Maestría

Seguridad Informática Avanzada

Nº de RVOE: 20231900

RVOE

EDUCACIÓN SUPERIOR

tech universidad tecnológica

tech universidad tecnológica

Maestría
Seguridad Informática Avanzada

Nº de RVOE: **20231900**

Fecha de RVOE: **06/07/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Acceso web: www.techtitute.com/mx/informatica/maestria/maestria-seguridad-informatica-avanzada

Índice

01 Presentación — pág. 4

02 Plan de estudios — pág. 8

03 Objetivos — pág. 20

04 Competencias — pág. 26

05 ¿Por qué nuestro programa? — pág. 30

06 Salidas profesionales — pág. 34

07 Idiomas gratuitos — pág. 38

08 Metodología — pág. 42

09 Dirección del curso — pág. 50

10 Requisitos de acceso y proceso de admisión — pág. 56

11 Titulación — pág. 60

01

Presentación

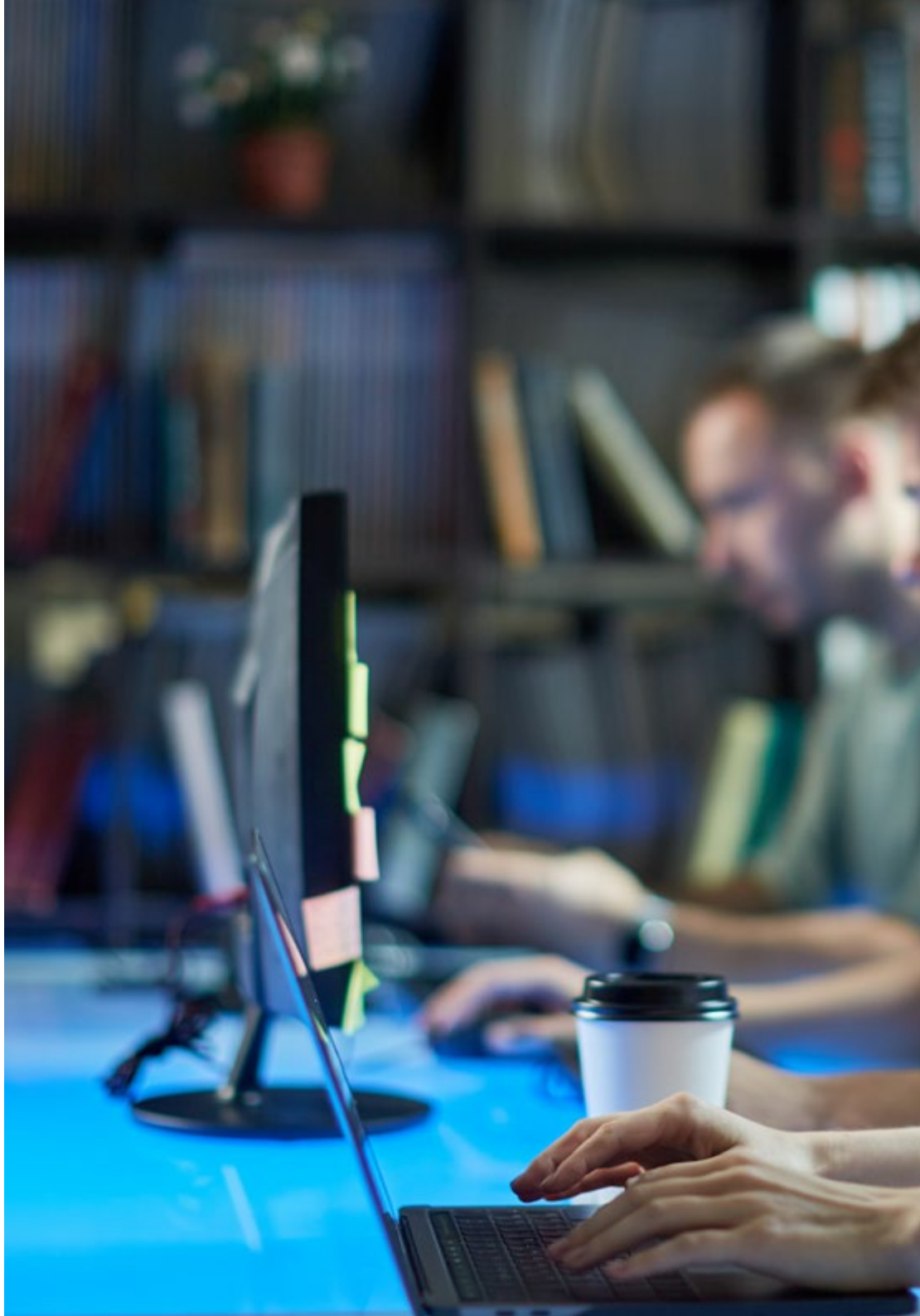
La seguridad de comunicación entre dispositivos provistos con tecnología IoT es una de las ramas más crecientes dentro de la Ciberseguridad. Esto se debe a que cada día, los hogares tienen más recursos informáticos interconectados, con acceso a información personal y familiar más sensible. Por eso, mantenerse actualizado en este ámbito del sector digital es prioritario, pero, al mismo tiempo, se considera una competencia avanzada que trasciende a las aptitudes y conocimientos generales de los profesionales habituales del sector. TECH quiere que sus egresados se desmarquen en ese contexto ofreciéndoles un intensivo y riguroso programa. En la titulación, 100% online, podrán abordar todos los avances en cuanto a prevención de riesgos y evaluación de vulnerabilidades digitales. Todo ello bajo la guía de un claustro docente de prestigio y la eficiencia académica del método de aprendizaje *Relearning*.

Este programa 100% online es la actualización universitaria que estabas esperando para impulsar tu carrera y acceder a puestos de relevancia en empresas tecnológicas de prestigio"

El análisis forense de ciberataques se ha convertido en una disciplina con múltiples aristas en los últimos años. A través de ella se pueden identificar el origen y las consecuencias totales de un ataque digital. De ello, a su vez, se desprende el desarrollo de herramientas y estrategias de gestión avanzadas para prevenir otras amenazas similares. Igualmente, este campo de estudios ha dado lugar a importantes debates éticos sobre cómo se controla la información de activos en una empresa o de sus potenciales clientes.

A pesar de esta diversidad de funciones y potencialidades, todavía no se reconoce a cabalidad el rol de la ciberseguridad en las empresas. Muchas compañías son deficientes en cuanto a la protección de sus datos o los de sus clientes debido a ineficientes programas de control y prevención de riesgos. Prueba de ellos son sucesos lamentables como el secuestro de información médica que han experimentado hospitales de diversas partes del mundo por hackers inescrupulosos. No obstante, poco a poco, cada vez más organizaciones son conscientes de la necesidad de atender a esta problemática y poner sus seguridades en las manos más especializadas. Así, ante los profesionales en Seguridad Informática Avanzada se abre una importante ventana de oportunidades de crecimiento laboral.

TECH, a partir de ese contexto, ha desarrollado este programa de carácter oficial. El temario, compuesto por 10 exhaustivos módulos, refiere aristas innovadoras como los fundamentos de la seguridad informática hasta la protección de infraestructuras y el análisis forense. También, examinarán las técnicas centradas en la protección de tecnologías basadas en el Internet de las cosas (IoT) o aquellas que facilitan la programación en la Nube. Por otro lado, podrán analizar los últimos criterios sobre gestión de la identidad y permisos de acceso.



Todos esos contenidos estarán disponibles en una plataforma 100% online, con materiales multimedia interactivos como vídeos e infografías. Además, estos serán impartidos por un claustro docente de excelencia, integrado por los expertos más capacitados del panorama global. Asimismo, TECH ha dispuesto el uso de método didácticos avanzados y eficientes como el *Relearning*. Esta estrategia educativa promueve la repetición de conceptos a lo largo de los módulos, potenciando que los alumnos consigan familiarizarse con ellos de manera profunda hasta incorporarlos a su praxis cotidiana. Con todas estas ventajas, esta Maestría en Seguridad Informática Avanzada constituye un ejemplo de puesta al día rigurosa, personalizada y ajustada a las necesidades más imperativas del contexto digital.

TECH brinda la oportunidad de obtener la Maestría en Seguridad Informática Avanzada en un formato 100% en línea, con titulación directa y un programa diseñado para aprovechar cada tarea en la adquisición de competencias para desempeñar un papel relevante en la empresa. Pero, además, con este programa, el estudiante tendrá acceso al estudio de idiomas extranjeros y formación continuada de modo que pueda potenciar su etapa de estudio y logre una ventaja competitiva con los egresados de otras universidades menos orientadas al mercado laboral.

Un camino creado para conseguir un cambio positivo a nivel profesional, relacionándose con los mejores y formando parte de la nueva generación de informáticos capaces de desarrollar su labor en cualquier lugar del mundo.

> *¡Esta es la oportunidad que estabas esperando! Inscríbete en TECH y completa 10 módulos académicos en 20 meses de manera personalizada, en correspondencia con tus responsabilidades”*

02

Plan de estudios

El temario de este programa oficial de TECH está compuesto por 10 módulos en los cuales el alumno podrá analizar e interiorizar todos los avances el ámbito de la Ciberseguridad Informática. La titulación, conformada según las experiencias de los mayores expertos de este campo, se sustenta en materiales académicos actualizados y en una amplia variedad de recursos multimedia que facilitan la asimilación rápida y flexible de los conceptos y herramientas de trabajo más complejas.

Vídeos, infografías, resúmenes interactivos y otros materiales multimedia dispuestos en esta titulación te permitirán vencer el proceso académico con totales garantías de superación"

Estos contenidos están dispuestos en una plataforma 100% online, que no está restringida a ningún horario específico. Por el contrario, cada alumno tendrá la oportunidad de acceder a los materiales de manera individual, en el momento que así lo estime conveniente. Para ello, solo necesitará de un dispositivo conectado a Internet y algún resquicio de tiempo que se inserte entre sus demás responsabilidades.

Al mismo tiempo, este programa cuenta con metodologías didácticas disruptivas como el Relearning. Esta estrategia educativa, basada en la reiteración, conseguirá que los egresados se adapten al entorno profesional de la Seguridad Informática Avanzada desde la etapa educativa. Así, al completar la titulación, estarán listos para enfrentar todo tipo de demandas, exigencias y desafíos en el plano laboral.

