Grand Master

Computer Science, Ciberseguridad y Análisis de Datos



tech universidad tecnológica



tech universidad tecnológica

Grand Master

Computer Science, Ciberseguridad y Análisis de Datos

Modalidad: **Online**
Duración: **2 años**
Titulación: **TECH Universidad Tecnológica**
Horas lectivas: **3.000 h.**
Acceso web: **www.techtitute.com/informatica/grand-master/grand-master-computer-science-ciberseguridad-analisis-datos**

Índice

01 Presentación — pág. 4

02 Objetivos — pág. 8

03 Competencias — pág. 20

04 Dirección del curso — pág. 24

05 Estructura y contenido — pág. 32

06 Metodología — pág. 60

07 Titulación — pág. 68

01

Presentación

En un mundo como el actual, que avanza hacia la completa digitalización, el profesional de la Informática necesita mantener sus capacidades totalmente puestas al día para poder seguir actuando en su campo de competencia de manera óptima, sin perder ninguno de los avances que, de manera vertiginosa, se van incorporando a este territorio. La aparición de nuevos sistemas de generación de datos e información se han convertido en el centro del desarrollo de muchas industrias e individuos. Cada vez más procesos, operaciones y tareas básicas de todo tipo se realizan a través de un dispositivo electrónico. Pero este progreso tiene también ciertos riesgos, ya que todo tipo de dispositivos y aplicaciones digitales pueden ser susceptibles de recibir ataques informáticos. Por este motivo, se ha ideado un programa 100% online que se centra en abordar todas las líneas de conocimientos necesarios para el procesamiento y extracción de datos, el abordaje de la Ciberseguridad y la profundización en *Computer Science*, siguiendo una perspectiva teórica y práctica.





Conviértete en un experto de la Ciberseguridad dominando la Computer Science y analítica de datos, mejorando enormemente tu empleabilidad en un sector cada vez más pujante"

Impulsada por los continuos avances que experimenta la Informática, no sólo la tecnología ha disfrutado de grandes mejoras, sino también las propias herramientas digitales con las que se realizan numerosas tareas en la actualidad. La otra cara de la moneda es que dichos avances han conllevado también el aumento de vulnerabilidades Informáticas. Por esta razón, cada vez más empresas buscan profesionales especializados en Ciberseguridad que sean capaces de proporcionarles la protección adecuada contra todo tipo de ataques informáticos.

En este Grand Master, el informático podrá profundizar en aspectos como la seguridad en el desarrollo y diseño de sistemas, las mejores técnicas criptográficas o la seguridad en entornos *Cloud Computing*. Asimismo, el presente programa se centra en los fundamentos de programación y la estructura de datos, la algoritmia y complejidad, así como el diseño avanzado de algoritmos, la programación avanzada, o los procesadores de lenguajes y la Informática gráfica, entre otros aspectos. Todo ello, contando con numerosos recursos didácticos multimedia, impartidos por el profesorado más prestigioso y especializado en el ámbito.

Por otro lado, esta titulación aborda, desde una perspectiva técnica y de negocio, la ciencia del dato, ofreciendo todos los conocimientos necesarios para la extracción del conocimiento oculto en ellos. De esta forma, los informáticos podrán analizar con detalles los distintos algoritmos, plataformas y herramientas más actuales para la exploración, visualización, manipulación, procesamiento y análisis de los datos. Todo lo anterior, complementado con el desarrollo de habilidades empresariales, necesarias para alcanzar un perfil a nivel ejecutivo capaz de tomar decisiones claves en una empresa.

Así, esta capacitación proporciona al profesional las herramientas y habilidades específicas para que desarrolle con éxito su actividad profesional en el amplio entorno de la computación. Trabajando competencias claves como el conocimiento de la realidad y práctica diaria en distintas áreas Informáticas y desarrollando la responsabilidad en el seguimiento y supervisión de su trabajo, así como habilidades específicas dentro de cada campo.

Con esta titulación, los informáticos serán capaces de especializarse en Computer Science, Ciberseguridad y Análisis de Datos convirtiéndose en la oportunidad perfecta para potenciar su carrera profesional. Todo esto, será tangible gracias a un programa 100% online, que se adapta a las necesidades diarias de los profesionales, por lo que solo será necesario contar con un dispositivo con conexión a internet para empezar a trabajar por un perfil profesional completo y con proyección internacional.

