Grand Master

Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Aval/Membresía

ebea

Economics, Business
and Enterprise Association

tech global university

tech global university

Grand Master
Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

- Modalidad: **online**
- Duración: **2 años**
- Titulación: **TECH Global University**
- Acreditación: **120 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

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

Índice

01

Presentación del programa

La ciberseguridad es hoy un eje esencial para proteger a personas y organizaciones frente al aumento de amenazas digitales. Así, esta área abarca la protección de sistemas y datos sensibles, así como la supervisión e implementación de estrategias que reduzcan riesgos y fortalezcan la respuesta ante incidentes. Por lo tanto, el Director de Ciberseguridad lidera funciones críticas: establecer políticas, gestionar riesgos tecnológicos y coordinar equipos. En este contexto, TECH lanza un completo programa universitario, enfocado en preparar a profesionales capaces de enfrentar los retos de la transformación digital. Este programa profundiza en la detección de vulnerabilidades y en la adopción de soluciones, a través de una metodología 100% online que garantiza la resiliencia y continuidad operativa dentro de cualquier entidad.

Un programa exhaustivo y 100% online, exclusivo de TECH y con una perspectiva internacional respaldada por nuestra afiliación con la Economics, Business and Enterprise Association"

La Alta Dirección de Ciberseguridad ha sido fundamental para garantizar la estabilidad y continuidad de las organizaciones en un mundo digitalizado y altamente interconectado. Así, a través de la implementación de estrategias de seguridad robustas y la adopción de tecnologías avanzadas, se han mitigado riesgos y prevenidos ataques con consecuencias catastróficas. Siendo así, en sectores críticos como la banca, la salud y las infraestructuras públicas, la seguridad se ha fortalecido gracias a la gobernanza y el cumplimiento normativo, impulsados por líderes especializados en esta área.

Esta disciplina ha permitido a las organizaciones establecer entornos de trabajo digitales más seguros, fortaleciendo así la confianza de clientes, socios y usuarios. En consecuencia, los resultados exitosos han generado un ahorro significativo de millones de dólares en pérdidas económicas potenciales, al mismo tiempo que han promovido una cultura organizacional en la que la seguridad es una prioridad compartida. Además, ha demostrado ser esencial para proteger la innovación, la reputación y la sostenibilidad de las organizaciones en un panorama en constante evolución.

En este sentido, el Grand Master de TECH está diseñado para especializar a informáticos en el liderazgo de estrategias de seguridad efectivas. Por ello, a lo largo del programa, el profesional se enfocará en el desarrollo de habilidades directivas y una visión empresarial estratégica. Además, tendrá acceso a una especialización de vanguardia que lo prepara para destacarse en una carrera altamente demandada en el mercado global. En esta misma línea, el plan de estudios contempla una cuidada selección de *Masterclasses* de alto nivel, impartidas por reconocidos Directores Invitados Internacionales.

Gracias a la membresía en la **Economics, Business and Enterprise Association (EBEA)**, el egresado accederá a publicaciones, recursos digitales y seminarios online para mantenerse actualizado. Asimismo, podrá participar en conferencias anuales y optar al reconocimiento profesional EBEA, impulsando su crecimiento y excelencia profesional en economía y negocios.

Este **Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** contiene el programa universitario más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en informática
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que están concebidos recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)
- Las lecciones teóricas, preguntas al experto, foros de discusión de temas controvertidos y trabajos de reflexión individual
- La disponibilidad de acceso a los contenidos desde cualquier dispositivo fijo o portátil con conexión a internet

Las Masterclasses magistrales te brindarán una oportunidad única de aprendizaje directo con figuras de gran prestigio en el ámbito profesional, quienes comparten sus estrategias y metodologías"

Conviértete en el protector de las infraestructuras tecnológicas con el método Relearning que se adapta a tu ritmo de aprendizaje”

Desarrolla las habilidades necesarias para estar a la altura de los desafíos del futuro sin descuidar tus actividades actuales.

Se parte de la universidad digital más grande del mundo y especialízate desde cualquier lugar del mundo.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la Informática, que vierten en este programa la experiencia de su trabajo, además de reconocidos especialistas de sociedades de referencia y universidades de prestigio.

Su contenido multimedia, elaborado con la última tecnología educativa, permitirá al profesional un aprendizaje situado y contextualizado, es decir, un entorno simulado que proporcionará un estudio inmersivo programado para entrenarse ante situaciones reales.

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

02

¿Por qué estudiar en TECH?

TECH es la mayor Universidad digital del mundo. Con un impresionante catálogo de más de 14.000 programas universitarios, disponibles en 11 idiomas, se posiciona como líder en empleabilidad, con una tasa de inserción laboral del 99%. Además, cuenta con un enorme claustro de más de 6.000 profesores de máximo prestigio internacional.

Estudia en la mayor universidad digital del mundo y asegura tu éxito profesional. El futuro empieza en TECH”

La mejor universidad online del mundo según FORBES

La prestigiosa revista Forbes, especializada en negocios y finanzas, ha destacado a TECH como «la mejor universidad online del mundo». Así lo han hecho constar recientemente en un artículo de su edición digital en el que se hacen eco del caso de éxito de esta institución, «gracias a la oferta académica que ofrece, la selección de su personal docente, y un método de aprendizaje innovador orientado a formar a los profesionales del futuro».

El mejor claustro docente top internacional

El claustro docente de TECH está integrado por más de 6.000 profesores de máximo prestigio internacional. Catedráticos, investigadores y altos ejecutivos de multinacionales, entre los cuales se destacan Isaiah Covington, entrenador de rendimiento de los Boston Celtics; Magda Romanska, investigadora principal de MetaLAB de Harvard; Ignacio Wistuba, presidente del departamento de patología molecular traslacional del MD Anderson Cancer Center; o D.W Pine, director creativo de la revista TIME, entre otros.

La mayor universidad digital del mundo

TECH es la mayor universidad digital del mundo. Somos la mayor institución educativa, con el mejor y más amplio catálogo educativo digital, cien por cien online y abarcando la gran mayoría de áreas de conocimiento. Ofrecemos el mayor número de titulaciones propias, titulaciones oficiales de posgrado y de grado universitario del mundo. En total, más de 14.000 títulos universitarios, en diez idiomas distintos, que nos convierten en la mayor institución educativa del mundo.

Los planes de estudio más completos del panorama universitario

TECH ofrece los planes de estudio más completos del panorama universitario, con temarios que abarcan conceptos fundamentales y, al mismo tiempo, los principales avances científicos en sus áreas científicas específicas. Asimismo, estos programas son actualizados continuamente para garantizar al alumnado la vanguardia académica y las competencias profesionales más demandadas. De esta forma, los títulos de la universidad proporcionan a sus egresados una significativa ventaja para impulsar sus carreras hacia el éxito.

Un método de aprendizaje único

TECH es la primera universidad que emplea el *Relearning* en todas sus titulaciones. Se trata de la mejor metodología de aprendizaje online, acreditada con certificaciones internacionales de calidad docente, dispuestas por agencias educativas de prestigio. Además, este disruptivo modelo académico se complementa con el "Método del Caso", configurando así una estrategia de docencia online única. También en ella se implementan recursos didácticos innovadores entre los que destacan vídeos en detalle, infografías y resúmenes interactivos.

La universidad online oficial de la NBA

TECH es la universidad online oficial de la NBA. Gracias a un acuerdo con la mayor liga de baloncesto, ofrece a sus alumnos programas universitarios exclusivos, así como una gran variedad de recursos educativos centrados en el negocio de la liga y otras áreas de la industria del deporte. Cada programa tiene un currículo de diseño único y cuenta con oradores invitados de excepción: profesionales con una distinguida trayectoria deportiva que ofrecerán su experiencia en los temas más relevantes.

Líderes en empleabilidad

TECH ha conseguido convertirse en la universidad líder en empleabilidad. El 99% de sus alumnos obtienen trabajo en el campo académico que ha estudiado, antes de completar un año luego de finalizar cualquiera de los programas de la universidad. Una cifra similar consigue mejorar su carrera profesional de forma inmediata. Todo ello gracias a una metodología de estudio que basa su eficacia en la adquisición de competencias prácticas, totalmente necesarias para el desarrollo profesional.

Google Partner Premier

El gigante tecnológico norteamericano ha otorgado a TECH la insignia Google Partner Premier. Este galardón, solo al alcance del 3% de las empresas del mundo, pone en valor la experiencia eficaz, flexible y adaptada que esta universidad proporciona al alumno. El reconocimiento no solo acredita el máximo rigor, rendimiento e inversión en las infraestructuras digitales de TECH, sino que también sitúa a esta universidad como una de las compañías tecnológicas más punteras del mundo.

La universidad mejor valorada por sus alumnos

Los alumnos han posicionado a TECH como la universidad mejor valorada del mundo en los principales portales de opinión, destacando su calificación más alta de 4,9 sobre 5, obtenida a partir de más de 1.000 reseñas. Estos resultados consolidan a TECH como la institución universitaria de referencia a nivel internacional, reflejando la excelencia y el impacto positivo de su modelo educativo.

03

Plan de estudios

Esta oportunidad académica está diseñada para especializar a líderes estratégicos capaces de gestionar la seguridad de la información en organizaciones globales. En ese sentido, a través de un enfoque integral y actualizado, el programa abarca áreas clave como la gobernanza de la ciberseguridad y la gestión de riesgos. De este modo, los informáticos desarrollarán habilidades directivas para liderar equipos de alto rendimiento e implementar políticas de seguridad. Además, mientras adquieren conocimientos sobre las últimas tendencias y tecnologías emergentes, los egresados aprenderán a enfrentar los retos del entorno digital y a liderar la seguridad en el futuro.

TECH te prepara para ser el estratega que previene, detecta y mitiga Ciberamenazas de todo el entorno empresarial global”

Módulo 1. Ciberinteligencia y ciberseguridad

1.1. Ciberinteligencia
- 1.1.1. Ciberinteligencia
  - 1.1.1.1. La inteligencia
    - 1.1.1.1.1. Ciclo de inteligencia
  - 1.1.1.2. Ciberinteligencia
  - 1.1.1.3. Ciberinteligencia y ciberseguridad
- 1.1.2. El analista de inteligencia
  - 1.1.2.1. El rol del analista de inteligencia
  - 1.1.2.2. Los sesgos del analista de inteligencia en la actividad evaluativa

1.2. Ciberseguridad
- 1.2.1. Las capas de seguridad
- 1.2.2. Identificación de las ciberamenazas
  - 1.2.2.1. Amenazas externas
  - 1.2.2.2. Amenazas internas
- 1.2.3. Acciones adversas
  - 1.2.3.1. Ingeniería social
  - 1.2.3.2. Métodos comúnmente usados

1.3. Técnicas y herramientas de inteligencias
- 1.3.1. OSINT
- 1.3.2. SOCMINT
- 1.3.3. HUMIT
- 1.3.4. Distribuciones de Linux y herramientas
- 1.3.5. OWISAM
- 1.3.6. OWISAP
- 1.3.7. PTES
- 1.3.8. OSSTM

1.4. Metodologías de evaluación
- 1.4.1. El análisis de inteligencia
- 1.4.2. Técnicas de organización de la información adquirida
- 1.4.3. Fiabilidad y credibilidad de las fuentes de información
- 1.4.4. Metodologías de análisis
- 1.4.5. Presentación de los resultados de la inteligencia

1.5. Auditorías y documentación
- 1.5.1. La auditoría en seguridad informática
- 1.5.2. Documentación y permisos para auditoría
- 1.5.3. Tipos de auditoría
- 1.5.4. Entregables
  - 1.5.4.1. Informe técnico
  - 1.5.4.2. Informe ejecutivo

1.6. Anonimato en la red
- 1.6.1. Uso de anonimato
- 1.6.2. Técnicas de anonimato (Proxy, VPN)
- 1.6.3. Redes TOR, Freenet e IP2

1.7. Amenazas y tipos de seguridad
- 1.7.1. Tipos de amenazas
- 1.7.2. Seguridad física
- 1.7.3. Seguridad en redes
- 1.7.4. Seguridad lógica
- 1.7.5. Seguridad en aplicaciones web
- 1.7.6. Seguridad en dispositivos móviles

1.8. Normativa y *compliance*
- 1.8.1. RGPD
- 1.8.2. La estrategia nacional de ciberseguridad 2019
- 1.8.3. Familia ISO 27000
- 1.8.4. Marco de ciberseguridad NIST
- 1.8.5. PIC
- 1.8.6. ISO 27032
- 1.8.7. Normativas *cloud*
- 1.8.8. SOX
- 1.8.9. PCI

1.9. Análisis de riesgos y métricas
- 1.9.1. Alcance de riesgos
- 1.9.2. Los activos
- 1.9.3. Las amenazas
- 1.9.4. Las vulnerabilidades
- 1.9.5. Evaluación del riesgo
- 1.9.6. Tratamiento del riesgo

1.10. Organismos importantes en materia de ciberseguridad
- 1.10.1. NIST
- 1.10.2. ENISA
- 1.10.3. INCIBE
- 1.10.4. OEA
- 1.10.5. UNASUR - PROSUR

Módulo 2. Seguridad en Host

2.1. Copias de seguridad
- 2.1.1. Estrategias para las copias de seguridad
- 2.1.2. Herramientas para Windows
- 2.1.3. Herramientas para Linux
- 2.1.4. Herramientas para MacOS

2.2. Antivirus de usuario
- 2.2.1. Tipos de antivirus
- 2.2.2. Antivirus para Windows
- 2.2.3. Antivirus para Linux
- 2.2.4. Antivirus para MacOS
- 2.2.5. Antivirus para smartphones

2.3. Detectores de intrusos - HIDS
- 2.3.1. Métodos de detección de intrusos
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Firewall local
- 2.4.1. Firewalls para Windows
- 2.4.2. Firewalls para Linux
- 2.4.3. Firewalls para MacOS

2.5. Gestores de contraseñas
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Detectores de *phishing*
- 2.6.1. Detección del *phishing* de forma manual
- 2.6.2. Herramientas *antiphishing*

2.7. *Spyware*
- 2.7.1. Mecanismos de evitación
- 2.7.2. Herramientas *antispyware*

2.8. Rastreadores
- 2.8.1. Medidas para proteger el sistema
- 2.8.2. Herramientas anti-rastreadores

2.9. EDR- *End Point Detection and Response*
- 2.9.1. Comportamiento del Sistema EDR
- 2.9.2. Diferencias entre EDR y antivirus
- 2.9.3. El futuro de los sistemas EDR

2.10. Control sobre la instalación de software
- 2.10.1. Repositorios y tiendas de software
- 2.10.2. Listas de software permitido o prohibido
- 2.10.3. Criterios de actualizaciones
- 2.10.4. Privilegios para instalar software

Módulo 3. Seguridad en red (perimetral)

3.1. Sistemas de detección y prevención de amenazas
- 3.1.1. Marco general de los incidentes de seguridad
- 3.1.2. Sistemas de defensa actuales: *Defense in Depth* y SOC
- 3.1.3. Arquitecturas de red actuales
- 3.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 3.1.4.1. Sistemas basados en red
  - 3.1.4.2. Sistemas basados en *host*
  - 3.1.4.3. Sistemas centralizados
- 3.1.5. Comunicación y detección de instancias/hosts, contenedores y serverless

3.2. Firewall
- 3.2.1. Tipos de firewalls
- 3.2.2. Ataques y mitigación
- 3.2.3. Firewalls comunes en kernel Linux
  - 3.2.3.1. UFW
  - 3.2.3.2. *Nftables* e *iptables*
  - 3.2.3.3. Firewalld
- 3.2.4. Sistemas de detección basados en logs del sistema
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts y DenyHosts
  - 3.2.4.3. Fai2ban

3.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 3.3.1. Ataques sobre IDS/IPS
- 3.3.2. Sistemas de IDS/IPS
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. Firewalls de siguiente generación (NGFW)
- 3.4.1. Diferencias entre NGFW y firewall tradicional
- 3.4.2. Capacidades principales
- 3.4.3. Soluciones comerciales
- 3.4.4. Firewalls para servicios de *cloud*
  - 3.4.4.1. Arquitectura Cloud VPC
  - 3.4.4.2. Cloud ACLs
  - 3.4.4.3. Security Group

3.5. *Proxy*
- 3.5.1. Tipos de *proxy*
- 3.5.2. Uso de *proxy*. Ventajas e inconvenientes

3.6. Motores de antivirus
- 3.6.1. Contexto general del malware e IOCs
- 3.6.2. Problemas de los motores de antivirus

3.7. Sistemas de protección de correo
- 3.7.1. Antispam
  - 3.7.1.1. Listas blancas y negras
  - 3.7.1.2. Filtros bayesianos
- 3.7.2. Mail Gateway (MGW)

3.8. SIEM
- 3.8.1. Componentes y arquitectura
- 3.8.2. Reglas de correlación y casos de uso
- 3.8.3. Retos actuales de los sistemas SIEM

3.9. SOAR
- 3.9.1. SOAR y SIEM: enemigos o aliados
- 3.9.2. El futuro de los sistemas SOAR

3.10. Otros sistemas basados en red
- 3.10.1. WAF
- 3.10.2. NAC
- 3.10.3. HoneyPots y HoneyNets
- 3.10.4. CASB

Módulo 4. Seguridad en smartphones

4.1. El mundo del dispositivo móvil
- 4.1.1. Tipos de plataformas móviles
- 4.1.2. Dispositivos Ios
- 4.1.3. Dispositivos Android

4.2. Gestión de la seguridad móvil
- 4.2.1. Proyecto de seguridad móvil OWASP
  - 4.2.1.1. Top 10 vulnerabilidades
- 4.2.2. Comunicaciones, redes y modos de conexión

4.3. El dispositivo móvil en el entorno empresarial
- 4.3.1. Riesgos
- 4.3.2. Políticas de seguridad
- 4.3.3. Monitorización de dispositivos
- 4.3.4. Gestión de dispositivos móviles (MDM)

4.4. Privacidad del usuario y seguridad de los datos
- 4.4.1. Estados de la información
- 4.4.2. Protección y confidencialidad de los datos
  - 4.4.2.1. Permisos
  - 4.4.2.2. Encriptación
- 4.4.3. Almacenamiento seguro de los datos
  - 4.4.3.1. Almacenamiento seguro en iOS
  - 4.4.3.2. Almacenamiento seguro en Android
- 4.4.4. Buenas prácticas en el desarrollo de aplicaciones

4.5. Vulnerabilidades y vectores de ataque
- 4.5.1. Vulnerabilidades
- 4.5.2. Vectores de ataque
  - 4.5.2.1. Malware
  - 4.5.2.2. Exfiltración de datos
  - 4.5.2.3. Manipulación de los datos

