Máster Título Propio

Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

MDCCISO



tech universidad tecnológica



tech universidad tecnológica

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

Idioma: **Español**
Modalidad: **Online**
Duración: **12 meses**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **1.500 h.**
Acceso web: **www.techtitute.com/escuela-de-negocios/master/master-direccion-ciberseguridad-ciso-chief-information-security-officer**

Índice

01 Bienvenida — pág. 4

02 ¿Por qué estudiar en TECH? — pág. 6

03 ¿Por qué nuestro programa? — pág. 10

04 Objetivos — pág. 14

05 Competencias — pág. 20

06 Estructura y contenido — pág. 26

07 Metodología — pág. 40

08 Perfil de nuestros alumnos — pág. 48

09 Dirección del curso — pág. 52

10 Impacto para tu carrera — pág. 58

11 Beneficios para tu empresa — pág. 62

12 Titulación — pág. 66

02

¿Por qué estudiar en TECH?

TECH es la mayor escuela de negocio 100% online del mundo. Se trata de una Escuela de Negocios de élite, con un modelo de máxima exigencia académica. Un centro de alto rendimiento internacional y de entrenamiento intensivo en habilidades directivas.





TECH es una universidad de vanguardia tecnológica, que pone todos sus recursos al alcance del alumno para ayudarlo a alcanzar el éxito empresarial"

En TECH Universidad Tecnológica

Innovación

La universidad ofrece un modelo de aprendizaje en línea que combina la última tecnología educativa con el máximo rigor pedagógico. Un método único con el mayor reconocimiento internacional que aportará las claves para que el alumno pueda desarrollarse en un mundo en constante cambio, donde la innovación debe ser la apuesta esencial de todo empresario.

"Caso de Éxito Microsoft Europa" por incorporar en los programas un novedoso sistema de multivídeo interactivo.

Máxima exigencia

El criterio de admisión de TECH no es económico. No se necesita realizar una gran inversión para estudiar en esta universidad. Eso sí, para titularse en TECH, se podrán a prueba los límites de inteligencia y capacidad del alumno. El listón académico de esta institución es muy alto...

95% | **de los alumnos de TECH finaliza sus estudios con éxito**

Networking

En TECH participan profesionales de todos los países del mundo, de tal manera que el alumno podrá crear una gran red de contactos útil para su futuro.

+100.000 **directivos capacitados cada año**

+200 **nacionalidades distintas**

Empowerment

El alumno crecerá de la mano de las mejores empresas y de profesionales de gran prestigio e influencia. TECH ha desarrollado alianzas estratégicas y una valiosa red de contactos con los principales actores económicos de los 7 continentes.

+500 | **acuerdos de colaboración con las mejores empresas**

Talento

Este programa es una propuesta única para sacar a la luz el talento del estudiante en el ámbito empresarial. Una oportunidad con la que podrá dar a conocer sus inquietudes y su visión de negocio.

TECH ayuda al alumno a enseñar al mundo su talento al finalizar este programa.

Contexto Multicultural

Estudiando en TECH el alumno podrá disfrutar de una experiencia única. Estudiará en un contexto multicultural. En un programa con visión global, gracias al cual podrá conocer la forma de trabajar en diferentes lugares del mundo, recopilando la información más novedosa y que mejor se adapta a su idea de negocio.

Los alumnos de TECH provienen de más de 200 nacionalidades.



Aprende con los mejores

El equipo docente de TECH explica en las aulas lo que le ha llevado al éxito en sus empresas, trabajando desde un contexto real, vivo y dinámico. Docentes que se implican al máximo para ofrecer una especialización de calidad que permita al alumno avanzar en su carrera y lograr destacar en el ámbito empresarial.

Profesores de 20 nacionalidades diferentes.

En TECH tendrás acceso a los análisis de casos más rigurosos y actualizados del panorama académico"

TECH busca la excelencia y, para ello, cuenta con una serie de características que hacen de esta una universidad única:

Análisis

En TECH se explora el lado crítico del alumno, su capacidad de cuestionarse las cosas, sus competencias en resolución de problemas y sus habilidades interpersonales.

Excelencia académica

En TECH se pone al alcance del alumno la mejor metodología de aprendizaje online. La universidad combina el método *Relearning* (metodología de aprendizaje de posgrado con mejor valoración internacional) con el Estudio de Caso. Tradición y vanguardia en un difícil equilibrio, y en el contexto del más exigente itinerario académico.

Economía de escala

TECH es la universidad online más grande del mundo. Tiene un portfolio de más de 10.000 posgrados universitarios. Y en la nueva economía, **volumen + tecnología = precio disruptivo**. De esta manera, se asegura de que estudiar no resulte tan costoso como en otra universidad.

03

¿Por qué nuestro programa?

Realizar el programa de TECH supone multiplicar las posibilidades de alcanzar el éxito profesional en el ámbito de la alta dirección empresarial.

