Grand Master

Secure Information Management



tech universidad tecnológica



tech universidad tecnológica

Grand Master

Secure Information Management

Modalidad: **Online**
Duración: **2 años**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **3.000 h.**
Acceso web: **www.techtitute.com/informatica/grand-master/grand-master-secure-information-management**

Índice

01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Competencias — pág. 18

04 Dirección del curso — pág. 22

05 Estructura y contenido — pág. 30

06 Metodología — pág. 50

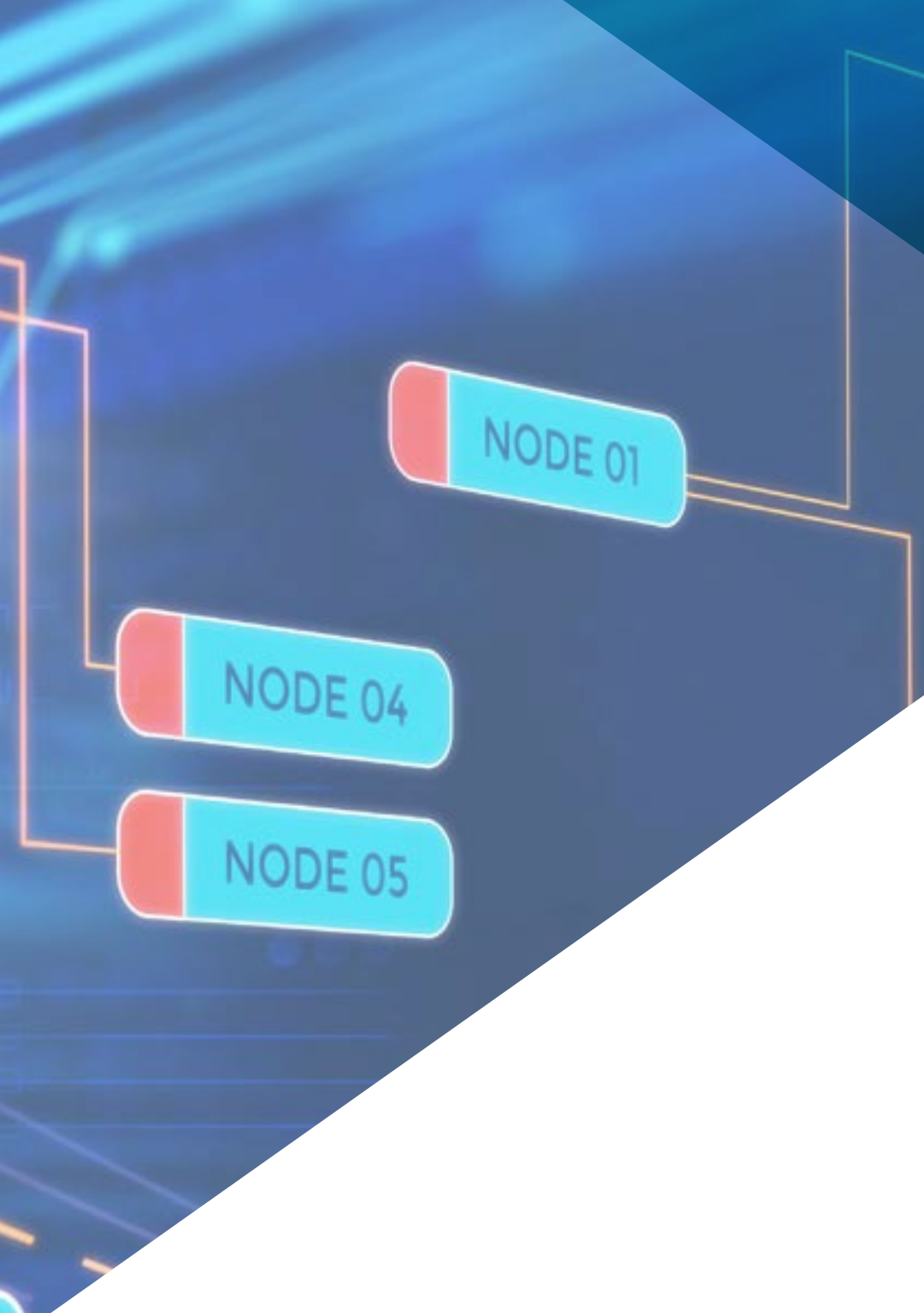
07 Titulación — pág. 58

01

Presentación

El mundo actual está dominado por el entorno digital. En él se gestiona una gran cantidad de actividades de diferentes ámbitos. Así, ya no se entienden el ocio, el trabajo o el contacto con amigos y familiares sin internet y todas las herramientas online existentes. Por esa razón, cantidades ingentes de información se transfieren a diario, desde datos inocuos en conversaciones a través de redes sociales y aplicaciones de mensajería, hasta información muy sensible de índole personal y profesional alojada en webs bancarias o empresariales. En este panorama tan complejo se necesitan especialistas que puedan gestionar todo tipo de información perteneciente a esas áreas, al tiempo que lo hacen con una adecuada atención a su seguridad. Numerosas compañías están buscando personal con este perfil para que protejan su información.





Cada día personas malintencionadas intentan comprometer la seguridad de empresas e instituciones que gestionan datos muy valiosos: tú podrías ser el gran protector de esa información"

Cada día, millones de personas realizan todo tipo de actividades en internet. Consultan las noticias, conversan con amigos y familiares, comparten opiniones en las redes sociales, realizan gestiones administrativas en diferentes empresas e instituciones, comparten todo tipo de archivos o hacen tareas relacionadas con el ámbito laboral. Así, cantidades incontables de datos se crean y transfieren a cada instante en todo el mundo.

Gestionarlos con la seguridad adecuada no es una labor sencilla, ya que requiere de una serie de conocimientos específicos de diversos campos que normalmente no estarían en contacto. Por esa razón, este Grand Master en Secure Information Management es una oportunidad muy destacada para todos aquellos ingenieros y profesionales de la informática que quieran integrar la gestión de información y la ciberseguridad para convertirse en los mayores especialistas en las dos áreas.

Numerosas empresas e instituciones manejan datos muy delicados y valiosos que necesitan una correcta administración, conservación y vigilancia. No abundan los expertos aún en ambas disciplinas y que se puedan encargar de su correcto manejo. Así, los alumnos que realicen esta titulación estarán en la mejor posición para alcanzar puestos de máxima importancia en las compañías que busquen asegurar su información digital.

Para ello, TECH ha diseñado los mejores contenidos y ha reunido a los mejores docentes, con una gran experiencia profesional en esas áreas, para que los alumnos reciban la enseñanza más completa posible y puedan progresar laboralmente.

Este **Grand Master en Secure Information Management** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en informática
- 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 la gestión y seguridad de datos digitales
- 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

Todo lo que hacemos en el ámbito digital queda registrado. Haz de internet un lugar más seguro gracias a este Grand Master”

Las mejores empresas del país te confiarán la gestión y seguridad de sus datos cuando finalices este programa”

Este Grand Master combina dos disciplinas esenciales para el futuro de tu carrera. Matricúlate ya y alcanza todos tus objetivos.

Apréndelo todo sobre gestión y seguridad de datos y observa cómo avanzas profesionalmente en muy poco tiempo.

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 contextual, 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 programa académico. Para ello, el profesional contará con la ayuda de un novedoso sistema de vídeo interactivo realizado por reconocidos expertos.



02

Objetivos

El principal objetivo de este Grand Master en Secure Information Management es brindar a sus alumnos los mejores conocimientos en dos ramas diferenciadas pero interrelacionadas de la informática y las ingenierías: la gestión de datos en el entorno digital y ciberseguridad. Combinando estas dos áreas, los informáticos y profesionales que cursen este programa serán capaces de aplicar las mejores soluciones en cada situación que se presente en su carrera laboral, ofreciendo las herramientas más adecuadas a sus empresas para administrar y proteger todo tipo de información delicada.





Tu objetivo es ser el mejor especialista de tu compañía y TECH te ofrece las herramientas para conseguirlo”

Objetivos generales

- Analizar los beneficios de la aplicación de técnicas de analítica del dato en cada departamento de la empresa
- Desarrollar las bases para el conocimiento de las necesidades y aplicaciones de cada departamento
- Generar conocimiento especializado para seleccionar la herramienta adecuada
- Proponer técnicas y objetivos para ser lo más productivos posible según el departamento
- Analizar el rol del analista en ciberseguridad
- Profundizar en la ingeniería social y sus métodos
- Examinar las metodologías OSINT, HUMINT, OWASP, PTEC, OSSTM y OWISAM
- Realizar un análisis de riesgo y conocer las métricas de riesgo
- Determinar el adecuado uso de anonimato y uso de redes como TOR, I2P y Freenet
- Compilar las normativas vigentes en materia de ciberseguridad
- Generar conocimiento especializado para realizar una auditoría de seguridad
- Desarrollar políticas de uso apropiadas
- Examinar los sistemas de detección y prevención de las amenazas más importantes
- Evaluar nuevos sistemas de detección de amenazas, así como su evolución respecto a soluciones más tradicionales
- Analizar las principales plataformas móviles actuales, características y uso de las mismas
- Identificar, analizar y evaluar riesgos de seguridad de las partes del proyecto IoT
- Evaluar la información obtenida y desarrollar mecanismos de prevención y *hacking*
- Aplicar la ingeniería inversa al entorno de la ciberseguridad
- Concretar las pruebas que hay que realizar al software desarrollado
- Recopilar todas las pruebas y datos existentes para llevar a cabo un informe forense
- Presentar debidamente el informe forense
- Analizar el estado actual y futuro de la seguridad informática
- Examinar los riesgos de las nuevas tecnologías emergentes
- Compilar las distintas tecnologías con relación a la seguridad informática

La ciberseguridad y la gestión de datos son disciplinas que evolucionan muy rápido. Realiza este Grand Master y obtén los conocimientos más actualizados"



Objetivos específicos

Módulo 1. Analítica del dato en la organización empresarial

- Desarrollar habilidades analíticas para tomar decisiones de calidad
- Examinar campañas de marketing y comunicación efectivas
- Determinar la Creación de cuadros de mando y kpi´s en función del departamento
- Generar conocimiento especializado para desarrollar análisis predictivos
- Proponer planes de negocio y de fidelización basados en estudios de mercado
- Desarrollar la capacidad de escuchar al cliente
- Aplicar conocimientos estadísticos, cuantitativos y técnicos en situaciones reales

Módulo 2. Gestión, manipulación de datos e información para ciencia de datos

- Realizar un análisis de datos
- Unificar datos diversos: lograr la consistencia de la información
- Producir información relevante, eficaz para la toma de decisiones
- Determinar las mejores prácticas para la gestión del dato según su tipología y usos
- Establecer políticas de acceso y reutilización de los datos
- Garantizar la seguridad y disponibilidad: disponibilidad, integridad y confidencialidad de la información
- Examinar las herramientas para la gestión del dato mediante lenguajes de programación

Módulo 3. Dispositivos y plataformas ioT como base para la ciencia de datos

- Identificar qué es IoT (Internet of Things) e IIoT (Industrial Internet of Things)
- Examinar el Consorcio de Internet Industrial
- Analizar qué es la arquitectura de referencia del IoT
- Abordar los sensores y dispositivos IoT y su clasificación
- Identificar los protocolos y tecnologías de comunicaciones empleadas en IoT
- Examinar las distintas plataformas Cloud en IoT: Propósito general, Industriales, de código abierto
- Desarrollar los mecanismos de intercambio de datos
- Establecer los requisitos y estrategias de seguridad
- Presentar las distintas áreas de aplicación IoT e IIoT

Módulo 4. Representación gráfica para análisis de datos

- Generar conocimiento especializado en representación y analítica de datos
- Examinar los diferentes tipos de datos agrupados
- Establecer las representaciones gráficas más usadas en diferentes ámbitos
- Determinar los principios del diseño en la visualización de datos
- Presentar la narrativa gráfica como herramienta
- Analizar las diferentes herramientas software para graficado y análisis exploratorio de datos