4.6. Principales amenazas
- 4.6.1. Usuario no forzado
- 4.6.2. Malware
  - 4.6.2.1. Tipos de malware
- 4.6.3. Ingeniería social
- 4.6.4. Fuga de datos
- 4.6.5. Robo de información
- 4.6.6. Redes Wi-Fi no seguras
- 4.6.7. Software desactualizado
- 4.6.8. Aplicaciones maliciosas
- 4.6.9. Contraseñas poco seguras
- 4.6.10. Configuración débil o inexistente de seguridad
- 4.6.11. Acceso físico
- 4.6.12. Pérdida o robo del dispositivo
- 4.6.13. Suplantación de identidad (integridad)
- 4.6.14. Criptografía débil o rota
- 4.6.15. Denegación de servicio (DoS)

4.7. Principales ataques
- 4.7.1. Ataques de *phishing*
- 4.7.2. Ataques relacionados con los modos de comunicación
- 4.7.3. Ataques de *smishing*
- 4.7.4. Ataques de *criptojacking*
- 4.7.5. *Man in The Middle*

4.8. *Hacking*
- 4.8.1. *Rooting* y *jailbreaking*
- 4.8.2. Anatomía de un ataque móvil
  - 4.8.2.1. Propagación de la amenaza
  - 4.8.2.2. Instalación de *malware* en el dispositivo
  - 4.8.2.3. Persistencia
  - 4.8.2.4. Ejecución del *payload* y extracción de la información
- 4.8.3. *Hacking* en dispositivos iOS: mecanismos y herramientas
- 4.8.4. *Hacking* en dispositivos Android: mecanismos y herramientas

4.9. Pruebas de penetración
- 4.9.1. iOS *PenTesting*
- 4.9.2. Android *PenTesting*
- 4.9.3. Herramientas

4.10. Protección y seguridad
- 4.10.1. Configuración de seguridad
  - 4.10.1.1. En dispositivos iOS
  - 4.10.1.2. En dispositivos Android
- 4.10.2. Medidas de seguridad
- 4.10.3. Herramientas de protección

Módulo 5. Seguridad en IoT

5.1. Dispositivos
- 5.1.1. Tipos de dispositivos
- 5.1.2. Arquitecturas estandarizadas
  - 5.1.2.1. ONEM2M
  - 5.1.2.2. IoTWF
- 5.1.3. Protocolos de aplicación
- 5.1.4. Tecnologías de conectividad

5.2. Dispositivos IoT. Áreas de aplicación
- 5.2.1. *SmartHome*
- 5.2.2. *SmartCity*
- 5.2.3. Transportes
- 5.2.4. *Wearables*
- 5.2.5. Sector salud
- 5.2.6. IioT

5.3. Protocolos de comunicación
- 5.3.1. MQTT
- 5.3.2. LWM2M
- 5.3.3. OMA-DM
- 5.3.4. TR-069

5.4. *SmartHome*
- 5.4.1. Domótica
- 5.4.2. Redes
- 5.4.3. Electrodomésticos
- 5.4.4. Vigilancia y seguridad

5.5. *SmartCity*
- 5.5.1. Iluminación
- 5.5.2. Meteorología
- 5.5.3. Seguridad

5.6. Transportes
- 5.6.1. Localización
- 5.6.2. Realización de pagos y obtención de servicios
- 5.6.3. Conectividad

5.7. *Wearables*
- 5.7.1. Ropa inteligente
- 5.7.2. Joyas inteligentes
- 5.7.3. Relojes inteligentes

5.8. Sector salud
- 5.8.1. Monitorización de ejercicio/Ritmo Cardiaco
- 5.8.2. Monitorización de pacientes y personas mayores
- 5.8.3. Implantadles
- 5.8.4. Robots quirúrgicos

5.9. Conectividad
- 5.9.1. Wi-Fi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Conectividad incorporada

5.10. Securización
- 5.10.1. Redes dedicadas
- 5.10.2. Gestor de contraseñas
- 5.10.3. Uso de protocolos cifrados
- 5.10.4. Consejos de uso

Módulo 6. Hacking ético

6.1. Entorno de trabajo
- 6.1.1. Distribuciones Linux
  - 6.1.1.1. Kali Linux - *Offensive Security*
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Sistemas de virtualización
- 6.1.3. *Sandbox*
- 6.1.4. Despliegue de laboratorios

6.2. Metodologías
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. *Footprinting*
- 6.3.1. Inteligencia de fuentes abiertas (OSINT)
- 6.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 6.3.3. Uso de herramientas pasivas

6.4. Escaneo de redes
- 6.4.1. Herramientas de escaneo
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3
  - 6.4.1.3. Otras herramientas de escaneo
- 6.4.2. Técnicas de escaneo
- 6.4.3. Técnicas de evasión de firewall e IDS
- 6.4.4. *Banner Grabbing*
- 6.4.5. Diagramas de red

6.5. Enumeración
- 6.5.1. Enumeración SMTP
- 6.5.2. Enumeración DNS
- 6.5.3. Enumeración de NetBIOS y Samba
- 6.5.4. Enumeración de LDAP
- 6.5.5. Enumeración de SNMP
- 6.5.6. Otras técnicas de enumeración

6.6. Análisis de vulnerabilidades
- 6.6.1. Soluciones de análisis de vulnerabilidades
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6.2. Sistemas de puntuación de vulnerabilidades
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

6.7. Ataques a redes inalámbrica
- 6.7.1. Metodología de hacking en redes inalámbricas
  - 6.7.1.1. Wi-Fi *Discovery*
  - 6.7.1.2. Análisis de tráfico
  - 6.7.1.3. Ataques del *aircrack*
    - 6.7.1.3.1. Ataques WEP
    - 6.7.1.3.2. Ataques WPA/WPA2
  - 6.7.1.4. Ataques de *Evil Twin*
  - 6.7.1.5. Ataques a WPS
  - 6.7.1.6. *Jamming*
- 6.7.2. Herramientas para la seguridad inalámbrica

6.8. Hackeo de servidores webs
- 6.8.1. *Cross Site Scripting*
- 6.8.2. CSRF
- 6.8.3. *Session Hijacking*
- 6.8.4. *SQLinjection*

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

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

Módulo 7. Ingeniería inversa

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

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

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

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

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

7.6. Arquitectura hardware ARM
- 7.6.1. Arquitectura de procesadores ARM
- 7.6.2. Estructuras de datos en ARM
- 7.6.3. Estructuras de código en ARM

7.7. Análisis de código estático
- 7.7.1. Desensambladores
- 7.7.2. IDA
- 7.7.3. Reconstructores de código

7.8. Análisis de código dinámico
- 7.8.1. Análisis del comportamiento
  - 7.8.1.1. Comunicaciones
  - 7.8.1.2. Monitorización
- 7.8.2. Depuradores de código en Linux
- 7.8.3. Depuradores de código en Windows

7.9. Sandbox
- 7.9.1. Arquitectura de un *sandbox*
- 7.9.2. Evasión de un *sandbox*
- 7.9.3. Técnicas de detección
- 7.9.4. Técnicas de evasión

7.9.5. Contramedidas
7.9.6. Sandbox en Linux
7.9.7. Sandbox en Windows
7.9.8. Sandbox en MacOS
7.9.9. Sandbox en Android
7.10. Análisis de malware
7.10.1. Métodos de análisis de malware
7.10.2. Técnicas de ofuscación de malware
7.10.2.1. Ofuscación de ejecutables
7.10.2.2. Restricción de entornos de ejecución
7.10.3. Herramientas de análisis de malware

Módulo 8. Desarrollo seguro

8.1. Desarrollo seguro
8.1.1. Calidad, funcionalidad y seguridad
8.1.2. Confidencialidad, integridad y disponibilidad
8.1.3. Ciclo de vida del desarrollo de software
8.2. Fase de requerimientos
8.2.1. Control de la autenticación
8.2.2. Control de roles y privilegios
8.2.3. Requerimientos orientados al riesgo
8.2.4. Aprobación de privilegios
8.3. Fases de análisis y diseño
8.3.1. Acceso a componentes y administración del sistema
8.3.2. Pistas de auditoría
8.3.3. Gestión de sesiones
8.3.4. Datos históricos
8.3.5. Manejo apropiado de errores
8.3.6. Separación de funciones
8.4. Fase de implementación y codificación
8.4.1. Aseguramiento del ambiente de desarrollo
8.4.2. Elaboración de la documentación técnica
8.4.3. Codificación segura
8.4.4. Seguridad en las comunicaciones
8.5. Buenas prácticas de codificación segura
8.5.1. Validación de datos de entrada
8.5.2. Codificación de los datos de salida
8.5.3. Estilo de programación
8.5.4. Manejo de registro de cambios
8.5.5. Prácticas criptográficas
8.5.6. Gestión de errores y logs
8.5.7. Gestión de archivos
8.5.8. Gestión de memoria
8.5.9. Estandarización y reutilización de funciones de seguridad
8.6. Preparación del servidor y *hardening*
8.6.1. Gestión de usuarios, grupos y roles en el servidor
8.6.2. Instalación de software
8.6.3. *Hardening* del servidor
8.6.4. Configuración robusta del entorno de la aplicación
8.7. Preparación de la BBDD y *hardening*
8.7.1. Optimización del motor de BBDD
8.7.2. Creación del usuario propio para la aplicación
8.7.3. Asignación de los privilegios precisos para el usuario
8.7.4. *Hardening* de la BBDD
8.8. Fase de pruebas
8.8.1. Control de calidad en controles de seguridad
8.8.2. Inspección del código por fases
8.8.3. Comprobación de la gestión de las configuraciones
8.8.4. Pruebas de caja negra
8.9. Preparación del Paso a producción
8.9.1. Realizar el control de cambios
8.9.2. Realizar procedimiento de paso a producción
8.9.3. Realizar procedimiento de *rollback*
8.9.4. Pruebas en fase de preproducción

8.10. Fase de mantenimiento
- 8.10.1. Aseguramiento basado en riesgos
- 8.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 8.10.3. Pruebas de mantenimiento de seguridad de caja negra

Módulo 9. Implementación práctica de políticas de seguridad en software y hardware

9.1. Implementación práctica de políticas de seguridad en software y hardware
- 9.1.1. Implementación de identificación y autorización
- 9.1.2. Implementación de técnicas de identificación
- 9.1.3. Medidas técnicas de autorización

9.2. Tecnologías de identificación y autorización
- 9.2.1. Identificador y OTP
- 9.2.2. Token USB o tarjeta inteligente PKI
- 9.2.3. La llave "Confidencial Defensa"
- 9.2.4. El RFID Activo

9.3. Políticas de seguridad en el acceso a software y sistemas
- 9.3.1. Implementación de políticas de control de accesos
- 9.3.2. Implementación de políticas de acceso a comunicaciones
- 9.3.3. Tipos de herramientas de seguridad para control de acceso

9.4. Gestión de acceso a usuarios
- 9.4.1. Gestión de los derechos de acceso
- 9.4.2. Segregación de roles y funciones de acceso
- 9.4.3. Implementación derechos de acceso en sistemas

9.5. Control de acceso a sistemas y aplicaciones
- 9.5.1. Norma del mínimo acceso
- 9.5.2. Tecnologías seguras de inicios de sesión
- 9.5.3. Políticas de seguridad en contraseñas

9.6. Tecnologías de sistemas de identificación
- 9.6.1. Directorio activo
- 9.6.2. OTP
- 9.6.3. PAP, CHAP
- 9.6.4. KERBEROS, DIAMETER, NTLM

9.7. Controles CIS para bastionado de sistemas
- 9.7.1. Controles CIS básicos
- 9.7.2. Controles CIS fundamentales
- 9.7.3. Controles CIS organizacionales

9.8. Seguridad en la operativa
- 9.8.1. Protección contra código malicioso
- 9.8.2. Copias de seguridad
- 9.8.3. Registro de actividad y supervisión

9.9. Gestión de las vulnerabilidades técnicas
- 9.9.1. Vulnerabilidades técnicas
- 9.9.2. Gestión de vulnerabilidades técnicas
- 9.9.3. Restricciones en la instalación de software

9.10. Implementación de prácticas de políticas de seguridad
- 9.10.1. Vulnerabilidades lógicas
- 9.10.2. Implementación de políticas de defensa

Módulo 10. Análisis forense

10.1. Adquisición de datos y duplicación
- 10.1.1. Adquisición de datos volátiles
  - 10.1.1.1. Información del sistema
  - 10.1.1.2. Información de la red
  - 10.1.1.3. Orden de volatilidad
- 10.1.2. Adquisición de datos estáticos
  - 10.1.2.1. Creación de una imagen duplicada
  - 10.1.2.2. Preparación de un documento para la cadena de custodia
- 10.1.3. Métodos de validación de los datos adquiridos
  - 10.1.3.1. Métodos para Linux
  - 10.1.3.2. Métodos para Windows

10.2. Evaluación y derrota de técnicas antiforenses
- 10.2.1. Objetivos de las técnicas antiforenses
- 10.2.2. Borrado de datos
  - 10.2.2.1. Borrado de datos y ficheros
  - 10.2.2.2. Recuperación de archivos
  - 10.2.2.3. Recuperación de particiones borradas
- 10.2.3. Protección por contraseña
- 10.2.4. Esteganografía
- 10.2.5. Borrado seguro de dispositivos
- 10.2.6. Encriptación

10.3. Análisis forense del sistema operativo
- 10.3.1. Análisis forense de Windows
- 10.3.2. Análisis forense de Linux
- 10.3.3. Análisis forense de Mac

10.4. Análisis forense de la red
- 10.4.1. Análisis de los logs
- 10.4.2. Correlación de datos
- 10.4.3. Investigación de la red
- 10.4.4. Pasos a seguir en el análisis forense de la red

10.5. Análisis forense web
- 10.5.1. Investigación de los ataques webs
- 10.5.2. Detección de ataques
- 10.5.3. Localización de direcciones IPs

10.6. Análisis forense de Bases de Datos
- 10.6.1. Análisis forense en MSSQL
- 10.6.2. Análisis forense en MySQL
- 10.6.3. Análisis forense en PostgreSQL
- 10.6.4. Análisis forense en MongoDB

10.7. Análisis forense en Cloud
- 10.7.1. Tipos de crímenes en Cloud
  - 10.7.1.1. Cloud como sujeto
  - 10.7.1.2. Cloud como objeto
  - 10.7.1.3. Cloud como herramienta
- 10.7.2. Retos del análisis forense en Cloud
- 10.7.3. Investigación de los servicios de almacenamiento el Cloud
- 10.7.4. Herramientas de análisis forense para Cloud

10.8. Investigación de crímenes de correo electrónico
- 10.8.1. Sistemas de correo
  - 10.8.1.1. Clientes de correo
  - 10.8.1.2. Servidor de correo
  - 10.8.1.3. Servidor SMTP
  - 10.8.1.4. Servidor POP3
  - 10.8.1.5. Servidor IMAP4
- 10.8.2. Crímenes de correo
- 10.8.3. Mensaje de correo
  - 10.8.3.1. Cabeceras estándar
  - 10.8.3.2. Cabeceras extendidas
- 10.8.4. Pasos para la investigación de estos crímenes
- 10.8.5. Herramientas forenses para correo electrónico

10.9. Análisis forense de móviles
- 10.9.1. Redes celulares
  - 10.9.1.1. Tipos de redes
  - 10.9.1.2. Contenidos del CDR
- 10.9.2. *Subscriber Identity Module* (SIM)
- 10.9.3. Adquisición lógica
- 10.9.4. Adquisición física
- 10.9.5. Adquisición del sistema de ficheros

10.10. Redacción y presentación de informes forenses
- 10.10.1. Aspectos importantes de un informe forense
- 10.10.2. Clasificación y tipos de informes
- 10.10.3. Guía para escribir un informe
- 10.10.4. Presentación del informe
  - 10.10.4.1. Preparación previa para testificar
  - 10.10.4.2. Deposición
  - 10.10.4.3. Trato con los medios

Módulo 11. Seguridad en el diseño y desarrollo de sistemas

11.1. Sistemas de Información
- 11.1.1. Dominios de un sistema de información
- 11.1.2. Componentes de un sistema de información
- 11.1.3. Actividades de un sistema de información
- 11.1.4. Ciclo de vida de un sistema de información
- 11.1.5. Recursos de un sistema de información

11.2. Sistemas de información. Tipología
- 11.2.1. Tipos de sistemas de información
  - 11.2.1.1. Empresarial
  - 11.2.1.2. Estratégicos
  - 11.2.1.3. Según el ámbito de la aplicación
  - 11.2.1.4. Específicos
- 11.2.2. Sistemas de Información. Ejemplos reales
- 11.2.3. Evolución de los sistemas de información: Etapas
- 11.2.4. Metodologías de los sistemas de información

11.3. Seguridad de los sistemas de información. Implicaciones legales
- 11.3.1. Acceso a datos
- 11.3.2. Amenazas de seguridad: Vulnerabilidades
- 11.3.3. Implicaciones legales: Delitos
- 11.3.4. Procedimientos de mantenimiento de un sistema de información

11.4. Seguridad de un sistema de información. Protocolos de seguridad
- 11.4.1. Seguridad de un sistema de información
  - 11.4.1.1. Integridad
  - 11.4.1.2. Confidencialidad
  - 11.4.1.3. Disponibilidad
  - 11.4.1.4. Autenticación
- 11.4.2. Servicios de seguridad
- 11.4.3. Protocolos de seguridad de la información. Tipología
- 11.4.4. Sensibilidad de un sistema de información

11.5. Seguridad en un sistema de información. Medidas y sistemas de control de acceso
- 11.5.1. Medidas de seguridad
- 11.5.2. Tipo de medidas de seguridad
  - 11.5.2.1. Prevención
  - 11.5.2.2. Detección
  - 11.5.2.3. Corrección
- 11.5.3. Sistemas de control de acceso. Tipología
- 11.5.4. Criptografía

11.6. Seguridad en redes e internet
- 11.6.1. Firewalls
- 11.6.2. Identificación digital
- 11.6.3. Virus y gusanos
- 11.6.4. Hacking
- 11.6.5. Ejemplos y casos reales

11.7. Delitos informáticos
- 11.7.1. Delito informático
- 11.7.2. Delitos informáticos. Tipología
- 11.7.3. Delito Informático. Ataque. Tipologías
- 11.7.4. El caso de la realidad virtual
- 11.7.5. Perfiles de delincuentes y víctimas. Tipificación del delito
- 11.7.6. Delitos informáticos. Ejemplos y casos reales