Es todo un reto que implica esfuerzo y dedicación, pero que abre las puertas a un futuro prometedor. El alumno aprenderá de la mano del mejor equipo docente y con la metodología educativa más flexible y novedosa.





Contamos con el más prestigioso cuadro docente y el temario más completo del mercado, lo que nos permite ofrecerte una capacitación de alto nivel académico"

Este programa aportará multitud de ventajas laborales y personales, entre ellas las siguientes:

01

Dar un impulso definitivo a la carrera del alumno

Estudiando en TECH el alumno podrá tomar las riendas de su futuro y desarrollar todo su potencial. Con la realización de este programa adquirirá las competencias necesarias para lograr un cambio positivo en su carrera en poco tiempo.

El 70% de los participantes de esta especialización logra un cambio positivo en su carrera en menos de 2 años.

02

Desarrollar una visión estratégica y global de la empresa

TECH ofrece una profunda visión de dirección general para entender cómo afecta cada decisión a las distintas áreas funcionales de la empresa.

Nuestra visión global de la empresa mejorará tu visión estratégica.

03

Consolidar al alumno en la alta gestión empresarial

Estudiar en TECH supone abrir las puertas de hacia panorama profesional de gran envergadura para que el alumno se posicione como directivo de alto nivel, con una amplia visión del entorno internacional.

Trabajarás más de 100 casos reales de alta dirección.

04

Asumir nuevas responsabilidades

Durante el programa se muestran las últimas tendencias, avances y estrategias, para que el alumno pueda llevar a cabo su labor profesional en un entorno cambiante.

El 45% de los alumnos consigue ascender en su puesto de trabajo por promoción interna.

05

Acceso a una potente red de contactos

TECH interrelaciona a sus alumnos para maximizar las oportunidades. Estudiantes con las mismas inquietudes y ganas de crecer. Así, se podrán compartir socios, clientes o proveedores.

Encontrarás una red de contactos imprescindible para tu desarrollo profesional.

06

Desarrollar proyectos de empresa de una forma rigurosa

El alumno obtendrá una profunda visión estratégica que le ayudará a desarrollar su propio proyecto, teniendo en cuenta las diferentes áreas de la empresa.

El 20% de nuestros alumnos desarrolla su propia idea de negocio.

07

Mejorar *soft skills* y habilidades directivas

TECH ayuda al estudiante a aplicar y desarrollar los conocimientos adquiridos y mejorar en sus habilidades interpersonales para ser un líder que marque la diferencia.

Mejora tus habilidades de comunicación y liderazgo y da un impulso a tu profesión.

08

Formar parte de una comunidad exclusiva

El alumno formará parte de una comunidad de directivos de élite, grandes empresas, instituciones de renombre y profesores cualificados procedentes de las universidades más prestigiosas del mundo: la comunidad TECH Universidad Tecnológica.

Te damos la oportunidad de especializarte con un equipo de profesores de reputación internacional.

04

Objetivos

Este Máster Título Propio de TECH está pensado para afianzar las capacidades profesionales de los directivos de empresas, quienes, además de estar ampliamente especializados en su área de actuación, encontrarán en este programa una oportunidad única para mejorar en un sector de gran importancia, puesto que aprenderán a prevenir posibles amenazas de internet que pueden ocasionar graves daños a los negocios. De esta manera, se convertirán en un profesional experto en diferentes ramas, por lo que podrán controlar todas las áreas de la compañía convirtiéndose, así, en Chief Information Security Officer.





Aumenta tu capacitación y logra tus objetivos laborales gracias a la capacitación superior que te ofrece TECH con este Máster Título Propio"

Tus objetivos son los nuestros.
Trabajamos conjuntamente para ayudarte a conseguirlos.

Este **Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** capacitará al alumno para:

01 Analizar el rol del analista en ciberseguridad

02 Profundizar en la ingeniería social y sus métodos

03 Examinar las metodologías OSINT, HUMINT, OWASP, PTEC OSSTM, OWISAM

04 Realizar un análisis de riesgo y conocer las métricas de riesgo



05 Determinar el adecuado uso de anonimato y uso de redes como TOR, I2P y Freenet

06 Compilar las normativas vigentes en materia de ciberseguridad



07 Generar conocimiento especializado para realizar una auditoría de seguridad

08 Desarrollar políticas de uso apropiadas

09 Examinar los sistemas de detección y prevención de las amenazas más importantes

10 Evaluar nuevos sistemas de detección de amenazas, así como su evolución respecto a soluciones más tradicionales

11 Analizar las principales plataformas móviles actuales, características y uso de las mismas

12 Identificar, analizar y evaluar riesgos de seguridad de las partes del proyecto IoT

13 Evaluar la información obtenida y desarrollar mecanismos de prevención y hacking

14 Aplicar la ingeniería inversa al entorno de la ciberseguridad



15 Concretar las pruebas que hay que realizar al software desarrollado

16 Recopilar todas las pruebas y datos existentes para llevar a cabo un informe forense



17 Presentar debidamente el informe forense

18 Analizar el estado actual y futuro de la seguridad informática

19 Examinar los riesgos de las nuevas tecnologías emergentes

20 Compilar las distintas tecnologías en relación a la seguridad informática

05

Competencias

Este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) ha sido diseñado pensando en mejorar la competitividad de los profesionales del sector empresarial. Por ello, al finalizar sus estudios, los alumnos habrán adquirido las competencias necesarias para desarrollar una praxis de calidad y actualizada en base a la metodología didáctica más innovadora. Sin duda, un programa que mejorará su capacitación y les permitirá ser más competitivo en su práctica diaria, al unificar todos los aspectos relevantes de la seguridad informática que los directivos deben conocer y poner en práctica.