Con métodos como el Testing y Retesting comprobarás tus progresos académicos de manera periódica y no abandonarás ningún módulo con dudas o sin haber interiorizado sus conceptos más complejos"

Módulo 1	Seguridad en el diseño y desarrollo de sistemas
Módulo 2	Arquitecturas y modelos de seguridad de la información
Módulo 3	Gestión de la seguridad en tecnologías de la información
Módulo 4	Análisis de riesgos y entorno de seguridad en tecnología de la información
Módulo 5	Criptografía en tecnología de la información
Módulo 6	Gestión de identidad y accesos en seguridad de las tecnologías de la información y las comunicaciones
Módulo 7	Seguridad en comunicaciones y operación software
Módulo 8	Seguridad en entornos de la nube
Módulo 9	Seguridad en comunicaciones de dispositivos de Internet de las Cosas (IoT)
Módulo 10	Plan de continuidad del negocio asociado a seguridad

Dónde, cuándo y cómo se imparte

Esta Maestría se ofrece 100% en línea, por lo que alumno podrá cursarla desde cualquier sitio, haciendo uso de una computadora, una tableta o simplemente mediante su smartphone.

Además, podrá acceder a los contenidos tanto online como offline. Para hacerlo offline bastará con descargarse los contenidos de los temas elegidos, en el dispositivo y abordarlos sin necesidad de estar conectado a internet.

El alumno podrá cursar la Maestría a través de sus 10 módulos, de forma autodirigida y asincrónica. Adaptamos el formato y la metodología para aprovechar al máximo el tiempo y lograr un aprendizaje a medida de las necesidades del alumno.

> *El Relearning, método didáctico por excelencia de TECH, es la herramienta fundamental de esta Maestría para ayudarte a adquirir competencias prácticas de modo rápido, flexible y eficiente"*

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
- 1.2.2. 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
- 1.4.2. Servicios de Seguridad
- 1.4.3. Protocolos de Seguridad de la Información
- 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
- 1.5.3. Sistemas de Control de Acceso. Tipología
- 1.5.4. Criptografía

1.6. Seguridad en Redes e Internet
- 1.6.1. Dispositivo de seguridad "Firewall"
- 1.6.2. Identificación Digital
- 1.6.3. Virus y Gusanos
- 1.6.4. Ejemplos y Casos Reales

1.7. Delitos Informáticos
- 1.7.1. Delitos informáticos. Tipología
- 1.7.2. Delito Informático. Ataque. Tipologías
- 1.7.3. El Caso de la Realidad Virtual
- 1.7.4. Perfiles de delincuentes y víctimas. Tipificación del delito
- 1.7.5. 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. Sistemas de Gestión de Seguridad
- 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. Re-evaluación 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

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 pruebas 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
- 2.10.2. Datos personales
- 2.10.3. Roles en el tratamiento de Datos personales
- 2.10.4. Derechos Acceso, Rectificación Cancelación y Oposición (ARCO)
- 2.10.5. El Delegado de Protección de Datos. Funciones

Módulo 3. Gestión de la seguridad en tecnologías de la información

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 Responsable de Seguridad Informática
- 3.2.1. Estructura organizativa
- 3.2.2. Las líneas de defensa
- 3.2.3. Organigrama de la oficina del responsable de seguridad
- 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
- 3.5.3. Gestión de Plataformas IDS e IPS
- 3.5.4. Análisis de Vulnerabilidades

3.6. Marco de trabajo de Ciberseguridad. Herramientas NIST y CSF
- 3.6.1. Metodología
  - 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
- 3.7.1. Protección
- 3.7.2. Detección
- 3.7.3. Respuesta

3.8. Auditorías de seguridad
- 3.8.1. Prueba de Intrusión
- 3.8.2. Ejercicios de herramienta equipo rojo
- 3.8.3. Auditorías de Código Fuente. Desarrollo seguro
- 3.8.4. Seguridad de Componentes
- 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
- 3.9.5. 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"

Módulo 4. Análisis de riesgos y entorno de seguridad en tecnología de la información

4.1. Análisis del Entorno
- 4.1.1. Análisis de la Situación Coyuntural
- 4.1.2. Análisis del Entorno General
- 4.1.3. Análisis de la situación interna

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 31000: 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
- 4.4.1. Objetivos
- 4.4.2. Método
- 4.4.3. Elementos
- 4.4.4. Técnicas
- 4.4.5. Herramientas disponibles

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. Proceso de práctica "Scrum" para la Gestión del riesgo
- 4.6.3. Metodología ágil de gestión de riesgos

4.7. Tecnologías para la Gestión del Riesgo
- 4.7.1. Inteligencia Artificial aplicada a la Gestión de Riesgos
- 4.7.2. Métodos de Preservación del Valor
- 4.7.3. Computación Cuántica. Oportunidad o Amenaza

4.8. Elaboración de Mapas de Riesgos 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

4.9. Gestión impulsada por el Riesgo o "Risk Driven"
- 4.9.1. Metodología "Risk Driven"
- 4.9.2. Metodología "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
- 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 tecnología de la información

5.1. Criptografía
- 5.1.1. Antecedentes
- 5.1.2. Fundamentos matemáticos
- 5.1.3. Componentes

5.2. Criptología
- 5.2.1. Antecedentes de la 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

5.4. 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
- 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. Algoritmo de cifrados de información DES
- 5.5.3. Algoritmo RC4
- 5.5.4. Esquema de cifrado por bloques AES
- 5.5.5. Combinación de cifrados de bloques
- 5.5.6. Derivación de claves

5.6. Criptografía asimétrica
- 5.6.1. Protocolo criptográfico Diffie-Hellman
- 5.6.2. Algoritmo de firma digital
- 5.6.3. Sistema criptográfico de clave pública RSA
- 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

5.8. Implementaciones
- 5.8.1. Protocolo de autenticación Kerberos
- 5.8.2. Procesador criptográfico IBM CCA
- 5.8.3. Programa de protección “Pretty Good Privacy” o PGP
- 5.8.4. Tarjetas inteligentes en medios de pago
- 5.8.5. Protocolos de telefonía móvil

5.9. Esteganografía
- 5.9.1. Fundamentos de Esteganografía
- 5.9.2. Fundamentos de 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 de las tecnologías de la información y las comunicaciones

6.1. Gestión de identidad y accesos
- 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 de múltiples factores o MFA
- 6.4.1. Autenticación MFA. Características
- 6.4.2. Contraseñas. Importancia
- 6.4.3. Ataques de Autenticación

6.5. Control de acceso lógico. Autenticación Biométrica
- 6.5.1. Autenticación Biométrica. Características
- 6.5.2. Autenticación biométrica. Requisitos
- 6.5.3. Funcionamiento
- 6.5.4. Modelos y técnicas

6.6. Sistemas de Gestión de Autenticación
- 6.6.1. Inicio de sesión único
- 6.6.2. Protocolo Kerberos
- 6.6.3. Protocolos AAA: autenticación, autorización y contabilización
- 6.6.4. Casos de Uso y Aplicación

6.7. Sistemas de Gestión de Autenticación: Sistemas AAA
- 6.7.1. Protocolo TACACS
- 6.7.2. Servidor RADIUS
- 6.7.3. Protocolo de red DIAMETER

6.8. Servicios de Control de Acceso
- 6.8.1. Cortafuegos
- 6.8.2. Redes Privadas Virtuales
- 6.8.3. Sistema de Detección de Intrusiones

6.9. Sistemas de Control de Acceso a la Red
- 6.9.1. Control de acceso a la red o "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. Antecedentes
- 7.2.2. Seguridad Física
- 7.2.3. 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. La red profunda o "Deep web"
- 7.4.3. Engaño o "Phishing"
- 7.4.4. Programa malicioso o "Malware"

7.5. Desarrollo Seguro en Comunicaciones y Operación Software
- 7.5.1. Protocolo de transferencia de hipertexto "HTTP"
- 7.5.2. Ciclo de Vida
- 7.5.3. Seguridad en preprocesador PHP
- 7.5.4. Seguridad NET
- 7.5.5. Mejores prácticas

7.6. Sistemas de Gestión de la Seguridad de la Información en Comunicaciones y Operación Software
- 7.6.1. Marco legal en protección de datos
- 7.6.2. Norma ISO 27021
- 7.6.3. Norma ISO 27017/18

7.7. Tecnologías SIEM
- 7.7.1. Bases y fundamentos
- 7.7.2. Tecnologías de Información de seguridad y gestión de eventos o SIEM
- 7.7.3. Operativa de un Centro de Operaciones de Seguridad

7.8. El Rol de la Seguridad en las Organizaciones
- 7.8.1. Roles en las organizaciones
- 7.8.2. Rol de los especialistas de Internet de las cosas en las compañías
- 7.8.3. Certificaciones reconocidas en el mercado

7.9. Análisis Forense
- 7.9.1. Análisis Forense
- 7.9.2. Metodología
- 7.9.3. 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 de la nube

8.1. Seguridad en Entornos de la nube
- 8.1.1. Antecedentes e importancia
- 8.1.2. Amenazas y riesgos seguridad
- 8.1.3. Aspectos clave de seguridad

8.2. Tipos de infraestructura en la nube
- 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 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 la nube de acceso público
- 8.9.1. Servicios de Amazon en la nube
- 8.9.2. Servicios de Microsoft en la nube
- 8.9.3. Servicios de Google en la nube
- 8.9.4. Servicios Oracle en la nube

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 de Internet de las Cosas (IoT)

9.1. Seguridad en Comunicaciones de Dispositivos provistos con internet o "IoT"
- 9.1.1. Telemetría
- 9.1.2. Conectividad Máquina a Máquina
- 9.1.3. Democratización de la Telemetría

9.2. Modelos de Referencia
- 9.2.1. Importancia
- 9.2.2. Características
- 9.2.3. Arquitectura simplificada

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

9.4. Conectividad del IoT
- 9.4.1. Tipos de Redes
- 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. Antecedentes
- 9.6.2. Casos de uso y Ecosistema
- 9.6.3. Seguridad en LoRaWAN

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

9.8. Tecnología Celular IoT
- 9.8.1. Tecnología Celular IoT
- 9.8.2. Casos de uso Celular y Ecosistema
- 9.8.3. Seguridad en Celular IoT

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

9.10. Otras tecnologías IoT
- 9.10.1. Importancia
- 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 seguridad

10.1. Plan de continuidad del negocio
- 10.1.1. Los Planes de Continuidad de Negocio
- 10.1.2. Aspectos CLAVE
- 10.1.3. Plan de valoración de la empresa

10.2. Métricas en un Plan de Continuidad de Negocio
- 10.2.1. Tiempo máximo tolerable
- 10.2.2. Niveles mínimos de Recuperación
- 10.2.3. Punto de Recuperación Objetivo

10.3. Proyectos de continuidad
- 10.3.1. Plan de Continuidad de Negocio
- 10.3.2. Plan de Continuidad de Tecnologías de la Información y las Comunicaciones
- 10.3.3. Plan de Recuperación ante Desastres