11.8. Plan de seguridad en un sistema de información
- 11.8.1. Plan de seguridad. Objetivos
- 11.8.2. Plan de seguridad. Planificación
- 11.8.3. Plan de riesgos. Análisis
- 11.8.4. Política de seguridad. Implementación en la organización
- 11.8.5. Plan de seguridad. Implementación en la organización
- 11.8.6. Procedimientos de seguridad. Tipos
- 11.8.7. Planes de seguridad. Ejemplos

11.9. Plan de contingencia
- 11.9.1. Plan de contingencia. Funciones
- 11.9.2. Plan de emergencia: Elementos y objetivos
- 11.9.3. Plan de contingencia en la organización. Implementación
- 11.9.4. Planes de contingencia. Ejemplos

11.10. Gobierno de la seguridad de sistemas de información
- 11.10.1. Normativa legal
- 11.10.2. Estándares
- 11.10.3. Certificaciones
- 11.10.4. Tecnologías

Módulo 12. Arquitecturas y modelos de seguridad de la información

12.1. Arquitectura de seguridad de la información
- 12.1.1. SGSI/PDS
- 12.1.2. Alineación estratégica
- 12.1.3. Gestión del riesgo
- 12.1.4. Medición del desempeño

12.2. Modelos de seguridad de la información
- 12.2.1. Basados en políticas de seguridad
- 12.2.2. Basados en herramientas de protección
- 12.2.3. Basados en equipos de trabajo

12.3. Modelo de seguridad. Componentes clave
- 12.3.1. Identificación de riesgos
- 12.3.2. Definición de controles
- 12.3.3. Evaluación continua de niveles de riesgo
- 12.3.4. Plan de concienciación de empleados, proveedores, socios, etc

12.4. Proceso de gestión de riesgos
- 12.4.1. Identificación de activos
- 12.4.2. Identificación de amenazas
- 12.4.3. Evaluación de riesgos
- 12.4.4. Priorización de controles
- 12.4.5. Reevaluación y riesgo residual

12.5. Procesos de negocio y seguridad de la información
- 12.5.1. Procesos de negocio
- 12.5.2. Evaluación de riesgos basados en parámetros de negocio
- 12.5.3. Análisis de impacto al negocio
- 12.5.4. Las operaciones de negocio y la seguridad de la información

12.6. Proceso de mejora continua
- 12.6.1. El ciclo de Deming
  - 12.6.1.1. Planificar
  - 12.6.1.2. Hacer
  - 12.6.1.3. Verificar
  - 12.6.1.4. Actuar

12.7. Arquitecturas de seguridad
- 12.7.1. Selección y homogeneización de tecnologías
- 12.7.2. Gestión de identidades. Autenticación
- 12.7.3. Gestión de accesos. Autorización
- 12.7.4. Seguridad de infraestructura de red
- 12.7.5. Tecnologías y soluciones de cifrado
- 12.7.6. Seguridad de equipos terminales (EDR)

12.8. El marco normativo
- 12.8.1. Normativas sectoriales
- 12.8.2. Certificaciones
- 12.8.3. Legislaciones

12.9. La norma ISO 27001
- 12.9.1. Implementación
- 12.9.2. Certificación
- 12.9.3. Auditorías y tests de intrusión
- 12.9.4. Gestión continua del riesgo
- 12.9.5. Clasificación de la información

12.10. Legislación sobre privacidad. RGPD (GDPR)
- 12.10.1. Alcance del reglamento general de protección de datos (RGPD)
- 12.10.2. Datos personales
- 12.10.3. Roles en el tratamiento de datos personales
- 12.10.4. Derechos ARCO
- 12.10.5. El DPO. Funciones

Módulo 13. Sistema de gestión de seguridad de información (SGSI)

13.1. Seguridad de la información. Aspectos clave
- 13.1.1. Seguridad de la información
  - 13.1.1.1. Confidencialidad
  - 13.1.1.2. Integridad
  - 13.1.1.3. Disponibilidad
  - 13.1.1.4. Medidas de seguridad de la Información

13.2. Sistema de gestión de la seguridad de la información
- 13.2.1. Modelos de gestión de seguridad de la información
- 13.2.2. Documentos para implantar un SGSI
- 13.2.3. Niveles y controles de un SGSI

13.3. Normas y estándares internacionales
- 13.3.1. Estándares internacionales en la seguridad de la información
- 13.3.2. Origen y evolución del estándar
- 13.3.3. Estándares internacionales gestión de la seguridad de la información
- 13.3.4. Otras normas de referencia

13.4. Normas ISO/IEC 27.000
- 13.4.1. Objeto y ámbito de aplicación
- 13.4.2. Estructura de la norma
- 13.4.3. Certificación
- 13.4.4. Fases de acreditación
- 13.4.5. Beneficios normas ISO/IEC 27.000

13.5. Diseño e implantación de un sistema general de seguridad de información
- 13.5.1. Fases de implantación de un sistema general de seguridad de la información
- 13.5.2. Plan de continuidad de negocio

13.6. Fase I: diagnóstico
- 13.6.1. Diagnóstico preliminar
- 13.6.2. Identificación del nivel de estratificación
- 13.6.3. Nivel de cumplimiento de estándares/normas

13.7. Fase II: preparación
- 13.7.1. Contexto de la organización
- 13.7.2. Análisis de normativas de seguridad aplicables
- 13.7.3. Alcance del sistema general de seguridad de información
- 13.7.4. Política del sistema general de seguridad de información
- 13.7.5. Objetivos del sistema general de seguridad de información

13.8. Fase III: planificación
- 13.8.1. Clasificación de activos
- 13.8.2. Valoración de riesgos
- 13.8.3. Identificación de amenazas y riesgos

13.9. Fase IV: implantación y seguimiento
- 13.9.1. Análisis de resultados
- 13.9.2. Asignación de responsabilidades
- 13.9.3. Temporalización del plan de acción
- 13.9.4. Seguimiento y auditorias

13.10. Políticas de seguridad en la gestión de incidentes
- 13.10.1. Fases
- 13.10.2. Categorización de incidentes
- 13.10.3. Procedimientos y gestión de incidentes

Módulo 14. Gestión de la seguridad IT

14.1. Gestión de la seguridad
- 14.1.1. Operaciones de seguridad
- 14.1.2. Aspecto legal y regulatorio
- 14.1.3. Habilitación del negocio
- 14.1.4. Gestión de riesgos
- 14.1.5. Gestión de identidades y accesos

14.2. Estructura del área de seguridad. La oficina del CISO
- 14.2.1. Estructura organizativa. Posición del CISO en la estructura
- 14.2.2. Las líneas de defensa
- 14.2.3. Organigrama de la oficina del CISO
- 14.2.4. Gestión presupuestaria

14.3. Gobierno de seguridad
- 14.3.1. Comité de seguridad
- 14.3.2. Comité de seguimiento de riesgos
- 14.3.3. Comité de auditoría
- 14.3.4. Comité de crisis

14.4. Gobierno de seguridad. Funciones
- 14.4.1. Políticas y normas
- 14.4.2. Plan director de seguridad
- 14.4.3. Cuadros de mando
- 14.4.4. Concienciación y formación
- 14.4.5. Seguridad en la cadena de suministro

14.5. Operaciones de seguridad
- 14.5.1. Gestión de identidades y accesos
- 14.5.2. Configuración de reglas de seguridad de red. Firewalls
- 14.5.3. Gestión de plataformas IDS/IPS
- 14.5.4. Análisis de vulnerabilidades

14.6. Marco de trabajo de ciberseguridad. NIST CSF
- 14.6.1. Metodología NIST
  - 14.6.1.1. Identificar
  - 14.6.1.2. Proteger
  - 14.6.1.3. Detectar
  - 14.6.1.4. Responder
  - 14.6.1.5. Recuperar

14.7. Centro de operaciones de seguridad (SOC). Funciones
- 14.7.1. Protección. *Red Team, pentesting, threat intelligence*
- 14.7.2. Detección. SIEM, *user behavior analytics*, *fraud prevention*
- 14.7.3. Respuesta

14.8. Auditorías de seguridad
- 14.8.1. Test de intrusión
- 14.8.2. Ejercicios de *red team*
- 14.8.3. Auditorías de código fuente. Desarrollo seguro
- 14.8.4. Seguridad de componentes (*software supply chain*)
- 14.8.5. Análisis forense

14.9. Respuesta a incidentes
- 14.9.1. Preparación
- 14.9.2. Detección, análisis y notificación
- 14.9.3. Contención, erradicación y recuperación
- 14.9.4. Actividad post incidente
  - 14.9.4.1. Retención de evidencias
  - 14.9.4.2. Análisis forense
  - 14.9.4.3. Gestión de brechas
- 14.9.5. Guías oficiales de gestión de ciberincidentes

14.10. Gestión de vulnerabilidades
- 14.10.1. Análisis de vulnerabilidades
- 14.10.2. Valoración de vulnerabilidad
- 14.10.3. Bastionado de sistemas
- 14.10.4. Vulnerabilidades de día 0. Zero-day

Módulo 15. Políticas de gestión de incidencias de seguridad

15.1. Políticas de gestión de incidencias de seguridad de la información y mejoras
- 15.1.1. Gestión de incidencias
- 15.1.2. Responsabilidades y procedimientos
- 15.1.3. Notificación de eventos

15.2. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 15.2.1. Datos de funcionamiento del sistema
- 15.2.2. Tipos de sistemas de detección de intrusos
- 15.2.3. Criterios para la ubicación de los IDS/IPS

15.3. Respuesta ante incidentes de seguridad
- 15.3.1. Procedimiento de recolección de información
- 15.3.2. Proceso de verificación de intrusión
- 15.3.3. Organismos CERT

15.4. Proceso de notificación y gestión de intentos de intrusión
- 15.4.1. Responsabilidades en el proceso de notificación
- 15.4.2. Clasificación de los incidentes
- 15.4.3. Proceso de resolución y recuperación

15.5. Análisis forense como política de seguridad
- 15.5.1. Evidencias volátiles y no volátiles
- 15.5.2. Análisis y recogida de evidencias electrónicas
  - 15.5.2.1. Análisis de evidencias electrónicas
  - 15.5.2.2. Recogida de evidencias electrónicas

15.6. Herramientas de Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 15.6.1. Snort
- 15.6.2. Suricata
- 15.6.3. Solar-Winds

15.7. Herramientas centralizadoras de eventos
- 15.7.1. SIM
- 15.7.2. SEM
- 15.7.3. SIEM

15.8. Guía de seguridad CCN-STIC 817
- 15.8.1. Gestión de ciberincidentes
- 15.8.2. Métricas e Indicadores

15.9. NIST SP800-61
- 15.9.1. Capacidad de respuesta antes incidentes de seguridad informática
- 15.9.2. Manejo de un incidente
- 15.9.3. Coordinación e información compartida

15.10. Norma ISO 27035
- 15.10.1. Norma ISO 27035. Principios de la gestión de incidentes
- 15.10.2. Guías para la elaboración de un plan para la gestión de incidentes
- 15.10.3. Guías de operaciones en la respuesta a incidentes

Módulo 16. Análisis de riesgos y entorno de seguridad IT

16.1. Análisis del entorno
- 16.1.1. Análisis de la situación coyuntural
  - 16.1.1.1. Entornos VUCA
    - 16.1.1.1.1. Volátil
    - 16.1.1.1.2. Incierto
    - 16.1.1.1.3. Complejo
    - 16.1.1.1.4. Ambiguo
  - 16.1.1.2. Entornos BANI
    - 16.1.1.2.1. Quebradizo
    - 16.1.1.2.2. Ansioso
    - 16.1.1.2.3. No lineal
    - 16.1.1.2.4. Incomprensible
- 16.1.2. Análisis del entorno general. PESTEL
  - 16.1.2.1. Político
  - 16.1.2.2. Económico
  - 16.1.2.3. Social
  - 16.1.2.4. Tecnológico
  - 16.1.2.5. Ecológico/Ambiental
  - 16.1.2.6. Legal
- 16.1.3. Análisis de la situación interna. DAFO
  - 16.1.3.1. Objetivos
  - 16.1.3.2. Amenazas
  - 16.1.3.3. Oportunidades
  - 16.1.3.4. Fortalezas

16.2. Riesgo e incertidumbre
- 16.2.1. Riesgo
- 16.2.2. Gerencia de riesgos
- 16.2.3. Estándares de gestión de riesgos

16.3. Directrices para la gestión de riesgos ISO 31.000:2018
- 16.3.1. Objeto
- 16.3.2. Principios
- 16.3.3. Marco de referencia
- 16.3.4. Proceso

16.4. Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT)
- 16.4.1. Metodología MAGERIT
  - 16.4.1.1. Objetivos
  - 16.4.1.2. Método
  - 16.4.1.3. Elementos
  - 16.4.1.4. Técnicas
  - 16.4.1.5. Herramientas disponibles (PILAR)

16.5. Transferencia del riesgo cibernético
- 16.5.1. Transferencia de riesgos
- 16.5.2. Riesgos cibernéticos. Tipología
- 16.5.3. Seguros de ciber riesgos

16.6. Metodologías ágiles para la gestión de riesgos
- 16.6.1. Metodologías ágiles
- 16.6.2. Scrum para la gestión del riesgo
- 16.6.3. *Agile risk management*

16.7. Tecnologías para la gestión del riesgo
- 16.7.1. Inteligencia artificial aplicada a la gestión de riesgos
- 16.7.2. *Blockchain* y criptografía. Métodos de preservación del valor
- 16.7.3. Computación cuántica. Oportunidad o amenaza

16.8. Elaboración de mapas de riesgos IT basados en metodologías ágiles
- 16.8.1. Representación de la probabilidad y el impacto en entornos ágiles
- 16.8.2. El riesgo como amenaza del valor
- 16.8.3. Re-evolución en la gestión de proyectos y procesos ágiles basados en KRIs

16.9. *Risk driven* en la gestión de riesgos
- 16.9.1. *Risk driven*
- 16.9.2. *Risk driven* en la gestión de riesgos
- 16.9.3. Elaboración de un modelo de gestión empresarial impulsado por el riesgo

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

Módulo 17. Políticas de seguridad para el análisis de amenazas en sistemas informáticos

17.1. La gestión de amenazas en las políticas de seguridad
- 17.1.1. La gestión del riesgo
- 17.1.2. El riesgo en seguridad
- 17.1.3. Metodologías en la gestión de amenazas
- 17.1.4. Puesta en marcha de metodologías

17.2. Fases de la gestión de amenazas
- 17.2.1. Identificación
- 17.2.2. Análisis
- 17.2.3. Localización
- 17.2.4. Medidas de salvaguarda

17.3. Sistemas de auditoria para localización de amenazas
- 17.3.1. Clasificación y flujo de información
- 17.3.2. Análisis de los procesos vulnerable

17.4. Clasificación del riesgo
- 17.4.1. Tipos de riesgo
- 17.4.2. Calculo de la probabilidad de amenaza
- 17.4.3. Riesgo residual

17.5. Tratamiento del Riesgo
- 17.5.1. Implementación de medidas de salvaguarda
- 17.5.2. Transferir o asumir

17.6. Control de riesgo
- 17.6.1. Proceso continuo de gestión de riesgo
- 17.6.2. Implementación de métricas de seguridad
- 17.6.3. Modelo estratégico de métricas en seguridad de la información

17.7. Metodologías prácticas para el análisis y control de amenazas
- 17.7.1. Catálogo de amenazas
- 17.7.2. Catálogo de medidas de control
- 17.7.3. Catálogo de salvaguardas

17.8. Norma ISO 27005
- 17.8.1. Identificación del riesgo
- 17.8.2. Análisis del riesgo
- 17.8.3. Evaluación del riesgo

17.9. Matriz de riesgo, impacto y amenazas
- 17.9.1. Datos, sistemas y personal
- 17.9.2. Probabilidad de amenaza
- 17.9.3. Magnitud del daño

17.10. Diseño de fases y procesos en el análisis de amenazas
- 17.10.1. Identificación elementos críticos de la organización
- 17.10.2. Determinación de amenazas e impactos
- 17.10.3. Análisis del impacto y riesgo
- 17.10.4. Metodologías

Módulo 18. Implementación práctica de políticas de seguridad ante ataques

18.1. *System Hacking*
- 18.1.1. Riesgos y vulnerabilidades
- 18.1.2. Contramedidas

18.2. DoS en servicios
- 18.2.1. Riesgos y vulnerabilidades
- 18.2.2. Contramedidas

18.3. *Session Hijacking*
- 18.3.1. El proceso de *Hijacking*
- 18.3.2. Contramedidas a *Hijacking*

18.4. Evasión de IDS, *Firewalls and Honeypots*
- 18.4.1. Técnicas de evasión
- 18.4.2. Implementación de contramedidas

18.5. *Hacking Web Servers*
- 18.5.1. Ataques a servidores webs
- 18.5.2. Implementación de medidas de defensa

18.6. *Hacking Web Applications*
- 18.6.1. Ataques a aplicaciones web
- 18.6.2. Implementación de medidas de defensa

18.7. *Hacking Wireless Networks*
- 18.7.1. Vulnerabilidades redes wifi
- 18.7.2. Implementación de medidas de defensa

18.8. *Hacking Mobile Platforms*
- 18.8.1. Vulnerabilidades de plataformas móviles
- 18.8.2. Implementación de contramedidas

18.9. *Ransomware*
- 18.9.1. Vulnerabilidades causantes del *Ransomware*
- 18.9.2. Implementación de contramedidas

18.10. Ingeniera social
- 18.10.1. Tipos de ingeniería social
- 18.10.2. Contramedidas para la ingeniería social

Módulo 19. Criptografía en IT

19.1. Criptografía
- 19.1.1. Criptografía
- 19.1.2. Fundamentos matemáticos

19.2. Criptología
- 19.2.1. Criptología
- 19.2.2. Criptoanálisis
- 19.2.3. Esteganografía y estegoanálisis

19.3. Protocolos criptográficos
- 19.3.1. Bloques básicos
- 19.3.2. Protocolos básicos
- 19.3.3. Protocolos intermedios
- 19.3.4. Protocolos avanzados
- 19.3.5. Protocolos exotéricos

19.4. Técnicas criptográficas
- 19.4.1. Longitud de claves
- 19.4.2. Manejo de claves
- 19.4.3. Tipos de algoritmos
- 19.4.4. Funciones resumen. *Hash*
- 19.4.5. Generadores de números pseudoaleatorios
- 19.4.6. Uso de algoritmos

19.5. Criptografía simétrica
- 19.5.1. Cifrados de bloque
- 19.5.2. DES (*Data Encryption Standard*)
- 19.5.3. Algoritmo RC4
- 19.5.4. AES (*Advanced Encryption Standard*)
- 19.5.5. Combinación de cifrados de bloques
- 19.5.6. Derivación de claves