Módulo 5. Herramientas de ciencia de datos

- Desarrollar habilidades para convertir los datos en información de la que se pueda extraer conocimiento
- Determinar las características principales de un dataset, su estructura, componentes y las implicaciones de su distribución en el modelado
- Fundamentar la toma de decisiones realizando análisis completos previos de los datos
- Desarrollar habilidades para resolver casos prácticos haciendo uso de técnicas de ciencia de datos
- Establecer las herramientas y métodos generales más apropiados para modelar cada dataset en función del preprocesamiento realizado
- Evaluar los resultados de forma analítica, comprendiendo el impacto de la estrategia escogida en las distintas métricas
- Demostrar capacidad crítica ante los resultados obtenidos tras aplicar métodos de preprocesamiento o modelado

Módulo 6. Minería de datos. selección, preprocesamiento y transformación

- Generar conocimiento especializado sobre los estadísticos previos para cualquier análisis y evaluación de datos
- Desarrollar las habilidades necesarias para la identificación, preparación y transformación de datos
- Evaluar las distintas metodologías presentadas e identificar ventajas e inconvenientes
- Examinar los problemas en entornos de datos de alta dimensionalidad
- Desarrollar la implementación de los algoritmos empleados para el preprocesamiento de datos
- Demostrar la capacidad de interpretar la visualización de los datos para un análisis descriptivo
- Desarrollar conocimiento avanzado sobre las diferentes técnicas de preparación de datos existentes para la limpieza, normalización y transformación de datos

Módulo 7. Predictibilidad y análisis de fenómenos estocásticos

- Analizar las Series Temporales
- Desarrollar la formulación y las propiedades básicas de los modelos univariantes de series temporales
- Examinar la metodología de modelización y predicción de Series Temporales reales
- Determinar los modelos univariantes incluyendo atípicos
- Aplicar modelos de regresión dinámica y aplicar la metodología de la construcción de dichos modelos a partir de series observadas
- Abordar el análisis espectral de series temporales univariantes, así como los aspectos fundamentales relacionados con la inferencia basada en el periodograma y su interpretación
- Estimar la probabilidad y la tendencia de una serie temporal para un horizonte temporal establecido

Módulo 8. Diseño y desarrollo de sistemas inteligentes

- Analizar el paso de información a conocimiento
- Desarrollar los diferentes tipos de técnicas de aprendizaje automático
- Examinar las métricas y puntuaciones para cuantificar la calidad de los modelos
- Implementar los distintos algoritmos de aprendizaje automático
- Identificar los modelos de razonamiento probabilístico
- Asentar las bases del aprendizaje profundo
- Evidenciar las competencias adquiridas para comprender los diferentes algoritmos de aprendizaje automático

Módulo 9. Arquitecturas y sistemas para uso intensivo de datos

- Determinar los requisitos de los sistemas de uso masivo de datos
- Examinar diferentes modelos de datos y analizar las bases de datos
- Analizar las funcionalidades clave para los sistemas distribuidos y su importancia en diferentes tipos de sistemas
- Evaluar qué aplicaciones de uso extendido utilizan los fundamentos de los sistemas distribuidos para diseñar sus sistemas
- Analizar el modo en el que las bases de datos almacenan y recuperan información
- Concretar los diferentes modelos de replicado y los problemas asociados
- Desarrollar las formas de particionado y las transacciones distribuidas
- Determinar los sistemas por lotes y los sistemas en (casi) tiempo real

Módulo 10. Aplicación práctica de la ciencia de datos en sectores de actividad empresarial

- Analizar el estado del arte de la Inteligencia Artificial (IA) y la analítica de datos
- Desarrollar conocimiento especializado sobre las tecnologías más utilizadas
- Generar una mejor comprensión de la tecnología mediante casos de uso
- Analizar las estrategias elegidas para seleccionar las mejores tecnologías a implementar
- Determinar los ámbitos de aplicación
- Examinar los riesgos reales y potenciales de la tecnología aplicada
- Proponer beneficios derivados del uso
- Identificar tendencias a futuro en sectores específicos

Módulo 11. Ciberinteligencia y ciberseguridad

- Desarrollar las metodologías usadas en materia de ciberseguridad
- Examinar el ciclo de inteligencia y establecer su aplicación en la Ciberinteligencia
- Determinar el papel del analista de inteligencia y los obstáculos de actividad evacuativa
- Analizar las metodologías OSINT, OWISAM, OSSTM, PTES, OWASP
- Establecer las herramientas más comunes para la producción de inteligencia
- Llevar a cabo un análisis de riesgos y conocer las métricas usadas
- Concretar las opciones de anonimato y el uso de redes como TOR, I2P, FreeNet
- Detallar las Normativas vigentes en Ciberseguridad

Módulo 12. Seguridad en host

- Concretar las políticas de backup de los datos de personales y profesionales
- Valorar las diferentes herramientas para dar soluciones a problemas específicos de seguridad
- Establecer mecanismos para tener un sistema actualizado
- Analizar el equipo para detectar intrusos
- Determinar las reglas de acceso al sistema
- Examinar y clasificar los correos para evitar fraudes
- Generar listas de software permitido

Módulo 13. Seguridad en red (Perimetral)

- Analizar las arquitecturas actuales de red para identificar el perímetro que debemos proteger
- Desarrollar las configuraciones concretas de firewall y en Linux para mitigar los ataques más comunes
- Compilar las soluciones más usadas como Snort y Suricata, así como su configuración
- Examinar las diferentes capas adicionales que proporcionan los Firewalls de nueva generación y funcionalidades de red en entornos Cloud
- Determinar las herramientas para la protección de la red y demostrar por qué son fundamentales para una defensa multicapa

Módulo 14. Seguridad en smartphones

- Examinar los distintos vectores de ataque para evitar convertirse en un blanco fácil
- Determinar los principales ataques y tipos de Malware a los que se exponen los usuarios de dispositivos móviles
- Analizar los dispositivos más actuales para establecer una mayor seguridad en la configuración
- Concretar los pasos principales para realizar una prueba de penetración tanto en plataformas iOS como en plataformas Android
- Desarrollar conocimiento especializado sobre las diferentes herramientas de protección y seguridad
- Establecer buenas prácticas en programación orientadas a dispositivos móvile



Módulo 15. Seguridad en IoT

- Analizar las principales arquitecturas de IoT
- Examinar las tecnologías de conectividad
- Desarrollar los protocolos de aplicación principales
- Concretar los diferentes tipos de dispositivos existentes
- Evaluar los niveles de riesgo y vulnerabilidades conocidas
- Desarrollar políticas de uso seguras
- Establecer las condiciones de uso apropiadas para estos dispositivos

Módulo 16. *Hacking* ético

- Examinar los métodos de IOSINT
- Recopilar la información disponible en medios públicos
- Escanear redes para obtener información de modo activo
- Desarrollar laboratorios de pruebas
- Analizar las herramientas para el desempeño del *Pentesting*
- Catalogar y evaluar las diferentes vulnerabilidades de los sistemas
- Concretar las diferentes metodologías de *hacking*

Módulo 17. Ingeniería inversa

- Analizar las fases de un compilador
- Examinar la arquitectura de procesadores x86 y la arquitectura de procesadores ARM
- Determinar los diferentes tipos de análisis
- Aplicar sandboxing en diferentes entornos
- Desarrollar las diferentes técnicas de análisis de malware
- Establecer las herramientas orientadas al análisis de malware

Módulo 18. Desarrollo seguro

- Establecer los requisitos necesarios para el correcto funcionamiento de una aplicación de forma segura
- Examinar los archivos de Logs para entender los mensajes de error
- Analizar los diferentes eventos y decidir qué mostrar al usuario y qué guardar en los logs
- Generar un Código Sanitizado, fácilmente verificable y de calidad
- Evaluar la documentación adecuada para cada fase del desarrollo
- Concretar el comportamiento del servidor para optimizar el sistema
- Desarrollar Código Modular, reusable y mantenible





Módulo 19. Análisis forense

- Identificar los diferentes elementos que ponen en evidencia un delito
- Generar conocimiento especializado para Obtener los datos de los diferentes medios antes de que se pierdan
- Recuperar los datos que hayan sido borrados intencionadamente
- Analizar los registros y los logs de los sistemas
- Determinar cómo se Duplican los datos para no alterar los originales
- Fundamentar las pruebas para que sean consistentes
- Generar un informe sólido y sin fisuras
- Presentar las conclusiones de forma coherente
- Establecer cómo Defender el informe ante la autoridad competente
- Concretar estrategias para que el teletrabajo sea seguro

Módulo 20. Retos actuales y futuros en seguridad informática

- Examinar el uso de las Criptomonedas, el impacto en la economía y la seguridad
- Analizar la situación de los usuarios y el grado de analfabetismo digital
- Determinar el ámbito de uso de *Blockchain*
- Presentar alternativas a IPv4 en el Direccionamiento de Redes
- Desarrollar estrategias para formar a la población en el uso correcto de las tecnologías
- Generar conocimiento especializado para hacer frente a los nuevos retos de seguridad y evitar la suplantación de identidad
- Concretar estrategias para que el teletrabajo sea seguro

03

Competencias

Los alumnos que completen este Grand Master en Secure Information Management serán capaces de realizar gran cantidad de tareas altamente especializadas en los ámbitos de la gestión de datos y la ciberseguridad. Así, esta titulación combina ambas ramas para ofrecer conocimientos complementarios que puedan cruzarse y emplearse en diferentes situaciones y entornos profesionales. De esta forma, los alumnos llevarán a cabo un proceso de aprendizaje integral que los guiará para ser auténticos especialistas en la materia.





Tus nuevas habilidades te convertirán en el mayor especialista de tu entorno"

Competencias generales

- Desarrollar una perspectiva técnica y de negocio del análisis del dato
- Comprender los diferentes algoritmos, plataformas y herramientas más actuales para la exploración, visualización, manipulación, procesamiento y análisis de los datos
- Implementar una visión empresarial necesaria para la puesta en valor como elemento clave para la toma de decisiones
- Poder abordar problemas específicos al análisis del dato
- Conocer las metodologías usadas en materia de ciberseguridad
- Evaluar cada tipo de amenaza para ofrecer una solución óptima en cada caso
- Generar soluciones inteligentes completas para automatizar comportamientos ante incidentes
- Saber cómo evaluar los riesgos asociados a las vulnerabilidades tanto fuera como dentro de la empresa
- Conocer la evolución y el impacto del IoT a lo largo del tiempo
- Demostrar que un sistema es vulnerable, atacarlo con fines preventivos y solventar dichos problemas
- Aplicar *sandboxing* en diferentes entornos
- Conocer las directrices que debe seguir un buen desarrollador para cumplir con la seguridad necesaria



Competencias específicas

- Especializarse en *data science* desde la perspectiva técnica y de negocio
- Visualizar datos del modo más adecuado para favorecer su compartición y la comprensión por diferentes perfiles
- Abordar las áreas funcionales fundamentales de la organización donde la ciencia de datos puede aportar un mayor valor
- Desarrollar el ciclo de vida del dato, su tipología y las tecnologías y fases necesarias para su gestión
- Procesar y manipular datos mediante lenguajes y librerías específicas
- Desarrollar conocimiento avanzado en las técnicas fundamentales de minería de datos para la selección, el preprocesamiento y la transformación de datos
- Especializarse en los principales algoritmos de *machine learning* para la extracción de conocimiento oculto en los datos
- Generar conocimiento especializado en las arquitecturas y sistemas software necesarias para el uso intensivo de datos
- Determinar cómo el IoT puede suponer una fuente de generación de datos e información clave sobre la que aplicar ciencia de datos para extracción de conocimiento
- Analizar las diferentes formas de aplicación de ciencia de datos en distintos sectores o verticales mediante el aprendizaje de ejemplos reales
- Realizar operaciones de seguridad defensiva
- Tener una percepción profunda y especializada sobre la seguridad informática
- Ostentar conocimiento especializado en el ámbito de la ciberseguridad y ciberinteligencia
- Tener conocimientos profundos sobre aspectos fundamentales como el ciclo de inteligencia, fuentes de inteligencia, ingeniería social, metodología OSINT, HUMINT, anonimización y análisis de riesgos, metodologías existentes (OWASP, OWISAM, OSSTM, PTES) y normativas vigentes en materia de ciberseguridad
- Entender la importancia de idear una defensa multicapa, también conocida como *defense in depth*, que cubra todos los aspectos de una red corporativa donde algunos de los conceptos y sistemas que veremos podrán ser utilizados y aplicados también en un ambiente doméstico
- Saber aplicar procesos de seguridad para smartphones y dispositivos portátiles
- Conocer los medios para realizar el llamado *hacking* ético y proteger una empresa de un ciberataque
- Investigar un incidente de ciberseguridad
- Conocer las diferentes técnicas de ataque y defensa existentes
- Analizar el rol del analista en ciberseguridad y conocer el funcionamiento de la ingeniería social y sus métodos

¿Quieres distinguirte de otros especialistas, pero no sabes cómo? Este Grand Master es lo que buscas”

04

Dirección del curso

Esta titulación está impartida por los mejores profesores de los ámbitos de la ciberseguridad y la gestión digital de datos. Su experiencia garantiza que los alumnos recibirán los contenidos más completos y actualizados para que puedan aplicarlos directamente en sus carreras profesionales. De esta forma, los docentes de este Grand Master en Secure Information Management transmitirán todos sus conocimientos a los estudiantes, asegurando que estos se conviertan en especialistas altamente cualificados y demandados por las grandes compañías de sus países.