10.4. Gestión de Riesgos asociada al plan de continuidad
- 10.4.1. Análisis de Impacto sobre el negocio
- 10.4.2. Beneficios de la implantación de un Plan
- 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 Plan de continuidad
- 10.6.1. Identificación de procesos en el alcance del Plan
- 10.6.2. Identificación de áreas críticas del negocio
- 10.6.3. Identificación de dependencias entre áreas y procesos
- 10.6.4. Determinación de la protección de dispositivos móviles adecuada
- 10.6.5. Entregables. Creación de un plan

10.7. Fase de Determinación de la Estrategia de Continuidad
- 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
- 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 Plan
- 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
- 10.10.1. Norma ISO 22301:2019
- 10.10.2. Norma ISO 22313:2020
- 10.10.3. Otras normas ISO e internacionales relacionadas

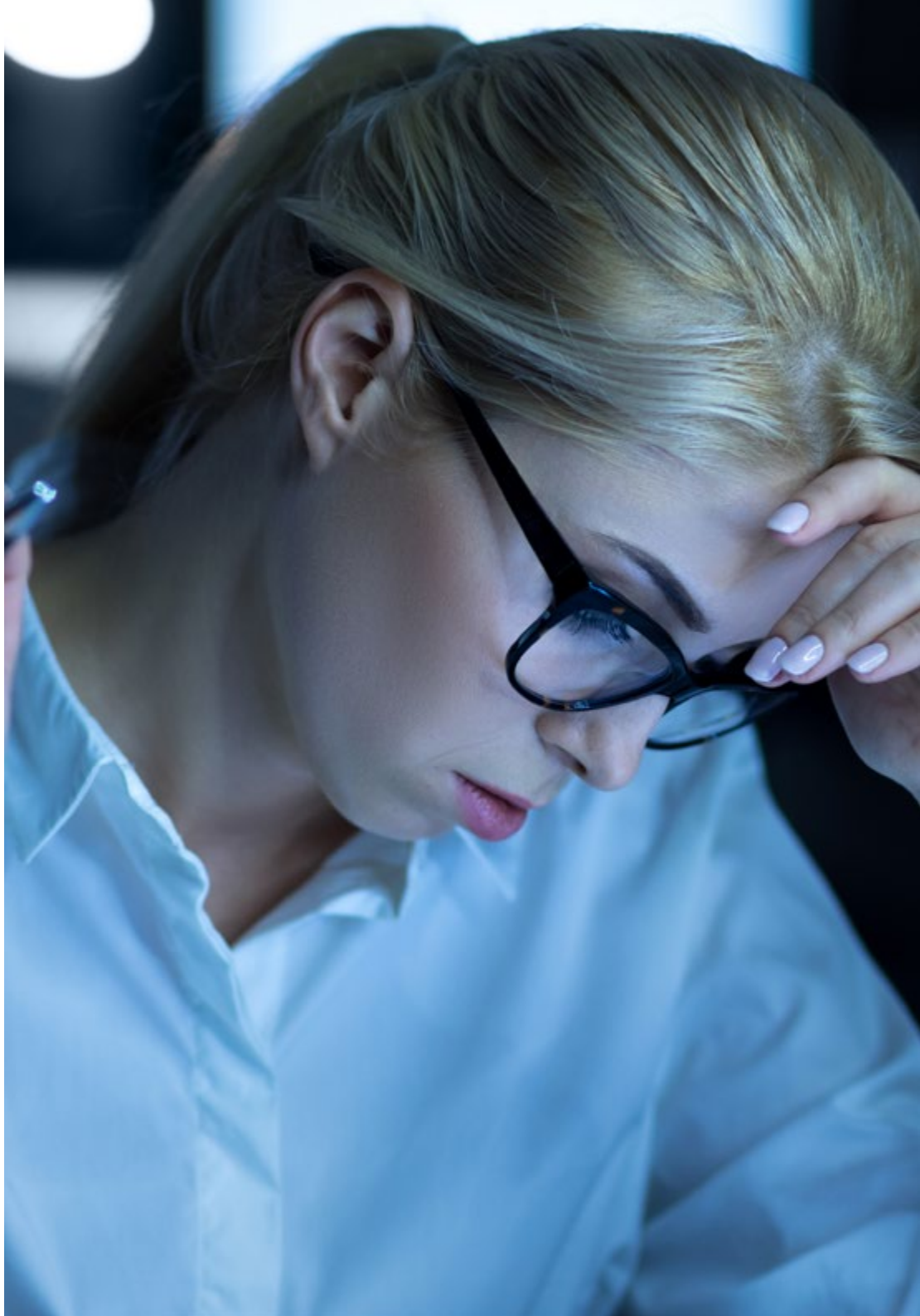
03
Objetivos

Esta Maestría es idónea para aquellos profesionales que buscan ampliar sus horizontes en el campo de la protección y defensa de la información digital. A través de un enfoque integral, el programa les brindará competencias teórico-prácticas avanzadas y les facilitará la comprensión de los aspectos ético-legales más acuciantes de esta área profesional. Así, el objetivo fundamental será prepararlos para enfrentar todas las problemáticas actuales y, al mismo tiempo, brindarles una visión a futuro de las herramientas y estrategias que les ayudarán a solventar situaciones complejas en las próximas décadas de evolución de esta esfera del mundo informático.

Este programa de estudios te permitirá ahondar en sus contenidos de manera personalizada, sin horarios restrictivos ni cronogramas evaluativos continuos”

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
- Diferenciar 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)
- Examinar el Modelo de Gestión de Riesgos basado en la ISO 31.000
- Ahondar en la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Abordar los certificados digitales, la Infraestructura de Clave Pública (PKI) y desarrollar el concepto de gestión de identidades
- Dominar diferentes métodos de autenticación, generando conocimiento especializado sobre el ecosistema de seguridad informática
- Detallar los ámbitos de seguridad en Cloud, los servicios y herramientas en cada uno de los ámbitos de seguridad
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN, analizando de forma comparativa la seguridad de cada una de ellas



Objetivos específicos

Módulo 1. Seguridad en el diseño y desarrollo de sistemas

- Analizar los elementos más destacados de un Sistema de Información, sus componentes, actividades y ciclo de vida
- Examinar todos los aspectos clave que garantizan la eficiencia en su diseño y desarrollo, centrando la seguridad como uno de los aspectos básicos a tener en cuenta
- Delimitar las principales amenazas de seguridad en el acceso a los datos y redes de un Sistema de Información
- Identificar las implicaciones legales y los procedimientos que hacen seguros los sistemas, con el propósito de salvaguardar todo tipo de información y datos críticos en las empresas

Módulo 2. Arquitecturas y modelos de seguridad de la información

- Diferenciar las características y componentes más importantes implicados en la Arquitectura y Modelos de Seguridad de la Información
- Detallar sus procesos, estructuras y contratos, considerando el tipo de Modelo de Seguridad a implantar
- Evaluar la gestión de riesgos, la administración de recursos, las métricas, los cuadros de mando asociados, y el marco normativo y legislación a aplicar

Módulo 3. Gestión de la seguridad en tecnologías de la información

- Correlacionar los elementos más importantes en torno a la Ciberseguridad o Seguridad de la Información, así como las características que el entorno actual requiere para afrontar y gestionar este ámbito de una manera estructurada
- Dominar el empleo de las técnicas más actuales, considerando todas las dimensiones de la seguridad, sin descuidar ningún aspecto
- Implementar medidas de protección técnicas y diversos procedimientos para evitar posibles peligros, amenazas y ataques sufridos por los sistemas de información de muchas organizaciones

Módulo 4. Análisis de riesgos y entorno de seguridad en tecnología de la información

- Ahondar en los elementos más importantes relacionados con las últimas tendencias en Gestión Inteligente de Riesgos
- Analizar el diseño y la aplicación de nuevas metodologías de gestión de riesgos propias, basadas en el concepto Ágile
- Transformar los riesgo y amenazas en oportunidades, aportando un verdadero valor diferencial frente a la competencia

Módulo 5. Criptografía en tecnología de la información

- Emplear las técnicas más importantes para la protección de la información, a través del estudio de los distintos algoritmos criptográficos
- Manejar las herramientas matemáticas en las que se basan la mayoría de las técnicas y algoritmos
- Examinar la ciencia de la Criptología y su relación con ramas como Criptografía, Criptoanálisis, Esteganografía y Estegoanálisis

Módulo 6. Gestión de identidad y accesos en seguridad de las tecnologías de la información y las comunicaciones

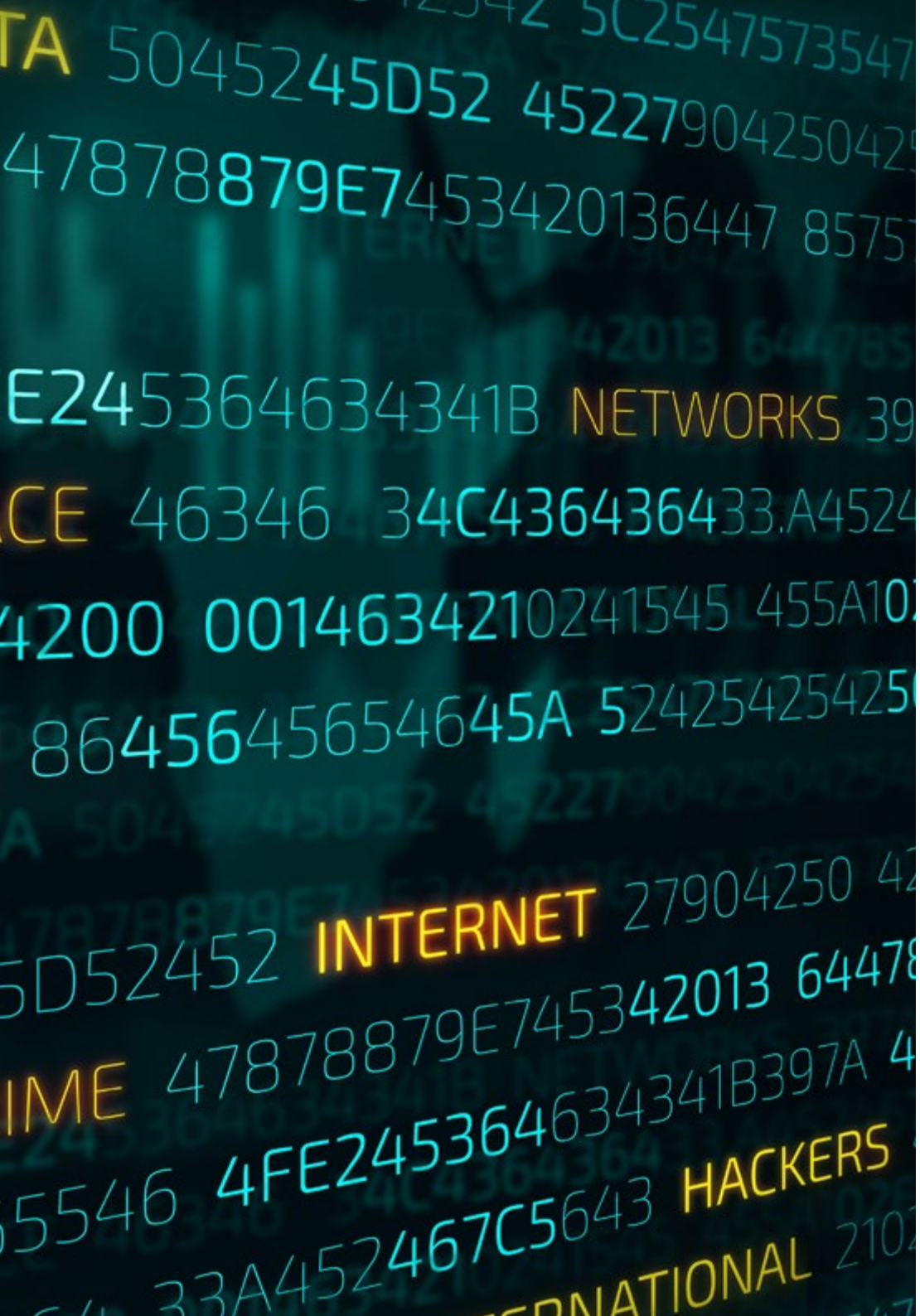
- Valorar la importancia de la confidencialidad, así como la Gestión de la Identidad y Accesos en la Seguridad de las Tecnologías de la Información y las Comunicaciones
- Implementar el análisis de los métodos de protección de la información y sistemas biométricos, considerando el impacto que éstas tienen al momento de la autenticación en las redes sociales, cuentas de correo, dispositivos
- Asegurar que la información confidencial de una compañía no llegue a las personas equivocadas, no autorizadas