19.6. Criptografía asimétrica
- 19.6.1. Diffie-Hellman
- 19.6.2. DSA (*Digital Signature Algorithm*)
- 19.6.3. RSA (Rivest, Shamir y Adleman)
- 19.6.4. Curva elíptica
- 19.6.5. Criptografía asimétrica. Tipología

19.7. Certificados digitales
- 19.7.1. Firma digital
- 19.7.2. Certificados X509
- 19.7.3. Infraestructura de clave pública (PKI)

19.8. Implementaciones
- 19.8.1. Kerberos
- 19.8.2. IBM CCA
- 19.8.3. *Pretty Good Privacy* (PGP)
- 19.8.4. ISO *Authentication Framework*
- 19.8.5. SSL y TLS
- 19.8.6. Tarjetas inteligentes en medios de pago (EMV)
- 19.8.7. Protocolos de telefonía móvil
- 19.8.8. *Blockchain*

19.9. Esteganografía
- 19.9.1. Esteganografía
- 19.9.2. Estegoanálisis
- 19.9.3. Aplicaciones y usos

19.10. Criptografía cuántica
- 19.10.1. Algoritmos cuánticos
- 19.10.2. Protección de algoritmos frente a computación cuántica
- 19.10.3. Distribución de claves cuántica

Módulo 20. Gestión de identidad y accesos en seguridad IT

20.1. Gestión de identidad y accesos (IAM)
- 20.1.1. Identidad digital
- 20.1.2. Gestión de identidad
- 20.1.3. Federación de identidades

20.2. Control de acceso físico
- 20.2.1. Sistemas de protección
- 20.2.2. Seguridad de las áreas
- 20.2.3. Instalaciones de recuperación

20.3. Control de acceso lógico
- 20.1.1. Autenticación: Tipología
- 20.1.2. Protocolos de autenticación
- 20.1.3. Ataques de autenticación

20.4. Control de acceso lógico. Autenticación MFA
- 20.4.1. Control de acceso lógico. Autenticación MFA
- 20.4.2. Contraseñas. Importancia
- 20.4.3. Ataques de autenticación

20.5. Control de acceso lógico. Autenticación biométrica
- 20.5.1. Control de Acceso Lógico. Autenticación biométrica
  - 20.5.1.1. Autenticación biométrica. Requisitos
- 20.5.2. Funcionamiento
- 20.5.3. Modelos y técnicas

20.6. Sistemas de gestión de autenticación
- 20.6.1. *Single sign on*
- 20.6.2. Kerberos
- 20.6.3. Sistemas AAA

20.7. Sistemas de gestión de autenticación: Sistemas AAA
- 20.7.1. TACACS
- 20.7.2. RADIUS
- 20.7.3. DIAMETER

20.8. Servicios de control de acceso
- 20.8.1. FW - Cortafuegos
- 20.8.2. VPN - Redes Privadas Virtuales
- 20.8.3. IDS - Sistema de Detección de Intrusiones

20.9. Sistemas de control de acceso a la red
- 20.9.1. NAC
- 20.9.2. Arquitectura y elementos
- 20.9.3. Funcionamiento y estandarización

20.10. Acceso a redes inalámbricas
- 20.10.1. Tipos de redes inalámbricas
- 20.10.2. Seguridad en redes inalámbricas
- 20.10.3. Ataques en redes inalámbricas

Módulo 21. Seguridad en comunicaciones y operación software

21.1. Seguridad informática en comunicaciones y operación software
- 21.1.1. Seguridad informática
- 21.1.2. Ciberseguridad
- 21.1.3. Seguridad en la nube

21.2. Seguridad informática en comunicaciones y operación software. Tipología
- 21.2.1. Seguridad física
- 21.2.2. Seguridad lógica

21.3. Seguridad en comunicaciones
- 21.3.1. Principales elementos
- 21.3.2. Seguridad de redes
- 21.3.3. Mejores prácticas

21.4. Ciberinteligencia
- 21.4.1. Ingeniería social
- 21.4.2. *Deep web*
- 21.4.3. *Phishing*
- 21.4.4. *Malware*

21.5. Desarrollo seguro en comunicaciones y operación software
- 21.1.1. Desarrollo seguro. Protocolo HTTP
- 21.1.2. Desarrollo seguro. Ciclo de vida
- 21.1.3. Desarrollo seguro. Seguridad PHP
- 21.1.4. Desarrollo seguro. Seguridad NET
- 21.1.5. Desarrollo seguro. Mejores prácticas

21.6. Sistemas de gestión de la seguridad de la información en comunicaciones y operación software
- 21.6.1. GDPR
- 21.6.2. ISO 27021
- 21.6.3. ISO 27017/18

21.7. Tecnologías SIEM
- 21.7.1. Tecnologías SIEM
- 21.7.2. Operativa de SOC
- 21.7.3. SIEM *vendors*

21.8. El rol de la seguridad en las organizaciones
- 21.8.1. Roles en las organizaciones
- 21.8.2. Rol de los especialistas IoT en las compañías
- 21.8.3. Certificaciones reconocidas en el mercado

21.9. Análisis forense
- 21.9.1. Análisis forense
- 21.9.2. Análisis forense. Metodología
- 21.9.3. Análisis forense. Herramientas e implantación

21.10. La ciberseguridad en la actualidad
- 21.10.1. Principales ataques informáticos
- 21.10.2. Previsiones de empleabilidad
- 21.10.3. Retos

Módulo 22. Seguridad en entornos *cloud*

22.1. Seguridad en entornos *cloud computing*
- 22.1.1. Seguridad en entornos *cloud computing*
- 22.1.2. Seguridad en entornos *cloud computing*. Amenazas y riesgos seguridad
- 22.1.3. Seguridad en entornos *cloud computing*. Aspectos clave de seguridad

22.2. Tipos de infraestructura *cloud*
- 22.2.1. Público
- 22.2.2. Privado
- 22.2.3. Híbrido

22.3. Modelo de gestión compartida
- 22.3.1. Elementos de seguridad gestionados por proveedor
- 22.3.2. Elementos gestionados por cliente
- 22.3.3. Definición de la estrategia para seguridad

22.4. Mecanismos de prevención
- 22.4.1. Sistemas de gestión de autenticación
- 22.4.2. Sistema de gestión de autorización: Políticas de acceso
- 22.4.3. Sistemas de gestión de claves

22.5. Securización de sistemas
- 22.5.1. Securización de los sistemas de almacenamiento
- 22.5.2. Protección de los sistemas de base de datos
- 22.5.3. Securización de datos en tránsito

22.6. Protección de infraestructura
- 22.6.1. Diseño e implementación de red segura
- 22.6.2. Seguridad en recursos de computación
- 22.6.3. Herramientas y recursos para protección de infraestructura

22.7. Detección de las amenazas y ataques
- 22.7.1. Sistemas de auditoría, *logging* y monitorización
- 22.7.2. Sistemas de eventos y alarmas
- 22.7.3. Sistemas SIEM

22.8. Respuesta ante incidentes
- 22.8.1. Plan de respuesta a incidentes
- 22.8.2. La continuidad de negocio
- 22.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

22.9. Seguridad en *clouds* públicos
- 22.9.1. AWS (Amazon Web Services)
- 22.9.2. Microsoft Azure
- 22.9.3. Google GCP
- 22.9.4. Oracle Cloud

22.10. Normativa y cumplimiento
- 22.10.1. Cumplimiento de normativas de seguridad
- 22.10.2. Gestión de riesgos
- 22.10.3. Personas y proceso en las organizaciones

Módulo 23. Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información

23.1. Políticas de monitorización de sistemas de la información
- 23.1.1. Monitorización de Sistemas
- 23.1.2. Métricas
- 23.1.3. Tipos de métricas

23.2. Auditoria y registro en Sistemas
- 23.2.1. Auditoria y registro en Windows
- 23.2.2. Auditoria y registro en Linux

23.3. Protocolo SNMP. *Simple Network Management Protocol*
- 23.3.1. Protocolo SNMP
- 23.3.2. Funcionamiento de SNMP
- 23.3.3. Herramientas SNMP

23.4. Monitorización de redes
- 23.4.1. La monitorización de red en sistemas de control
- 23.4.2. Herramientas de monitorización para sistemas de control

23.5. Nagios. Sistema de monitorización de redes
- 23.5.1. Nagios
- 23.5.2. Funcionamiento de Nagios
- 23.5.3. Instalación de Nagios

23.6. Zabbix. Sistema de monitorización de redes
- 23.6.1. Zabbix
- 23.6.2. Funcionamiento de Zabbix
- 23.6.3. Instalación de Zabbix

23.7. Cacti. Sistema de monitorización de redes
- 23.7.1. Cacti
- 23.7.2. Funcionamiento de Cacti
- 23.7.3. Instalación de Cacti

23.8. Pandora. Sistema de monitorización de redes
- 23.8.1. Pandora
- 23.8.2. Funcionamiento de Pandora
- 23.8.3. Instalación de Pandora

23.9. SolarWinds. Sistema de monitorización de redes
- 23.9.1. SolarWinds
- 23.9.2. Funcionamiento de SolarWinds
- 23.9.3. Instalación de SolarWinds

23.10. Normativa sobre monitorización
- 23.10.1. Controles CIS sobre auditoria y registro
- 23.10.2. NIST 800-123 (EEUU)

Módulo 24. Seguridad en comunicaciones de dispositivos Iot

24.1. De la telemetría al IoT
- 24.1.1. Telemetría
- 24.1.2. Conectividad M2M
- 24.1.3. Democratización de la telemetría

24.2. Modelos de referencia IoT
- 24.2.1. Modelo de referencia IoT
- 24.2.2. Arquitectura simplificada IoT

24.3. Vulnerabilidades de seguridad del IoT
- 24.3.1. Dispositivos IoT
- 24.3.2. Dispositivos IoT. Casuística de uso
- 24.3.3. Dispositivos IoT. Vulnerabilidades

24.4. Conectividad del IoT
- 24.4.1. Redes PAN, LAN, WAN
- 24.4.2. Tecnologías inalámbricas no IoT
- 24.4.3. Tecnologías inalámbricas LPWAN

24.5. Tecnologías LPWAN
- 24.5.1. El triángulo de hierro de las redes LPWAN
- 24.5.2. Bandas de frecuencia libres vs. Bandas licenciadas
- 24.5.3. Opciones de tecnologías LPWAN

24.6. Tecnología LoRaWAN
- 24.6.1. Tecnología LoRaWAN
- 24.6.2. Casos de uso LoRaWAN. Ecosistema
- 24.6.3. Seguridad en LoRaWAN

24.7. Tecnología Sigfox
- 24.7.1. Tecnología Sigfox
- 24.7.2. Casos de uso Sigfox. Ecosistema
- 24.7.3. Seguridad en Sigfox

24.8. Tecnología Celular IoT
- 24.8.1. Tecnología Celular IoT (NB-IoT y LTE-M)
- 24.8.2. Casos de uso Celular IoT. Ecosistema
- 24.8.3. Seguridad en Celular IoT

24.9. Tecnología WiSUN
- 24.9.1. Tecnología WiSUN
- 24.9.2. Casos de uso WiSUN. Ecosistema
- 24.9.3. Seguridad en WiSUN

24.10. Otras tecnologías IoT
- 24.10.1. Otras tecnologías IoT
- 24.10.2. Casos de uso y ecosistema de otras tecnologías IoT
- 24.10.3. Seguridad en otras tecnologías IoT

Módulo 25. Plan de continuidad del negocio asociado a la seguridad

25.1. Plan de continuidad de negocio
- 25.1.1. Los planes de continuidad de negocio (PCN)
- 25.1.2. Plan de continuidad de negocio (PCN). Aspectos clave
- 25.1.3. Plan de continuidad de negocio (PCN) para la valoración de la empresa

25.2. Métricas en un plan de continuidad de negocio (PCN)
- 25.2.1. *Recovery time objective* (RTO) y *recovery point objective* (RPO)
- 25.2.2. Tiempo máximo tolerable (MTD)
- 25.2.3. Niveles mínimos de recuperación (ROL)
- 25.2.4. Punto de recuperación objetivo (RPO)

25.3. Proyectos de continuidad. Tipología
- 25.3.1. Plan de continuidad de negocio (PCN)
- 25.3.2. Plan de continuidad de TIC (PCTIC)
- 25.3.3. Plan de recuperación ante desastres (PRD)

25.4. Gestión de riesgos asociada al PCN
- 25.4.1. Análisis de impacto sobre el negocio
- 25.4.2. Beneficios de la implantación de un PCN
- 25.4.3. Mentalidad basada en riesgos

25.5. Ciclo de vida de un plan de continuidad de negocio
- 25.5.1. Fase 1: Análisis de la organización
- 25.5.2. Fase 2: Determinación de la estrategia de continuidad
- 25.5.3. Fase 3: Respuesta a la contingencia
- 25.5.4. Fase 4: Prueba, mantenimiento y revisión

25.6. Fase del análisis de la organización de un PCN
- 25.6.1. Identificación de procesos en el alcance del PCN
- 25.6.2. Identificación de áreas críticas del negocio
- 25.6.3. Identificación de dependencias entre áreas y procesos
- 25.6.4. Determinación del MTD adecuado
- 25.6.5. Entregables. Creación de un plan

25.7. Fase de determinación de la estrategia de continuidad en un PCN
- 25.7.1. Roles en la fase de determinación de la estrategia
- 25.7.2. Tareas de la fase de determinación de la estrategia
- 25.7.3. Entregables

25.8. Fase de respuesta a la contingencia en un PCN
- 25.8.1. Roles en la fase de respuesta
- 25.8.2. Tareas en esta fase
- 25.8.3. Entregables

25.9. Fase de pruebas, mantenimiento y revisión de un PCN
- 25.9.1. Roles en la fase de pruebas, mantenimiento y revisión
- 25.9.2. Tareas en la fase de pruebas, mantenimiento y revisión
- 25.9.3. Entregables

25.10. Normas ISO asociadas a los planes de continuidad de negocio (PCN)
- 25.10.1. ISO 22301:2019
- 25.10.2. ISO 22313:2020
- 25.10.3. Otras normas ISO e internacionales relacionadas

Módulo 26. Política de Recuperación Práctica de Desastres de Seguridad

26.1. DRP. Plan de Recuperación de Desastres
- 26.1.1. Objetivo de un DRP
- 26.1.2. Beneficios de un DRP
- 26.1.3. Consecuencias de ausencia de un DRP y no actualizado

26.2. Guía para definir un DRP (Plan de Recuperación de Desastres)
- 26.2.1. Alcance y objetivos
- 26.2.2. Diseño de la estrategia de recuperación
- 26.2.3. Asignación de roles y responsabilidades
- 26.2.4. Realización de un Inventario de hardware, software y servicios
- 26.2.5. Tolerancia para tiempo de inactividad y pérdida de datos
- 26.2.6. Establecimiento de los tipos específicos de DRP's que se requieren
- 26.2.7. Realización de un Plan de formación, concienciación y comunicación

26.3. Alcance y objetivos de un DRP (Plan de Recuperación de Desastres)
- 26.3.1. Garantía de respuesta
- 26.3.2. Componentes tecnológicos
- 26.3.3. Alcance de la política de continuidad

26.4. Diseño de la Estrategia de un DRP (Recuperación de Desastre)
- 26.4.1. Estrategia de Recuperación de Desastre
- 26.4.2. Presupuesto
- 26.4.3. Recursos Humanos y Físicos
- 26.4.4. Posiciones gerenciales en riesgo
- 26.4.5. Tecnología
- 26.4.6. Datos

26.5. Continuidad de los procesos de la información
- 26.5.1. Planificación de la continuidad
- 26.5.2. Implantación de la continuidad
- 26.5.3. Verificación evaluación de la continuidad

26.6. Alcance de un BCP (Plan de Continuidad Empresarial)
- 26.6.1. Determinación de los procesos de mayor criticidad
- 26.6.2. Enfoque por activo
- 26.6.3. Enfoque por proceso

26.7. Implementación de los procesos garantizados de negocio
- 26.7.1. Actividades Prioritarias (AP)
- 26.7.2. Tiempos de recuperación ideales (TRI)
- 26.7.3. Estrategias de supervivencia

26.8. Análisis de la organización
- 26.8.1. Obtención de información
- 26.8.2. Análisis de impacto sobre negocio (BIA)
- 26.8.3. Análisis de riesgos en la organización

26.9. Respuesta a la contingencia
- 26.9.1. Plan de crisis
- 26.9.2. Planes operativos de recuperación de entornos
- 26.9.3. Procedimientos técnicos de trabajo o de incidentes

26.10. Norma Internacional ISO 27031 BCP
- 26.10.1. Objetivos
- 26.10.2. Términos y definiciones
- 26.10.3. Operación

Módulo 27. Implementación de políticas de seguridad física y ambiental en la empresa

27.1. Áreas seguras
- 27.1.1. Perímetro de seguridad física
- 27.1.2. Trabajo en áreas seguras
- 27.1.3. Seguridad de oficinas, despachos y recursos

27.2. Controles físicos de entrada
- 27.2.1. Políticas de control de acceso físico
- 27.2.2. Sistemas de control físico de entrada

27.3. Vulnerabilidades de accesos físicos
- 27.3.1. Principales vulnerabilidades físicas
- 27.3.2. Implementación de medidas de salvaguardas

27.4. Sistemas biométricos fisiológicos
- 27.4.1. Huella dactilar
- 27.4.2. Reconocimiento facial
- 27.4.3. Reconocimiento de iris y retina
- 27.4.4. Otros sistemas biométricos fisiológicos

27.5. Sistemas biométricos de comportamiento
- 27.5.1. Reconocimiento de firma
- 27.5.2. Reconocimiento de escritor
- 27.5.3. Reconocimiento de voz
- 27.5.4. Otros sistemas biométricos de comportamientos

27.6. Gestión de riesgos en biometría
- 27.6.1. Implementación de sistemas biométricos
- 27.6.2. Vulnerabilidades de los sistemas biométricos

27.7. Implementación de políticas en *hosts*
- 27.7.1. Instalación de suministro y seguridad de cableado
- 27.7.2. Emplazamiento de los equipos
- 27.7.3. Salida de los equipos fuera de las dependencias
- 27.7.4. Equipo informático desatendido y política de puesto despejado

27.8. Protección ambiental
- 27.8.1. Sistemas de protección ante incendios
- 27.8.2. Sistemas de protección ante seísmos
- 27.8.3. Sistemas de protección antiterremotos

27.9. Seguridad en centro de procesamiento de datos
- 27.9.1. Puertas de seguridad
- 27.9.2. Sistemas de videovigilancia (CCTV)
- 27.9.3. Control de seguridad

