrales

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

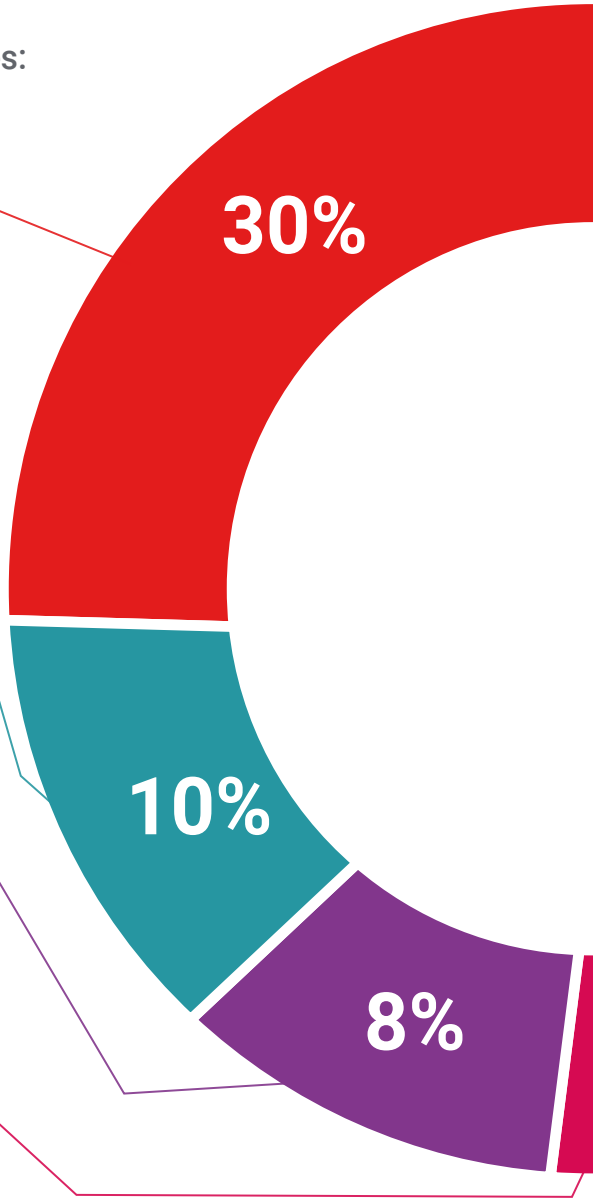
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