Módulo 7. Seguridad en comunicaciones y operación software

- Abordar los elementos más importantes relacionados con el Ecosistema de Seguridad Informática en el contexto de un mundo hiperconectado
- Determinar los riesgos que supone para las compañías no tener un entorno de Seguridad Informática, con el propósito de establecer las bases de un centro de operaciones en materia de ciberseguridad

Módulo 8. Seguridad en entornos de la nube

- Interpretar el modelo de responsabilidad compartida que rige los despliegues en la nube de acceso público, así como los mecanismos de seguridad disponibles
- Delimitar los mecanismos como los procesos a implementar; considerando los servicios y herramientas en cada uno de los ámbitos de seguridad, con el propósito de poner en marcha cualquier proyecto de implantación en la nube



Módulo 9. Seguridad en comunicaciones de dispositivos de Internet de las Cosas (IoT)

- Examinar la la Arquitectura simplificada del Internet de las Cosas (IoT), así como los elementos implicados en la Transmisión de Datos
- Identificar la tecnología de conectividad, la lógica en el intercambio de información y el diseño de un sitio web, considerando la capa de transmisión de datos
- Establecer las mejores opciones de conectividad para afrontar un proyecto, con especial énfasis en tecnologías de transmisión inalámbrica

Módulo 10. Plan de continuidad del negocio asociado a seguridad

- Analizar elementos clave que conforman un Plan de Continuidad asociada seguridad, a través del estudio de las fases del mismo y las prácticas que se deben adoptar para la minimización, o eliminación total de los riesgos
- Dominar como la guía ISO-22301; con el propósito de lograr la integración de todos los elementos dentro de la Gestión de Riesgos global de la compañía

Alcanza tus objetivos y metas profesionales gracias a las competencias que adquirirás egresándote de esta Maestría 100% online"

04

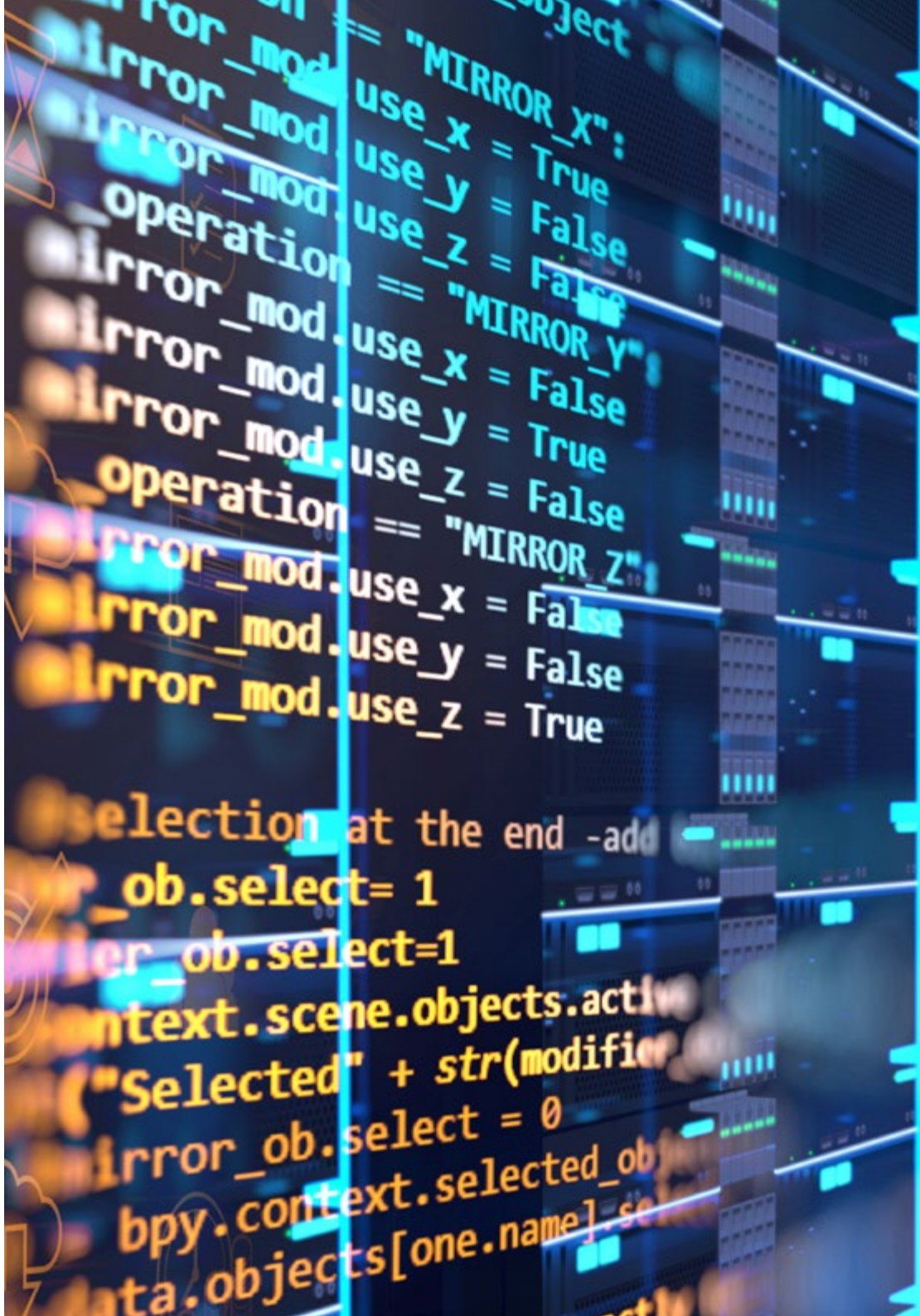
Competencias

Esta Maestría nace con la finalidad de proporcionar al alumno una especialización de alta calidad. Así, tras superar con éxito esta exclusiva titulación, el egresado habrá desarrollado las habilidades y destrezas necesarias para desempeñar un trabajo de primer nivel. Asimismo, obtendrá una visión innovadora y multidisciplinar de su campo laboral. Por ello, este vanguardista programa de TECH representa una oportunidad sin parangón para todo aquel profesional que quiera destacar en su sector y convertirse en un experto.

¿Quieres convertirte en un experto en la detección de ataques cibernéticos avanzados? No dudes más y matricúlate ahora en esta Maestría de TECH"

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
- Diferenciar los riesgos que supone a las compañías no tener un entorno de seguridad informática
- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Desplegar 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



- 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
- Poner en marcha el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en Cloud
- Valorar las diferencias en las implementaciones concretas de diferentes vendedores de Cloud pública
- Determinar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN, a partir de las especificaciones básicas de esas tecnologías

Actualiza tus competencias con la metodología teórico-práctica más eficiente del panorama académico actual, el Relearning de TECH”

05

¿Por qué nuestro programa?

Esta titulación brinda varias oportunidades excepcionales a los alumnos. Por un lado, tendrán en sus manos el conocimiento más especializado y desarrollarán las habilidades técnicas avanzadas para proteger información y datos en el entorno digital actual. Igualmente, serán capaces de detectar y contener amenazas, haciendo un uso competo de los marcos legales y políticos relacionados con esta área en concreto. En definitiva, se trata de una Maestría donde se ahonda en los desafíos contemporáneos y futuras de la ciberseguridad, proporcionado competencias específicas que les permitirán desarrollar una carrera de prestigio.

Desde cualquier dispositivo conectado a Internet, podrás completar el estudio de los 10 módulos que integran esta Maestría 100% online”

01 Orientación 100% laboral

Materiales didácticos actualizados y metodologías de estudio vanguardistas potenciarán al máximo el aprendizaje con TECH. A su vez, cada alumno tendrá ante sí una potente orientación laboral que le permitirá conocer de antemano todas las problemáticas que definen el campo de la Ciberseguridad y cómo darles solución de la manera más avanzada posible.

02 La mejor institución

TECH se ha convertido en un paradigma para la educación digital a escala internacional. La revista Forbes ha reconocido a esta institución académica como la mejor del mundo. Para esta categorización se ha apoyado en su catálogo con más de 10.000 títulos universitarios, sus métodos vanguardistas de aprendizaje y la disponibilidad de facilitar el estudio de modo 100% online.

03 Titulación directa

No hará falta que el estudiante haga una tesina, ni examen final, ni nada más para poder egresar y obtener su título. En TECH, el alumno tendrá una vía directa de titulación.