27.10. Normativa internacional de la seguridad física
- 27.10.1. IEC 62443-2-1 (europea)
- 27.10.2. NERC CIP-005-5 (EEUU)
- 27.10.3. NERC CIP-014-2 (EEUU)

Módulo 28. Políticas de comunicaciones seguras en la empresa

28.1. Gestión de la seguridad en las redes
- 28.1.1. Control y monitorización de red
- 28.1.2. Segregación de redes
- 28.1.3. Sistemas de seguridad en redes

28.2. Protocolos seguros de comunicación
- 28.2.1. Modelo TCP/IP
- 28.2.2. Protocolo IPSEC
- 28.2.3. Protocolo TLS

28.3. Protocolo TLS 1.3
- 28.3.1. Fases de un proceso TLS1.3
- 28.3.2. Protocolo *Handshake*
- 28.3.3. Protocolo de registro
- 28.3.4. Diferencias con TLS 1.2

28.4. Algoritmos criptográficos
- 28.4.1. Algoritmos criptográficos usados en comunicaciones
- 28.4.2. *Cipher-suites*
- 28.4.3. Algoritmos criptográficos permitidos para TLS 1.3

28.5. Funciones Digest
- 28.5.1. MD6
- 28.5.2. SHA

28.6. PKI. Infraestructura de clave pública
- 28.6.1. PKI y sus entidades
- 28.6.2. Certificado digital
- 28.6.3. Tipos de certificados digital

28.7. Comunicaciones de túnel y transporte
- 28.7.1. Comunicaciones túnel
- 28.7.2. Comunicaciones transporte
- 28.7.3. Implementación túnel cifrado

28.8. SSH. *Secure Shell*
- 28.8.1. SSH. Cápsula segura
- 28.8.2. Funcionamiento de SSH
- 28.8.3. Herramientas SSH

28.9. Auditoria de sistemas criptográficos
- 28.9.1. Pruebas de integridad
- 28.9.2. Testeo sistema criptográfico

28.10. Sistemas criptográficos
- 28.10.1. Vulnerabilidades sistemas criptográficos
- 28.10.2. Salvaguardas en criptografía

Módulo 29. Aspectos organizativos en política de seguridad de la información

29.1. Organización interna
- 29.1.1. Asignación de responsabilidades
- 29.1.2. Segregación de tareas
- 29.1.3. Contactos con autoridades
- 29.1.4. Seguridad de la información en gestión de proyectos

29.2. Gestión de activos
- 29.2.1. Responsabilidad sobre los activos
- 29.2.2. Clasificación de la información
- 29.2.3. Manejo de los soportes de almacenamiento

29.3. Políticas de seguridad en los procesos de negocio
- 29.3.1. Análisis de los procesos de negocio vulnerables
- 29.3.2. Análisis de impacto de negocio
- 29.3.3. Clasificación procesos respecto al impacto de negocio

29.4. Políticas de seguridad ligada a los Recursos Humanos
- 29.4.1. Antes de contratación
- 29.4.2. Durante la contratación
- 29.4.3. Cese o cambio de puesto de trabajo

29.5. Políticas de seguridad en dirección
- 29.5.1. Directrices de la dirección en seguridad de la información
- 29.5.2. BIA- Analizando el impacto
- 29.5.3. Plan de recuperación como política de seguridad

29.6. Adquisición y mantenimientos de los sistemas de información
- 29.6.1. Requisitos de seguridad de los sistemas de información
- 29.6.2. Seguridad en los datos de desarrollo y soporte
- 29.6.3. Datos de prueba

29.7. Seguridad con suministradores
- 29.7.1. Seguridad informática con suministradores
- 29.7.2. Gestión de la prestación del servicio con garantía
- 29.7.3. Seguridad en la cadena de suministro

29.8. Seguridad operativa
- 29.8.1. Responsabilidades en la operación
- 29.8.2. Protección contra código malicioso
- 29.8.3. Copias de seguridad
- 29.8.4. Registros de actividad y supervisión

29.9. Gestión de la seguridad y normativas
- 29.9.1. Cumplimiento de los requisitos legales
- 29.9.2. Revisiones en la seguridad de la información

29.10. Seguridad en la gestión para la continuidad de negocio
- 29.10.1. Continuidad de la seguridad de la información
- 29.10.2. Redundancias

Con este completísimo temario de TECH, te convertirás en un líder visionario que garantiza la protección a largo plazo de la organización”

04

Objetivos docentes

Este Grand Master tiene como objetivo capacitar líderes estratégicos capaces de gestionar la seguridad de la información en cualquier tipo de organización. Así, a lo largo del programa, los especialistas desarrollarán competencias para identificar, evaluar y mitigar riesgos cibernéticos, implementar políticas de seguridad efectivas. Además, se les proporcionará una comprensión profunda de las tecnologías emergentes y las mejores prácticas en arquitectura de seguridad, garantizando la protección de datos y la continuidad del negocio. También, el programa fomenta una visión empresarial integrada de la ciberseguridad, alineando las iniciativas con los objetivos corporativos y asegurando el cumplimiento de normativas internacionales.

En esta especialización 100% online encontrarás el material didáctico y las investigaciones más actualizadas del panorama universitario"

Objetivos generales

- Desarrollar habilidades para liderar la estrategia de ciberseguridad en organizaciones empresariales
- Aplicar principios de gestión de riesgos en la protección de la información y los sistemas tecnológicos
- Adquirir competencias en la implementación de políticas y marcos de seguridad cibernética
- Implementar estrategias de prevención y mitigación ante amenazas cibernéticas avanzadas
- Potenciar habilidades en la gestión de incidentes y respuesta ante ataques de ciberseguridad
- Diseñar estrategias de protección contra el ransomware y otros ataques cibernéticos disruptivos
- Fomentar habilidades en la implementación de planes de continuidad de negocio y recuperación ante desastres cibernéticos
- Poner en práctica enfoques de gestión de identidad y acceso (IAM) para controlar el acceso a sistemas y aplicaciones
- Optimizar competencias en la integración de soluciones de ciberseguridad en la infraestructura de TI de la empresa
- Crear estrategias de seguridad en la integración de tecnologías emergentes como la inteligencia artificial y el IoT

Objetivos específicos

Módulo 1. Ciberinteligencia y ciberseguridad

- Desarrollar las habilidades necesarias para implementar estrategias de ciberinteligencia y Ciberseguridad
- Proteger los sistemas informáticos ante amenazas cibernéticas mediante la recopilación, análisis y uso de inteligencia digital

Módulo 2. Seguridad en Host

- Capacitar en la implementación de medidas de seguridad en sistemas host
- Asegurar la protección de servidores y dispositivos frente a vulnerabilidades, *malware* y accesos no autorizados

Módulo 3. Seguridad en red (perimetral)

- Proporcionar los conocimientos necesarios para proteger las redes informáticas a nivel perimetral
- Manejar técnicas y herramientas de seguridad como firewalls, VPNs y sistemas de detección de intrusos

Módulo 4. Seguridad en *smartphones*

- Brindar una comprensión completa sobre la seguridad en dispositivos móviles
- Ahondar en la protección contra amenazas como *malware*, pérdida de datos y ataques a través de aplicaciones móviles

Módulo 5. Seguridad en IoT

- Capacitar en la implementación de políticas de seguridad para dispositivos IoT
- Proteger la infraestructura y los datos generados por dispositivos conectados a través de redes y plataformas IoT

Módulo 6. Hacking ético

- Desarrollar las competencias necesarias para realizar pruebas de penetración y auditorías de seguridad utilizando técnicas de hacking ético
- Ser capaz de identificar vulnerabilidades y prevenir ataque

Módulo 7. Ingeniería inversa

- Dominar técnicas de ingeniería inversa para analizar y comprender el funcionamiento de software y *hardware*
- Identificar posibles vulnerabilidades y soluciones de seguridad

Módulo 8. Desarrollo seguro

- Enseñar las mejores prácticas de desarrollo seguro de software
- Aplicar principios de seguridad durante todo el ciclo de vida del desarrollo para minimizar riesgos y vulnerabilidades en las aplicaciones

Módulo 9. Implementación práctica de políticas de seguridad en software y *hardware*

- Proporcionar los conocimientos necesarios para diseñar e implementar políticas de seguridad robustas en software y hardware
- Asegurar la protección contra amenazas internas y externas

Módulo 10. Análisis forense

- Desarrollar las competencias en el análisis forense digital
- Analizar la recolección, preservación y análisis de pruebas digitales en casos de incidentes de seguridad informática

Módulo 11. Seguridad en el diseño y desarrollo de sistemas
- Abordar la integración de medidas de seguridad desde las fases de diseño y desarrollo de sistemas informáticos
- Garantizar la protección contra posibles vulnerabilidades desde el inicio del proyecto

Módulo 12. Arquitecturas y modelos de seguridad de la información
- Proporcionar los conocimientos necesarios sobre las arquitecturas y modelos de seguridad de la información
- Diseñar e implementar sistemas robustos que protejan los datos y recursos de la organización

Módulo 13. Sistema de gestión de seguridad de información (SGSI)
- Implementar un Sistema de Gestión de Seguridad de la Información
- Proteger la información empresarial de manera efectiva, asegurando el cumplimiento de las normativas y buenas prácticas

Módulo 14. Gestión de la seguridad IT
- Brindar los conocimientos necesarios para gestionar de manera efectiva la seguridad en las infraestructuras tecnológicas de la empresa
- Minimizar los riesgos y garantizar la continuidad operativa

Módulo 15. Políticas de gestión de incidencias de seguridad
- Capacitar en la creación y aplicación de políticas eficaces para la gestión de incidencias de seguridad
- Establecer protocolos claros para la detección, análisis y respuesta ante brechas de seguridad

Módulo 16. Análisis de riesgos y entorno de seguridad IT
- Proporcionar los conocimientos necesarios para realizar un análisis de riesgos en el entorno de TI, identificando amenazas y vulnerabilidades
- Aplicar estrategias de mitigación para asegurar la infraestructura tecnológica

Módulo 17. Políticas de seguridad para el análisis de amenazas en sistemas informáticos
- Capacitar en el desarrollo de políticas de seguridad para identificar, analizar y mitigar las amenazas en los sistemas informáticos
- Usar herramientas y métodos adecuados para proteger los activos digitales de la organización

Módulo 18. Implementación práctica de políticas de seguridad ante ataques
- Implementar políticas de seguridad eficaces ante posibles ataques
- Asegurar la protección de los sistemas y la información crítica en la organización

Módulo 19. Criptografía en IT
- Enseñar los fundamentos y aplicaciones de la criptografía en el ámbito de la tecnología de la información
- Implementar algoritmos de cifrado y seguridad en la transmisión de datos

Módulo 20. Gestión de identidad y accesos en seguridad IT
- Desarrollar las habilidades necesarias para gestionar la identidad y los accesos en sistemas de TI
- Establecer políticas de autenticación y control de acceso para proteger los recursos y datos de la organización

Módulo 21. Seguridad en comunicaciones y operación software

- Capacitar en la protección de las comunicaciones digitales y en la implementación de medidas de seguridad en la operación de software
- Garantizar la confidencialidad, integridad y disponibilidad de la información

Módulo 22. Seguridad en entornos *cloud*

- Implementar políticas de seguridad en entornos de computación en la nube
- Asegurar que los datos y las aplicaciones sean protegidos contra accesos no autorizados y ataques

Módulo 23. Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información

- Capacitar en el uso de herramientas de monitoreo para evaluar la efectividad de las políticas de seguridad en los sistemas de información
- Profundizar en la detección temprana de vulnerabilidades y ataques

Módulo 24. Seguridad en comunicaciones de dispositivos Iot

- Desarrollar competencias en la implementación de medidas de seguridad para proteger las comunicaciones entre dispositivos IoT
- Minimizar los riesgos asociados con el intercambio de datos entre dispositivos conectados

Módulo 25. Plan de continuidad del negocio asociado a la seguridad

- desarrollar un plan de continuidad del negocio que garantice la protección y recuperación rápida de los sistemas
- Establecer protocolos para velar por los datos esenciales en caso de incidentes de seguridad

Módulo 26. Política de Recuperación Práctica de Desastres de Seguridad

- Crear políticas de recuperación ante desastres
- Asegurar la rápida restauración de los sistemas y la protección de los datos en caso de incidentes graves de seguridad

Módulo 27. Implementación de políticas de seguridad física y ambiental en la empresa

- Capacitar en la implementación de políticas de seguridad física y ambiental para proteger los recursos físicos de la organización
- Asegurar el entorno adecuado para el funcionamiento seguro de los sistemas tecnológicos

Módulo 28. Políticas de comunicaciones seguras en la empresa

- Brindar los conocimientos para desarrollar políticas de comunicaciones seguras dentro de la organización
- Proteger las redes y canales de comunicación contra el espionaje y las filtraciones de información

Módulo 29. Aspectos organizativos en política de seguridad de la información

- Proporcionar las herramientas necesarias para implementar políticas organizativas en la gestión de la seguridad de la información
- Establecer roles, responsabilidades y procesos adecuados para proteger los activos de información

05

Salidas profesionales

Al finalizar este itinerario académico los egresados de este Grand Master estarán plenamente capacitados para asumir roles clave en la protección y gestión de la seguridad de la información en diversas organizaciones. Además, podrán liderar estrategias de seguridad en empresas multinacionales, gestionando y mitigando riesgos cibernéticos. De igual manera, estarán preparados para ocupar puestos que requieren habilidades para liderar iniciativas de ciberseguridad y garantizar la protección de los activos digitales en cualquier sector.

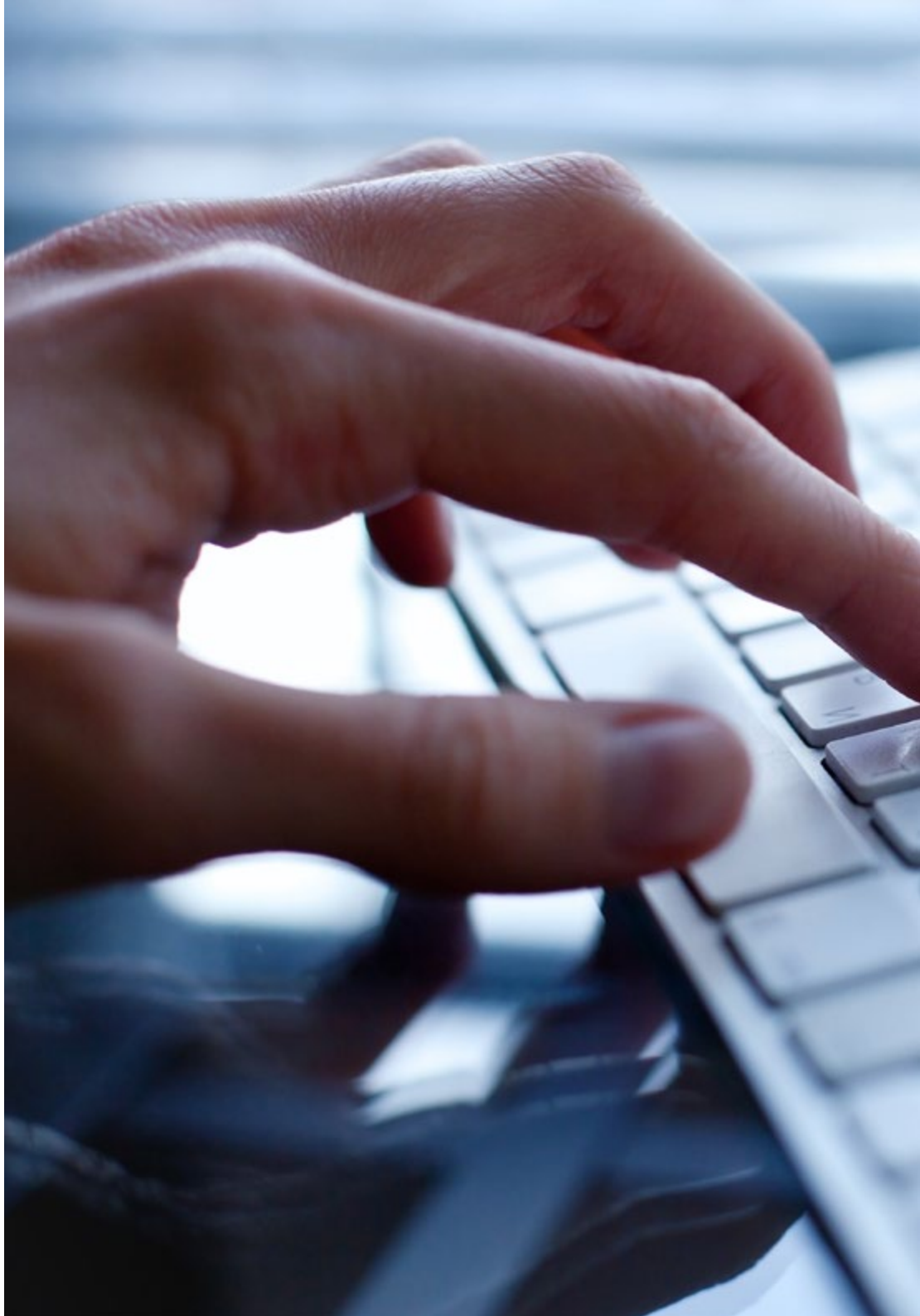
Con este Grand Master te especializarás como un Director capaz de anticipar los riesgos y proteger la información crítica"