Los mejores especialistas te enseñan cómo ser un profesional destacado en el sector”

Dirección



Dr. Peralta Martín-Palomino, Arturo

- CEO y CTO en Prometeus Global Solutions
- CTO en Korporate Technologies en Korporate Technologies
- CTO en AI Shephers GmbH
- Doctor en Ingeniería Informática por la Universidad de Castilla la Mancha
- Doctor en Economía, Empresas y Finanzas por la Universidad Camilo José Cela. Premio Extraordinario de Doctorado
- Doctor en Psicología por la Universidad de Castilla la Mancha
- Máster en Tecnologías Informáticas Avanzadas por la Universidad de Castilla la Mancha
- Máster MBA+E (Máster en Administración de Empresas e Ingeniería de Organización) por la Universidad de Castilla la Mancha
- Profesor asociado, con docencia en Grado y Máster en Ingeniería Informática, en Universidad de Castilla la Mancha
- Profesor de Máster en Big Data y Data Science en Universidad Internacional de Valencia
- Profesor de Máster en Industria 4.0 y del Máster en Diseño Industrial y Desarrollo de producto
- Miembro del Grupo de Investigación SMILe de la Universidad de Castilla la Mancha



Dña. Fernández Sapena, Sonia

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

Profesores

D. Armero Fernández, Rafael

- Business Intelligence Consultant en SDG Group
- Digital Engineer en Mi-GSO
- Logistic Engineer en Torrecid S.A
- Quality Intern en INDRA
- Graduado en Ingeniería Aeroespacial por la Universidad Politécnica de Valencia
- Máster en Professional Development 4.0 por la Universidad de Alcalá de Henares

D. Peris Morillo, Luis Javier

- Technical Lead en Capitole Consulting
- Senior Technical Lead y Delivery Lead Support en HCL
- Agile Coach y Director de Operaciones en Mirai Advisory
- Desarrollador, Team Lead, Scrum Máster, Agile Coach, Product Manager en DocPath
- Ingeniería Superior en Informática por la ESI de Ciudad Real (UCLM)
- Posgrado en Gestión de proyectos por la CEOE - Confederación Española de Organizaciones Empresariales
- +50 MOOCs cursados, impartidas por universidades muy reconocidas tales como Stanford University, Michigan University, Yonsei University, Universidad Politécnica de Madrid, etc.

D. Montoro Montarroso, Andrés

- Investigador en el grupo SMILe de la Universidad de Castilla-La Mancha
- Científico de Datos en Prometeus Global Solutions
- Grado en Ingeniería Informática por la Universidad de Castilla-La Mancha Especialidad en Ciencias de la Computación
- Máster en Ciencia de Datos e Ingeniería de Computadores por la Universidad de Granada

Dña. Fernández Meléndez, Galina

- Analista de Datos en ADN Mobile Solution
- Procesos ETL, minería de datos, análisis y visualización de datos, establecimiento de KPI's, diseño e implementación de Dashboard., control de gestión. Desarrollo en R, manejo de SQL, entre otros
- Determinación de patrones, modelos predictivos, aprendizaje automático
- Licenciatura en Administración de Empresas. Universidad Bicentenaria de Aragua-Caracas
- Diplomado en Planificación y Finanzas Públicas. Escuela Venezolana De Planificación-Escuela De Hacienda
- Máster en Análisis de Datos e Inteligencia de Negocio. Universidad De Oviedo
- MBA en Administración y Dirección De Empresas (Escuela De Negocios Europea De Barcelona)
- Máster en Big Data y Business Intelligence (Escuela de Negocios Europea de Barcelona)

Dña. Pedrajas Parabás, Elena

- Business Analyst en Management Solutions en Madrid
- Investigadora en el Departamento de Informática y Análisis Numérico en la Universidad de Córdoba
- Investigadora en el Centro Singular de Investigación en Tecnologías Inteligentes en Santiago de Compostela
- Licenciada en Ingeniería Informática. Máster en Ciencia de datos e Ingeniería de Computadores. Experiencia Docente

Dña. Martínez Cerrato, Yésica

- Técnico de producto de seguridad electrónica en Securitas Seguridad España
- Analista de inteligencia Empresarial en Ricopia Technologies (Alcalá de Henares) Grado en Ingeniería Electrónica de Comunicaciones en Escuela Politécnica Superior, Universidad de Alcalá
- Responsable de formar a las nuevas incorporaciones respecto a los softwares de gestión comercial (CRM, ERP,INTRANET), producto y procedimientos en Ricopia Technologies (Alcalá de Henares)
- Responsable de formar a nuevos becarios incorporados a las Aulas de Informática en la Universidad de Alcalá
- Gestora de proyectos en el área de Integración de Grandes Cuentas en Correos y Telégrafos (Madrid)
- Técnico Informático-Responsable aulas informáticas OTEC, Universidad de Alcalá (Alcalá de Henares)
- Profesora de clases de Informática en Asociación ASALUMA (Alcalá de Henares)
- Beca de formación como Técnico Informático en OTEC, Universidad de Alcalá (Alcalá de Henares)

D. Fondón Alcalde, Rubén

- Analista de negocio en gestión del valor del cliente en Vodafone España
- Jefe de integración de servicios en Entelgy para Telefónica Global Solutions
- Administrador de cuentas en línea de servidores clónicos en EDM Electronics
- Analista de Negocios para el Sur de Europa en Vodafone Global Enterprise
- Ingeniero de Telecomunicaciones por la Universidad Europea de Madrid
- Máster en Big Data y Analytics por la Universidad Internacional de Valencia

D. Díaz Díaz-Chirón, Tobias

- Investigador en el laboratorio ArCO de la Universidad de Castilla-La Mancha, grupo dedicado a proyectos relacionados con arquitecturas y redes de computadores
- Consultor en Blue Telecom, compañía dedicada al sector de las telecomunicaciones
- Ingeniero Superior en Informática por la Universidad de Castilla-La Mancha

D. Tato Sánchez, Rafael

- Gestión de proyectos en INDRA SISTEMAS S.A. Gestión del contrato de mantenimiento de instalaciones de sistemas inteligentes de transporte dependientes del Centro de Control y Gestión de Tráfico de la Dirección General de Tráfico en Madrid
- Director técnico en INDRA SISTEMAS S.A. responsable del Centro de Control y Gestión de Tráfico de la Dirección General de Tráfico en Madrid
- Ingeniero de sistemas. ENA TRÁFICO S.A.
- Ingeniero Técnico Industrial en Electricidad por la Universidad Politécnica de Madrid
- Grado en Ingeniería en Electrónica Industrial y Automática por la Universidad Europea de Madrid
- Certificación profesional. SSCE0110: Docencia para la formación Profesional para el empleo
- Máster en Industria 4.0 por la Universidad Internacional de La Rioja (UNIR)

D. Catalá Barba, José Francisco

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

D. Jiménez Ramos, Álvaro

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

Dña. Marcos Sbarbaro, Victoria Alicia

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

D. Peralta Alonso, Jon

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



D. Redondo, Jesús Serrano

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

Los principales profesionales en la materia se han unido para ofrecerte los conocimientos más amplios en este campo, de tal manera que puedas desarrollarte con totales garantías de éxito"

05

Estructura y contenido

Los contenidos de este Grand Master en Secure Information Management se han diseñado atendiendo al estado actual de la profesión, de forma que los alumnos reciban los mejores conocimientos posibles y puedan aplicarlos a su ámbito laboral. Así, a lo largo de los 20 módulos que componen esta titulación, los estudiantes podrán aprenderlo todo sobre gestión y seguridad de datos e información digitales, convirtiéndose en auténticos especialistas en la materia.





No hay un programa mejor. Este Grand Master te ofrece todo lo que necesitas para ser el mayor experto en estas áreas"

Módulo 1. Analítica del dato en la organización empresarial

1.1. Análisis de negocio
- 1.1.1. Análisis de negocio
- 1.1.2. Estructura del dato
- 1.1.3. Fases y elementos

1.2. Analítica del dato en la empresa
- 1.2.1. Cuadros de mando y Kpi's por departamentos
- 1.2.2. Informes operativos, tácticos y estratégicos
- 1.2.3. Analítica del dato aplicada a cada departamento
  - 1.2.3.1. Marketing y comunicación
  - 1.2.3.2. Comercial
  - 1.2.3.3. Atención al cliente
  - 1.2.3.4. Compras
  - 1.2.3.5. Administración
  - 1.2.3.6. RR.HH.
  - 1.2.3.7. Producción
  - 1.2.3.8. IT

1.3. Marketing y comunicación
- 1.3.1. Kpi's a medir, aplicaciones y beneficios
- 1.3.2. Sistemas de marketing y *data warehouse*
- 1.3.3. Implementación de una estructura de analítica del dato en Marketing
- 1.3.4. Plan de marketing y comunicación
- 1.3.5. Estrategias, predicción y gestión de campañas

1.4. Comercial y ventas
- 1.4.1. Aportaciones de analítica del dato en el área comercial
- 1.4.2. Necesidades del departamento de Ventas
- 1.4.3. Estudios de mercado

1.5. Atención al cliente
- 1.5.1. Fidelización
- 1.5.2. Calidad personal e inteligencia emocional
- 1.5.3. Satisfacción del cliente

1.6. Compras
- 1.6.1. Analítica del dato para estudios de mercado
- 1.6.2. Analítica del dato para estudios de competencia
- 1.6.3. Otras aplicaciones

1.7. Administración
- 1.7.1. Necesidades en el departamento de administración
- 1.7.2. *Data Warehouse* y análisis de riesgo financiero
- 1.7.3. *Data Warehouse* y análisis de riesgo de crédito

1.8. Recursos humanos
- 1.8.1. RR.HH y beneficios de la analítica del dato
- 1.8.2. Herramientas de analítica del dato en el departamento de RR.HH.
- 1.8.3. Aplicación de analítica del dato en los RR.HH.