Este **Grand Master en Computer Science, Ciberseguridad y Análisis de Datos** 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 para la Ciberseguridad y el Análisis de Datos
- 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

De forma cómoda y sencilla, adquiere los conocimientos necesarios en Computer Science, Ciberseguridad y Análisis de Datos para realizar programaciones Informáticas de calidad”

TECH pone a tu servicio un material didáctico amplio y claro, que incorpora todos los temas de interés en la actualidad, para que sigas avanzando en computación”

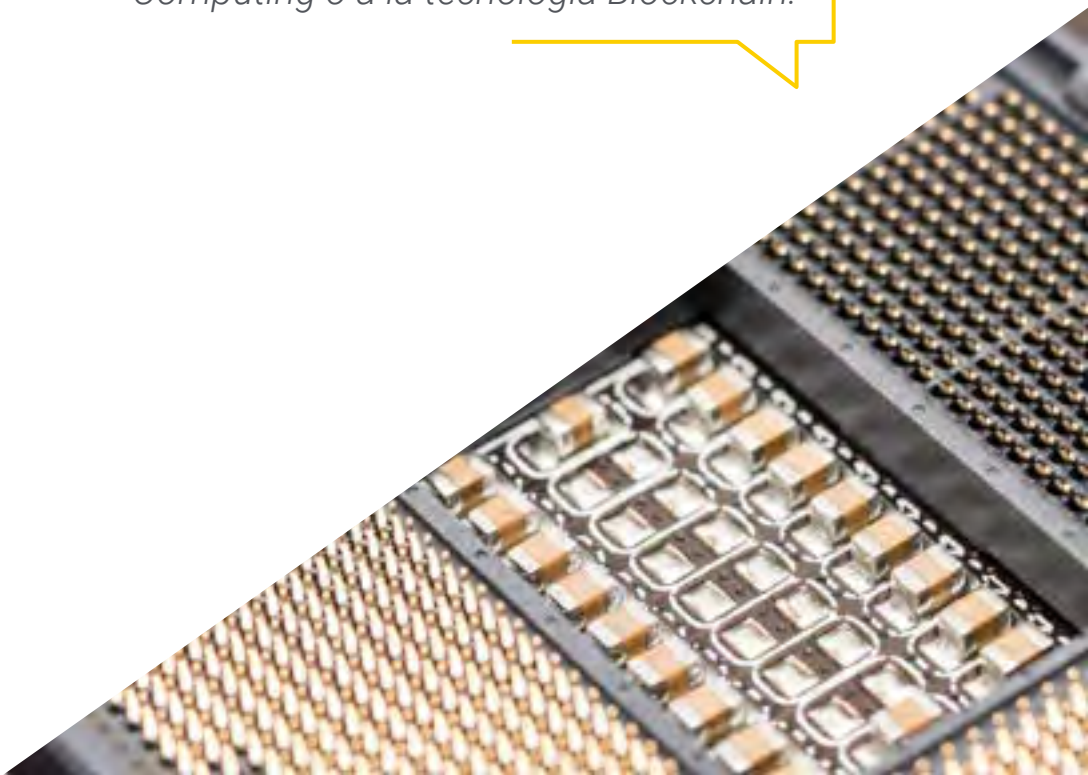
Potencia tu carrera determinando la creación de cuadros de mando y KPI’s en función del departamento en el que trabajes.

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

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



02

Objetivos

El Grand Master en Computer Science, Ciberseguridad y Análisis de Datos se ha creado de manera específica para el informático que busca avanzar en este campo de forma rápida y con calidad real. Por este motivo, se ha organizado un programa con base en objetivos realistas y de alto valor que le impulsarán a otro nivel de trabajo en este campo. El profesional se centrará en el estudio de las diferentes técnicas, tecnologías y fases necesarias para la computación, desde una perspectiva a disruptiva, completa y actualizada.