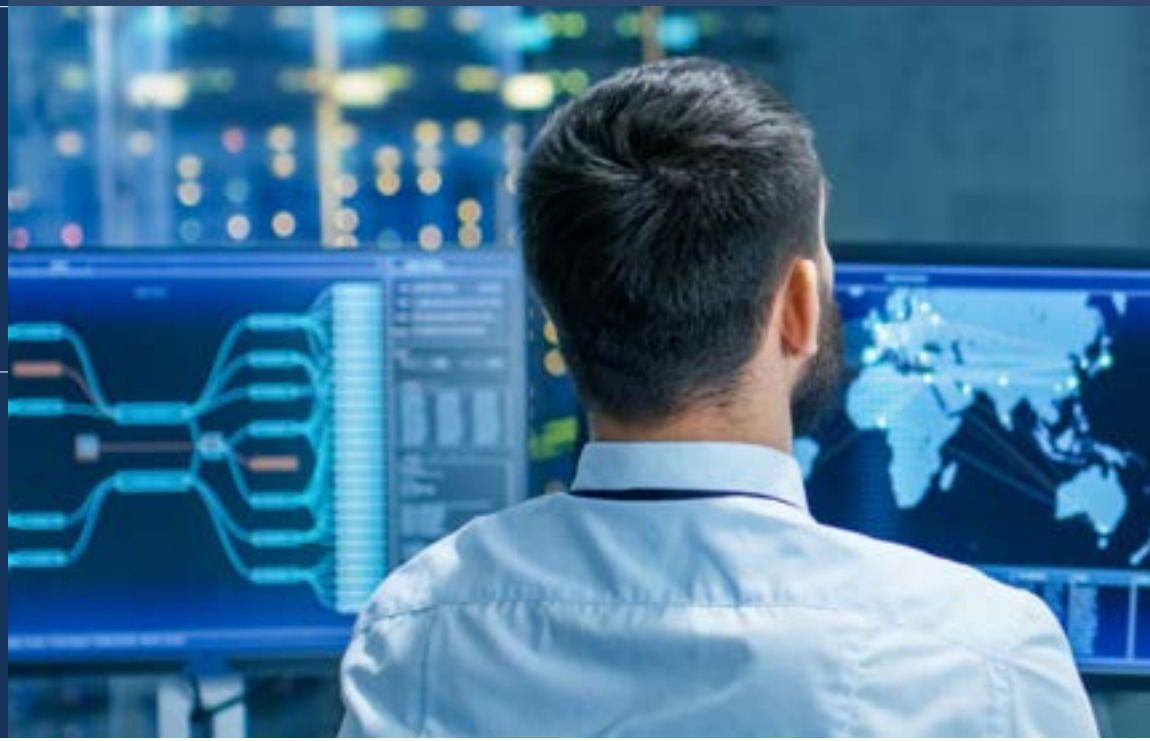
Adéntrate en el estudio de la seguridad informática y mejora tus habilidades para controlar las posibles amenazas de la red"