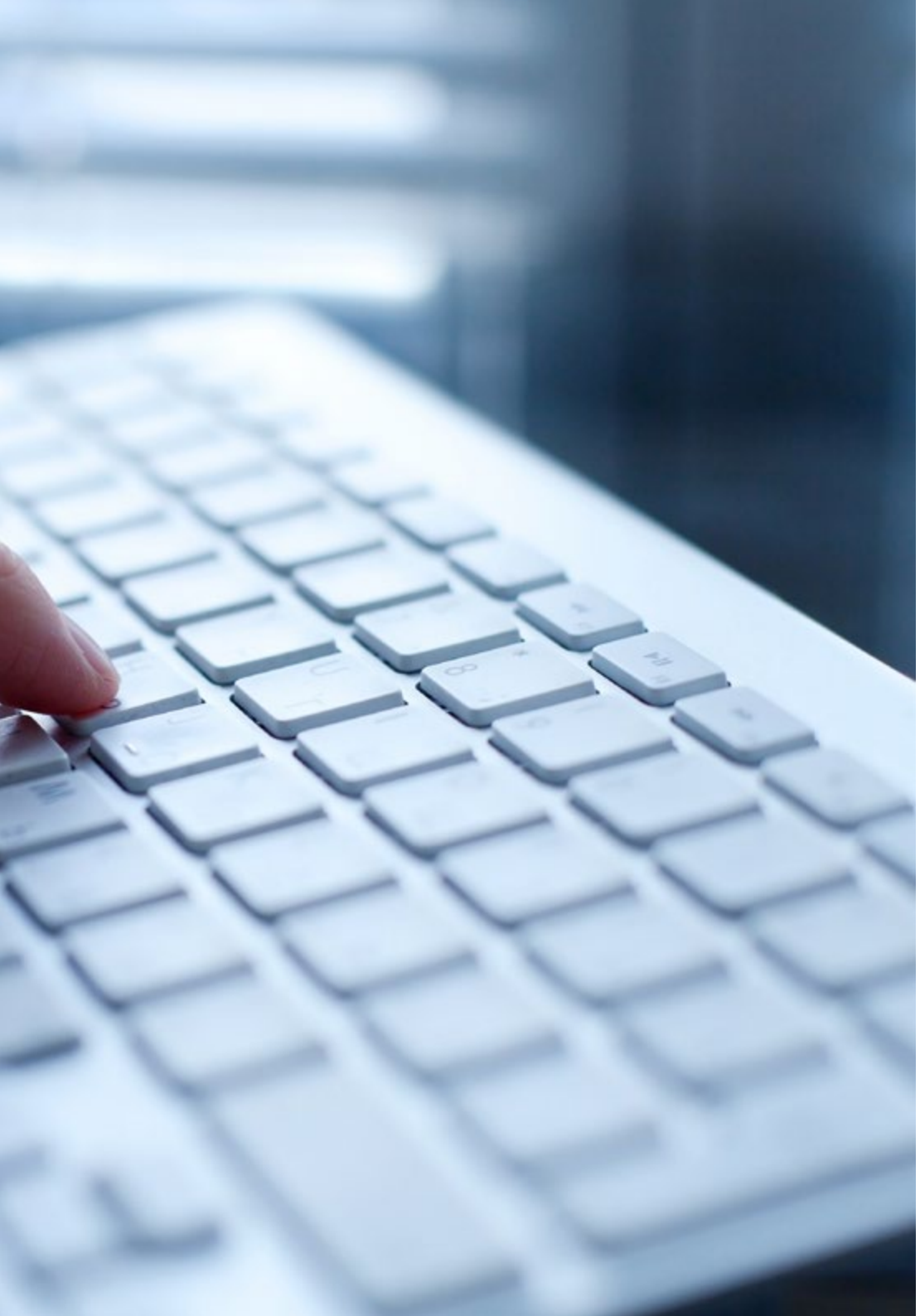
Perfil del egresado

El egresado será un líder informático estratégico con una profunda comprensión de la seguridad de la información en el contexto de organizaciones globales. Así, estará capacitado para diseñar e implementar políticas de seguridad avanzadas y liderar equipos multidisciplinarios. Asimismo, contará con sólidas habilidades de gestión y gobernanza, lo que le permitirá abordar los desafíos de la ciberseguridad en diversos sectores, garantizando la protección de los activos digitales. Por ello, esta oportunidad le proporcionará las herramientas necesarias para estar al tanto de las últimas tendencias tecnológicas y adaptarse a los rápidos cambios en el panorama digital.

Prepárate para ser uno de los mejores profesionales, minimizando el impacto de los ciberataques y recuperando la normalidad rápidamente.

- **Liderazgo estratégico y adaptabilidad:** liderar equipos multidisciplinarios y gestionar políticas de seguridad, adaptándose a los rápidos cambios tecnológicos y emergentes en ciberseguridad
- **Gestión de riesgos y toma de decisiones informadas:** identificar, evaluar y mitigar riesgos cibernéticos, tomando decisiones basadas en datos y análisis detallados
- **Análisis crítico y gestión de incidentes:** reconocer vulnerabilidades, gestionar incidentes de seguridad y coordinar la respuesta ante crisis, garantizando la continuidad del negocio
- **Comunicación efectiva y pensamiento estratégico:** comunicar riesgos y soluciones de forma clara a diferentes stakeholders, adoptando un enfoque global y estratégico para la protección de activos digitales





Después de realizar el programa universitario, podrás desempeñar tus conocimientos y habilidades en los siguientes cargos:

1. **Chief Information Security Officer (CISO):** líder estratégico encargado de la protección de la información y la ciberseguridad en toda la organización, desarrollando políticas y supervisando la infraestructura de seguridad digital.
2. **Director de Ciberseguridad:** responsable de la gestión y supervisión de los equipos de seguridad informática, desarrollando e implementando estrategias para proteger la infraestructura tecnológica de la empresa.
3. **Gerente de Seguridad Informática:** gestor y coordinador de las políticas de seguridad digital, supervisando la protección de datos y sistemas informáticos ante posibles amenazas.
4. **Consultor de Ciberseguridad:** asesor en empresas sobre la mejor manera de implementar y gestionar políticas de ciberseguridad, ayudando a mitigar riesgos y cumpliendo con normativas internacionales.
5. **Gerente de Gestión de Riesgos Informáticos:** encargado de identificar, evaluar y mitigar los riesgos cibernéticos que puedan afectar la seguridad de la información y los sistemas tecnológicos de la organización.
6. **Jefe de Seguridad de la Información:** supervisor y coordinador de todas las iniciativas relacionadas con la protección de los datos y sistemas informáticos dentro de la organización.
7. **Especialista en Pruebas de Penetración (Pentester):** encargado de realizar pruebas de intrusión controladas para identificar vulnerabilidades en sistemas, redes y aplicaciones.
8. **Analista de Ingeniería Inversa en Ciberseguridad:** responsable de desensamblar y analizar software malicioso o desconocido para descubrir su funcionamiento interno, detectar vulnerabilidades, y desarrollar medidas de protección y parches de seguridad.

06

Licencias de software incluidas

TECH es referencia en el mundo universitario por combinar la última tecnología con las metodologías docentes para potenciar el proceso de enseñanza-aprendizaje. Para ello, ha establecido una red de alianzas que le permite tener acceso a las herramientas de software más avanzadas del mundo profesional.

Al matricularte recibirás, de forma completamente gratuita, las credenciales de uso académico de las siguientes aplicaciones de software profesional”

TECH ha establecido una red de alianzas profesionales en la que se encuentran los principales proveedores de software aplicado a las diferentes áreas profesionales. Estas alianzas permiten a TECH tener acceso al uso de centenares de aplicaciones informáticas y licencias de software para acercarlas a sus estudiantes.

Las licencias de software para uso académico permitirán a los estudiantes utilizar las aplicaciones informáticas más avanzadas en su área profesional, de modo que podrán conocerlas y aprender su dominio sin tener que incurrir en costes. TECH se hará cargo del procedimiento de contratación para que los alumnos puedan utilizarlas de modo ilimitado durante el tiempo que estén estudiando el programa de Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer), y además lo podrán hacer de forma completamente gratuita.

TECH te dará acceso gratuito al uso de las siguientes aplicaciones de software:

Google Career Launchpad

Google Career Launchpad es una solución para desarrollar habilidades digitales en tecnología y análisis de datos. Con un valor estimado de **5.000 dólares**, se incluye de forma **gratuita** en el programa universitario de TECH, brindando acceso a laboratorios interactivos y certificaciones reconocidas en el sector.

Esta plataforma combina capacitación técnica con casos prácticos, usando tecnologías como BigQuery y Google AI. Ofrece entornos simulados para experimentar con datos reales, junto a una red de expertos para orientación personalizada.

Funcionalidades destacadas:

- **Cursos especializados:** contenido actualizado en cloud computing, machine learning y análisis de datos
- **Laboratorios en vivo:** prácticas con herramientas reales de Google Cloud sin configuración adicional
- **Certificaciones integradas:** preparación para exámenes oficiales con validez internacional
- **Mentorías profesionales:** sesiones con expertos de Google y partners tecnológicos
- **Proyectos colaborativos:** retos basados en problemas reales de empresas líderes

En conclusión, **Google Career Launchpad** conecta a los usuarios con las últimas tecnologías del mercado, facilitando su inserción en áreas como inteligencia artificial y ciencia de datos con credenciales respaldadas por la industria.

Gracias a TECH podrás utilizar gratuitamente las mejores aplicaciones de software de tu área profesional”

07

Metodología de estudio

TECH es la primera universidad en el mundo que combina la metodología de los ***case studies*** con el ***Relearning***, un sistema de aprendizaje 100% online basado en la reiteración dirigida.

Esta disruptiva estrategia pedagógica ha sido concebida para ofrecer a los profesionales la oportunidad de actualizar conocimientos y desarrollar competencias de un modo intensivo y riguroso. Un modelo de aprendizaje que coloca al estudiante en el centro del proceso académico y le otorga todo el protagonismo, adaptándose a sus necesidades y dejando de lado las metodologías más convencionales.

TECH te prepara para afrontar nuevos retos en entornos inciertos y lograr el éxito en tu carrera"

El alumno: la prioridad de todos los programas de TECH

En la metodología de estudios de TECH el alumno es el protagonista absoluto. Las herramientas pedagógicas de cada programa han sido seleccionadas teniendo en cuenta las demandas de tiempo, disponibilidad y rigor académico que, a día de hoy, no solo exigen los estudiantes sino los puestos más competitivos del mercado.

Con el modelo educativo asincrónico de TECH, es el alumno quien elige el tiempo que destina al estudio, cómo decide establecer sus rutinas y todo ello desde la comodidad del dispositivo electrónico de su preferencia. El alumno no tendrá que asistir a clases en vivo, a las que muchas veces no podrá acudir. Las actividades de aprendizaje las realizará cuando le venga bien. Siempre podrá decidir cuándo y desde dónde estudiar.

"En TECH NO tendrás clases en directo (a las que luego nunca puedes asistir)"

Los planes de estudios más exhaustivos a nivel internacional

TECH se caracteriza por ofrecer los itinerarios académicos más completos del entorno universitario. Esta exhaustividad se logra a través de la creación de temarios que no solo abarcan los conocimientos esenciales, sino también las innovaciones más recientes en cada área.

Al estar en constante actualización, estos programas permiten que los estudiantes se mantengan al día con los cambios del mercado y adquieran las habilidades más valoradas por los empleadores. De esta manera, quienes finalizan sus estudios en TECH reciben una preparación integral que les proporciona una ventaja competitiva notable para avanzar en sus carreras.

Y además, podrán hacerlo desde cualquier dispositivo, pc, tableta o smartphone.

El modelo de TECH es asincrónico, de modo que te permite estudiar con tu pc, tableta o tu smartphone donde quieras, cuando quieras y durante el tiempo que quieras”

Case studies o Método del caso

El método del caso ha sido el sistema de aprendizaje más utilizado por las mejores escuelas de negocios del mundo. Desarrollado en 1912 para que los estudiantes de Derecho no solo aprendiesen las leyes a base de contenidos teóricos, su función era también presentarles situaciones complejas reales. Así, podían tomar decisiones y emitir juicios de valor fundamentados sobre cómo resolverlas. En 1924 se estableció como método estándar de enseñanza en Harvard.

Con este modelo de enseñanza es el propio alumno quien va construyendo su competencia profesional a través de estrategias como el *Learning by doing* o el *Design Thinking*, utilizadas por otras instituciones de renombre como Yale o Stanford.

Este método, orientado a la acción, será aplicado a lo largo de todo el itinerario académico que el alumno emprenda junto a TECH. De ese modo se enfrentará a múltiples situaciones reales y deberá integrar conocimientos, investigar, argumentar y defender sus ideas y decisiones. Todo ello con la premisa de responder al cuestionamiento de cómo actuaría al posicionarse frente a eventos específicos de complejidad en su labor cotidiana.

Método *Relearning*

En TECH los *case studies* son potenciados con el mejor método de enseñanza 100% online: el *Relearning*.

Este método rompe con las técnicas tradicionales de enseñanza para poner al alumno en el centro de la ecuación, proveyéndole del mejor contenido en diferentes formatos. De esta forma, consigue repasar y reiterar los conceptos clave de cada materia y aprender a aplicarlos en un entorno real.

En esta misma línea, y de acuerdo a múltiples investigaciones científicas, la reiteración es la mejor manera de aprender. Por eso, TECH ofrece entre 8 y 16 repeticiones de cada concepto clave dentro de una misma lección, presentada de una manera diferente, con el objetivo de asegurar que el conocimiento sea completamente afianzado durante el proceso de estudio.

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

Un Campus Virtual 100% online con los mejores recursos didácticos

Para aplicar su metodología de forma eficaz, TECH se centra en proveer a los egresados de materiales didácticos en diferentes formatos: textos, vídeos interactivos, ilustraciones y mapas de conocimiento, entre otros. Todos ellos, diseñados por profesores cualificados que centran el trabajo en combinar casos reales con la resolución de situaciones complejas mediante simulación, el estudio de contextos aplicados a cada carrera profesional y el aprendizaje basado en la reiteración, a través de audios, presentaciones, animaciones, imágenes, etc.

Y es que las últimas evidencias científicas en el ámbito de las Neurociencias apuntan a la importancia de tener en cuenta el lugar y el contexto donde se accede a los contenidos antes de iniciar un nuevo aprendizaje. Poder ajustar esas variables de una manera personalizada favorece que las personas puedan recordar y almacenar en el hipocampo los conocimientos para retenerlos a largo plazo. Se trata de un modelo denominado *Neurocognitive context-dependent e-learning* que es aplicado de manera consciente en esta titulación universitaria.

Por otro lado, también en aras de favorecer al máximo el contacto mentor-alumno, se proporciona un amplio abanico de posibilidades de comunicación, tanto en tiempo real como en diferido (mensajería interna, foros de discusión, servicio de atención telefónica, email de contacto con secretaría técnica, chat y videoconferencia).

Asimismo, este completísimo Campus Virtual permitirá que el alumnado de TECH organice sus horarios de estudio de acuerdo con su disponibilidad personal o sus obligaciones laborales. De esa manera tendrá un control global de los contenidos académicos y sus herramientas didácticas, puestas en función de su acelerada actualización profesional.

> *La modalidad de estudios online de este programa te permitirá organizar tu tiempo y tu ritmo de aprendizaje, adaptándolo a tus horarios”*

La eficacia del método se justifica con cuatro logros fundamentales:

1. Los alumnos que siguen este método no solo consiguen la asimilación de conceptos, sino un desarrollo de su capacidad mental, mediante ejercicios de evaluación de situaciones reales y aplicación de conocimientos.
2. El aprendizaje se concreta de una manera sólida en capacidades prácticas que permiten al alumno una mejor integración en el mundo real.
3. Se consigue una asimilación más sencilla y eficiente de las ideas y conceptos, gracias al planteamiento de situaciones que han surgido de la realidad.
4. La sensación de eficiencia del esfuerzo invertido se convierte en un estímulo muy importante para el alumnado, que se traduce en un interés mayor en los aprendizajes y un incremento del tiempo dedicado a trabajar en el curso.

La metodología universitaria mejor valorada por sus alumnos

Los resultados de este innovador modelo académico son constatables en los niveles de satisfacción global de los egresados de TECH.

La valoración de los estudiantes sobre la calidad docente, calidad de los materiales, estructura del curso y sus objetivos es excelente. No en valde, la institución se convirtió en la universidad mejor valorada por sus alumnos según el índice global score, obteniendo un 4,9 de 5.

Accede a los contenidos de estudio desde cualquier dispositivo con conexión a Internet (ordenador, tablet, smartphone) gracias a que TECH está al día de la vanguardia tecnológica y pedagógica.

Podrás aprender con las ventajas del acceso a entornos simulados de aprendizaje y el planteamiento de aprendizaje por observación, esto es, Learning from an expert.

Así, en este programa estarán disponibles los mejores materiales educativos, preparados a conciencia:

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 que creará nuestra manera de trabajo online, con las técnicas más novedosas que nos permiten ofrecerte una gran calidad, en cada una de las piezas que pondremos a tu servicio.

Prácticas de habilidades y competencias

Realizarás 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.

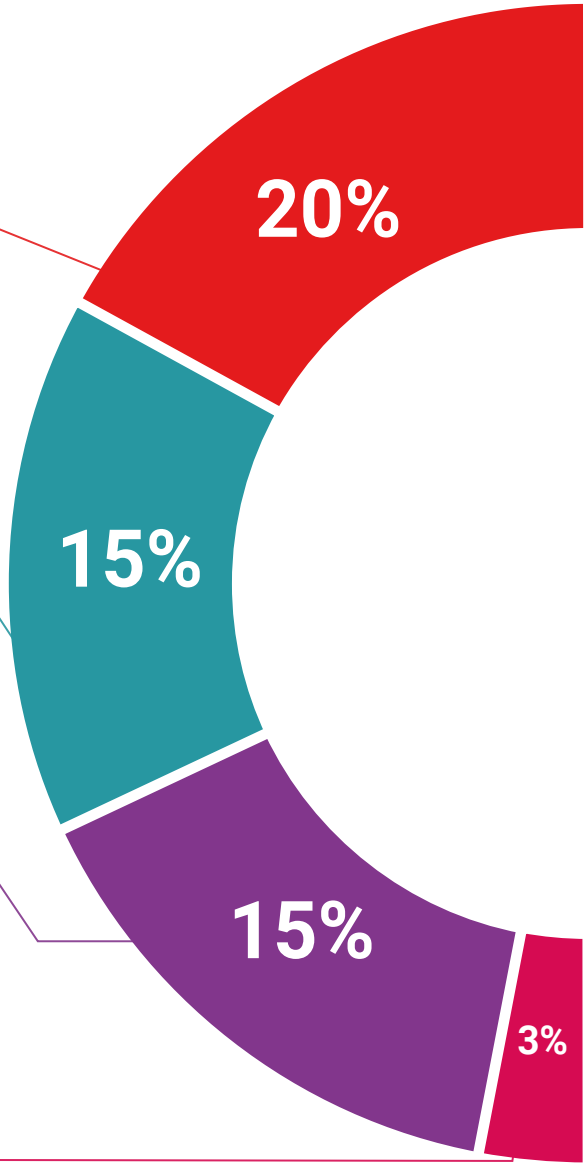
Resúmenes interactivos

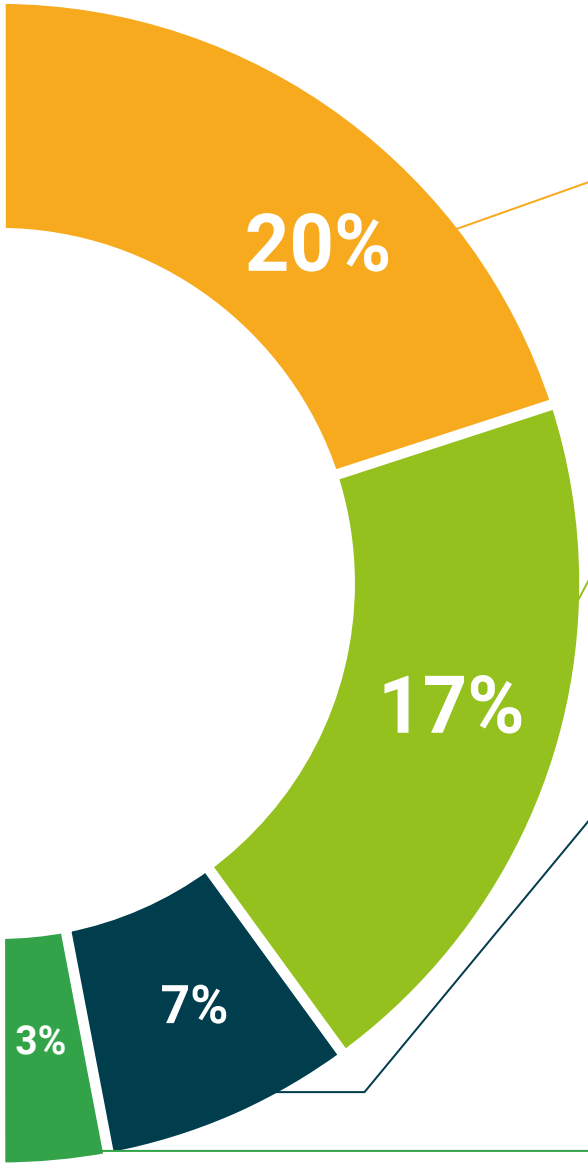
Presentamos los contenidos de manera atractiva y dinámica en píldoras multimedia que incluyen audio, vídeos, imágenes, esquemas y mapas conceptuales con el fin de afianzar el conocimiento.