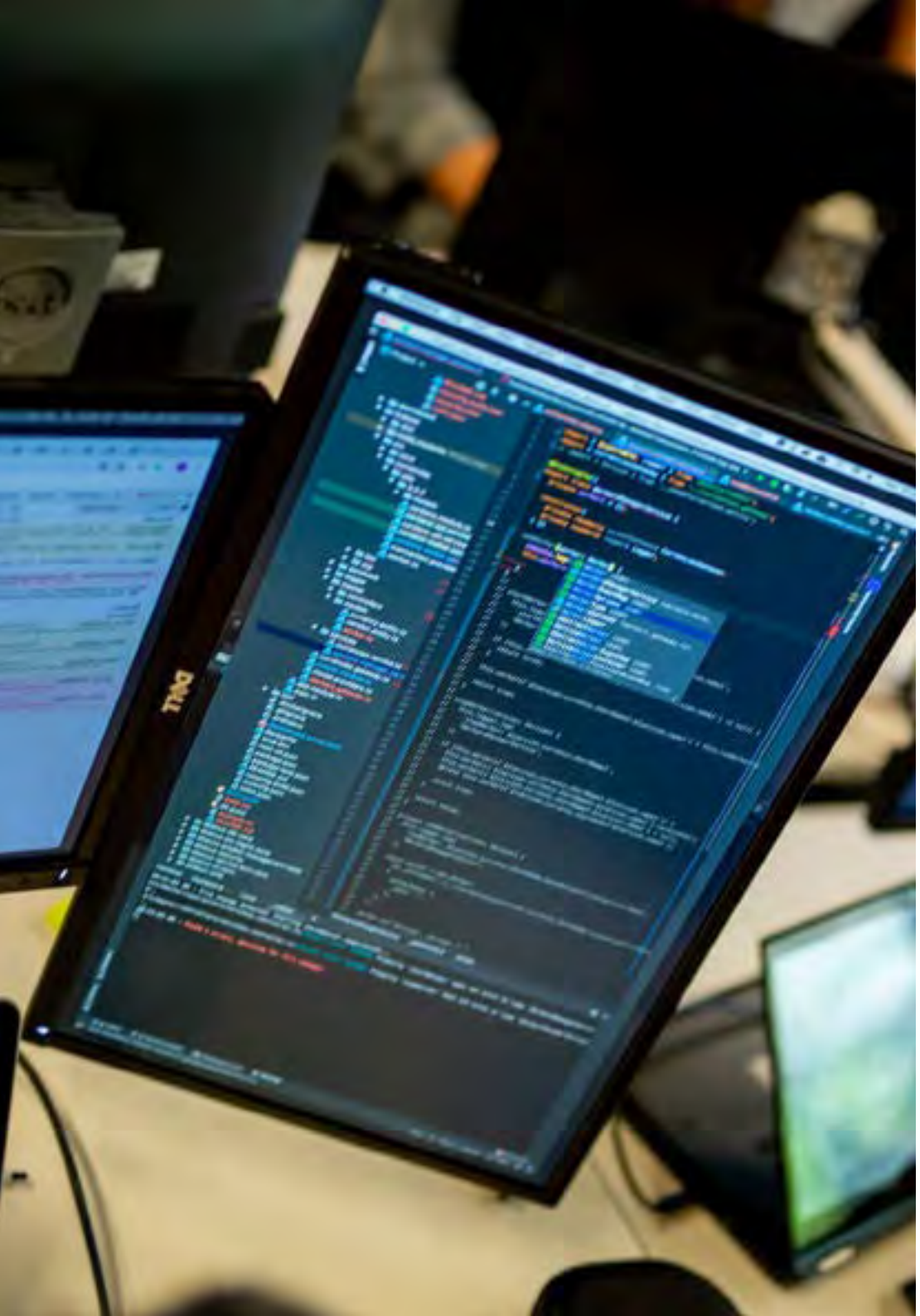




TECH pone a tu servicio una titulación de alta calidad que te permita intervenir con solvencia en computación, garantizando la seguridad de tu empresa"

Objetivos generales

- Estar al día científica y tecnológicamente, así como preparar para el ejercicio profesional de la computación y los lenguajes de forma transversal y versátil adaptada a las nuevas tecnologías e innovaciones en este campo
- Generar conocimiento especializado sobre un sistema de información, tipos y aspectos de seguridad que deben ser tenidos en cuenta
- Identificar las vulnerabilidades de un sistema de información
- Desarrollar la normativa legal y tipificación del delito atacando a un sistema de información
- Evaluar los diferentes modelos de arquitectura de seguridad para establecer el modelo más adecuado a la organización
- Identificar los marcos normativos de aplicación y las bases reguladoras de los mismos
- Analizar la estructura organizativa y funcional de un área de seguridad de la información (la oficina del CISO)
- Analizar y desarrollar el concepto de riesgo, incertidumbre dentro del entorno en que vivimos
- Examinar el modelo de gestión de riesgos basado en la Iso 31.000
- Examinar la ciencia de la criptología y la relación con sus ramas: criptografía, criptoanálisis, esteganografía y estegoanálisis
- Analizar los tipos de criptografía según el tipo de algoritmo y según su uso
- Examinar los certificados digitales
- Examinar la Infraestructura de Clave Pública (PKI)
- Desarrollar el concepto de gestión de identidades
- Identificar los métodos de autenticación
- Generar conocimiento especializado sobre el ecosistema de seguridad Informática
- Evaluar el conocimiento en término de Ciberseguridad
- Identificar los ámbitos de seguridad en *Cloud*
- Analizar los servicios y herramientas en cada uno de los ámbitos de seguridad
- Desarrollar las especificaciones de seguridad de cada tecnología LPWAN
- Analizar de forma comparativa la seguridad de las tecnologías LPWAN
- 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



Objetivos específicos

Módulo 1. Fundamentos de programación

- Comprender la estructura básica de un ordenador, el software y de los lenguajes de programación de propósito general
- Aprender a diseñar e interpretar algoritmos, que son la base necesaria para poder desarrollar programas informáticos
- Entender los elementos esenciales de un programa informático, como son los distintos tipos de datos, operadores, expresiones, sentencias, E/S y sentencias de control
- Comprender las distintas estructuras de datos disponibles en los lenguajes de programación de propósito general tanto estáticas como dinámicas, así como adquirir los conocimientos esenciales para el manejo de ficheros
- Conocer las distintas técnicas de pruebas en los programas informáticos y la importancia de generar una buena documentación junto con un buen código fuente
- Aprender los conceptos básicos del lenguaje de programación C++, uno de los más usados a nivel mundial