04 Los mejores recursos pedagógicos 100% online

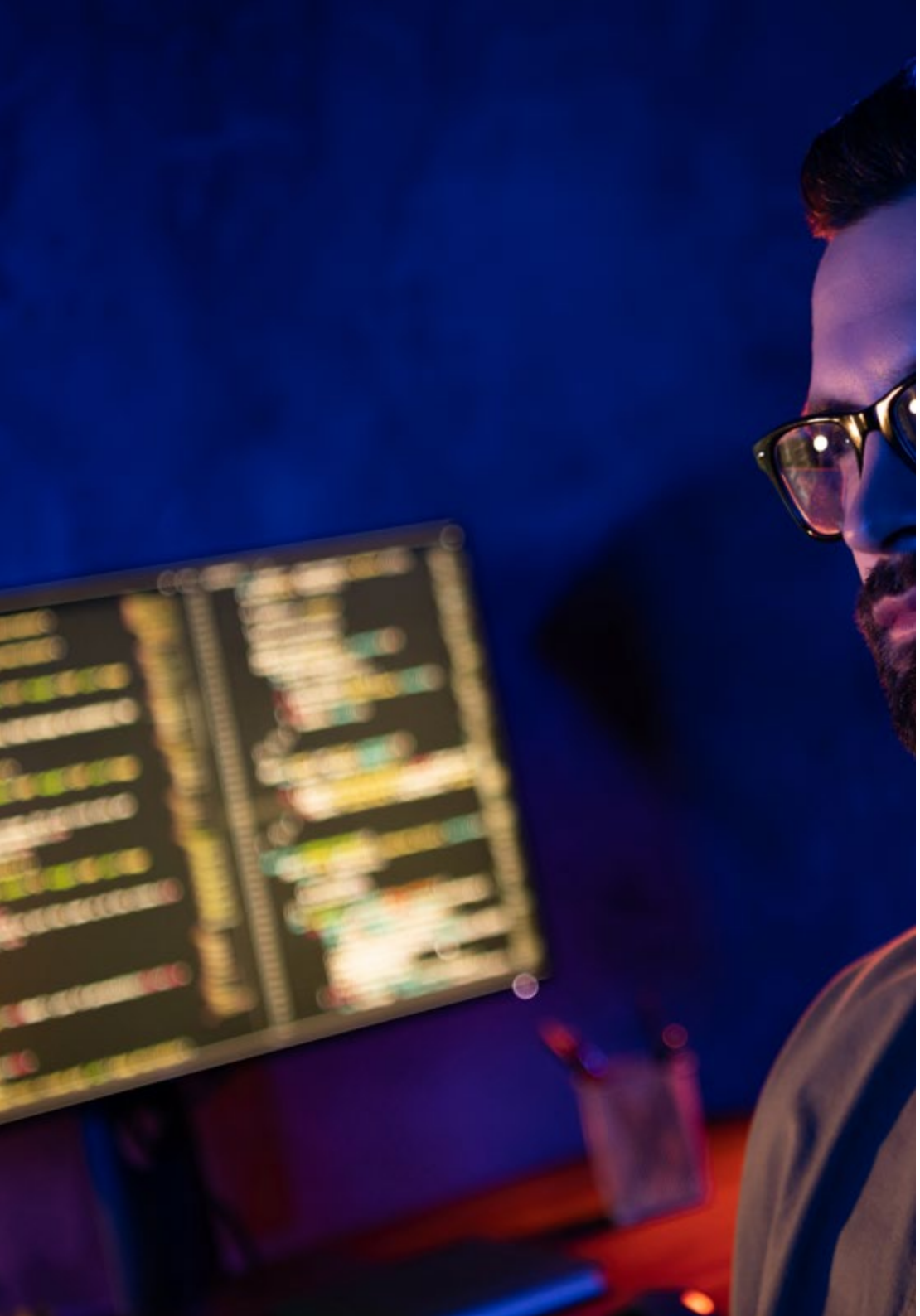
TECH Universidad Tecnológica pone al alcance de los estudiantes de esta Maestría la última metodología educativa en línea, basada en una tecnología internacional de vanguardia, que permite estudiar sin tener que asistir a clase, y sin renunciar a adquirir ninguna competencia indispensable en la ciberseguridad avanzada.

05 Educación adaptada al mundo real

Para que el proceso académico se adapte a las demandas del contexto laboral, TECH se apoya en diversas metodologías de aprendizaje. En el caso de este programa en Seguridad Informática Avanzada, resultan definitorios los casos de estudio de la Escuela de Harvard y el método Relearning. Ambas estrategias didácticas facilitarán al egresado la incorporación inmediata de conceptos y soluciones técnicas basadas en las posibles amenazas digitales del mundo real.

06 Aprender idiomas y obtener su certificado oficial

TECH da la posibilidad, además de obtener la certificación oficial de Inglés en el nivel B2, de seleccionar de forma optativa hasta otros 6 idiomas en los que, si el alumno desea, podrá certificarse.



07 Mejorar tus habilidades directivas

El liderazgo es esencial en materia de Seguridad Informática Avanzada puesto que los profesionales del sector deben pautar la forma en que los directivos y empleados conservan y protegen sus datos. A través de esta Maestría, el alumnado consolidará sus aptitudes para establecer políticas y normativas internas que disminuyan problemas como el robo de contraseñas y la entrada de malewares al ecosistema de datos empresarial.

08 Especialización integral

Los programas de TECH Universidad Tecnológica son diseñados teniendo en cuenta las principales demandas del mercado laboral. Por eso, en esta Maestría se analizan las problemáticas más complejas que enfrenta hoy la seguridad informática y sus potenciales soluciones a partir de la tecnología más avanzada. Con esa especialización integral, el egresado tendrá la oportunidad de poner en práctica todo lo aprendido en los escenarios y retos más diferenciados.

09 Formar parte de una comunidad exclusiva

Para los informáticos, esta titulación de TECH es sinónimo de rigurosidad académica y, al mismo tiempo, de una oportunidad sin precedentes de establecer contactos profesionales. Esto es posible gracias a la gran cantidad de expertos que integran sus claustros y a la diversa comunidad de alumnos de la institución, distribuidos en la mayoría de los países del mundo.

06

Salidas profesionales

La Seguridad Informática Avanzada es un campo que, en los últimos años, se ha convertido en una prioridad para empresas y organizaciones de cualquier índole. Por eso, al completar esta Maestría, los egresados tendrán acceso a las salidas profesionales más diversas. Su completísimo temario académico, les permitirá ahondar en las técnicas más actualizadas de protección de datos, detección de vulnerabilidad y prevención de ataques cibernéticos. Al conseguir una elevada especialización en esas áreas, conseguirán desempeñarse con eficiencia y asumir los retos más imperativos de este contexto laboral.

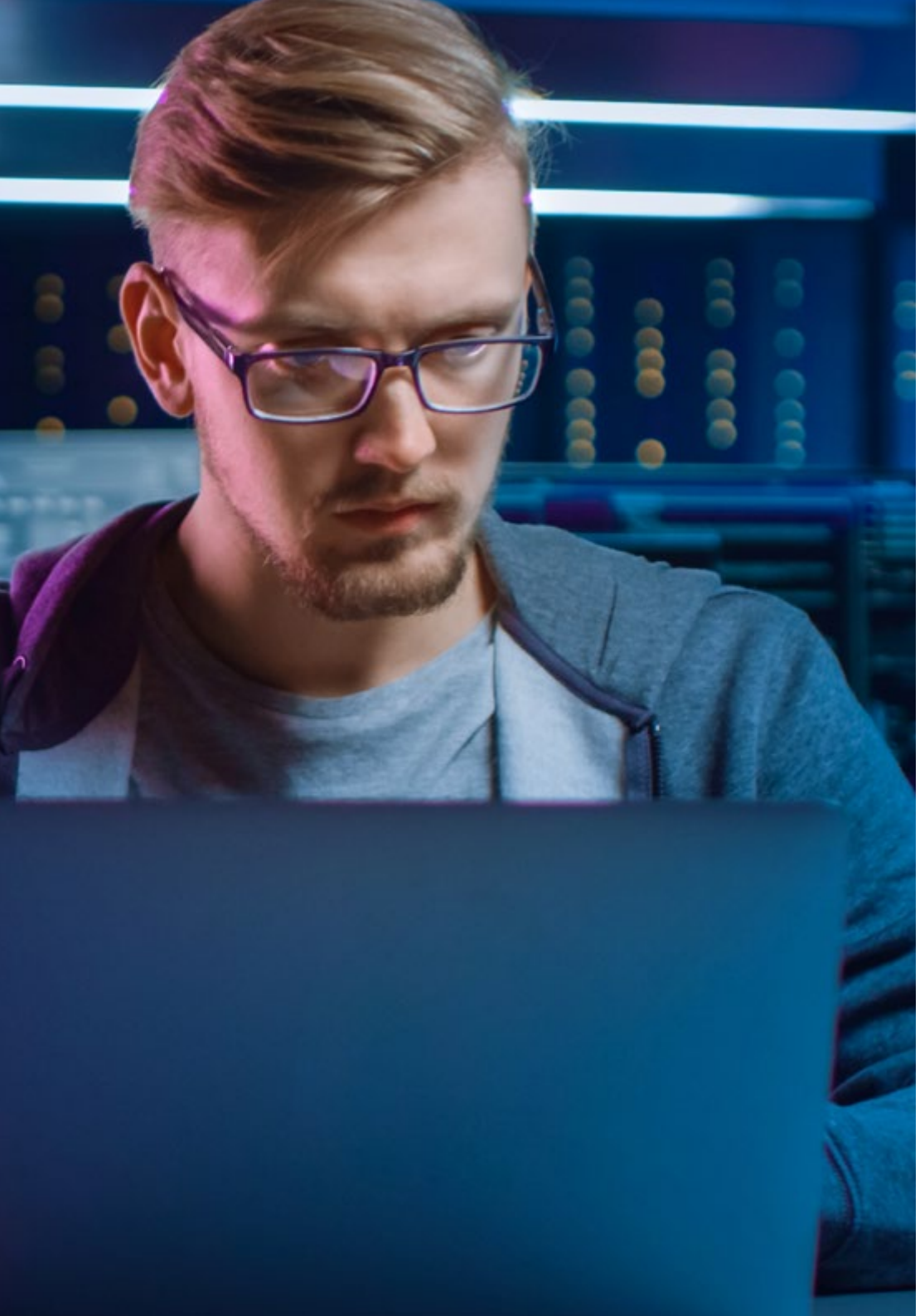
Prepárate para disímiles oportunidades profesionales en el campo de la Ciberseguridad Avanzada a través del estudio de esta Maestría oficial de TECH"

Perfil profesional

Esta Maestría oficial de TECH garantiza a los profesionales de la ciberseguridad el dominio de diferentes herramientas y técnicas avanzadas. De manera general, el temario se afana en convertirlos en grandes expertos en la detección de amenazas digitales y la implementación de mecanismos de contención cada vez más sofisticados. A su vez, les proporciona un cabal recorrido por las principales estrategias de control de la identidad y accesos que disminuirá el riesgo de vulnerabilidades informáticas en su entorno de empleo.