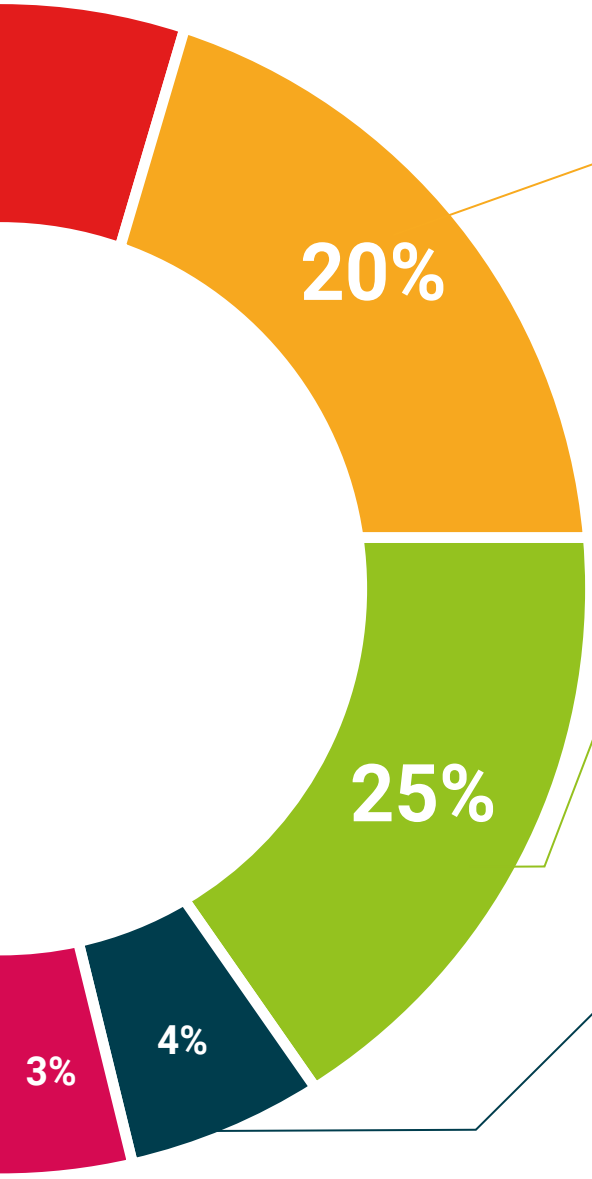
Prácticas de habilidades y competencias

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

Lecturas complementarias

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





Case studies

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

Resúmenes interactivos

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

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

Testing & Retesting

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

07

Titulación

El Máster Título Propio MBA en Dirección de Ciberseguridad Avanzada (CISO) garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Máster Título Propio expedido por TECH Universidad Tecnológica.

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

Este **Máster Título Propio MBA en Dirección de Ciberseguridad Avanzada (CISO)** contiene el programa más completo y actualizado del mercado.

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

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

Título: **Máster Título Propio MBA en Dirección de Ciberseguridad Avanzada (CISO)**

N.º Horas Oficiales: **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

MBA en Dirección de Ciberseguridad (CISO)

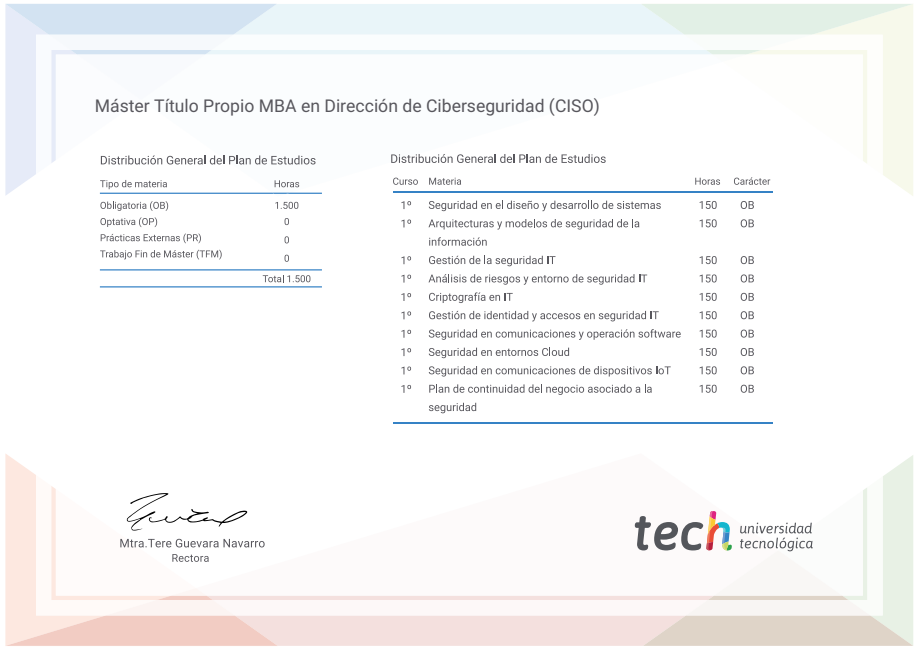
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio MBA en Dirección de Ciberseguridad (CISO)

Distribución General del Plan de Estudios

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

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Seguridad en el diseño y desarrollo de sistemas	150	OB
1º	Arquitecturas y modelos de seguridad de la información	150	OB
1º	Gestión de la seguridad IT	150	OB
1º	Análisis de riesgos y entorno de seguridad IT	150	OB
1º	Criptografía en IT	150	OB
1º	Gestión de identidad y accesos en seguridad IT	150	OB
1º	Seguridad en comunicaciones y operación software	150	OB
1º	Seguridad en entornos Cloud	150	OB
1º	Seguridad en comunicaciones de dispositivos IoT	150	OB
1º	Plan de continuidad del negocio asociado a la seguridad	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

Máster Título Propio
MBA en Dirección de Ciberseguridad Avanzada (CISO)

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

Máster Título Propio

MBA en Dirección de Ciberseguridad Avanzada (CISO)

tech universidad tecnológica