Módulo 2. Estructura de Datos

- Aprender los fundamentos de la programación en el lenguaje C++, incluyendo clases, variables, expresiones condicionales y objetos
- Entender los tipos abstractos de datos, los tipos de estructuras de datos lineales, estructuras de datos jerárquicas simples y complejas, así como su implementación en C++
- Comprender el funcionamiento de estructuras de datos avanzadas distintas de las habituales
- Conocer la teoría y la práctica relacionada con el uso de montículos y colas de prioridad
- Aprender el funcionamiento de las tablas *Hash*, como tipos abstractos de datos y funciones
- Entender la teoría de Grafos, así como algoritmos y concepto avanzados sobre Grafos

Módulo 3. Algoritmia y complejidad

- Aprender las principales estrategias de diseño de algoritmos, así como los distintos métodos y medidas para de cálculo de los mismos
- Conocer los principales algoritmos de ordenación usados en el desarrollo de software
- Entender el funcionamiento de los distintos algoritmos con árboles, *Heaps* y Grafos
- Comprender el funcionamiento de los algoritmos *Greedy*, su estrategia y ejemplos de su uso en los principales problemas conocidos. Conoceremos también el uso de algoritmos *Greedy* sobre Grafos
- Aprenderemos las principales estrategias de búsqueda de caminos mínimos, con el planteamiento de problemas esenciales del ámbito y algoritmos para su resolución
- Entender la técnica de *Backtracking* y sus principales usos, así como otras técnicas alternativas

Módulo 4. Diseño avanzado de algoritmos

- Profundizar en el diseño avanzado de algoritmos, analizando algoritmos recursivos y tipo divide y conquista, así como realizando análisis amortizado
- Comprender los conceptos de programación dinámica y los algoritmos para problemas NP
- Entender el funcionamiento de la optimización combinatoria, así como los distintos algoritmos de aleatorización y algoritmos paralelos
- Conocer y comprender el funcionamiento de los distintos métodos de búsqueda local y con candidatos
- Aprender los mecanismos de verificación de formal de programas y de programas iterativos, incluyendo la lógica de primer orden y el sistema formal de Hoare
- Aprender el funcionamiento de algunos de los principales métodos numéricos como el método de la bisección, el método de Newton-Raphson y el método de la secante

Módulo 5. Programación avanzada

- Profundizar en los conocimientos de programación, especialmente en lo relacionado a la programación orientada a objetos, y los distintos tipos de relaciones entre clases existentes
- Conocer los distintos patrones de diseño para problemas orientados a objetos
- Aprender sobre la programación orientada a eventos y el desarrollo de *Interfaces* de usuario con Qt
- Adquirir los conocimientos esenciales de la programación concurrente, los procesos y los hilos
- Aprender a gestionar el uso de los hilos y la sincronización, así como la resolución de los problemas comunes dentro de la programación concurrente
- Entender la importancia de la documentación y las pruebas en el desarrollo del software

Módulo 6. Informática teórica

- Comprender los conceptos matemáticos teóricos esenciales tras la Informática, como son la lógica proposicional, la teoría de conjuntos y los conjuntos numerables y no numerables
- Entender los conceptos de lenguajes y gramáticas formales, así como el de máquinas de Turing en sus distintas variantes
- Aprender sobre los distintos tipos de problemas indecibles y de problemas intratables, incluyendo las distintas variantes de los mismos y sus aproximaciones
- Comprender el funcionamiento de las distintas clases de lenguajes basados en la aleatorización y otros tipos de clases y gramáticas
- Conocer otros sistemas de avanzados cómputo como son la computación con membranas, la computación con ADN y la computación cuántica

Módulo 7. Teoría de autómatas y lenguajes formales

- Comprender la teoría de autómatas y lenguajes formales, aprendiendo los conceptos de alfabetos, cadenas y lenguajes, así como a realizar demostraciones formales
- Profundizar en los distintos tipos de autómatas finitos, ya sean deterministas o no deterministas
- Aprender los conceptos básicos y avanzados relacionados con los lenguajes y las expresiones regulares, así como la aplicación del lema de bombeo y la clausura de los lenguajes regulares
- Entender las gramáticas independientes de contexto, así como el funcionamiento de los autómatas a Pila
- Profundizar en las formas normales, el lema de bombeo de las gramáticas independientes de contexto y propiedades de los lenguajes independientes de contexto

Módulo 8. Procesadores de lenguajes

- Introducir los conceptos relacionados con el proceso de compilación y los distintos tipos de análisis: léxico, sintáctico y semántico
- Conocer el funcionamiento de un analizador léxico, su implementación y recuperación de errores
- Profundizar en el conocimiento del análisis sintáctico, tanto descendente como ascendente, pero profundizando especialmente en los distintos tipos de analizadores sintácticos ascendentes
- Entender el funcionamiento de los analizadores semánticos, la tradición dirigida por la sintaxis, la tabla de símbolos y los distintos tipos
- Aprender los distintos mecanismos de generación de código, tanto en entornos de ejecución como para la generación de código intermedio
- Sentar las bases de la optimización de código, incluyendo la reordenación de expresiones y la optimización de bucles