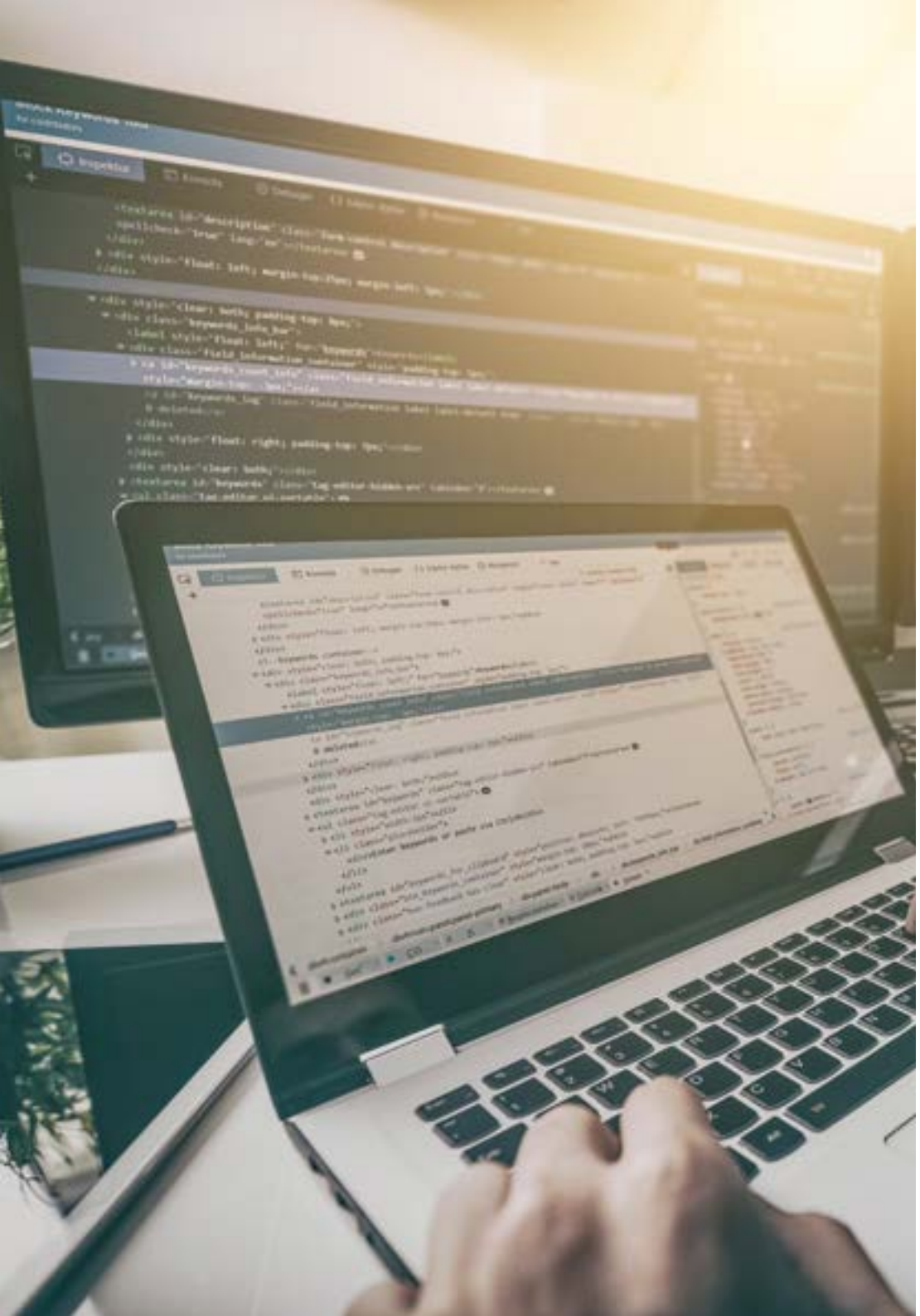
1.9. Producción
- 1.9.1. Análisis de datos en un departamento de producción
- 1.9.2. Aplicaciones
- 1.9.3. Beneficios

1.10. IT
- 1.10.1. Departamento de IT
- 1.10.2. Analítica del dato y transformación digital
- 1.10.3. Innovación y productividad

Módulo 2. Gestión, manipulación de datos e información para ciencia de datos

2.1. Estadística. Variables, índices y ratios
- 2.1.1. La Estadística
- 2.1.2. Dimensiones estadísticas
- 2.1.3. Variables, índices y ratios

2.2. Tipología del dato
- 2.2.1. Cualitativos
- 2.2.2. Cuantitativos
- 2.2.3. Caracterización y categorías



2.3. Conocimiento de los datos a partir de medidas
- 2.3.1. Medidas de centralización
- 2.3.2. Medidas de dispersión
- 2.3.3. Correlación

2.4. Conocimiento de los datos a partir de gráficos
- 2.4.1. Visualización según el tipo de dato
- 2.4.2. Interpretación de información gráfica
- 2.4.3. Customización de gráficos con R

2.5. Probabilidad
- 2.5.1. Probabilidad
- 2.5.2. Función de probabilidad
- 2.5.3. Distribuciones

2.6. Recolección de datos
- 2.6.1. Metodología de recolección
- 2.6.2. Herramientas de recolección
- 2.6.3. Canales de recolección

2.7. Limpieza del dato
- 2.7.1. Fases de la limpieza de datos
- 2.7.2. Calidad del dato
- 2.7.3. Manipulación de datos (con R)

2.8. Análisis de datos, interpretación y valoración de resultados
- 2.8.1. Medidas estadísticas
- 2.8.2. Índices de relación
- 2.8.3. Minería de datos

2.9. Almacén del dato (*Data Warehouse*)
- 2.9.1. Elementos
- 2.9.2. Diseño

2.10. Disponibilidad del dato
- 2.10.1. Acceso
- 2.10.2. Utilidad
- 2.10.3. Seguridad

Módulo 3. Dispositivos y plataformas IoT como base para la ciencia de datos

3.1. *Internet of Things*
- 3.1.1. Internet del futuro, *Internet of Things*
- 3.1.2. El consorcio de internet industrial

3.2. Arquitectura de referencia
- 3.2.1. La Arquitectura de referencia
- 3.2.2. Capas
- 3.2.3. Componentes

3.3. Sensores y dispositivos IoT
- 3.3.1. Componentes principales
- 3.3.2. Sensores y actuadores

3.4. Comunicaciones y protocolos
- 3.4.1. Protocolos. Modelo OSI
- 3.4.2. Tecnologías de comunicación

3.5. Plataformas *cloud* para IoT e IIoT
- 3.5.1. Plataformas de propósito general
- 3.5.2. Plataformas Industriales
- 3.5.3. Plataformas de código abierto

3.6. Gestión de datos en plataformas IoT
- 3.6.1. Mecanismos de gestión de datos. Datos abiertos
- 3.6.2. Intercambio de datos y visualización

3.7. Seguridad en IoT
- 3.7.1. Requisitos y áreas de seguridad
- 3.7.2. Estrategias de seguridad en IIoT

3.8. Aplicaciones de IoT
- 3.8.1. Ciudades inteligentes
- 3.8.2. Salud y condición física
- 3.8.3. Hogar inteligente
- 3.8.4. Otras aplicaciones

3.9. Aplicaciones de IIoT
- 3.9.1. Fabricación
- 3.9.2. Transporte
- 3.9.3. Energía
- 3.9.4. Agricultura y ganadería
- 3.9.5. Otros sectores

3.10. Industria 4.0
- 3.10.1. IoRT *(Internet of Robotics Things)*
- 3.10.2. Fabricación aditiva 3D
- 3.10.3. *Big Data Analytics*

Módulo 4. Representación gráfica para análisis de datos

4.1. Análisis exploratorio
- 4.1.1. Representación para análisis de información
- 4.1.2. El valor de la representación gráfica
- 4.1.3. Nuevos paradigmas de la representación gráfica

4.2. Optimización para ciencia de datos
- 4.2.1. La Gama cromática y el diseño
- 4.2.2. La Gestalt en la representación gráfica
- 4.2.3. Errores a evitar y consejos

4.3. Fuentes de datos básicos
- 4.3.1. Para representación de calidad
- 4.3.2. Para representación de cantidad
- 4.3.3. Para representación de tiempo

4.4. Fuentes de datos complejos
- 4.4.1. Archivos, listados y BBDD
- 4.4.2. Datos abiertos
- 4.4.3. Datos de generación continua

4.5. Tipos de gráficas
- 4.5.1. Representaciones básicas
- 4.5.2. Representación de bloques
- 4.5.3. Representación para análisis de dispersión
- 4.5.4. Representaciones circulares
- 4.5.5. Representaciones burbujas
- 4.5.6. Representaciones geográficas

4.6. Tipos de visualización
- 4.6.1. Comparativas y relacional
- 4.6.2. Distribución
- 4.6.3. Jerárquica

4.7. Diseño de informes con representación gráfica
- 4.7.1. Aplicación de gráficas en informes de marketing
- 4.7.2. Aplicación de gráficas en cuadros de mando y Kpi's
- 4.7.3. Aplicación de gráficas en planes estratégicos
- 4.7.4. Otros usos: ciencia, salud, negocio

4.8. Narración gráfica
- 4.8.1. La narración gráfica
- 4.8.2. Evolución
- 4.8.3. Utilidad

4.9. Herramientas orientadas a visualización
- 4.9.1. Herramientas avanzadas
- 4.9.2. Software en línea
- 4.9.3. *Open Source*

4.10. Nuevas tecnologías en la visualización de datos
- 4.10.1. Sistemas para virtualización de la realidad
- 4.10.2. Sistemas para aumento y mejora de la realidad
- 4.10.3. Sistemas inteligentes

Módulo 5. Herramientas de ciencia de datos

5.1. Ciencia de datos
- 5.1.1. La ciencia de datos
- 5.1.2. Herramientas avanzadas para el científico de datos

5.2. Datos, información y conocimiento
- 5.2.1. Datos, información y conocimiento
- 5.2.2. Tipos de datos
- 5.2.3. Fuentes de datos

5.3. De los datos a la información
- 5.3.1. Análisis de datos
- 5.3.2. Tipos de análisis
- 5.3.3. Extracción de Información de un *Dataset*

5.4. Extracción de información mediante visualización
- 5.4.1. La visualización como herramienta de análisis
- 5.4.2. Métodos de visualización
- 5.4.3. Visualización de un conjunto de datos

5.5. Calidad de los datos
- 5.5.1. Datos de calidad
- 5.5.2. Limpieza de datos
- 5.5.3. Preprocesamiento básico de datos

5.6. *Dataset*
- 5.6.1. Enriquecimiento del *dataset*
- 5.6.2. La maldición de la dimensionalidad
- 5.6.3. Modificación de nuestro conjunto de datos

5.7. Desbalanceo
- 5.7.1. Desbalanceo de clases
- 5.7.2. Técnicas de mitigación del desbalanceo
- 5.7.3. Balanceo de un *dataset*

5.8. Modelos no supervisados
- 5.8.1. Modelo no supervisado
- 5.8.2. Métodos
- 5.8.3. Clasificación con modelos no supervisados

5.9. Modelos supervisados
- 5.9.1. Modelo supervisado
- 5.9.2. Métodos
- 5.9.3. Clasificación con modelos supervisados

5.10. Herramientas y buenas prácticas
- 5.10.1. Buenas prácticas para un científico de datos
- 5.10.2. El mejor modelo
- 5.10.3. Herramientas útiles

Módulo 6. Minería de datos. selección, preprocesamiento y transformación

6.1. La inferencia estadística
- 6.1.1. Estadística descriptiva vs. Inferencia estadística
- 6.1.2. Procedimientos paramétricos
- 6.1.3. Procedimientos no paramétricos

6.2. Análisis exploratorio
- 6.2.1. Análisis descriptivo
- 6.2.2. Visualización
- 6.2.3. Preparación de datos

6.3. Preparación de datos
- 6.3.1. Integración y limpieza de datos
- 6.3.2. Normalización de datos
- 6.3.3. Transformando atributos

6.4. Los Valores perdidos
- 6.4.1. Tratamiento de valores perdidos
- 6.4.2. Métodos de imputación de máxima verosimilitud
- 6.4.3. Imputación de valores perdidos usando aprendizaje automático

6.5. El ruido en los datos
- 6.5.1. Clases de ruido y atributos
- 6.5.2. Filtrado de ruido
- 6.5.3. El efecto del ruido

6.6. La maldición de la dimensionalidad
- 6.6.1. *Oversampling*
- 6.6.2. *Undersampling*
- 6.6.3. Reducción de datos multidimensionales

6.7. De atributos continuos a discretos
- 6.7.1. Datos continuos versus discretos
- 6.7.2. Proceso de discretización

6.8. Los datos
- 6.8.1. Selección de datos
- 6.8.2. Perspectivas y criterios de selección
- 6.8.3. Métodos de selección

6.9. Selección de Instancias
- 6.9.1. Métodos para la selección de instancias
- 6.9.2. Selección de prototipos
- 6.9.3. Métodos avanzados para la selección de instancias