01 Conocer las metodologías usadas en materia de ciberseguridad

02 Evaluar cada tipo de amenaza para ofrecer una solución óptima en cada caso

03 Generar soluciones inteligentes completas para automatizar comportamientos ante incidentes

04 Evaluar los riesgos asociados a las vulnerabilidades tanto fuera como dentro de la empresa



05 Conocer la evolución y el impacto del IoT a lo largo del tiempo



06 Demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas

07 Saber aplicar *Sandboxing* en diferentes entornos

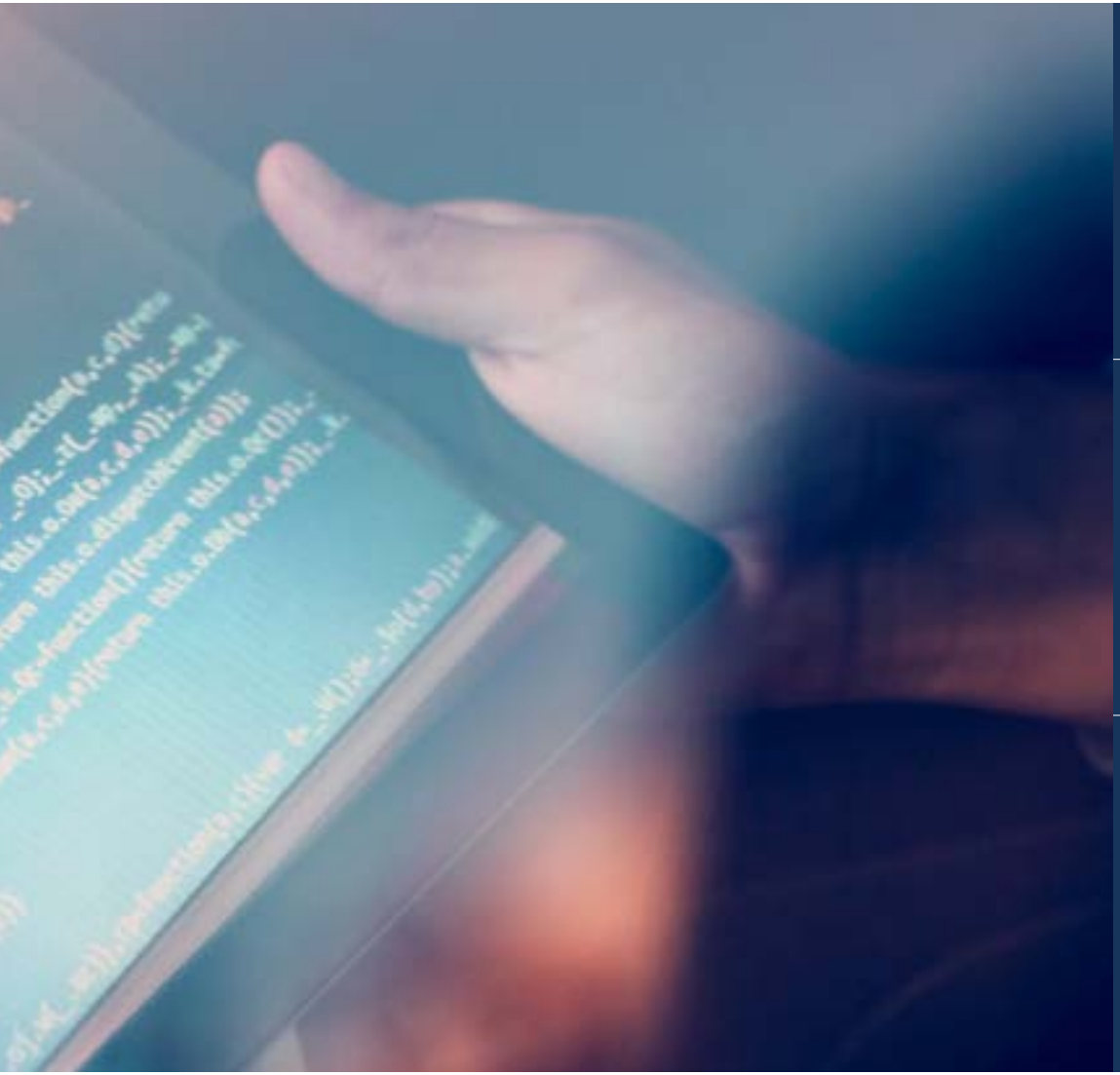
08 Conocer las directrices que debe seguir un buen desarrollador para cumplir con la seguridad necesaria

09 Realizar operaciones de seguridad defensiva

10 Tener una percepción profunda y especializada sobre la seguridad informática

11 Aplicar procesos de seguridad para smartphones y dispositivos portátiles





12 Conocer los medios para realizar el llamado *Hacking* ético y proteger una empresa de un ciberataque

13 Ser capaz de investigar un incidente de ciberseguridad

14 Diferenciar entre las técnicas de ataque y defensa existentes

06

Estructura y contenido

Este programa de TECH ha sido diseñado pensando en las necesidades de especialización de los profesionales de los negocios que desean ampliar sus conocimientos hacia la seguridad informática, un campo fundamental para poder controlar esas posibles amenazas que pueden suponer un gran riesgo para la empresa. De esta manera, el Máster Título Propio les permitirá adquirir esos conocimientos específicos que podrán aplicar a su práctica laboral. Y, para ello, usarán una metodología totalmente online que les permitirá compaginar su estudio con el resto de sus obligaciones diarias.





Este programa será fundamental para detectar posibles ciberataques en tu empresa”

Plan de estudios

El Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) de TECH Universidad Tecnológica es un programa intensivo que prepara a los alumnos para afrontar retos y decisiones empresariales en el ámbito de la seguridad informática. Su contenido está pensado para favorecer el desarrollo de las competencias directivas que permitan la toma de decisiones con un mayor rigor en entornos inciertos.

A lo largo de 1.500 horas de estudio, el alumno estudiará multitud de casos prácticos mediante el trabajo individual, lo que le permitirá adquirir las habilidades necesarias para desarrollarse con éxito en su práctica diaria. Se trata, por tanto, de una auténtica inmersión en situaciones reales de negocio.