Módulo 9. Informática gráfica y visualización

- Introducir los conceptos esenciales de la Informática gráfica y la visualización por ordenador, como la teoría del color y sus modelos y las propiedades de la luz
- Comprender el funcionamiento de las primitivas de salida y sus algoritmos, tanto de dibujo de líneas, como de dibujo de circunferencias y de relleno
- Profundizar en el estudio de las distintas transformaciones tanto 2D como 3D, y sus sistemas de coordenadas y visualización por ordenador
- Aprender a realizar proyecciones y cortes en 3D, así como la eliminación de superficies ocultas
- Aprender la teoría relacionada con la interpolación y curvas paramétricas, así como lo relacionado con las Curvas Bézier y los *B-Splines*

Módulo 10. Computación bioinspirada

- Introducir el concepto de computación bioinspirada, así como comprender el funcionamiento de los distintos tipos de algoritmos de adaptación social y de algoritmos genéticos
- Profundizar en el estudio de los distintos modelos de computación evolutiva, conociendo sus estrategias, programación, algoritmos y modelos basados en estimación de distribuciones
- Entender las principales estrategias de exploración-explotación del espacio para algoritmos genéticos
- Comprender el funcionamiento de la programación evolutiva aplicada a problemas de aprendizaje y de los problemas multiobjetivo
- Aprender los conceptos esenciales relacionados con redes neuronales y entender el funcionamiento de casos de uso reales aplicados a áreas tan dispares como la investigación médica, la economía y la visión artificial

Módulo 11. Seguridad en el diseño y desarrollo de sistemas

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

Módulo 12. Arquitecturas y modelos de seguridad de la información

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





Módulo 13. Gestión de la seguridad IT

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

Módulo 14. Análisis de riesgos y entorno de Seguridad IT

- Examinar, con una visión holística, el entorno en el que nos movemos
- Identificar los principales riesgos y oportunidades que pueden afectar a la consecución de nuestros objetivos
- Analizar los riesgos en base a las mejores prácticas a nuestro alcance
- Evaluar el posible impacto de dichos riesgos y oportunidades
- Desarrollar técnicas que nos permitan tratar los riesgos y oportunidades de manera que maximicemos nuestro aporte de valor
- Examinar en profundidad las diferentes técnicas de transferencia de riesgos, así como de valor

- Generar valor desde el diseño de modelos propios para la gestión ágil de riesgos
- Examinar los resultados para proponer mejoras continuas en gestión de proyectos y procesos basados en modelos de gestión impulsados por el riesgo o *Risk-Driven*
- Innovar y transformar los datos generales en información relevante para la toma de decisiones basadas en el riesgo

Módulo 15. Criptografía en IT

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

Módulo 16. Gestión de identidad y accesos en seguridad IT

- Desarrollar el concepto de identidad digital
- Evaluar el control de acceso físico a la información
- Fundamentar la autenticación biométrica y la autenticación MFA
- Evaluar ataques relacionados con la confidencialidad de la información
- Analizar la federación de identidades
- Establecer el control de acceso a la red

Módulo 17. Seguridad en comunicaciones y operación software

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

Módulo 18. Seguridad en entornos *cloud*

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

Módulo 19. Seguridad en comunicaciones de dispositivos Iot

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

Módulo 20. Plan de continuidad del negocio asociado a la seguridad

- Presentar los elementos clave de cada fase y analizar las características del plan de continuidad de negocio (PCN)
- Fundamentar la necesidad de un Plan de Continuidad para el Negocio
- Determinar los mapas de éxito y riesgo de cada fase del plan de continuidad de negocio
- Concretar cómo se establece un plan de acción para la implantación
- Evaluar la completitud de un Plan de Continuidad del Negocio (PCN)
- Desarrollar el plan de implantación con éxito de un plan de continuidad para nuestro negocio

Módulo 21. 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 22. 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 23. 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 24. 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 25. 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 26. 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 27. 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 28. 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 29. 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 30. 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

Alcanza la excelencia cumpliendo con un programa que te capacitará para generar conocimiento especializado en Computer Science, Ciberseguridad y Análisis de Datos”

03

Competencias

Tras superar las evaluaciones del presente programa, el informático habrá adquirido las competencias necesarias para conocer los principios fundamentales de la computación con la capacidad de trabajar con lenguajes de programación y datos. Esto le permitirá ser capaz de aspirar a una mejora en sus labores diarias en esta área de especialización, lo que se convierte en una oportunidad para ofrecer conocimiento de valor al momento de tomar decisiones que afecten el funcionamiento de los departamentos de una empresa.