Perfil investigativo

TECH ofrece a su alumnado un programa de estudios vanguardista donde pondrán mantenerse actualizado sobre los avances más destacados en materia de Seguridad Informática. Así, conseguirán desarrollar su capacidad de interpretación del contexto de riesgos e incorporar soluciones basadas en la última evidencia científica. Estas competencias les permitirán asumir roles investigativos como el de forense de ciberseguridad, consiguiendo interpretar a cabalidad del alcance de los ataques e identificando sus fuentes. Con todas esas habilidades en la mano, podrán posicionarse en las posiciones laborales más exhaustivas del momento.



Perfil ocupacional y campo de acción

Tras culminar esta titulación, el alumno dispondrá de todas las aptitudes y destrezas prácticas para desarrollar labores en el campo de la Ciberseguridad con pensamiento crítico y resolutivo. Sus respuestas ante situaciones desafiantes serán resolutivas y basadas en la información científico-técnica más avanzada. Todo ello gracias a la versatilidad de los contenidos ofrecidos en este programa 100% online.

El egresado de TECH en Seguridad Informática Avanzada estará preparado para desempeñar los siguientes puestos de trabajo:

- Analista avanzado de Seguridad Informática
- Administrador Senior de Sistemas y Redes
- Perito/Forense Informático
- Director tecnológico en empresas informáticas
- *Chief Information Security Officer*
- Arquitecto de Ciberseguridad
- Consultor auditor de Seguridad Informática
- Hacker ético

Con tan solo un clic, podrás ampliar tus perspectivas profesionales y alcanzar tus metas de superación en empresas prestigiosas que precisan de los mejores expertos en Ciberseguridad"

07

Idiomas gratuitos

Convencidos de que la formación en idiomas es fundamental en cualquier profesional para lograr una comunicación potente y eficaz, TECH ofrece un itinerario complementario al plan de estudios curricular, en el que el alumno, además de adquirir las competencias en la Maestría, podrá aprender idiomas de un modo sencillo y práctico.

TECH te incluye el estudio de idiomas en la Maestría de forma ilimitada y gratuita”

En el mundo competitivo de hoy, hablar otros idiomas forma parte clave de nuestra cultura moderna. Hoy en día resulta imprescindible disponer de la capacidad de hablar y comprender otros idiomas, además de lograr un certificado oficial que acredite y reconozca nuestra competencia en aquellos que dominemos. De hecho, ya son muchos las escuelas, las universidades y las empresas que sólo aceptan a candidatos que certifican su nivel mediante un certificado oficial en base al Marco Común Europeo de Referencia para las Lenguas (MCER).

El Marco Común Europeo de Referencia para las Lenguas es el máximo sistema oficial de reconocimiento y acreditación del nivel del alumno. Aunque existen otros sistemas de validación, estos proceden de instituciones privadas y, por tanto, no tienen validez oficial. El MCER establece un criterio único para determinar los distintos niveles de dificultad de los cursos y otorga los títulos reconocidos sobre el nivel de idioma que poseemos.

TECH ofrece los únicos cursos intensivos de preparación para la obtención de certificaciones oficiales de nivel de idiomas, basados 100% en el MCER. Los 48 Cursos de Preparación de Nivel idiomático que tiene la Escuela de Idiomas de TECH están desarrollados en base a las últimas tendencias metodológicas de aprendizaje online, el enfoque orientado a la acción y el enfoque de adquisición de compentencia lingüística, con la finalidad de prepararte para los exámenes oficiales de certificación de nivel.

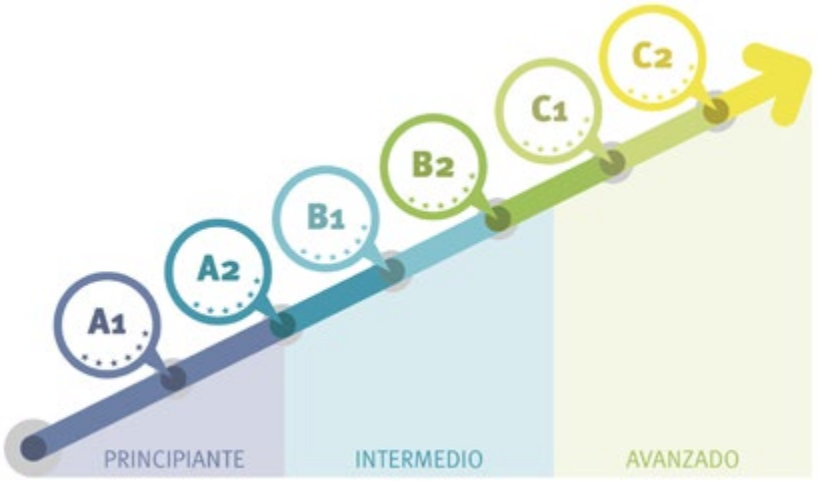
El estudiante aprenderá, mediante actividades en contextos reales, la resolución de situaciones cotidianas de comunicación en entornos simulados de aprendizaje y se enfrentará a simulacros de examen para la preparación de la prueba de certificación de nivel.

"Solo el coste de los Cursos de Preparación de idiomas y los exámenes de certificación, que puedes llegar a hacer gratis, valen más de 3 veces el precio de la Maestría"

48 Cursos de Preparación de Nivel para la certificación oficial de 8 idiomas en los niveles MCRL A1,A2, B1, B2, C1 y C2”

TECH incorpora, como contenido extracurricular al plan de estudios oficial, la posibilidad de que el alumno estudie idiomas, seleccionando aquellos que más le interesen de entre la gran oferta disponible:

- Podrá elegir los Cursos de Preparación de Nivel de los idiomas, y nivel que desee, de entre los disponibles en la Escuela de Idiomas de TECH, mientras estudie la maestría, para poder prepararse el examen de certificación de nivel.
- En cada programa de idiomas tendrá acceso a todos los niveles MCER, desde el nivel A1 hasta el nivel C2.
- Podrá presentarse a un único examen telepresencial de certificación de nivel, con un profesor nativo experto en evaluación lingüística. Si supera el examen, TECH le expedirá un certificado de nivel de idioma.
- Estudiar idiomas NO aumentará el coste del programa. El estudio ilimitado y la certificación única de cualquier idioma, están incluidas en la maestría.



08
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

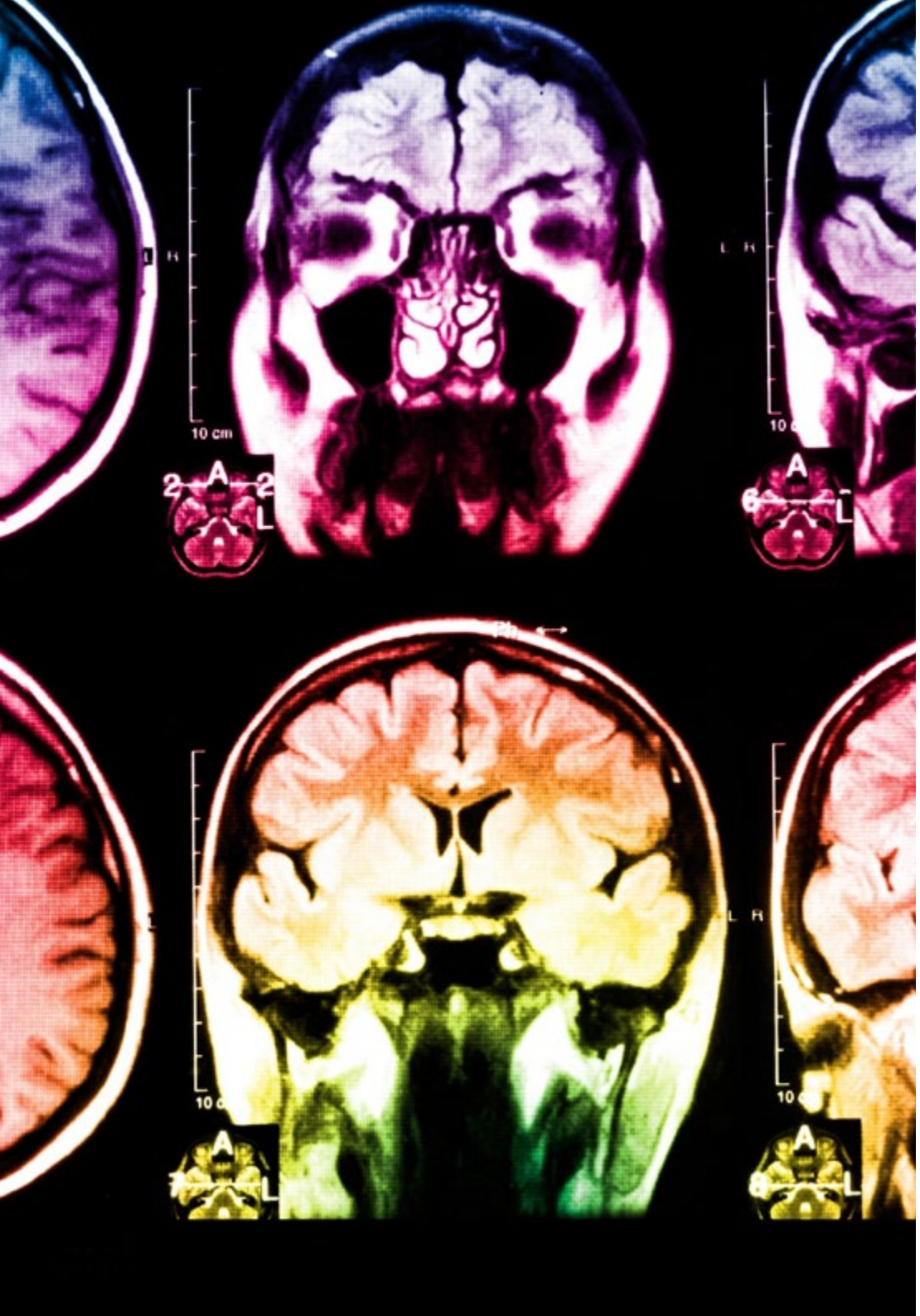
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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.