Este programa trata en profundidad diferentes áreas de la empresa y está diseñado para que los directivos entiendan la ciberseguridad desde una perspectiva estratégica, internacional e innovadora.

Un plan pensado para especialmente para los alumnos, enfocado a su mejora profesional y que les prepara para alcanzar la excelencia en el ámbito de la dirección y la gestión de seguridad informática. Un programa que entiende sus necesidades y las de su empresa mediante un contenido innovador basado en las últimas tendencias, y apoyado por la mejor metodología educativa y un claustro excepcional, que les otorgará competencias para resolver situaciones críticas de forma creativa y eficiente.

Este Máster Título Propio se desarrolla a lo largo de 12 meses y se divide en 10 módulos:

Módulo 1	Ciberinteligencia y ciberseguridad
Módulo 2	Seguridad en *Host*
Módulo 3	Seguridad en red (perimetral)
Módulo 4	Seguridad en *Smartphones*
Módulo 5	Seguridad en IoT
Módulo 6	*Hacking* ético
Módulo 7	Ingeniería inversa
Módulo 8	Desarrollo seguro
Módulo 9	Análisis forense
Módulo 10	Retos actuales y futuros en seguridad informática



¿Dónde, cuándo y cómo se imparte?

TECH ofrece la posibilidad de desarrollar este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) de manera totalmente online. Durante los 12 meses que dura la especialización, el alumno podrá acceder a todos los contenidos de este programa en cualquier momento, lo que le permitirá autogestionar su tiempo de estudio.

Una experiencia educativa única, clave y decisiva para impulsar tu desarrollo profesional y dar el salto definitivo.

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

1.2. Ciberseguridad

1.2.1. Las capas de aeguridad
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 auditoria en seguridad informática
1.5.2. Documentación y permisos para auditoria
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 9
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 antirrastreadores

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 formado
4.6.2. Malware
4.6.2.1. Tipos de malware
4.6.3. Ingeniería social
4.6.4. Fuga de datos
4.6.5. Robo de información
4.6.6. Redes 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´s*
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. SQL *Injection*

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

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

Módulo 7. Ingeniería inversa

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

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

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

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

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

7.6. 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 anti-forenses
9.2.1. Objetivos de las técnicas anti-forenses
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 por 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. Criptomonedas
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 educación 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 capacitación que deben adoptar las empresas

Este programa te abrirá las puertas a un nuevo mundo profesional"

08

Perfil de nuestros alumnos

Este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) es un programa dirigido a profesionales que deseen mejorar su capacitación a través de la educación de calidad. Alumnos que quieren ampliar sus conocimientos en otra rama vinculada con los negocios como puede ser la informática, pero, más concretamente, la seguridad informática. Un programa dirigido a profesionales con experiencia, pero que creen en especialización superior como método para mejorar a nivel personal y profesional.



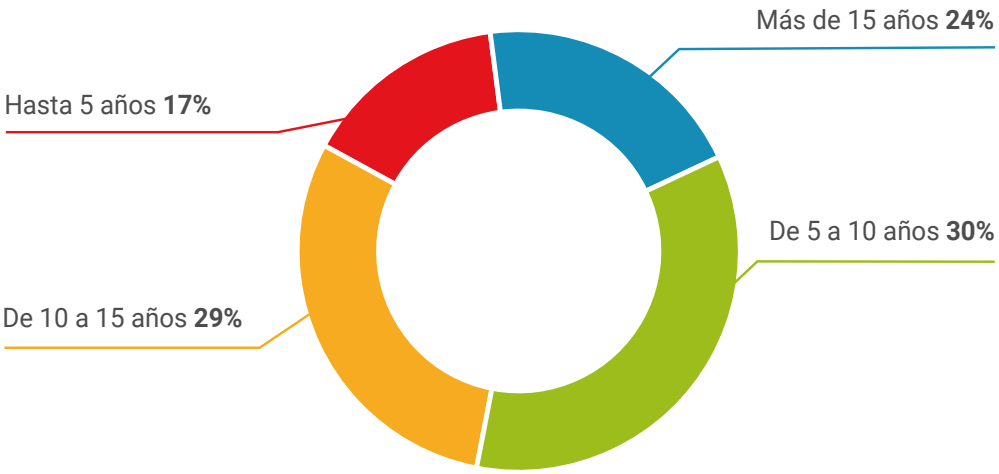


Los alumnos de TECH son profesionales con amplia experiencia que buscan una mejora laboral”