Adquiere las competencias necesarias para llevar tu profesión al máximo nivel, gracias a este Grand Master que te permitirá actualizarte y adaptarte al nuevo entorno informático"

Competencias generales

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



Competencias específicas

- Diseñar algoritmos para desarrollar programas informáticos y aplicar el lenguaje de programación
- Comprender y utilizar la estructura de datos informáticos
- Utilizar los algoritmos necesarios para la resolución de problemas informáticos
- Conocer en profundidad el diseño avanzado de algoritmos, así como los métodos de búsqueda
- Llevar a cabo tareas de programación Informática
- Comprender y aplicar la teoría que existe detrás de la Informática, como es el caso de las matemáticas
- Conocer la teoría de autómatas y aplicar el lenguaje informático
- Conocer los fundamentos teóricos de los lenguajes de programación y las técnicas de procesamiento léxico, sintáctico y semántico asociadas
- Comprender los conceptos básicos de matemática y complejidad computacional para aplicarlos a la resolución de problemas informáticos
- Conocer y aplicar los principios fundamentales de la computación para realizar nuevos desarrollos informáticos
- Desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI)
- Identificar los elementos claves que conforman un SGSI
- Aplicar la metodología MAGERIT para evolucionar el modelo y llevarlo un paso más allá
- Diseñar nuevas metodologías de gestión de riesgos propias, basadas en el concepto *Agile Risk Management*
- Identificar, analizar, evaluar y tratar los riesgos a los que se enfrenta el profesional desde una nueva perspectiva empresarial basada en un modelo *Risk-Driven* o impulsado por el riesgo que permita no sólo sobrevivir en propio entorno, sino impulsar el aporte de valor propio
- Examinar el proceso de diseño de una estrategia de seguridad al desplegar servicios corporativos en *Cloud*
- Evaluar las diferencias en las implementaciones concretas de diferentes vendedores de *Cloud* pública
- Evaluar las opciones de conectividad IoT para afrontar un proyecto, con especial énfasis en tecnologías LPWAN
- Presentar las especificaciones básicas de las principales tecnologías LPWAN para el IoT
- 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

04

Dirección del curso

Abordar con éxito el ámbito de Computer Science, la Ciberseguridad y el Análisis de Datos exige una profundización completa y detallada. Por esa razón, TECH ha reunido al mejor profesorado especializado en cada área. Así, el informático cuenta con el acompañamiento de profesionales de renombre que ponen a su disposición sus múltiples años de experiencia y capacitación. De esta forma, los informáticos pueden tener la seguridad de recibir conocimientos actuales y específicos de un sector en auge a nivel internacional.





Disfrutarás del acompañamiento y supervisión de un cuadro docente que está al tanto de los últimos avances en Ciberseguridad y Análisis de Datos”

Dirección



D. Olalla Bonal, Martín

- Especialista técnico en *Blockchain* en IBM SPGI
- Especialista en ventas técnicas en *Blockchain*. IBM
- Director de Arquitectura. *Blocknitive*
- Técnico en electrónica digital
- *Blockchain Architect -IT Infrastructure Architect* - Gestor de proyectos IT. Ámbitos de negocio: Software, Infraestructura, Telecomunicaciones



Dr. Peralta Martín-Palomino, Arturo

- CEO y CTO en Prometeus Global Solutions
- CTO 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

Profesores

D. Tobal Redondo, Javier

- Gerente del programa de innovación de aplicaciones de HUAWEI
- Responsable de seguridad de la información de la división de medios de pago. Amadeus IT Group
- Jefe de seguridad de la información de FINTONIC, Servicios Financieros
- Ingeniero de servicios y arquitecto en el área de Planificación y arquitectura de servicios y
- seguridad en Amena / Orange España
- Licenciado en Informática por la Universidad de Deusto (Bilbao, España)
- Posgrado en Informática Industrial. Escuela de Ingeniería Industrial. Bilbao

D. Gonzalo Alonso, Félix

- Director general y fundador. Smart REM Solutions
- Socio fundador y responsable de ingeniería de riesgos e Innovación. Dynargy
- Gerente y socio fundador. Risknova (Gabinete pericial especializado en tecnología)
- Licenciado en Ingeniería de Organización Industrial por la Universidad Pontificia de Comillas ICAI
- Graduado en Ingeniería técnica Industrial especialidad Electrónica Industrial por la Universidad Pontificia de Comillas ICAI
- Máster en Dirección Aseguradora por ICEA (Instituto para la Colaboración entre Entidades Aseguradoras)

D. Sevillano Izquierdo, Javier

- Global Cyber Security Architect en Vodafone España
- Chief Technology Security Office (CTSO) en Vodafone España
- Responsable Seguridad Tecnológica en Bankia
- Responsable Seguridad Tecnológica en Caja Madrid
- Manager Seguridad en Sistema 4B
- SEINCA - Analista senior
- Técnico superior en Informática Empresarial por Instituto Cibernos

D. Entrenas, Alejandro

- Entelgy Innotec
- 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

D. Nogales Ávila, Javier

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

D. Gómez Rodríguez, Antonio

- Ingeniero de soluciones Cloud en Oracle
- Director de Proyectos en Sopra Group
- Director de Proyectos en Everis
- Jefe de Proyectos en Empresa pública de Gestion de Programas Culturales en la Consejería de Cultura de Andalucía
- Analista de Sistemas de Información en Sopra Group
- Licenciado en Ingeniería Superior de Telecomunicación por la Universidad Politécnica de Cataluña
- Postgrado en Tecnologías y Sistemas de Información por el Instituto Catalán de Tecnología
- *E-Business* Master por la Escuela de Negocios La Salle