6.10. Preprocesamiento de datos en entornos *Big Data*
- 6.10.1. *Big Data*
- 6.10.2. Preprocesamiento "clásico" versus masivo
- 6.10.3. *Smart Data*

Módulo 7. Predictibilidad y análisis de fenómenos estocásticos

7.1. Series de tiempo
- 7.1.1. Series de tiempo
- 7.1.2. Utilidad y aplicabilidad
- 7.1.3. Casuística relacionada

7.2. La Serie temporal
- 7.2.1. Tendencia Estacionalidad de ST
- 7.2.2. Variaciones típicas
- 7.2.3. Análisis de residuos

7.3. Tipologías
- 7.3.1. Estacionarias
- 7.3.2. No estacionarias
- 7.3.3. Transformaciones y ajustes

7.4. Esquemas para series temporales
- 7.4.1. Esquema (modelo) aditivo
- 7.4.2. Esquema (modelo) multiplicativo
- 7.4.3. Procedimientos para determinar el tipo de modelo

7.5. Métodos básicos de *forecast*
- 7.5.1. Media
- 7.5.2. *Naïve*
- 7.5.3. *Naïve* estacional
- 7.5.4. Comparación de métodos

7.6. Análisis de residuos
- 7.6.1. Autocorrelación
- 7.6.2. ACF de residuos
- 7.6.3. Test de correlación

7.7. Regresión en el contexto de series temporales
- 7.7.1. ANOVA
- 7.7.2. Fundamentos
- 7.7.3. Aplicación práctica

7.8. Modelos predictivos de series temporales
- 7.8.1. ARIMA
- 7.8.2. Suavizado exponencial

7.9. Manipulación y análisis de Series temporales con R
- 7.9.1. Preparación de los datos
- 7.9.2. Identificación de patrones
- 7.9.3. Análisis del modelo
- 7.9.4. Predicción

7.10. Análisis gráficos combinados con R
- 7.10.1. Situaciones habituales
- 7.10.2. Aplicación práctica para resolución de problemas sencillos
- 7.10.3. Aplicación práctica para resolución de problemas avanzados

Módulo 8. Diseño y desarrollo de sistemas inteligentes

8.1. Preprocesamiento de datos
- 8.1.1. Preprocesamiento de datos
- 8.1.2. Transformación de datos
- 8.1.3. Minería de datos

8.2. Aprendizaje Automático
- 8.2.1. Aprendizaje supervisado y no supervisado
- 8.2.2. Aprendizaje por refuerzo
- 8.2.3. Otros paradigmas de aprendizaje

8.3. Algoritmos de clasificación
- 8.3.1. Aprendizaje Automático Inductivo
- 8.3.2. SVM y KNN
- 8.3.3. Métricas y puntuaciones para clasificación

8.4. Algoritmos de Regresión
- 8.4.1. Regresión lineal, regresión logística y modelos no lineales
- 8.4.2. Series temporales
- 8.4.3. Métricas y puntuaciones para regresión

8.5. Algoritmos de Agrupamiento
- 8.5.1. Técnicas de agrupamiento jerárquico
- 8.5.2. Técnicas de agrupamiento particional
- 8.5.3. Métricas y puntuaciones para *clustering*

8.6. Técnicas de reglas de asociación
- 8.6.1. Métodos para la extracción de reglas
- 8.6.2. Métricas y puntuaciones para los algoritmos de reglas de asociación

8.7. Técnicas de clasificación avanzadas. Multiclasificadores
- 8.7.1. Algoritmos de *Bagging*
- 8.7.2. Clasificador "*Random Forests*"
- 8.7.3. "*Boosting*" para árboles de decisión

8.8. Modelos gráficos probabilísticos
- 8.8.1. Modelos probabilísticos
- 8.8.2. Redes bayesianas. Propiedades, representación y parametrización
- 8.8.3. Otros modelos gráficos probabilísticos

8.9. Redes Neuronales
- 8.9.1. Aprendizaje automático con redes neuronales artificiales
- 8.9.2. Redes *feedforward*

8.10. Aprendizaje profundo
- 8.10.1. Redes *feedforward* profundas
- 8.10.2. Redes neuronales convolucionales y modelos de secuencia
- 8.10.3. Herramientas para implementar redes neuronales profundas

Módulo 9. Arquitecturas y sistemas para uso intensivo de datos

9.1. Requisitos no funcionales. Pilares de las aplicaciones de datos masivos
- 9.1.1. Fiabilidad
- 9.1.2. Adaptabilidad
- 9.1.3. Mantenibilidad

9.2. Modelos de datos
- 9.2.1. Modelo relacional
- 9.2.2. Modelo documental
- 9.2.3. Modelo de datos tipo grafo

9.3. Bases de datos. Gestión del almacenamiento y recuperación de datos
- 9.3.1. Índices hash
- 9.3.2. Almacenamiento estructurado en log
- 9.3.3. Árboles B

9.4. Formatos de codificación de datos
- 9.4.1. Formatos específicos del lenguaje
- 9.4.2. Formatos estandarizados
- 9.4.3. Formatos de codificación binarios
- 9.4.4. Flujo de datos entre procesos

9.5. Replicación
- 9.5.1. Objetivos de la replicación
- 9.5.2. Modelos de replicación
- 9.5.3. Problemas con la replicación

9.6. Transacciones distribuidas
- 9.6.1. Transacción
- 9.6.2. Protocolos para transacciones distribuidas
- 9.6.3. Transacciones serializables

9.7. Particionado
- 9.7.1. Formas de particionado
- 9.7.2. Interacción de índice secundarios y particionado
- 9.7.3. Rebalanceo de particiones

9.8. Procesamiento de datos *offline*
- 9.8.1. Procesamiento por lotes
- 9.8.2. Sistemas de ficheros distribuidos
- 9.8.3. *MapReduce*

9.9. Procesamiento de datos en tiempo real
- 9.9.1. Tipos de *broker* de mensajes
- 9.9.2. Representación de bases de datos como flujos de datos
- 9.9.3. Procesamiento de flujos de datos

9.10. Aplicaciones prácticas en la empresa
- 9.10.1. Consistencia en lecturas
- 9.10.2. Enfoque holístico de datos
- 9.10.3. Escalado de un servicio distribuido

Módulo 10. Aplicación práctica de la ciencia de datos en sectores de actividad empresarial

10.1. Sector sanitario
- 10.1.1. Implicaciones de la IA y la analítica de datos en el sector sanitario
- 10.1.2. Oportunidades y desafíos

10.2. Riesgos y tendencias en sector sanitario
- 10.2.1. Uso en el sector sanitario
- 10.2.2. Riesgos potenciales relacionados con el uso de IA

10.3. Servicios financieros
- 10.3.1. Implicaciones de la IA y la analítica de datos en el sector de los servicios financiero
- 10.3.2. Uso en los servicios financieros
- 10.3.3. Riesgos potenciales relacionados con el uso de IA

10.4. Retail
- 10.4.1. Implicaciones de la IA y la analítica de datos en el sector del retail
- 10.4.2. Uso en el retail
- 10.4.3. Riesgos potenciales relacionados con el uso de IA

10.5. Industria 4.0
- 10.5.1. Implicaciones de la IA y la analítica de datos en la Industria 4.0
- 10.5.2. Uso en la Industria 4.0

10.6. Riesgos y tendencias en Industria 4.0
- 10.6.1. Riesgos potenciales relacionados con el uso de IA

10.7. Administración pública
- 10.7.1. Implicaciones de la IA y la analítica de datos en la administración pública
- 10.7.2. Uso en la administración pública
- 10.7.3. Riesgos potenciales relacionados con el uso de IA

10.8. Educación
- 10.8.1. Implicaciones de la IA y la analítica de datos en la educación
- 10.8.2. Riesgos potenciales relacionados con el uso de IA

10.9. Silvicultura y agricultura
- 10.9.1. Implicaciones de la IA y la analítica de datos en la silvicultura y agricultura
- 10.9.2. Uso en silvicultura y agricultura
- 10.9.3. Riesgos potenciales relacionados con el uso de IA

10.10. Recursos humanos
- 10.10.1. Implicaciones de la IA y la analítica de datos en la gestión de recursos humanos
- 10.10.2. Aplicaciones prácticas en el mundo empresarial
- 10.10.3. Riesgos potenciales relacionados con el uso de IA

Módulo 11. Ciberinteligencia y ciberseguridad

11.1. Ciberinteligencia
- 11.1.1. Ciberinteligencia
  - 11.1.1.2. La inteligencia
    - 11.1.1.2.1. Ciclo de inteligencia
  - 11.1.1.3. Ciberinteligencia
  - 11.1.1.4. Ciberinteligencia y ciberseguridad
- 11.1.2. El Analista de Inteligencia
  - 11.1.2.1. El rol del analista de inteligencia
  - 11.1.2.2. Los sesgos del analista de inteligencia en la actividad evaluativa

11.2. Ciberseguridad
- 11.2.1. Las capas de seguridad
- 11.2.2. Identificación de las ciberamenazas
  - 11.2.2.1. Amenazas externas
  - 11.2.2.2. Amenazas internas
- 11.2.3. Acciones adversas
  - 11.2.3.1. Ingeniería social
  - 11.2.3.2. Métodos comúnmente usados

11.3. Técnicas y herramientas de inteligencias
- 11.3.1. OSINT
- 11.3.2. SOCMINT
- 11.3.3. HUMIT
- 11.3.4. Distribuciones de Linux y herramientas
- 11.3.5. OWISAM
- 11.3.6. OWISAP
- 11.3.7. PTES
- 11.3.8. OSSTM

11.4. Metodologías de evaluación
- 11.4.1. El análisis de inteligencia
- 11.4.2. Técnicas de organización de la información adquirida
- 11.4.3. Fiabilidad y credibilidad de las fuentes de información
- 11.4.4. Metodologías de análisis
- 11.4.5. Presentación de los resultados de la inteligencia

11.5. Auditorías y documentación
- 11.5.1. La auditoría en seguridad informática
- 11.5.2. Documentación y permisos para auditoria
- 11.5.3. Tipos de auditoría
- 11.5.4. Entregables
  - 11.5.4.1. Informe técnico
  - 11.5.4.2. Informe ejecutivo

11.6. Anonimato en la red
- 11.6.1. Uso de anonimato
- 11.6.2. Técnicas de anonimato (Proxy, VPN)
- 11.6.3. Redes TOR, Freenet e IP2

11.7. Amenazas y tipos de seguridad
- 11.7.1. Tipos de amenazas
- 11.7.2. Seguridad física
- 11.7.3. Seguridad en redes
- 11.7.4. Seguridad lógica
- 11.7.5. Seguridad en aplicaciones web
- 11.7.6. Seguridad en dispositivos móviles

11.8. Normativa y *compliance*
- 11.8.1. RGPD
- 11.8.2. La estrategia nacional de ciberseguridad 2011
- 11.8.3. Familia ISO 27000
- 11.8.4. Marco de ciberseguridad NIST
- 11.8.5. PIC
- 11.8.6. ISO 27032
- 11.8.7. Normativas *cloud*
- 11.8.8. SOX
- 11.8.9. PCI

11.9. Análisis de riesgos y métricas
- 11.9.1. Alcance de riesgos
- 11.9.2. Los activos
- 11.9.3. Las amenazas
- 11.9.4. Las vulnerabilidades
- 11.9.5. Evaluación del riesgo
- 11.9.6. Tratamiento del riesgo

11.10. Organismos importantes en materia de ciberseguridad
- 11.10.1. NIST
- 11.10.2. ENISA
- 11.10.3. INCIBE
- 11.10.4. OEA
- 11.10.5. UNASUR - PROSUR

Módulo 12. Seguridad en host

12.1. Copias de seguridad
- 12.1.1. Estrategias para las copias de seguridad
- 12.1.2. Herramientas para Windows
- 12.1.3. Herramientas para Linux
- 12.1.4. Herramientas para MacOS

12.2. Antivirus de usuario
- 12.2.1. Tipos de antivirus
- 12.2.2. Antivirus para Windows
- 12.2.3. Antivirus para Linux
- 12.2.4. Antivirus para MacOS
- 12.2.5. Antivirus para smartphones