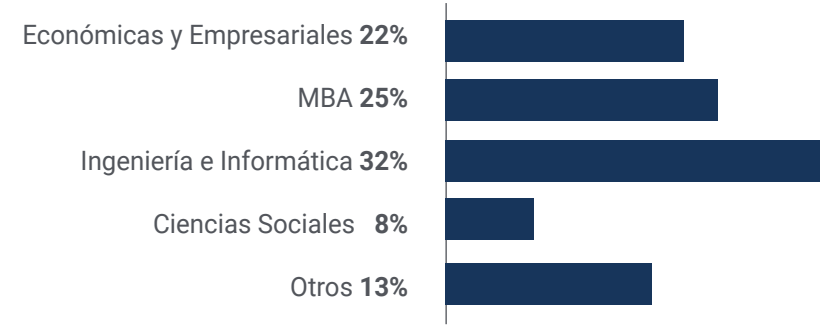
Edad media

Entre **35** y **45** años

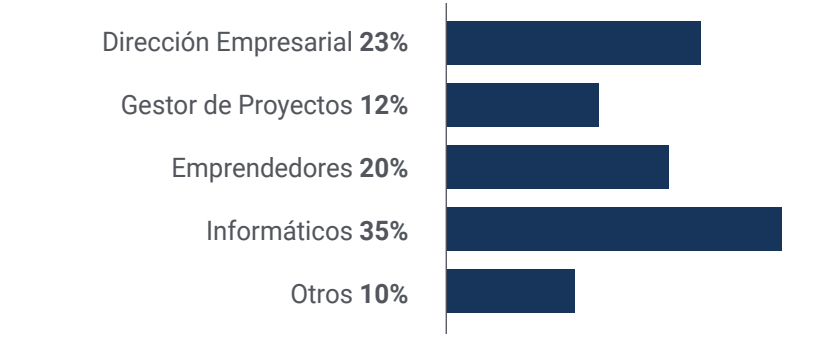
Años de experiencia



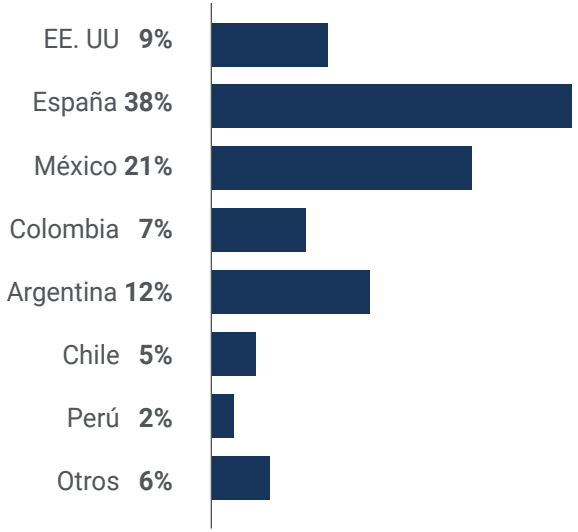
Formación



Perfil académico



Distribución geográfica





Jaime Díaz

Chief Revenue Officer

"En el ámbito empresarial en el que trabajo, manejamos gran cantidad de información confidencial y datos relevantes que, en manos inadecuadas, pueden generar un gran problema a la compañía. Por ello, llevaba tiempo pensando en ampliar mis conocimientos en ciberseguridad, con el objetivo de controlar, yo mismo, todos los procesos que pueden ser más sensibles ante una amenaza informática. Gracias a este programa de TECH, he logrado mejorar mi capacitación y actuar con más seguridad en mi trabajo"

09

Dirección del curso

Los docentes de este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) son profesionales con amplia experiencia en el sector, tanto a nivel profesional como educativo. Su especialización en este campo les permite tener la cualificación necesaria para ofrecer a los alumnos un estudio completo y de gran calidad sobre materias que serán útiles en su labor diaria en el ámbito empresarial. Sin duda, personas que creen en los estudios superiores como método para avanzar en su profesión y mejorar la competitividad de su negocio.