D. del Valle Arias, Jorge

- Director de División IoT en Diode España
- Smart Cities Business Growth Manager Spain en Itron Inc
- Consultor IoT
- Sales Manager IoT & Celular en Aicox Soluciones
- Fundador y CEO de Sensor Intelligence
- Director de Operaciones en Codium Networks
- Jefe del Área de Electrónica en Aitemin
- Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid
- Executive MBA por la International Graduate School de La Salle de Madrid

D. Gozalo Fernández, Juan Luis

- Ingeniero Informático
- Profesor Asociado en DevOps y en Blockchain en UNIR
- Exdirector Blockchain DevOps en Alastria
- Director Desarrollo Aplicación Móvil Tinkerlink en Cronos Telecom
- Director Informática en Banco Santander
- Director Tecnología Gestión de Servicio IT en Barclays Bank España
- Licenciado en Ingeniería Superior Informática por la Universidad Nacional Educación a Distancia (UNED)

Dña. Jurado Jabonero, Lorena

- Responsable de Seguridad de la Información (CISO) en Grupo Pascual
- Graduada en Ingeniería Informática por la Universidad Alfonso X El Sabio
- Ingeniero Técnico en Informática de Gestión por la Universidad Politécnica de Madrid
- Conocimientos: ISO 27001, ISO 27701, ISO 22301, ISO 20000, RGPD/LOPDGDD, NIST CSF, CSA, ITIL, PCI, etc

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
- Licenciado 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. Lidera un equipo en Inditex en la unidad de logística de su plataforma abierta
- Senior Technical Lead y Delivery Lead Support en HCL
- Agile Coach y Director de Operaciones en Mirai Advisory
- Miembro del comité de dirección en calidad de Director de Operaciones
- Desarrollador, Team Lead, Scrum Master, Agile Coach, Product Manager en DocPath
- Ingeniería Superior en Informática por la ESI de Ciudad Real (UCLM)
- Posgraduado 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
- Varias certificaciones, algunas de las más destacables o recientes son Azure Fundamentals

Dña. Pedrajas Parabá, 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

D. Montoro Montarroso, Andrés

- Investigador en el grupo SMILe de la Universidad de Castilla-La Mancha
- Científico de Datos en Prometeus Global Solutions
- Graduado en Ingeniería Informática por la Universidad de Castilla-La Mancha
- Máster en Ciencia de Datos e Ingeniería de Computadores por la Universidad de Granada
- Profesor invitado en la asignatura de Sistemas Basados en el Conocimiento de la Escuela Superior de Informática de Ciudad Real impartiendo la conferencia: "Técnicas Avanzadas de Inteligencia Artificial: Búsqueda y análisis de potenciales radicales en Medios Sociales"
- Profesor invitado en la asignatura de Minería de Datos de la Escuela Superior de Informática de Ciudad Real impartiendo la conferencia: "Aplicaciones del Procesamiento de Lenguaje Natural: Lógica Borrosa al análisis de mensajes en redes sociales"
- Ponente en el Seminario sobre Prevención de la Corrupción en administraciones públicas e Inteligencia Artificial. Facultad de Ciencias Jurídicas y Sociales de Toledo. Conferencia titulada "Técnicas de Inteligencia Artificial". Ponente en el primer Seminario Internacional de Derecho Administrativo e Inteligencia Artificial (DAIA). Organiza Centro de Estudios Europeos Luis Ortega Álvarez e Institut de Recerca TransJus. Conferencia titulada "Análisis de Sentimientos para la prevención de mensajes de odio en las redes sociales"

D. Fondón Alcalde, Rubén

- Business Analyst para segmento pyme en Vodafone España
- Business Analyst para Southern Europe en Vodafone Global Enterprise
- Consultor senior de procesos en Unisys para Telefónica Global Solutions
- Service Integration Leader en Entelgy para Telefónica Global Solutions
- Licenciado en Ingeniería de Telecomunicaciones por la Universidad Europea de Madrid
- Master en *Big Data* y Analytics por la Universidad Internacional de Valencia