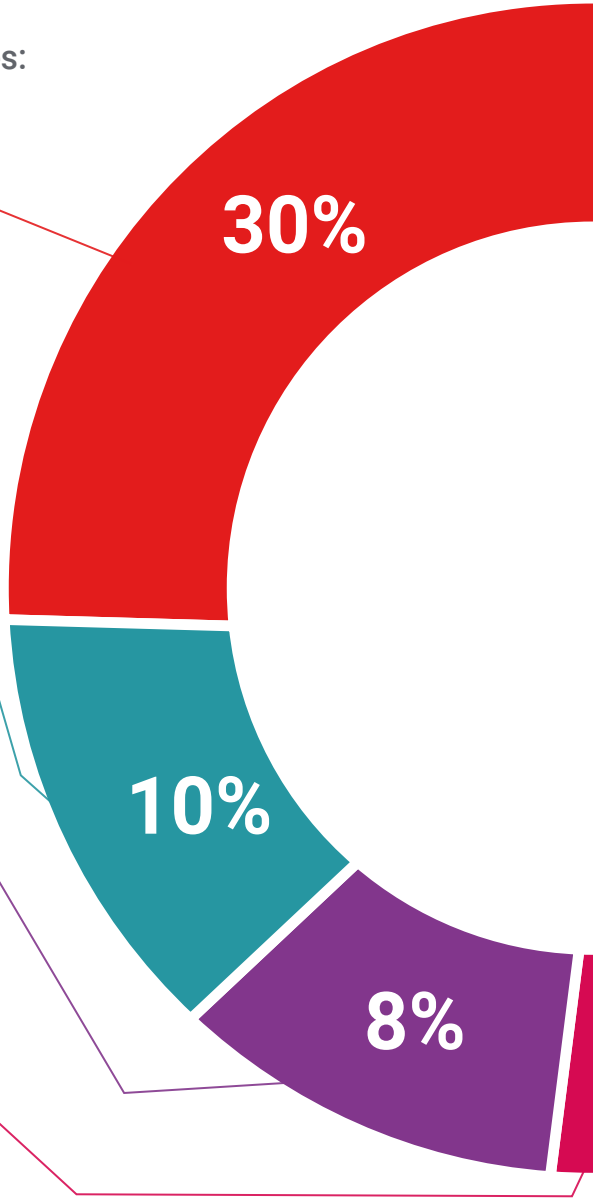
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

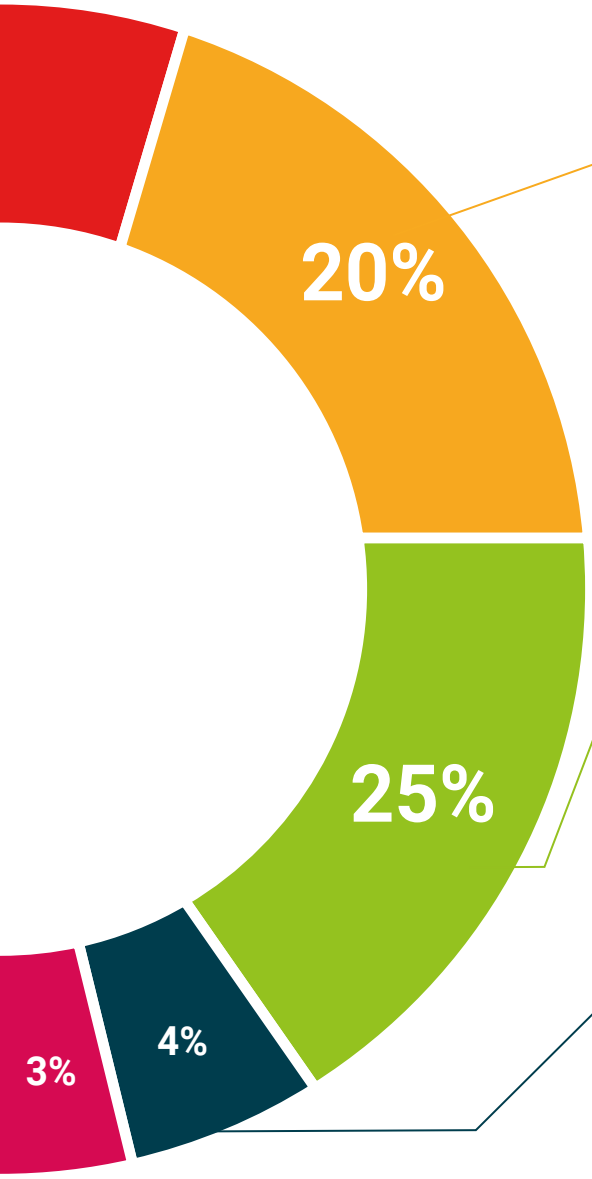
Prácticas de habilidades y competencias

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.

09
Dirección del curso

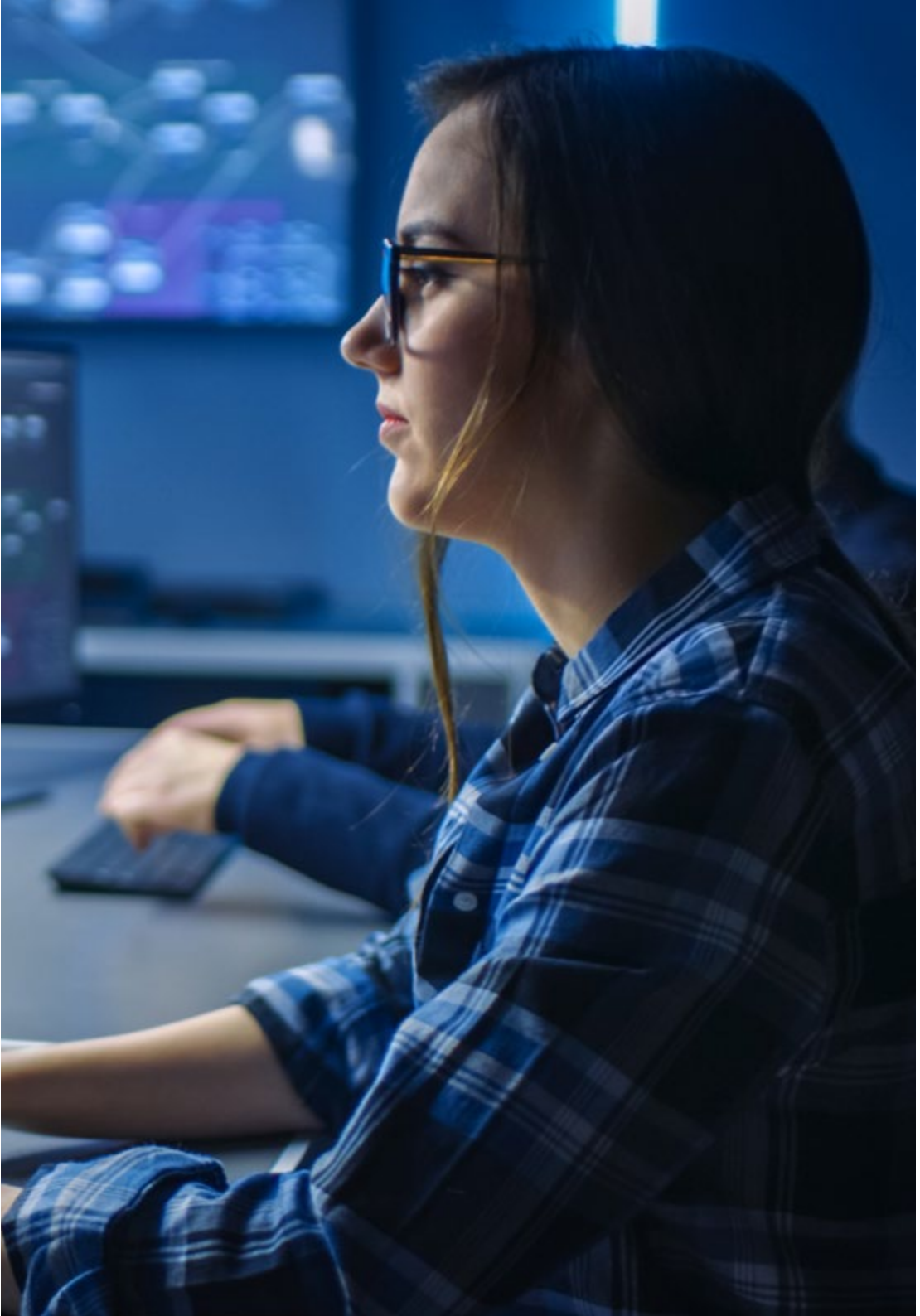
TECH ha conformado para este temario un claustro de primer nivel. Sus miembros son grandes expertos en Ciberseguridad que trabajan, de modo activo, en diferentes empresas ofreciendo competencias avanzadas contra diferentes tipos de ataques. Sus experiencias y las herramientas con que trabajan han sido englobadas en este temario. Así, la titulación se distingue por ser una opción académica de primer nivel, acorde con las demandas y desafíos más retadores del panorama digital actual.

Maneja las herramientas digitales de gestión de la identidad más avanzadas a través de la guía personalizada del mejor claustro docente"

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 Equipo 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 S.L.



Profesores

Dr. Gonzalo Alonso, Félix

- Director general y fundador de Smart REM Solutions
- Responsable de Ingeniería de Riesgos e Innovación en Dynargy
- Gerente y socio fundador del gabinete pericial de tecnologías Risknova
- Máster en Dirección Aseguradora por el Instituto para la Colaboración entre Entidades Aseguradoras
- Grado en Ingeniería Técnica Industrial, especialidad Electrónica Industrial por la Universidad Pontificia de Comillas