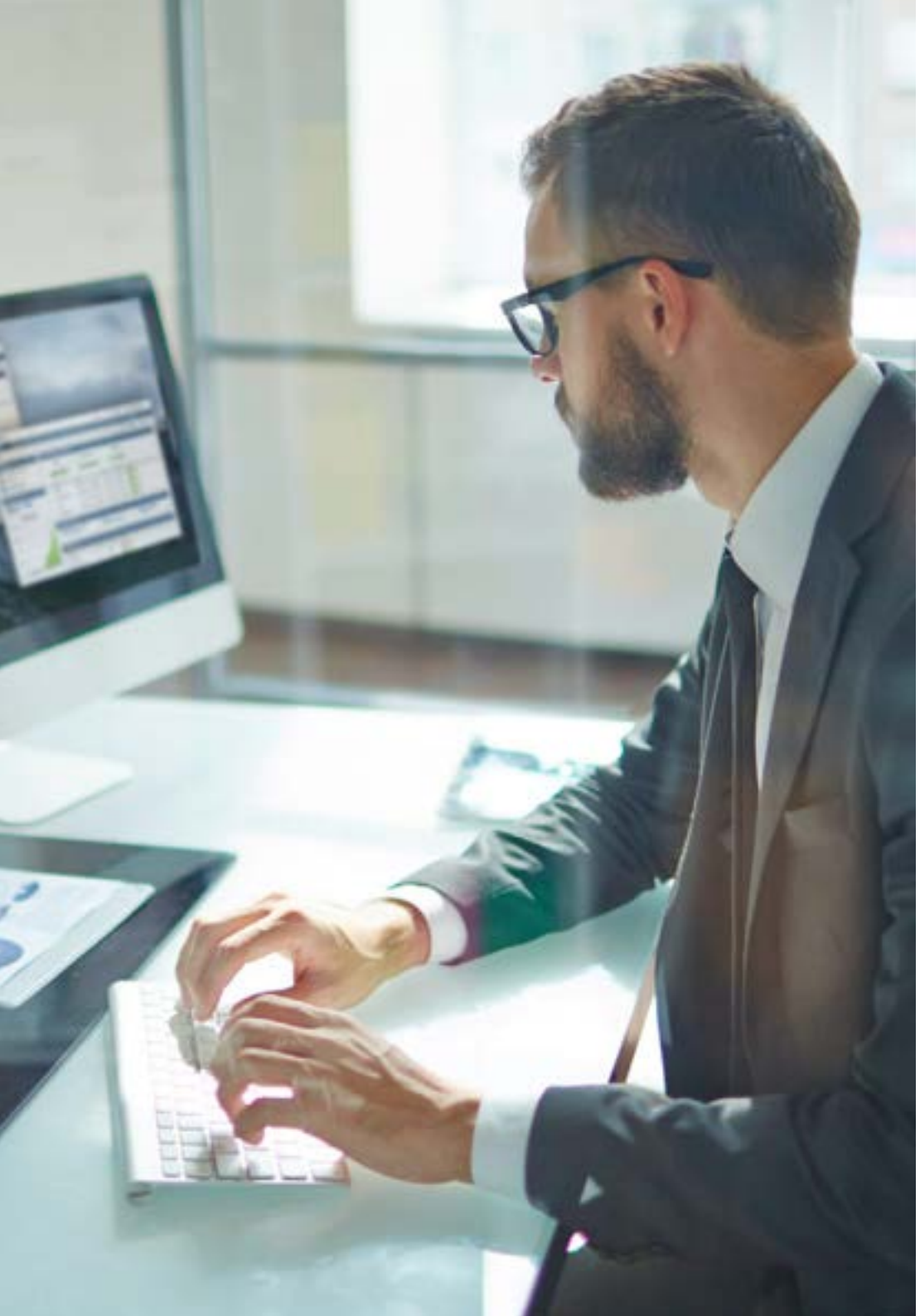
Un cuadro docente con amplia experiencia para ayudar a tu especialización en ciberseguridad"

Dirección



Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético. Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones. Madrid
- Instructora certificada E-Council. Madrid
- 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). Universidad de las Islas Baleares
- Ingeniera en Informática. Universidad de Alcalá de Henares. Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training. Madrid
- Microsoft Azure Security Techonologies. E-Council. Madrid



Profesores

D. Catalá Barba, José Francisco

- Mando intermedio en el MINISDEF Distintos cometidos y responsabilidades dentro del GOE III, tales como administración y gestión de incidencias de la red interna, realización de programas a medida para diferentes áreas, cursos de formación a los usuarios de la red y al personal del grupo en general
- Técnico electrónico en Factoría Ford sita en Almusafes, Valencia, programaciónde robots, PLC,s, reparación y mantenimiento
- Técnico Electrónico
- Desarrollador de aplicaciones para dispositivos móviles

D. Jiménez Ramos, Álvaro

- Analista de seguridad Senior 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

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60 UK
- Analista Programadora para la gestión, coordinación y documentación de entorno virtualizado de alarmas de seguridad en cliente
- Analista Programadora de aplicaciones Java para cajeros automáticos en cliente
- Profesional del Desarrollo de Software para aplicación de validación de firma y gestión documental en cliente
- Técnico de Sistemas para la migración de equipos y para la gestión, mantenimiento y formación de dispositivos móviles PDAs en cliente
- Ingeniería Técnica de Informática de Sistemas Universitat Oberta de Catalunya
- Máster en Seguridad Informática y Hacking Ético Oficial de EC- Council y CompTIA por la Escuela Profesional de Nuevas Tecnologías CICE

D. Peralta Alonso, Jon

- Abogado / DPO Altia Consultores S.A.
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC. Universidad Pública del País Vasco (UPV-EHU)
- Abogado / Asesor jurídico. Arriaga Asociados Asesoramiento Jurídico y Económico, S.L.
- Asesor jurídico / Pasante. Despacho de profesional: Oscar Padura
- Grado en Derecho. Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos. EIS Innovative School
- Máster Universitario en Abogacía. Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil. Universidad Internacional Isabel I de Castilla