12.3. Detectores de intrusos - HIDS
- 12.3.1. Métodos de detección de intrusos
- 12.3.2. *Sagan*
- 12.3.3. *Aide*
- 12.3.4. *Rkhunter*

12.4. *Firewall* local
- 12.4.1. *Firewalls* para Windows
- 12.4.2. *Firewalls* para Linux
- 12.4.3. *Firewalls* para MacOS

12.5. Gestores de contraseñas
- 12.5.1. *Password*
- 12.5.2. *LastPass*
- 12.5.3. *KeePass*
- 12.5.4. *Sticky Password*
- 12.5.5. *RoboForm*

12.6. Detectores de *phishing*
- 12.6.1. Detección del *phishing* de forma manual
- 12.6.2. Herramientas *antiphishing*

12.7. *Spyware*
- 12.7.1. Mecanismos de evitación
- 12.7.2. Herramientas *antispyware*

12.8. Rastreadores
- 12.8.1. Medidas para proteger el sistema
- 12.8.2. Herramientas anti-rastreadores

12.9. EDR- *End Point Detection and Response*
- 12.9.1. Comportamiento del sistema EDR
- 12.9.2. Diferencias entre EDR y antivirus
- 12.9.3. El futuro de los sistemas EDR

12.10. Control sobre la instalación de software
- 12.10.1. Repositorios y tiendas de software
- 12.10.2. Listas de software permitido o prohibido
- 12.10.3. Criterios de actualizaciones
- 12.10.4. Privilegios para instalar software

Módulo 13. Seguridad en red (Perimetral)

13.1. Sistemas de detección y prevención de amenazas
- 13.1.1. Marco general de los incidentes de seguridad
- 13.1.2. Sistemas de defensa actuales: *Defense in Depth* y SOC
- 13.1.3. Arquitecturas de red actuales
- 13.1.4. Tipos de herramientas para la detección y prevención de incidentes
  - 13.1.4.1. Sistemas basados en red
  - 13.1.4.2. Sistemas basados en host
  - 13.1.4.3. Sistemas centralizados
- 13.1.5. Comunicación y detección de instancias/*hosts*, contenedores y *serverless*

13.2. *Firewall*
- 13.2.1. Tipos de *firewalls*
- 13.2.2. Ataques y mitigación
- 13.2.3. *Firewalls* comunes en kernel Linux
  - 13.2.3.1. UFW
  - 13.2.3.2. Nftables e iptables
  - 13.2.3.3. *Firewall*
- 13.2.4. Sistemas de detección basados en logs del sistema
  - 13.2.4.1. TCP *Wrappers*
  - 13.2.4.2. *BlockHosts* y *DenyHosts*
  - 13.2.4.3. Fai2ban

13.3. Sistemas de detección y prevención de intrusiones (IDS/IPS)
- 13.3.1. Ataques sobre IDS/IPS
- 13.3.2. Sistemas de IDS/IPS
  - 13.3.2.1. *Snort*
  - 13.3.2.2. Suricata

13.4. *Firewalls* de siguiente generación (NGFW)
- 13.4.1. Diferencias entre NGFW y Firewall tradicional
- 13.4.2. Capacidades principales
- 13.4.3. Soluciones comerciales
- 13.4.4. Firewalls para servicios de *Cloud*
  - 13.4.4.1. Arquirtectura *Cloud* VPC
  - 13.4.4.2. *Cloud* ACLs
  - 13.4.4.3. *Security Group*

13.5. Proxy
- 13.5.1. Tipos de Proxy
- 13.5.2. Uso de Proxy. Ventajas e inconvenientes

13.6. Motores de antivirus
- 13.6.1. Contexto general del *Malware* e IOCs
- 13.6.2. Problemas de los motores de antivirus

13.7. Sistemas de protección de correo
- 13.7.1. Antispam
  - 13.7.1.1. Listas blancas y negras
  - 13.7.1.2. Filtros bayesiano
- 13.7.2. *Mail Gateway* (MGW)

13.8. SIEM
- 13.8.1. Componentes y arquitectura
- 13.8.2. Reglas de correlación y casos de uso
- 13.8.3. Retos actuales de los sistemas SIEM

13.9. SOAR
- 13.9.1. SOAR y SIEM: enemigos o aliados
- 13.9.2. El futuro de los sistemas SOAR

13.10. Otros sistemas basados en red
- 13.10.1. WAF
- 13.10.2. NAC
- 13.10.3. HoneyPots y HoneyNets
- 13.10.4. CASB

Módulo 14. Seguridad en smartphones

14.1. El mundo del dispositivo móvil
- 14.1.1. Tipos de plataformas móviles
- 14.1.2. Dispositivos iOS
- 14.1.3. Dispositivos Android

14.2. Gestión de la Seguridad Móvil
- 14.2.1. Proyecto de Seguridad Móvil OWASP
  - 14.2.1.1. Top 10 Vulnerabilidades
- 14.2.2. Comunicaciones, redes y modos de conexión

14.3. El dispositivo móvil en el entorno empresarial
- 14.3.1. Riesgos
- 14.3.2. Políticas de seguridad
- 14.3.3. Monitorización de dispositivos
- 14.3.4. Gestión de dispositivos móviles (MDM)

14.4. Privacidad del usuario y seguridad de los datos
- 14.4.1. Estados de la información
- 14.4.2. Protección y confidencialidad de los datos
  - 14.4.2.1. Permisos
  - 14.4.2.2. Encriptación
- 14.4.3. Almacenamiento seguro de los datos
  - 14.4.3.1. Almacenamiento seguro en iOS
  - 14.4.3.2. Almacenamiento seguro en Android
- 14.4.4. Buenas prácticas en el desarrollo de aplicaciones

14.5. Vulnerabilidades y vectores de ataque
- 14.5.1. Vulnerabilidades
- 14.5.2. Vectores de ataque
  - 14.5.2.1. *Malware*
  - 14.5.2.2. Exfiltración de datos
  - 14.5.2.3. Manipulación de los datos

14.6. Principales amenazas
- 14.6.1. Usuario no forzado
- 14.6.2. *Malware*
  - 14.6.2.1. Tipos de *Malware*
- 14.6.3. Ingeniería social
- 14.6.4. Fuga de datos
- 14.6.5. Robo de información
- 14.6.6. Redes *Wi-Fi* no seguras
- 14.6.7. Software desactualizado
- 14.6.8. Aplicaciones maliciosas
- 14.6.9. Contraseñas poco seguras
- 14.6.10. Configuración débil o inexistente de seguridad
- 14.6.11. Acceso físico

14.6.12. Pérdida o robo del dispositivo
14.6.13. Suplantación de identidad (Integridad)
14.6.14. Criptografía débil o rota
14.6.15. Denegación de Servicio (DoS)
14.7. Principales ataques
14.7.1. Ataques de *phishing*
14.7.2. Ataques relacionados con los modos de comunicación
14.7.3. Ataques de *Smishing*
14.7.4. Ataques de *Criptojacking*
14.7.5. *Man in The Middle*
14.8. *Hacking*
14.8.1. *Rooting y Jailbreaking*
14.8.2. Anatomía de un ataque móvil
14.8.2.1. Propagación de la amenaza
14.8.2.2. Instalación de *malware* en el dispositivo
14.8.2.3. Persistencia
14.8.2.4. Ejecución del *Payload* y extracción de la información
14.8.3. *Hacking* en dispositivos iOS: mecanismos y herramientas
14.8.4. *Hacking* en dispositivos Android: mecanismos y herramientas
14.9. Pruebas de penetración
14.9.1. *iOS PenTesting*
14.9.2. *Android PenTesting*
14.9.3. Herramientas
14.10. Protección y seguridad
14.10.1. Configuración de seguridad
14.10.1.1. En dispositivos iOS
14.10.1.2. En dispositvos Android
14.10.2. Medidas de seguridad
14.10.3. Herramientas de protección

Módulo 15. Seguridad en IoT

15.1. Dispositivos
15.1.1. Tipos de dispositivos
15.1.2. Arquitecturas estandarizadas
15.1.2.1. ONEM2M
15.1.2.2. IoTWF
15.1.3. Protocolos de aplicación
15.1.4. Tecnologías de conectividad
15.2. Dispositivos IoT. Áreas de aplicación
15.2.1. *SmartHome*
15.2.2. *SmartCity*
15.2.3. Transportes
15.2.4. *Wearables*
15.2.5. Sector salud
15.2.6. IioT
15.3. Protocolos de comunicación
15.3.1. MQTT
15.3.2. LWM2M
15.3.3. OMA-DM
15.3.4. TR-069
15.4. *SmartHome*
15.4.1. Domótica
15.4.2. Redes
15.4.3. Electrodomésticos
15.4.4. Vigilancia y seguridad
15.5. *SmartCity*
15.5.1. Iluminación
15.5.2. Meteorología
15.5.3. Seguridad
15.6. Transportes
15.6.1. Localización
15.6.2. Realización de pagos y obtención de servicios
15.6.3. Conectividad

15.7. *Wearables*
- 15.7.1. Ropa inteligente
- 15.7.2. Joyas inteligentes
- 15.7.3. Relojes inteligentes

15.8. Sector salud
- 15.8.1. Monitorización de ejercicio/ritmo cardiaco
- 15.8.2. Monitorización de pacientes y personas mayores
- 15.8.3. Implantables
- 15.8.4. Robots quirúrgicos

15.9. Conectividad
- 15.9.1. *Wi-Fi/Gateway*
- 15.9.2. *Bluetooth*
- 15.9.3. Conectividad incorporada

15.10. Securización
- 15.10.1. Redes dedicadas
- 15.10.2. Gestor de contraseñas
- 15.10.3. Uso de protocolos cifrados
- 15.10.4. Consejos de uso

Módulo 16. *Hacking* ético

16.1. Entorno de trabajo
- 16.1.1. Distribuciones Linux
  - 16.1.1.1. Kali Linux - Offensive Security
  - 16.1.1.2. Parrot OS
  - 16.1.1.3. Ubuntu
- 16.1.2. Sistemas de virtualización
- 16.1.3. *Sandbox*
- 16.1.4. Despliegue de laboratorios

16.2. Metodologías
- 16.2.1. OSSTM
- 16.2.2. OWASP
- 16.2.3. NIST
- 16.2.4. PTES
- 16.2.5. ISSAF

16.3. *Footprinting*
- 16.3.1. Inteligencia de fuentes abiertas (OSINT)
- 16.3.2. Búsqueda de brechas y vulnerabilidades de datos
- 16.3.3. Uso de herramientas pasivas

16.4. Escaneo de redes
- 16.4.1. Herramientas de escaneo
  - 16.4.1.1. Nmap
  - 16.4.1.2. Hping3
  - 16.4.1.3. Otras herramientas de escaneo
- 16.4.2. Técnicas de escaneo
- 16.4.3. Técnicas de evasión de *Firewall* e IDS
- 16.4.4. *Banner Grabbing*
- 16.4.5. Diagramas de red

16.5. Enumeración
- 16.5.1. Enumeración SMTP
- 16.5.2. Enumeración DNS
- 16.5.3. Enumeración de NetBIOS y Samba
- 16.5.4. Enumeración de LDAP
- 16.5.5. Enumeración de SNMP
- 16.5.6. Otras técnicas de enumeración

16.6. Análisis de vulnerabilidades
- 16.6.1. Soluciones de análisis de vulnerabilidades
  - 16.6.1.1. Qualys
  - 16.6.1.2. Nessus
  - 16.6.1.3. CFI LanGuard
- 16.6.2. Sistemas de puntuación de vulnerabilidades
  - 16.6.2.1. CVSS
  - 16.6.2.2. CVE
  - 16.6.2.3. NVD

16.7. Ataques a redes *inalámbricas*
- 16.7.1. Metodología de *hacking* en redes inalámbricas
  - 16.7.1.1. Wi-Fi Discovery
  - 16.7.1.2. Análisis de tráfico
  - 16.7.1.3. Ataques del *aircrack*
    - 16.7.1.3.1. Ataques WEP
    - 16.7.1.3.2. Ataques WPA/WPA2
  - 16.7.1.4. Ataques de *Evil Twin*
  - 16.7.1.5. Ataques a WPS
  - 16.7.1.6. *Jamming*
- 16.7.2. Herramientas para la seguridad inalámbrica