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

Lecturas complementarias

Artículos recientes, documentos de consenso, guías internacionales... En nuestra biblioteca virtual tendrás acceso a todo lo que necesitas para completar tu capacitación.





Case Studies

Completarás una selección de los mejores *case studies* de la materia. Casos presentados, analizados y tutorizados por los mejores especialistas del panorama internacional.

Testing & Retesting

Evaluamos y reevaluamos periódicamente tu conocimiento a lo largo del programa. Lo hacemos sobre 3 de los 4 niveles de la Pirámide de Miller.

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 nuestras futuras decisiones difíciles.

Guías rápidas de actuación

TECH ofrece los contenidos más relevantes del curso en forma de fichas o guías rápidas de actuación. Una manera sintética, práctica y eficaz de ayudar al estudiante a progresar en su aprendizaje.

08

Cuadro docente

Este Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer), cuenta con un cuadro docente compuesto por profesionales en activo que conocen a la perfección el estado actual de esta área, y que trasladarán, por tanto, todas las claves de la ciberseguridad actual al informático. De este modo, se garantiza que el estudiante de este programa universitario obtenga los últimos avances en este campo, al poder acceder a ellos gracias al prestigioso profesorado que ha seleccionado TECH.

TECH te ofrece los Directores y Docentes más especializados para que tu enfoque y aprendizaje sea el mejor”

Director Invitado Internacional

El Doctor Frederic Lemieux es reconocido a nivel internacional como experto innovador y líder inspirador en los campos de la **Inteligencia**, **Seguridad Nacional**, **Seguridad Interna**, **Ciberseguridad** y **Tecnologías Disruptivas**. Y es que su constante dedicación y relevantes aportaciones en Investigación y Educación, le posicionan como una figura clave en la **promoción de la seguridad** y el **entendimiento de las tecnologías emergentes** en la actualidad. Durante su trayectoria profesional, ha conceptualizado y dirigido programas académicos de vanguardia en diversas instituciones de renombre, como la **Universidad de Montreal**, la **Universidad George Washington** y la **Universidad de Georgetown**.

A lo largo de su extenso bagaje, ha publicado múltiples libros de gran relevancia, todos ellos relacionados con la **inteligencia criminal**, la **labor policial**, las **amenazas cibernéticas** y la **seguridad internacional**. Asimismo, ha contribuido de manera significativa al campo de la **Ciberseguridad** con la publicación de numerosos artículos en revistas académicas, las cuales examinan el control del crimen durante desastres importantes, la lucha contra el terrorismo, las agencias de inteligencia y la cooperación policial. Además, ha sido panelista y ponente principal en diversas conferencias nacionales e internacionales, consolidándose como un referente en el ámbito académico y profesional.

El Doctor Lemieux ha desempeñado roles editoriales y evaluativos en diferentes organizaciones académicas, privadas y gubernamentales, reflejando su influencia y compromiso con la excelencia en su campo de especialización. De esta forma, su prestigiosa carrera académica lo ha llevado a desempeñarse como Profesor de Prácticas y Director de Facultad de los programas MPS en **Inteligencia Aplicada**, **Gestión de Riesgos en Ciberseguridad**, **Gestión Tecnológica** y **Gestión de Tecnologías de la Información** en la **Universidad de Georgetown**.

Dr. Lemieux, Frederic

- Director del Máster en Cybersecurity Risk Management en Georgetown, Washington, Estados Unidos
- Director del Máster en Technology Management en la Universidad de Georgetown
- Director del Máster en Applied Intelligence en la Universidad de Georgetown
- Profesor de Prácticas en la Universidad de Georgetown
- Doctor en Criminología por la School of Criminology en la Universidad de Montreal
- Licenciado en Sociología y Minor Degree en Psicología por la Universidad de Laval
- Miembro de: New Program Roundtable Committee, Universidad de Georgetown

Gracias a TECH podrás aprender con los mejores profesionales del mundo"

Directora Invitada Internacional

Con más de 20 años de experiencia en el diseño y la dirección de equipos globales de **adquisición de talento**, Jennifer Dove es experta en **contratación** y **estrategia tecnológica**. A lo largo de su experiencia profesional ha ocupado puestos directivos en varias organizaciones tecnológicas dentro de empresas de la lista ***Fortune* 50**, como **NBCUniversal** y **Comcast**. Su trayectoria le ha permitido destacar en entornos competitivos y de alto crecimiento.

Como **Vicepresidenta de Adquisición de Talento** en **Mastercard**, se encarga de supervisar la estrategia y la ejecución de la incorporación de talento, colaborando con los líderes empresariales y los responsables de **Recursos Humanos** para cumplir los objetivos operativos y estratégicos de contratación. En especial, su finalidad es **crear equipos diversos**, **inclusivos** y **de alto rendimiento** que impulsen la innovación y el crecimiento de los productos y servicios de la empresa. Además, es experta en el uso de herramientas para atraer y retener a los mejores profesionales de todo el mundo. También se encarga de **amplificar** la **marca de empleador** y la propuesta de valor de **Mastercard** a través de publicaciones, eventos y redes sociales.

Jennifer Dove ha demostrado su compromiso con el desarrollo profesional continuo, participando activamente en redes de profesionales de **Recursos Humanos** y contribuyendo a la incorporación de numerosos trabajadores a diferentes empresas. Tras obtener su licenciatura en **Comunicación Organizacional** por la Universidad de **Miami**, ha ocupado cargos directivos de selección de personal en empresas de diversas áreas.

Por otra parte, ha sido reconocida por su habilidad para liderar transformaciones organizacionales, **integrar tecnologías** en los **procesos de reclutamiento** y desarrollar programas de liderazgo que preparan a las instituciones para los desafíos futuros. También ha implementado con éxito programas de **bienestar laboral** que han aumentado significativamente la satisfacción y retención de empleados.

Dña. Dove, Jennifer

- Vicepresidenta de Adquisición de Talentos en Mastercard, Nueva York, Estados Unidos
- Directora de Adquisición de Talentos en NBCUniversal Media, Nueva York, Estados Unidos
- Responsable de Selección de Personal Comcast
- Directora de Selección de Personal en Rite Hire Advisory
- Vicepresidenta Ejecutiva de la División de Ventas en Ardor NY Real Estate
- Directora de Selección de Personal en Valerie August & Associates
- Ejecutiva de Cuentas en BNC
- Ejecutiva de Cuentas en Vault
- Graduada en Comunicación Organizacional por la Universidad de Miami

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

Director Invitado Internacional

Líder tecnológico con décadas de experiencia en las **principales multinacionales tecnológicas**, Rick Gauthier se ha desarrollado de forma prominente en el campo de los **servicios** en la **nube** y mejora de procesos de extremo a extremo. Ha sido reconocido como un líder y responsable de equipos con gran eficiencia, mostrando un talento natural para garantizar un alto nivel de compromiso entre sus trabajadores.

Posee dotes innatas en la estrategia e innovación ejecutiva, desarrollando nuevas ideas y respaldando su éxito con datos de calidad. Su trayectoria en **Amazon** le ha permitido administrar e integrar los servicios informáticos de la compañía en Estados Unidos. En **Microsoft** ha liderado un equipo de 104 personas, encargadas de proporcionar infraestructura informática a nivel corporativo y apoyar a departamentos de ingeniería de productos en toda la compañía.

Esta experiencia le ha permitido destacarse como un directivo de alto impacto, con habilidades notables para aumentar la eficiencia, productividad y satisfacción general del cliente.

D. Gauthier, Rick

- Director regional de IT en Amazon, Seattle, Estados Unidos
- Jefe de programas sénior en Amazon
- Vicepresidente de Wimmer Solutions
- Director sénior de servicios de ingeniería productiva en Microsoft
- Titulado en Ciberseguridad por Western Governors University
- Certificado Técnico en *Commercial Diving* por Divers Institute of Technology
- Titulado en Estudios Ambientales por The Evergreen State College

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

Director Invitado Internacional

Romi Arman es un reputado experto internacional con más de dos décadas de experiencia en **Transformación Digital**, **Marketing**, **Estrategia** y **Consultoría**. A través de esa extendida trayectoria, ha asumido diferentes riesgos y es un permanente **defensor** de la **innovación** y el **cambio** en la coyuntura empresarial. Con esa experticia, ha colaborado con directores generales y organizaciones corporativas de todas partes del mundo, empujándoles a dejar de lado los modelos tradicionales de negocios. Así, ha contribuido a que compañías como la energética Shell se conviertan en **verdaderos líderes del mercado**, centradas en sus **clientes** y el **mundo digital**.

Las estrategias diseñadas por Arman tienen un impacto latente, ya que han permitido a varias corporaciones **mejorar las experiencias de los consumidores**, **el personal** y **los accionistas** por igual. El éxito de este experto es cuantificable a través de métricas tangibles como el **CSAT**, el **compromiso de los empleados** en las instituciones donde ha ejercido y el crecimiento del **indicador financiero EBITDA** en cada una de ellas.

También, en su recorrido profesional ha nutrido y **liderado equipos de alto rendimiento** que, incluso, han recibido galardones por su **potencial transformador**. Con Shell, específicamente, el ejecutivo se ha propuesto siempre superar tres retos: **satisfacer** las complejas **demandas** de **descarbonización** de los clientes, **apoyar** una **"descarbonización rentable"** y **revisar** un panorama fragmentado de **datos**, **digital y tecnológico**. Así, sus esfuerzos han evidenciado que para lograr un éxito sostenible es fundamental partir de las necesidades de los consumidores y sentar las bases de la transformación de los procesos, los datos, la tecnología y la cultura.

Por otro lado, el directivo destaca por su dominio de las **aplicaciones empresariales** de la **Inteligencia Artificial**, temática en la que cuenta con un posgrado de la Escuela de Negocios de Londres. Al mismo tiempo, ha acumulado experiencias en **IoT** y el **Salesforce**.

D. Arman, Romi

- Director de Transformación Digital (CDO) en la Corporación Energética Shell, Londres, Reino Unido
- Director Global de Comercio Electrónico y Atención al Cliente en la Corporación Energética Shell
- Gestor Nacional de Cuentas Clave (fabricantes de equipos originales y minoristas de automoción) para Shell en Kuala Lumpur, Malasia
- Consultor Sénior de Gestión (Sector Servicios Financieros) para Accenture desde Singapur
- Licenciado en la Universidad de Leeds
- Posgrado en Aplicaciones Empresariales de la IA para Altos Ejecutivos de la Escuela de Negocios de Londres
- Certificación Profesional en Experiencia del Cliente CCXP
- Curso de Transformación Digital Ejecutiva por IMD

¿Deseas actualizar tus conocimientos con la más alta calidad educativa? TECH te ofrece el contenido más actualizado del mercado académico, diseñado por auténticos expertos de prestigio internacional"

Director Invitado Internacional

Manuel Arens es un **experimentado profesional** en el manejo de datos y líder de un equipo altamente cualificado. De hecho, Arens ocupa el cargo de **gerente global de compras** en la división de Infraestructura Técnica y Centros de Datos de Google, empresa en la que ha desarrollado la mayor parte de su carrera profesional. Con base en Mountain View, California, ha proporcionado soluciones para los desafíos operativos del gigante tecnológico, tales como la **integridad de los datos maestros**, las **actualizaciones de datos de proveedores** y la **priorización** de los mismos. Ha liderado la planificación de la cadena de suministro de centros de datos y la evaluación de riesgos del proveedor, generando mejoras en el proceso y la gestión de flujos de trabajo que han resultado en ahorros de costos significativos.

Con más de una década de trabajo proporcionando soluciones digitales y liderazgo para empresas en diversas industrias, tiene una amplia experiencia en todos los aspectos de la prestación de soluciones estratégicas, incluyendo **Marketing**, **análisis de medios**, **medición** y **atribución**. De hecho, ha recibido varios reconocimientos por su labor, entre ellos el **Premio al Liderazgo BIM**, el **Premio a la Liderazgo Search**, **Premio al Programa de Generación de Leads de Exportación** y el **Premio al Mejor Modelo de Ventas de EMEA**.

Asimismo, Arens se desempeñó como **Gerente de Ventas** en Dublín, Irlanda. En este puesto, construyó un equipo de 4 a 14 miembros en tres años y lideró al equipo de ventas para lograr resultados y colaborar bien entre sí y con equipos interfuncionales. También ejerció como **Analista Sénior** de Industria, en Hamburgo, Alemania, creando storylines para más de 150 clientes utilizando herramientas internas y de terceros para apoyar el análisis. Desarrolló y redactó informes en profundidad para demostrar su dominio del tema, incluyendo la comprensión de los **factores macroeconómicos** y **políticos/regulatorios** que afectan la adopción y difusión de la tecnología.

También ha liderado equipos en empresas como **Eaton**, **Airbus** y **Siemens**, en los que adquirió valiosa experiencia en gestión de cuentas y cadena de suministro. Destaca especialmente su labor para superar continuamente las expectativas mediante la **construcción de valiosas relaciones con los clientes** y **trabajar de forma fluida con personas en todos los niveles de una organización**, incluyendo stakeholders, gestión, miembros del equipo y clientes. Su enfoque impulsado por los datos y su capacidad para desarrollar soluciones innovadoras y escalables para los desafíos de la industria lo han convertido en un líder prominente en su campo.

D. Arens, Manuel

- Gerente Global de Compras en Google, Mountain View, Estados Unidos
- Responsable principal de Análisis y Tecnología B2B en Google, Estados Unidos
- Director de ventas en Google, Irlanda
- Analista Industrial Sénior en Google, Alemania
- Gestor de cuentas en Google, Irlanda
- Accounts Payable en Eaton, Reino Unido
- Gestor de Cadena de Suministro en Airbus, Alemania

¡Apuesta por TECH! Podrás acceder a los mejores materiales didácticos, a la vanguardia tecnológica y educativa, implementados por reconocidos especialistas de renombre internacional en la materia"

Director Invitado Internacional

Andrea La Sala es un **experimentado ejecutivo** del **Marketing** cuyos proyectos han tenido un **significativo impacto** en el **entorno de la Moda**. A lo largo de su exitosa carrera ha desarrollado disímiles tareas relacionadas con **Productos**, **Merchandising** y **Comunicación**. Todo ello, ligado a marcas de prestigio como **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein**, entre otras.

Los resultados de este directivo de **alto perfil internacional** han estado vinculados a su probada capacidad para **sintetizar información** en marcos claros y ejecutar **acciones concretas** alineadas a objetivos **empresariales específicos**. Además, es reconocido por su **proactividad** y **adaptación a ritmos acelerados** de trabajo. A todo ello, este experto adiciona una **fuerte conciencia comercial**, **visión de mercado** y una **auténtica pasión** por los **productos**.

Como **Director Global de Marca y Merchandising** en **Giorgio Armani**, ha supervisado disímiles **estrategias de Marketing** para **ropas** y **accesorios**. Asimismo, sus tácticas han estado centradas en el **ámbito minorista** y las **necesidades** y el **comportamiento del consumidor**. Desde este puesto, La Sala también ha sido responsable de configurar la comercialización de productos en diferentes mercados, actuando como **jefe de equipo** en los **departamentos de Diseño**, **Comunicación** y **Ventas**.

Por otro lado, en empresas como **Calvin Klein** o el **Gruppo Coin**, ha emprendido proyectos para impulsar la **estructura**, el **desarrollo** y la **comercialización** de **diferentes colecciones**. A su vez, ha sido encargado de crear **calendarios eficaces** para las **campañas** de compra y venta. Igualmente, ha tenido bajo su dirección los **términos**, **costes**, **procesos** y **plazos de entrega** de diferentes operaciones.

Estas experiencias han convertido a Andrea La Sala en uno de los principales y más cualificados **líderes corporativos** de la **Moda** y el **Lujo**. Una alta capacidad directiva con la que ha logrado implementar de manera eficaz el **posicionamiento positivo** de **diferentes marcas** y redefinir sus indicadores clave de rendimiento (KPI).

D. La Sala, Andrea

- Director Global de Marca y Merchandising Armani Exchange en Giorgio Armani, Milán, Italia
- Director de Merchandising en Calvin Klein
- Responsable de Marca en Gruppo Coin
- Brand Manager en Dolce&Gabbana
- Brand Manager en Sergio Tacchini S.p.A.
- Analista de Mercado en Fastweb
- Graduado de Business and Economics en la Università degli Studi del Piemonte Orientale

Los profesionales más cualificados y experimentados a nivel internacional te esperan en TECH para ofrecerte una enseñanza de primer nivel, actualizada y basada en la última evidencia científica. ¿A qué esperas para matricularte?"

Director Invitado Internacional

Mick Gram es sinónimo de innovación y excelencia en el campo de la **Inteligencia Empresarial** a nivel internacional. Su exitosa carrera se vincula a puestos de liderazgo en multinacionales como **Walmart** y **Red Bull**. Asimismo, este experto destaca por su visión para **identificar tecnologías emergentes** que, a largo plazo, alcanzan un impacto imperecedero en el entorno corporativo.