D. Redondo, Jesús Serrano

- Desarrollador FrontEnd Junior y Técnico de Ciberseguridad Junior
- Desarrollador FrontEnd en Telefónica, Madrid
- Desarrollador de FrontEnd. Best Pro Consulting SL, Madrid
- Instalador de equipos y servicios de Telecomunicaciones. Grupo Zener, Castilla y León
- Instalador de equipos y servicios de Telecomunicaciones. Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática. CFTIC Getafe, Madrid
- Técnico Superior: Sistemas Telecomunicaciones e Informáticos. IES Trinidad Arroyo, Palencia
- Técnico Superior: Instalaciones Electrotécnicas MT y BT. IES Trinidad Arroyo, Palencia
- Formación en Ingeniería inversa, estenografía, cifrado. Academia Hacker Incibe (Talentos Incibe)

TECH ha seleccionado cuidadosamente al equipo docente de este programa para que puedas aprender de los mejores especialistas de la actualidad"

10

Impacto para tu carrera

La realización de este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) sumará un plus de calidad a la cualificación de los profesionales de los negocios, al ofrecer todo ese conocimiento que, aunque parezca totalmente alejado de su labor diaria, puede ser de gran utilidad para controlar esos procesos informáticos que pueden llegar a albergar algún elemento externo dañino que afecte a toda la organización. Por eso, la especialización superior en este campo se vuelve indispensable, tanto a nivel personal como profesionales de los alumnos, pero también para las empresas en las que se desarrollen laboralmente.





TECH pone todos sus recursos académicos a disposición de sus alumnos para que adquieran las habilidades necesarias que los dirijan hacia el éxito"

¿Estás preparado para dar el salto?
Una excelente mejora profesional te espera

Este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) de TECH Universidad Tecnológica es un programa intensivo y de gran valor dirigido a mejorar las habilidades laborales de los alumnos en un área de amplia competencia. Sin duda, es una oportunidad única para mejorar a nivel profesional, pero también personal, ya que implica esfuerzo y dedicación.

Los alumnos que deseen superarse a sí mismos, conseguir un cambio positivo a nivel profesional y relacionarse con los mejores, encontrarán en TECH su sitio.

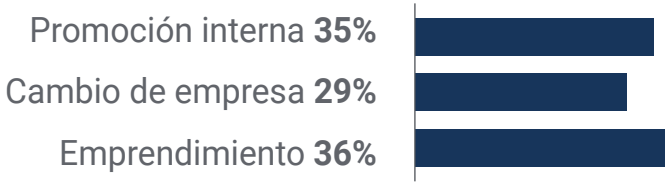
Un programa de gran nivel académico con el que dirigir tu carrera hacia el éxito.

La realización de este Máster Título Propio permitirá a los alumnos adquirir la competitividad necesaria para dar un giro radical a su carrera.

Momento del cambio



Tipo de cambio



Mejora salarial

La realización de este programa supone para nuestros alumnos un incremento salarial de más del **25,22%**



11

Beneficios para tu empresa

Este Máster Título Propio en Dirección de Ciberseguridad (CISO, Chief Information Security Officer) contribuye a elevar el talento de la organización a su máximo potencial mediante la especialización de líderes de alto nivel. De esta manera, los profesionales de los negocios podrán aportar un plus de calidad a su empresa, al tener ellos mismos las capacidades necesarias para controlar los procesos de ciberseguridad. Un programa que se adapta a los alumnos para que adquieran las herramientas necesarias que, posteriormente, podrán aplicar en su práctica diaria, logrando grandes beneficios para su empresa.





Un programa indispensable para los profesionales de los negocios que deseen controlar y gestionar los posibles problemas de Ciberseguridad"

Desarrollar y retener el talento en las empresas es la mejor inversión a largo plazo.

01

Crecimiento del talento y del capital intelectual

Aportará a la empresa nuevos conceptos, estrategias y perspectivas que pueden provocar cambios relevantes en la organización.

02

Retención de directivos de alto potencial evitando la fuga de talentos

Este programa refuerza el vínculo de la empresa con el directivo y abre nuevas vías de crecimiento profesional dentro de la misma.

03

Construcción de agentes de cambio

Será capaz de tomar decisiones en momentos de incertidumbre y crisis, ayudando a la organización a superar los obstáculos.

04

Incremento de las posibilidades de expansión internacional

Gracias a este programa, la empresa entrará en contacto con los principales mercados de la economía mundial.



05 **Desarrollo de proyectos propios**
El profesional podrá trabajar en un proyecto real o desarrollar nuevos proyectos en el ámbito de I+D o de desarrollo de negocio de su compañía.

06 **Aumento de la competitividad**
Este programa dotará a los alumnos de las competencias necesarias para asumir los nuevos desafíos e impulsar así la organización.

12

Titulación

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





Supera con éxito este programa y recibe tu titulación universitaria sin necesidad de realizar complicados trámites"

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

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

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

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

N.º Horas Oficiales: **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

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

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

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


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

Distribución General del Plan de Estudios

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

Distribución General del Plan de Estudios

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

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

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

Idioma: **Español**

Modalidad: **Online**

Duración: **12 meses**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **1.500 h.**

Máster Título Propio

Dirección de Ciberseguridad (CISO, Chief Information Security Officer)



tech universidad tecnológica