Dr. Entrenas, Alejandro

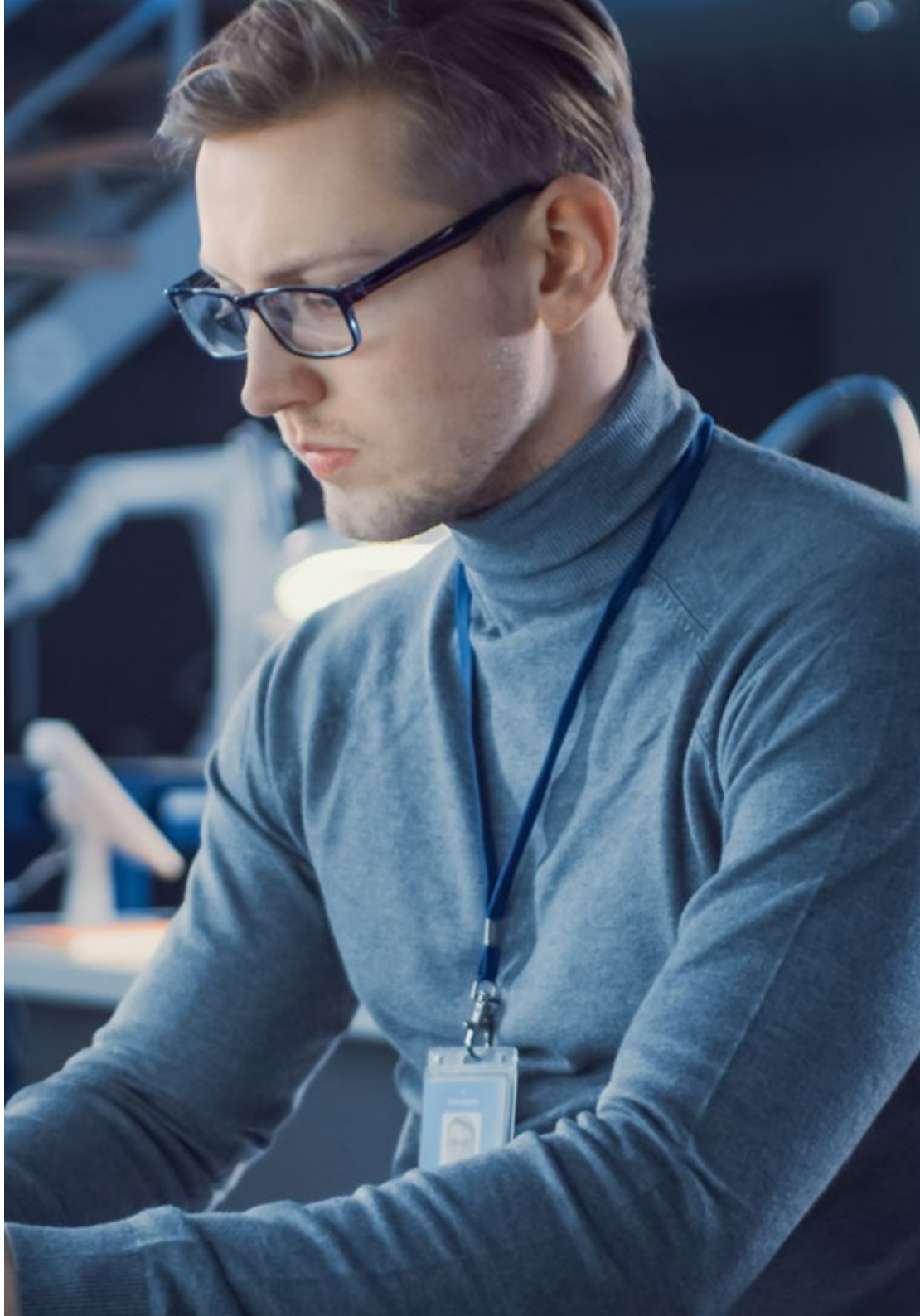
- Jefe de Proyecto en Ciberseguridad. Entelgy Innotec Security
- Consultor de Ciberseguridad. Entelgy
- Analista de Seguridad de la Información. Innovery España
- Analista en Seguridad de la Información. Atos
- Licenciado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Córdoba
- 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

Dr. Gómez Rodríguez, Antonio

- Ingeniero Principal de Soluciones Cloud para Oracle
- Coorganizador de Malaga 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 La Salle
- Postgrado en Tecnologías y Sistemas de Información, Instituto Catalán de Tecnología
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña

D. 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



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). Grupo Pascual
- Cybersecurity Manager. KPMG España
- Consultor de procesos TI / Control y Gestión de Proyectos de Infraestructura. Bankia
- Ingeniero Herramientas Explotación. Dalkia
- Desarrollador aplicaciones. Universidad Politécnica de Madrid
- Desarrollador. Grupo Banco Popular
- Graduada en Ingeniería Informática. Universidad Alfonso X El Sabio
- Ingeniero Técnico en Informática de Gestión. Universidad Politécnica de Madrid
- Certified Data Privacy Solutions Engineer (CDPSE). ISACA

Dr. Nogales Ávila, Javier
- *Cloud and Technology Consultant* en Indra
- *Associate Technology Consultant* en Accenture
- Graduado en Ingeniería de Organización Industrial por la Universidad de Jaén
- MBA en Administración y Dirección de Empresas por *ThePower Business School*

D. Ortega Esteban, Octavio
- Programador de aplicaciones informáticas y desarrollador de web freelance
- *Chief Operating Officer* en *Smallsquid* SL
- Administrador de Ortega y Serrano *e-Commerce*
- Docente en cursos de Certificados de Profesionalidad en la rama de Informática y Comunicaciones
- Docente en cursos de Seguridad Informática
- Licenciado en Psicología por la Universidad Oberta de Catalunya
- Técnico Superior Universitario en Análisis, Diseño y Soluciones del *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

D. Rodrigo Estébanez, Juan Manuel
- 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

10

Requisitos de acceso y proceso de admisión

El proceso de admisión de TECH es el más sencillo de las universidades en línea en todo el país. Podrás comenzar la Maestría sin trámites ni demoras: empieza a preparar la documentación y entrégala más adelante, sin premuras. Lo más importante para TECH es que los procesos administrativos, para ti, sean sencillos y no te ocasionen retrasos, ni incomodidades.

Ayudándote desde el inicio, TECH ofrece el procedimiento de admisión más sencillo y rápido de todas las universidades en línea del país”

Requisitos de acceso

Para poder acceder a los estudios de Maestría en Seguridad Informática Avanzada, será necesario haber cursado una licenciatura o título equivalente, en el área de conocimiento relacionada con Informática, Tecnologías computacionales, Tecnologías web, Ciencias Computacionales, Ingeniería en Sistemas, Ingeniería de Software, Ingeniería en Comunicaciones, Ingeniería en Telemática y Comunicaciones, Ingeniería en Computación, Sistemas Computacionales, Sistemas de Información y Comunicación, etc. En caso de que el alumno no cuente con un título en el área mencionada, deberá acreditar documentalmente que cuenta con un mínimo de 2 años de experiencia en el área. Puede consultar requisitos establecidos en el Reglamento de TECH.

Proceso de admisión

Para TECH es del todo fundamental que, en el inicio de la relación académica, el alumno esté centrado en el proceso de enseñanza, sin demoras ni preocupaciones relacionadas con el trámite administrativo. Por ello, hemos creado un protocolo más sencillo en el que podrás concentrarte, desde el primer momento en tu capacitación, contando con un plazo mucho mayor de tiempo para la entrega de la documentación pertinente.

De esta manera, podrás incorporarte al curso tranquilamente. Algún tiempo más tarde, te informaremos del momento en el que podrás ir enviando los documentos, a través del campus virtual, de manera muy sencilla, cómoda y rápida. Sólo deberás cargarlos y enviarlos, sin traslados ni pérdidas de tiempo.

Una vez que llegue el momento podrás contar con nuestro soporte, si te hace falta. Todos los documentos que nos facilites deberán ser rigurosamente ciertos y estar en vigor en el momento en que los envías.

En cada caso, los documentos que debes tener listos para cargar en el campus virtual son:

Estudiantes con estudios universitarios realizados en México

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada de la Clave Única de Registro de Población (CURP)
- Copia digitalizada de Certificado de Estudios Totales de Licenciatura legalizado
- Copia digitalizada del título legalizado

En caso de haber estudiado la licenciatura fuera de méxico, consulta con tu asesor académico. Se requerirá documentación adicional en casos especiales, como inscripciones a la maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Estudiantes con estudios universitarios realizados fuera de México

Deberán subir al Campus Virtual, escaneados con calidad suficiente para su lectura, los siguientes documentos:

- Copia digitalizada del documento que ampare la identidad legal del alumno: acta de nacimiento, carta de naturalización, acta de reconocimiento, acta de adopción, Cédula de Identificación Personal o Documento Nacional de Identidad, Pasaporte, Certificado Consular o, en su caso, Documento que demuestre el estado de refugiado
- Copia digitalizada del Título, Diploma o Grado Académico oficiales de Licenciatura que ampare los estudios realizados en el extranjero
- Copia digitalizada del Certificado de Estudios de Licenciatura. En el que aparezcan las asignaturas con las calificaciones de los estudios cursados, que describan las unidades de aprendizaje, periodos en que se cursaron y calificaciones obtenidas

Se requerirá documentación adicional en casos especiales como inscripciones a maestría como opción de titulación o que no cuenten con el perfil académico que el plan de estudios requiera. Tendrás un máximo de 2 meses para cargar todos estos documentos en el campus virtual.

Es del todo necesario que atestigües que todos los documentos que nos facilitas son verdaderos y mantienen su vigencia en el momento en que los envías.

11

Titulación

Este programa permite alcanzar la titulación de Maestría en Seguridad Informática Avanzada obteniendo un título universitario válido por la Secretaría de Educación Pública, y optativamente, la Cédula Profesional de la Dirección General de Profesiones.

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

Este programa te permite alcanzar el grado de **Maestría en Seguridad Informática Avanzada**, obteniendo un reconocimiento universitario oficial válido tanto en tu país como de modo internacional.

Los títulos de la Universidad TECH están reconocidos por la Secretaría de Educación Pública (SEP). Este plan de estudios se encuentra incorporado al Sistema Educativo Nacional, con fecha 06 JULIO de 2023 y número de acuerdo de Registro de Validez Oficial de Estudios (RVOE): 20231900.

Puedes consultar la validez de este programa en el acuerdo de Registro de Validez Oficial de Estudios: **RVOE Maestría en Seguridad Informática Avanzada.**

Para más información sobre qué es el RVOE puedes consultar *aquí:*

RVOE
EDUCACIÓN SUPERIOR

Titulación: **Maestría en Innovación de Seguridad Informática Avanzada**

Nº de RVOE: **20231900**

Fecha de RVOE: **06/07/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Para recibir el presente título no será necesario realizar ningún trámite.
TECH Universidad realizará todas las gestiones oportunas ante las diferentes administraciones públicas en su nombre, para hacerle llegar a su domicilio*:

- Título de la Maestría
- Certificado total de estudios
- Cédula Profesional

Si requiere que cualquiera de estos documentos le lleguen apostillados a su domicilio, póngase en contacto con su asesor académico.
TECH Universidad se hará cargo de todos los trámites.


tech universidad tecnológica

Otorga el presente

GRADO

a

D/Dña _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MAESTRÍA

en

Seguridad Informática Avanzada

Con Reconocimiento de Validez Oficial de Estudios de la Secretaría de Educación Pública, según Acuerdo Nº. 20231900 en virtud de que demostró cumplir con los estudios correspondientes y aprobó conforme titulación automática el 06 Julio 2023.

A 06 de julio de 2023

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos

*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

Maestría
Seguridad Informática Avanzada

Nº de RVOE: **20231900**

Fecha de RVOE: **06/07/2023**

Modalidad: **100% en línea**

Duración: **20 meses**

Maestría
Seguridad Informática Avanzada

Nº de RVOE: 20231900

RVOE
EDUCACIÓN SUPERIOR

tech universidad tecnológica