Por otro lado, el ejecutivo es considerado un **pionero** en el **empleo de técnicas de visualización de datos** que simplificaron conjuntos complejos, haciéndolos accesibles y facilitadores de la toma de decisiones. Esta habilidad se convirtió en el pilar de su perfil profesional, transformándolo en un deseado activo para muchas organizaciones que apostaban por **recopilar información** y **generar acciones** concretas a partir de ellos.

Uno de sus proyectos más destacados de los últimos años ha sido la **plataforma Walmart Data Cafe**, la más grande de su tipo en el mundo que está anclada en la nube destinada al **análisis** de ***Big Data***. Además, ha desempeñado el cargo de **Director** de ***Business Intelligence*** en **Red Bull**, abarcando áreas como **Ventas**, **Distribución**, **Marketing** y **Operaciones de Cadena de Suministro**. Su equipo fue reconocido recientemente por su innovación constante en cuanto al uso de la nueva API de Walmart Luminate para *insights* de Compradores y Canales.

En cuanto a su formación, el directivo cuenta con varios Másteres y estudios de posgrado en centros de prestigio como la **Universidad de Berkeley**, en Estados Unidos, y la **Universidad de Copenhague**, en Dinamarca. A través de esa actualización continua, el experto ha alcanzado competencias de vanguardia. Así, ha llegado a ser considerado un **líder nato** de la **nueva economía mundial**, centrada en el impulso de los datos y sus posibilidades infinitas.

D. Gram, Mick

- Director de *Business Intelligence* y Análisis en Red Bull, Los Ángeles, Estados Unidos
- Arquitecto de soluciones de *Business Intelligence* para Walmart Data Cafe
- Consultor independiente de *Business Intelligence* y *Data Science*
- Director de *Business Intelligence* en Capgemini
- Analista Jefe en Nordea
- Consultor Jefe de *Bussiness Intelligence* para SAS
- Executive Education en IA y Machine Learning en UC Berkeley College of Engineering
- MBA Executive en e-commerce en la Universidad de Copenhague
- Licenciatura y Máster en Matemáticas y Estadística en la Universidad de Copenhague

¡Estudia en la mejor universidad online del mundo según Forbes! En este MBA tendrás acceso a una amplia biblioteca de recursos multimedia, elaborados por reconocidos docentes de relevancia internacional"

Director Invitado Internacional

Scott Stevenson es un distinguido experto del sector del **Marketing Digital** que, por más de 19 años, ha estado ligado a una de las compañías más poderosas de la industria del entretenimiento, **Warner Bros**. **Discovery**. En este rol, ha tenido un papel fundamental en la **supervisión de logística** y **flujos de trabajos creativos** en diversas plataformas digitales, incluyendo redes sociales, búsqueda, *display* y medios lineales.

El liderazgo de este ejecutivo ha sido crucial para impulsar **estrategias de producción** en **medios pagados**, lo que ha resultado en una notable **mejora** en las **tasas de conversión** de su empresa. Al mismo tiempo, ha asumido otros roles, como el de Director de Servicios de Marketing y Gerente de Tráfico en la misma multinacional durante su antigua gerencia.

A su vez, Stevenson ha estado ligado a la distribución global de videojuegos y **campañas de propiedad digital**. También, fue el responsable de introducir estrategias operativas relacionadas con la formación, finalización y entrega de contenido de sonido e imagen para **comerciales de televisión** y ***trailers***.

Por otro lado, el experto posee una Licenciatura en Telecomunicaciones de la Universidad de Florida y un Máster en Escritura Creativa de la Universidad de California, lo que demuestra su destreza en **comunicación** y **narración**. Además, ha participado en la Escuela de Desarrollo Profesional de la Universidad de Harvard en programas de vanguardia sobre el uso de la **Inteligencia Artificial** en los **negocios**. Así, su perfil profesional se erige como uno de los más relevantes en el campo actual del **Marketing** y los **Medios Digitales**.

D. Stevenson, Scott

- Director de Marketing Digital en Warner Bros. Discovery, Burbank, Estados Unidos
- Gerente de Tráfico en Warner Bros. Entertainment
- Máster en Escritura Creativa de la Universidad de California
- Licenciatura en Telecomunicaciones de la Universidad de Florida

¡Alcanza tus objetivos académicos y profesionales con los expertos mejor cualificados del mundo! Los docentes de este MBA te guiarán durante todo el proceso de aprendizaje"

Directora Invitada Internacional

Galardonada con el "*International Content Marketing Awards*" por su creatividad, liderazgo y calidad de sus contenidos informativos, Wendy Thole-Muir es una reconocida **Directora de Comunicación** altamente especializada en el campo de la **Gestión de Reputación**.

En este sentido, ha desarrollado una sólida trayectoria profesional de más de dos décadas en este ámbito, lo que le ha llevado a formar parte de prestigiosas entidades de referencia internacional como **Coca-Cola**. Su rol implica la supervisión y manejo de la comunicación corporativa, así como el control de la imagen organizacional. Entre sus principales contribuciones, destaca haber liderado la implementación de la **plataforma de interacción interna** Yammer. Gracias a esto, los empleados aumentaron su compromiso con la marca y crearon una comunidad que mejoró la transmisión de información significativamente.

Por otra parte, se ha encargado de gestionar la comunicación de las **inversiones estratégicas** de las empresas en diferentes países africanos. Una muestra de ello es que ha manejado diálogos en torno a las inversiones significativas en Kenya, demostrando el compromiso de las entidades con el desarrollo tanto económico como social del país. A su vez, ha logrado numerosos **reconocimientos** por su capacidad de gestionar la percepción sobre las firmas en todos los mercados en los que opera. De esta forma, ha logrado que las compañías mantengan una gran notoriedad y los consumidores las asocien con una elevada calidad.

Además, en su firme compromiso con la excelencia, ha participado activamente en reputados **Congresos** y **Simposios** a escala global con el objetivo de ayudar a los profesionales de la información a mantenerse a la vanguardia de las técnicas más sofisticadas para **desarrollar planes estratégicos de comunicación** exitosos. Así pues, ha ayudado a numerosos expertos a anticiparse a situaciones de crisis institucionales y a manejar acontecimientos adversos de manera efectiva.

Dña. Thole-Muir, Wendy

- Directora de Comunicación Estratégica y Reputación Corporativa en Coca-Cola, Sudáfrica
- Responsable de Reputación Corporativa y Comunicación en ABI at SABMiller de Lovania, Bélgica
- Consultora de Comunicaciones en ABI, Bélgica
- Consultora de Reputación y Comunicación de Third Door en Gauteng, Sudáfrica
- Máster en Estudios del Comportamiento Social por Universidad de Sudáfrica
- Máster en Artes con especialidad en Sociología y Psicología por Universidad de Sudáfrica
- Licenciatura en Ciencias Políticas y Sociología Industrial por Universidad de KwaZulu-Natal
- Licenciatura en Psicología por Universidad de Sudáfrica

Gracias a esta titulación universitaria, 100% online, podrás compaginar el estudio con tus obligaciones diarias, de la mano de los mayores expertos internacionales en el campo de tu interés. ¡Inscríbete ya!"

Dirección

Dña. Fernández Sapena, Sonia

- Formadora de Seguridad Informática y Hacking Ético en el Centro de Referencia Nacional de Getafe en Informática y Telecomunicaciones de Madrid
- Instructora certificada E-Council
- Formadora en las siguientes certificaciones: EXIN Ethical Hacking Foundation y EXIN Cyber & IT Security Foundation. Madrid
- Formadora acreditada experta por la CAM de los siguientes certificados de profesionalidad: Seguridad Informática (IFCT0190), Gestión de Redes de Voz y datos (IFCM0310), Administración de Redes departamentales (IFCT0410), Gestión de Alarmas en redes de telecomunicaciones (IFCM0410), Operador de Redes de voz y datos (IFCM0110), y Administración de servicios de internet (IFCT0509)
- Colaboradora externa CSO/SSA (*Chief Security Officer/Senior Security Architect*) en la Universidad de las Islas Baleares
- Ingeniera en Informática por la Universidad de Alcalá de Henares de Madrid
- Máster en DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

D. Olalla Bonal, Martín

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

Profesores

D. Oropesiano Carrizosa, Francisco

- Ingeniero Informático
- Técnico en Microinformática, Redes y Seguridad en CAS Training
- Desarrollador de Servicios Web, CMS, e-commerce, UI y UX en Fersa Reparaciones
- Gestor de Servicios Web, Contenidos, Correo y DNS en Oropesia Web & Network
- Diseñador Gráfico y de Aplicaciones Web en Xarxa Sakai Projectes SL
- Diplomado en Informática de Sistemas por la Universidad de Alcalá
- Máster en DevOps: Docker and Kubernetes por Cyber Business Center
- Técnico de Redes y Seguridad Informática por la Universidad de las Islas Baleares
- Experto en Diseño Gráfico por la Universidad Politécnica de Madrid

D. Peralta Alonso, Jon

- Consultor Sénior de Protección de Datos y Ciberseguridad en Altia
- Abogado / Asesor jurídico en Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Asesor Jurídico / Pasante en Despacho Profesional: Óscar Padura
- Grado en Derecho por la Universidad Pública del País Vasco
- Máster en Delegado de Protección de Datos por EIS Innovative School
- Máster Universitario en Abogacía por la Universidad Pública del País Vasco
- Máster Especialista en Práctica Procesal Civil por la Universidad Internacional Isabel I de Castilla
- Docente en Máster en Protección de Datos Personales, Ciberseguridad y Derecho de las TIC

D. Ortega López, Florencio

- Consultor de TIC y Seguridad
- Consultor de Seguridad en Gestión de Identidades en SIA Group
- Consultor de TIC y Seguridad como profesional independiente
- Profesor formador en Sector TI
- Graduado en Ingeniería Técnica Industrial por la Universidad de Alcalá
- Máster en Profesorado por la UNIR
- MBA en Gestión y Dirección de Empresas por IDE-CESEM
- Máster en Dirección y Gestión de Tecnología de la Información por IDE-CESEM
- Certified Information Security Management (CISM) por la ISACA

D. Solana Villarias, Fabián

- Consultor de Tecnologías de la Información
- Creador y Administrador de servicios de encuestas en Investigación, Planificación y Desarrollo SA
- Especialista en Mantenimiento de Mercados Financieros y Sistemas Informáticos en Iberia Financial Software
- Desarrollador Web y Especialista en Accesibilidad en Indra
- Licenciado en Ingeniería Superior de Sistemas por la Universidad de Gales/CESINE
- Diplomado en Ingeniería Técnica en Informática de Sistemas por la Universidad de Gales/ CESINE

Dña. López García, Rosa María

- Especialista en Información de Gestión
- Profesora en Linux Professional Institute
- Colaboradora en Academia Hacker Incibe
- Capitana de Talento en Ciberseguridad en Teamciberhack
- Administrativa y Gestora Contable y Financiera en Integra2Transportes
- Auxiliar Administrativo en Recursos de Compras en el Centro de Educación Cardenal Marcelo Espínola
- Técnico Superior en Ciberseguridad y *Hacking* Ético
- Miembro de: Ciberpatrulla

Dña. Marcos Sbarbaro, Victoria Alicia

- Desarrolladora de Aplicaciones Móviles Android Nativas en B60. UK
- Analista Programadora para la Gestión, Coordinación y Documentación del Entorno Virtualizado de Alarmas de Seguridad
- Analista Programadora de Aplicaciones Java para cajeros automáticos
- Profesional del Desarrollo de *Software* para Aplicación de Validación de Firma y Gestión Documental
- Técnico de Sistemas para la Migración de Equipos y para la Gestión, Mantenimiento y Formación de Dispositivos Móviles PDA
- Ingeniero Técnico de Informática de Sistemas por la Universidad Oberta de Cataluña
- Máster en Seguridad Informática y Hacking Ético Oficial de EC- Council y CompTIA por la Escuela Profesional de Nuevas Tecnologías CICE

D. Redondo, Jesús Serrano

- Desarrollador Web y Técnico en Ciberseguridad
- Desarrollador Web en Roams, Palencia
- Desarrollador *FrontEnd* en Telefónica, Madrid
- Desarrollador *FrontEnd* en Best Pro Consulting SL, Madrid
- Instalador de Equipos y Servicio de Telecomunicaciones en Grupo Zener, Castilla y León
- Instalador de Equipos y Servicios de Telecomunicaciones en Lican Comunicaciones SL, Castilla y León
- Certificado en Seguridad Informática por CFTIC Getafe, Madrid
- Técnico Superior en Sistemas Telecomunicaciones e Informáticos por IES Trinidad Arroyo, Palencia
- Técnico Superior en Instalaciones Electrotécnicas MT y BT por IES Trinidad Arroyo, Palencia
- Formación en Ingeniería Inversa, Estenografía y Cifrado por la Academia Hacker Incibe

D. Jiménez Ramos, Álvaro

- Analista de Ciberseguridad
- Analista de Seguridad Sénior en The Workshop
- Analista de Ciberseguridad L1 en Axians
- Analista de Ciberseguridad L2 en Axians
- Analista de Ciberseguridad en SACYR S.A.
- Grado en Ingeniería Telemática por la Universidad Politécnica de Madrid
- Máster de Ciberseguridad y Hacking Ético por CICE
- Curso Superior de Ciberseguridad por Deusto Formación

D. 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

D. Entrenas, Alejandro

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

D. Catalá Barba, José Francisco

- Técnico Electrónico Experto en Ciberseguridad
- Desarrollador de Aplicaciones para Dispositivos Móviles
- Técnico Electrónico en Mando Intermedio en el Ministerio de la Defensa de España
- Técnico Electrónico en Factoría Ford Sita en Valencia

D. Nogales Ávila, Javier
- Enterprise Cloud y Sourcing Senior Consultant en Quint
- Cloud y 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. Gómez Rodríguez, Antonio
- Ingeniero Principal de Soluciones Cloud para Oracle
- Coorganizador de Málaga Developer Meetup
- Consultor Especialista para Sopra Group y Everis
- Líder de equipos en System Dynamics
- Desarrollador de Softwares en SGO Software
- Máster en E-Business por la Escuela de Negocios de La Salle
- Postgrado en Tecnologías y Sistemas de Información por el Instituto Catalán de Tecnología
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña

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

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

D. 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

Dña. Jurado Jabonero, Lorena

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

D. Ortega Esteban, Octavio

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

D. Embid Ruiz, Mario

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

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

09

Titulación

El Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer) garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Grand Master expedido por TECH Global University.

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

Este programa te permitirá obtener el título propio de **Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)** avalado por **TECH Global University**, la mayor Universidad digital del mundo.

TECH Global University, es una Universidad Oficial Europea reconocida públicamente por el Gobierno de Andorra (***boletín oficial***). Andorra forma parte del Espacio Europeo de Educación Superior (EEES) desde 2003. El EEES es una iniciativa promovida por la Unión Europea que tiene como objetivo organizar el marco formativo internacional y armonizar los sistemas de educación superior de los países miembros de este espacio. El proyecto promueve unos valores comunes, la implementación de herramientas conjuntas y fortaleciendo sus mecanismos de garantía de calidad para potenciar la colaboración y movilidad entre estudiantes, investigadores y académicos.

Este título propio de **TECH Global University**, es un programa europeo de formación continua y actualización profesional que garantiza la adquisición de las competencias en su área de conocimiento, confiriendo un alto valor curricular al estudiante que supere el programa.

TECH es miembro de la **Economics, Business and Enterprise Association (EBEA)**, una entidad de prestigio dedicada a impulsar la excelencia profesional en ciencias empresariales. Esta vinculación fortalece su compromiso con la excelencia académica en el ámbito empresarial.

Aval/Membresía

Título: **Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)**

Modalidad: **online**

Duración: **2 años**

Acreditación: **120 ECTS**

tech global university

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

Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Se trata de un título propio de 3.600 horas de duración equivalente a 120 ECTS, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

TECH Global University es una universidad reconocida oficialmente por el Gobierno de Andorra el 31 de enero de 2024, que pertenece al Espacio Europeo de Educación Superior (EEES).

En Andorra la Vella, a 28 de febrero de 2024

Dr. Pedro Navarro Illana
Rector

código único TECH: AFWOR23S techtitute.com/titulos

Grand Master en Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Distribución General del Plan de Estudios

Curso	Materia	ECTS	Carácter
1º	Ciberinteligencia y ciberseguridad	4	OB
1º	Seguridad en Host	4	OB
1º	Seguridad en red (perimetral)	4	OB
1º	Seguridad en smartphones	4	OB
1º	Seguridad en IoT	4	OB
1º	Hacking ético	4	OB
1º	Ingeniería inversa	4	OB
1º	Desarrollo seguro	4	OB
1º	Implementación práctica de políticas de seguridad en software y hardware	4	OB
1º	Análisis forense	4	OB
1º	Seguridad en el diseño y desarrollo de sistemas	4	OB
1º	Arquitecturas y modelos de seguridad de la información	4	OB
1º	Sistema de gestión de seguridad de información (SGSI)	4	OB
1º	Gestión de la seguridad IT	4	OB
1º	Políticas de gestión de incidencias de seguridad	4	OB

Curso	Materia	ECTS	Carácter
2º	Análisis de riesgos y entorno de seguridad IT	4	OB
2º	Políticas de seguridad para el análisis de amenazas en sistemas informáticos	4	OB
2º	Implementación práctica de políticas de seguridad ante ataques	4	OB
2º	Criptografía en IT	4	OB
2º	Gestión de identidad y accesos en seguridad IT	4	OB
2º	Seguridad en comunicaciones y operación software	4	OB
2º	Seguridad en entornos cloud	4	OB
2º	Herramientas de Monitorización en Políticas de Seguridad de los sistemas de información	4	OB
2º	Seguridad en comunicaciones de dispositivos Iot	4	OB
2º	Plan de continuidad del negocio asociado a la seguridad	4	OB
2º	Política de Recuperación Práctica de Desastres de Seguridad	4	OB
2º	Implementación de políticas de seguridad física y ambiental en la empresa	4	OB
2º	Políticas de comunicaciones seguras en la empresa	4	OB
2º	Aspectos organizativos en política de seguridad de la información	8	OB

Dr. Pedro Navarro Illana
Rector

tech global university

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

tech global university

Grand Master

Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

- Modalidad: **online**
- Duración: **2 años**
- Titulación: **TECH Global University**
- Acreditación: **120 ECTS**
- Horario: **a tu ritmo**
- Exámenes: **online**

Grand Master

Alta Dirección de Ciberseguridad (CISO, Chief Information Security Officer)

Aval/Membresía

ebea

Economics, Business
and Enterprise Association

tech global university