16.8. Hackeo de servidores webs
- 16.8.1. *Cross site Scripting*
- 16.8.2. CSRF
- 16.8.3. *Session Hijacking*
- 16.8.4. *SQLinjection*

16.9. Explotación de vulnerabilidades
- 16.9.1. Uso de *exploits* conocidos
- 16.9.2. Uso de *metasploit*
- 16.9.3. Uso de *malware*
  - 16.9.3.1. Definición y alcance
  - 16.9.3.2. Generación de *malware*
  - 16.9.3.3. Bypass de soluciones antivirus

16.10. Persistencia
- 16.10.1. Instalación de rootkits
- 16.10.2. Uso de ncat
- 16.10.3. Uso de tareas programadas para backdoors
- 16.10.4. Creación de usuarios
- 16.10.5. Detección de HIDS

Módulo 17. Ingeniería inversa

17.1. Compiladores
- 17.1.1. Tipos de códigos
- 17.1.2. Fases de un compilador
- 17.1.3. Tabla de símbolos
- 17.1.4. Gestor de errores
- 17.1.5. Compilador GCC

17.2. Tipos de análisis en compiladores
- 17.2.1. Análisis léxico
  - 17.2.1.1. Terminología
  - 17.2.1.2. Componentes léxicos
  - 17.2.1.3. Analizador léxico LEX
- 17.2.2. Análisis sintáctico
  - 17.2.2.1. Gramáticas libres de contexto
  - 17.2.2.2. Tipos de análisis sintácticos
    - 17.2.2.2.1. Análisis descendente
    - 17.2.2.2.2. Análisis ascendente
  - 17.2.2.3. Árboles sintácticos y derivaciones
  - 17.2.2.4. Tipos de analizadores sintácticos
    - 17.2.2.4.1. Analizadores LR (*Left To Right*)
    - 17.2.2.4.2. Analizadores LALR
- 17.2.3. Análisis semántico
  - 17.2.3.1. Gramáticas de atributos
  - 17.2.3.2. S-Atribuidas
  - 17.2.3.3. L-Atribuidas

17.3. Estructuras de datos en ensamblador
- 17.3.1. Variables
- 17.3.2. Arrays
- 17.3.3. Punteros
- 17.3.4. Estructuras
- 17.3.5. Objetos

17.4. Estructuras de código en ensamblador
- 17.4.1. Estructuras de selección
  - 17.4.1.1. If, else if, Else
  - 17.4.1.2. Switch
- 17.4.2. Estructuras de iteración
  - 17.4.2.1. For
  - 17.4.2.2. While
  - 17.4.2.3. Uso del break
- 17.4.3. Funciones

17.5. Arquitectura Hardware x86
- 17.5.1. Arquitectura de procesadores x86
- 17.5.2. Estructuras de datos en x86
- 17.5.3. Estructuras de código en x86

17.6. Arquitectura Hardware ARM
- 17.6.1. Arquitectura de procesadores ARM
- 17.6.2. Estructuras de datos en ARM
- 17.6.3. Estructuras de código en ARM

17.7. Análisis de código estático
- 17.7.1. Desensambladores
- 17.7.2. IDA
- 17.7.3. Reconstructores de código

17.8. Análisis de código dinámico
- 17.8.1. Análisis del comportamiento
  - 17.8.1.1. Comunicaciones
  - 17.8.1.2. Monitorización
- 17.8.2. Depuradores de código en Linux
- 17.8.3. Depuradores de código en Windows

17.9. *Sandbox*
- 17.9.1. Arquitectura de un *Sandbox*
- 17.9.2. Evasión de un *Sandbox*
- 17.9.3. Técnicas de detección
- 17.9.4. Técnicas de evasión
- 17.9.5. Contramedidas
- 17.9.6. *Sandbox* en Linux
- 17.9.7. *Sandbox* en Windows
- 17.9.8. *Sandox* en MacOS
- 17.9.9. *Sandbox* en Android

17.10. Análisis de malware
- 17.10.1. Métodos de análisis de *malware*
- 17.10.2. Técnicas de ofuscación de *malware*
  - 17.10.2.1. Ofuscación de ejecutables
  - 17.10.2.2. Restricción de entornos de ejecución
- 17.10.3. Herramientas de análisis de *malware*

Módulo 18. Desarrollo seguro

18.1. Desarrollo seguro
- 18.1.1. Calidad, funcionalidad y seguridad
- 18.1.2. Confidencialidad, integridad y disponibilidad
- 18.1.3. Ciclo de vida del desarrollo de software

18.2. Fase de Requerimientos
- 18.2.1. Control de la autenticación
- 18.2.2. Control de roles y privilegios
- 18.2.3. Requerimientos orientados al riesgo
- 18.2.4. Aprobación de privilegios

18.3. Fases de análisis y diseño
- 18.3.1. Acceso a componentes y administración del sistema
- 18.3.2. Pistas de auditoría
- 18.3.3. Gestión de sesiones
- 18.3.4. Datos históricos
- 18.3.5. Manejo apropiado de errores
- 18.3.6. Separación de funciones

18.4. Fase de Implementación y codificación
- 18.4.1. Aseguramiento del ambiente de desarrollo
- 18.4.2. Elaboración de la documentación técnica
- 18.4.3. Codificación segura
- 18.4.4. Seguridad en las comunicaciones

18.5. Buenas prácticas de codificación segura
- 18.5.1. Validación de datos de entrada
- 18.5.2. Codificación de los datos de salida
- 18.5.3. Estilo de programación
- 18.5.4. Manejo de registro de cambios
- 18.5.5. Prácticas criptográficas
- 18.5.6. Gestión de errores y logs
- 18.5.7. Gestión de archivos
- 18.5.8. Gestión de memoria
- 18.5.9. Estandarización y reutilización de funciones de seguridad

18.6. Preparación del servidor y *Hardening*
- 18.6.1. Gestión de usuarios, grupos y roles en el servidor
- 18.6.2. Instalación de software
- 18.6.3. *Hardening* del servidor
- 18.6.4. Configuración robusta del entorno de la aplicación

18.7. Preparación de la BBDD y *Hardening*
- 18.7.1. Optimización del motor de BBDD
- 18.7.2. Creación del usuario propio para la aplicación
- 18.7.3. Asignación de los privilegios precisos para el usuario
- 18.7.4. *Hardening* de la BBDD

18.8. Fase de pruebas
- 18.8.1. Control de calidad en controles de seguridad
- 18.8.2. Inspección del código por fases
- 18.8.3. Comprobación de la gestión de las configuraciones
- 18.8.4. Pruebas de caja negra

18.9. Preparación del paso a producción
- 18.9.1. Realizar el control de cambios
- 18.9.2. Realizar procedimiento de paso a producción
- 18.9.3. Realizar procedimiento de *rollback*
- 18.9.4. Pruebas en fase de preproducción

18.10. Fase de mantenimiento
- 18.10.1. Aseguramiento basado en riesgos
- 18.10.2. Pruebas de mantenimiento de seguridad de caja blanca
- 18.10.3. Pruebas de mantenimiento de seguridad de caja negra

Módulo 19. Análisis forense

19.1. Adquisición de datos y duplicación
- 19.1.1. Adquisición de datos volátiles
  - 19.1.1.1. Información del sistema
  - 19.1.1.2. Información de la red
  - 19.1.1.3. Orden de volatilidad
- 19.1.2. Adquisición de datos estáticos
  - 19.1.2.1. Creación de una imagen duplicada
  - 19.1.2.2. Preparación de un documento para la cadena de custodia
- 19.1.3. Métodos de validación de los datos adquiridos
  - 19.1.3.1. Métodos para Linux
  - 19.1.3.2. Métodos para Windows

19.2. Evaluación y derrota de técnicas antiforenses
- 19.2.1. Objetivos de las técnicas antiforenses
- 19.2.2. Borrado de datos
  - 19.2.2.1. Borrado de datos y ficheros
  - 19.2.2.2. Recuperación de archivos
  - 19.2.2.3. Recuperación de particiones borradas
- 19.2.3. Protección por contraseña
- 19.2.4. Esteganografía
- 19.2.5. Borrado seguro de dispositivos
- 19.2.6. Encriptación

19.3. Análisis Forense del sistema operativo
- 19.3.1. Análisis forense de Windows
- 19.3.2. Análisis forense de Linux
- 19.3.3. Análisis forense de Mac

19.4. Análisis Forense de la red
- 19.4.1. Análisis de los logs
- 19.4.2. Correlación de datos
- 19.4.3. Investigación de la red
- 19.4.4. Pasos a seguir en el análisis forense de la red

19.5. Análisis forense Web
- 19.5.1. Investigación de los ataques webs
- 19.5.2. Detección de ataques
- 19.5.3. Localización de direcciones IPs

19.6. Análisis forense de bases de datos
- 19.6.1. Análisis forense en MSSQL
- 19.6.2. Análisis forense en MySQL
- 19.6.3. Análisis forense en PostgreSQL
- 19.6.4. Análisis forense en MongoDB

19.7. Análisis forense en *cloud*
- 19.7.1. Tipos de crímenes en *cloud*
  - 19.7.1.1. *Cloud* como sujeto
  - 19.7.1.2. *Cloud* como objeto
  - 19.7.1.3. *Cloud* como herramienta
- 19.7.2. Retos del análisis forense en *cloud*
- 19.7.3. Investigación de los servicios de almacenamiento el *cloud*
- 19.7.4. Herramientas de análisis forense para *cloud*

19.8. Investigación de crímenes de correo electrónico
- 19.8.1. Sistemas de correo
  - 19.8.1.1. Clientes de correo
  - 19.8.1.2. Servidor de correo
  - 19.8.1.3. Servidor SMTP
  - 19.8.1.4. Servidor POP3
  - 19.8.1.5. Servidor IMAP4
- 19.8.2. Crímenes de correo
- 19.8.3. Mensaje de correo
  - 19.8.3.1. Cabeceras estándar
  - 19.8.3.2. Cabeceras extendidas
- 19.8.4. Pasos para la investigación de estos crímenes
- 19.8.5. Herramientas forenses para correo electrónico

19.9. Análisis forense de móviles
- 19.9.1. Redes celulares
  - 19.9.1.1. Tipos de redes
  - 19.9.1.2. Contenidos del CDR
- 19.9.2. *Subscriber Identity Module* (SIM)
- 19.9.3. Adquisición lógica
- 19.9.4. Adquisición física
- 19.9.5. Adquisición del sistema de ficheros

19.10. Redacción y presentación de Informes forenses
- 19.10.1. Aspectos importantes de un Informe forense
- 19.10.2. Clasificación y tipos de informes
- 19.10.3. Guía para escribir un informe
- 19.10.4. Presentación del informe
  - 19.10.4.1. Preparación previa para testificar
  - 19.10.4.2. Deposición
  - 19.10.4.3. Trato con los medios

Módulo 20. Retos actuales y futuros en seguridad informática

20.1. Tecnología *blockchain*
- 20.1.2. Ámbitos de aplicación
- 20.1.3. Garantía de confidencialidad
- 20.1.4. Garantía de no-repudio

20.2. Dinero digital
- 20.2.1. Bitcoins
- 20.2.2. Critpomonedas
- 20.2.3. Minería de criptomonedas
- 20.2.4. Estafas piramidales
- 20.2.5. Otros potenciales delitos y problemas

20.3. *Deepfake*
- 20.3.2. Impacto en los medios
- 20.3.3. Peligros para la sociedad
- 20.3.4. Mecanismos de detección



20.4. El futuro de la inteligencia artificial
- 20.4.1. Inteligencia artificial y computación cognitiva
- 20.4.2. Usos para simplificar el servicio a clientes

20.5. Privacidad digital
- 20.5.1. Valor de los datos en la red
- 20.5.2. Uso de los datos en la red
- 20.5.3. Gestión de la privacidad e identidad digital

20.6. Ciberconflictos, cibercriminales y ciberataques
- 20.6.1. Impacto de la ciberseguridad en conflictos internacionales
- 20.6.2. Consecuencias de ciberataques en la población general
- 20.6.3. Tipos de cibercriminales. Medidas de protección

20.7. Teletrabajo
- 20.7.1. Revolución del teletrabajo durante y post Covid19
- 20.7.2. Cuellos de botella en el acceso
- 20.7.3. Variación de la superficie de ataque
- 20.7.4. Necesidades de los trabajadores

20.8. Tecnologías *wireless* emergentes
- 20.8.1. WPA3
- 20.8.2. 5G
- 20.8.3. Ondas milimétricas
- 20.8.4. Tendencia en *"Get Smart"* en vez de *"Get more"*

20.9. Direccionamiento futuro en redes
- 20.9.1. Problemas actuales con el direccionamiento IP
- 20.9.2. IPv6
- 20.9.2. IPv4+
- 20.9.3. Ventajas de IPv4+ sobre IPv4
- 20.9.4. Ventajas de IPv6 sobre IPv4

20.10. El reto de la concienciación de la formación temprana y continua de la población
- 20.10.1. Estrategias actuales de los gobiernos
- 20.10.2. Resistencia de la población al aprendizaje
- 20.10.3. Planes de formación que deben adoptar las empresas

06

Metodología

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

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





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

Estudio de Caso para contextualizar todo el contenido

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

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



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



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

Un método de aprendizaje innovador y diferente

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

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

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

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

Relearning Methodology

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

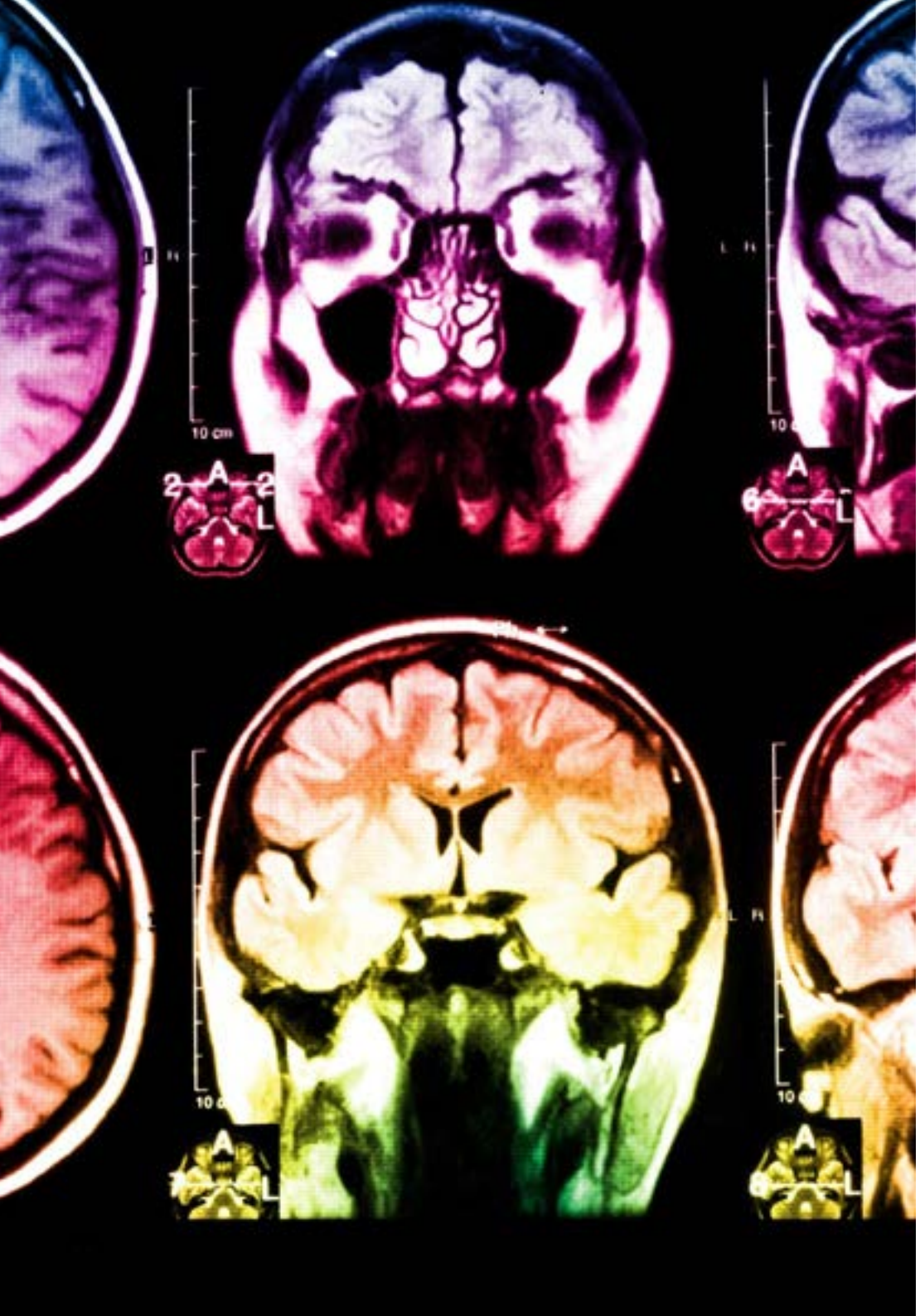
Potenciamos el Estudio de Caso con el mejor método de enseñanza 100% online: el Relearning.

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

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

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





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

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

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

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

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

Material de estudio

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

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

Clases magistrales

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

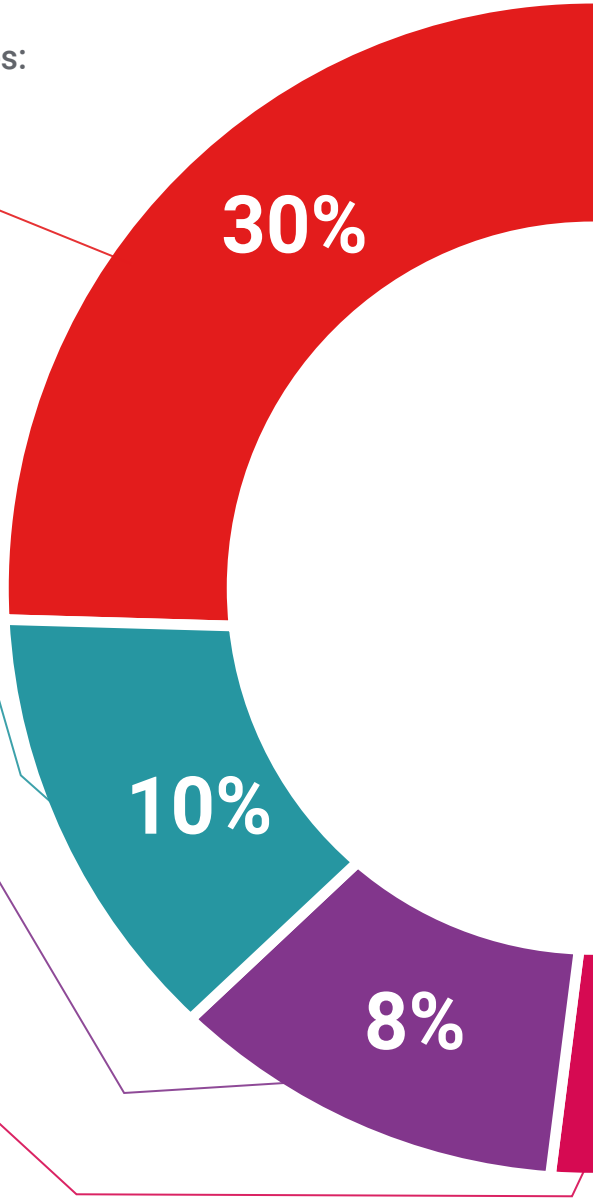
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

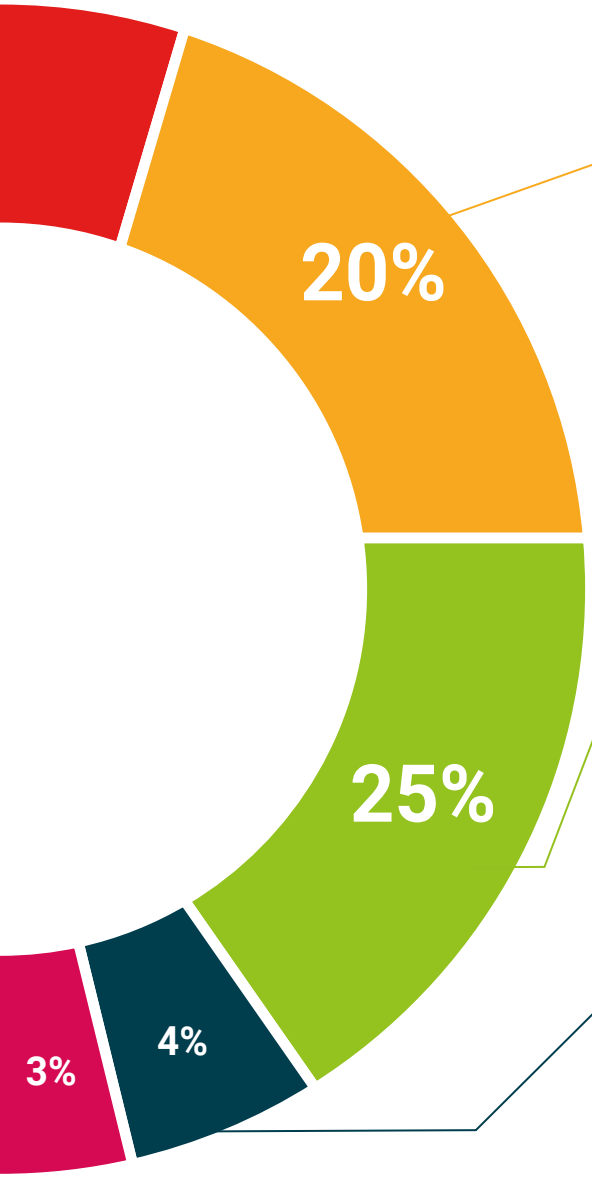
Prácticas de habilidades y competencias

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

Lecturas complementarias

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





Case studies

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

Resúmenes interactivos

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

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

Testing & Retesting

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

07

Titulación

El Grand Master en Secure Information Management garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de Grand Master expedido por TECH Universidad Tecnológica.





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

Este **Grand Master en Secure Information Management** contiene el programa más completo y actualizado del mercado.

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

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

Título: **Grand Master en Secure Information Management**

N.º Horas Oficiales: **3.000 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

GRAND MASTER

en

Secure Information Management

Se trata de un título propio de esta Universidad con una duración de 3.000 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Grand Master en Secure Information Management

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Analítica del dato en la organización empresarial	150	OB
1º	Gestión, manipulación de datos e información para ciencia de datos	150	OB
1º	Dispositivos y plataformas IoT como base para la ciencia de datos	150	OB
1º	Representación gráfica para análisis de datos	150	OB
1º	Herramientas de ciencia de datos	150	OB
1º	Minería de datos. selección, preprocesamiento y transformación	150	OB
1º	Predictibilidad y análisis de fenómenos estocásticos	150	OB
1º	Diseño y desarrollo de sistemas inteligentes	150	OB
1º	Arquitecturas y sistemas para uso intensivo de datos	150	OB
1º	Aplicación práctica de la ciencia de datos en sectores de actividad empresarial	150	OB
2º	Ciberinteligencia y ciberseguridad	150	OB
2º	Seguridad en Host	150	OB
2º	Seguridad en red (Perimetral)	150	OB
2º	Seguridad en smartphones	150	OB
2º	Seguridad en IoT	150	OB
2º	*Hacking* ético	150	OB
2º	Ingeniería inversa	150	OB
2º	Desarrollo seguro	150	OB
2º	Análisis forense	150	OB
2º	Retos actuales y futuros en seguridad informática	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

Grand Master

Secure Information Management

Modalidad: **Online**

Duración: **2 años**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **3.000 h.**

Grand Master

Secure Information Management



tech universidad tecnológica