Dña. Fernández Meléndez, Galina

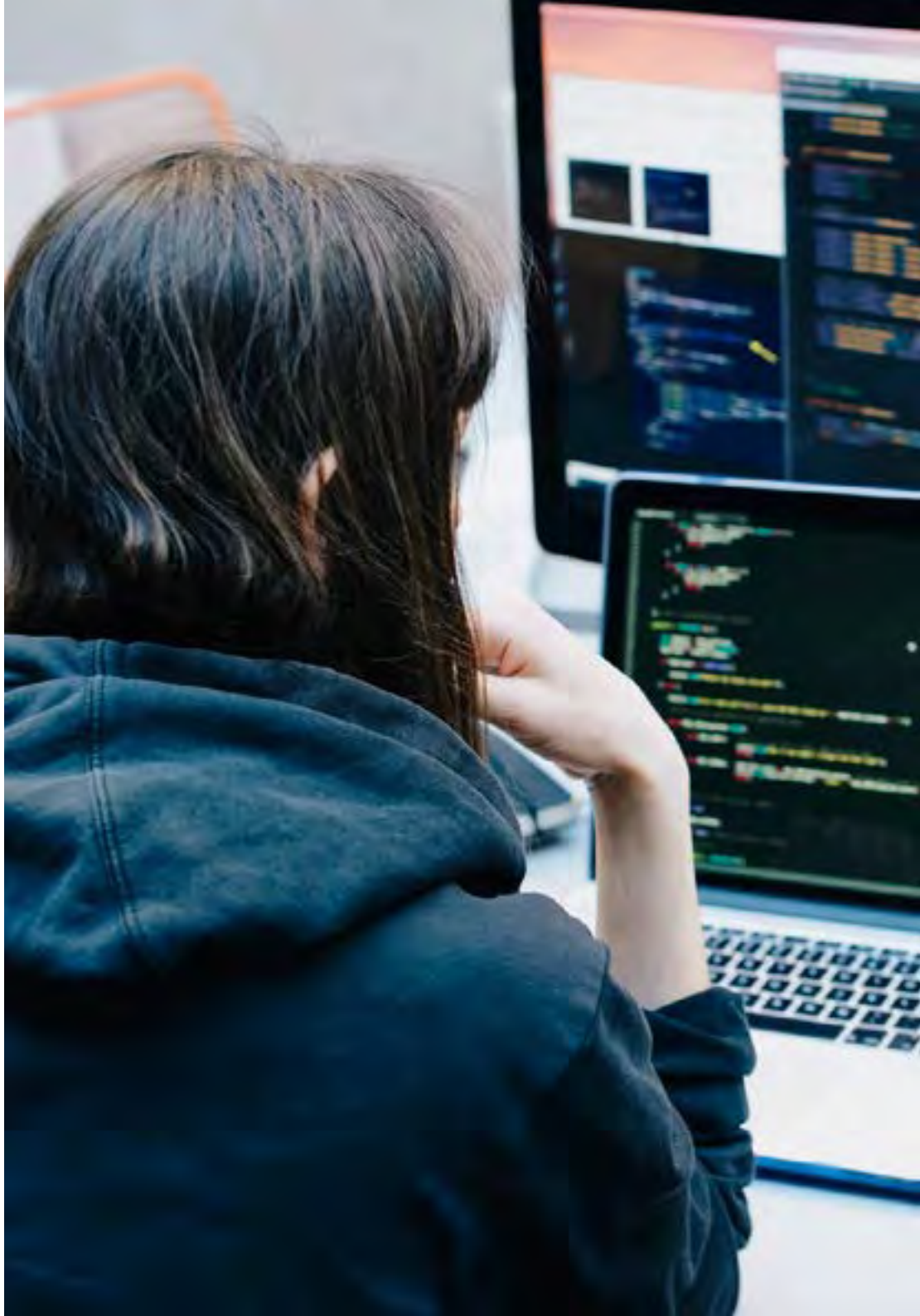
- Analista de Datos en ADN Mobile Solution
- Procesos ETL, minería de datos, análisis y visualización de datos, establecimiento de KPI's, diseño e implementación de Dashboard., control de gestión. Desarrollo en R, manejo de SQL, entre otros
- Determinación de patrones, modelos predictivos, aprendizaje 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)

D. Díaz Díaz-Chirón, Tobías

- 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
- Licenciado en Ingeniería Superior en Informática por la Universidad de Castilla-La Mancha

Dña. Martínez Cerrato, Yésica

- Técnico de producto de seguridad electrónica en Securitas Seguridad España
- Analista de inteligencia Empresarial en Ricopia Technologies
- 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 capacitar 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)
- Profesora de clases de Informática en Asociación ASALUMA
- Técnico Informático-Responsable aulas Informáticas OTEC por la Universidad de Alcalá
- Licenciada en Ingeniería Electrónica de Comunicaciones en Escuela Politécnica Superior por la Universidad de Alcalá
- Beca de especialización como Técnico Informático en OTEC por la Universidad de Alcalá

D. Tato Sánchez, Rafael

- Gestión de proyectos. INDRA SISTEMAS S.A
- Director técnico. INDRA SISTEMAS S.A
- Ingeniero de sistemas. ENA TRÁFICO S.A.U
- IFCD048PO: Metodología de gestión y desarrollo de proyectos de software con SCRUM
- Coursera: Machine Learning
- Udemy: Deep Learning A-Z. Hands-on Artificial Neural Networks
- Coursera: IBM: Fundamentals of Scalable Data Science
- Coursera: IBM: Applied AI with Deep Learning
- Coursera: IBM: Advance Machine Learning and Signal Processing
- Ingeniero en Electrónica Industrial y Automática por la Universidad Europea de Madrid
- Máster en Ingeniería Industrial habilitante por la Universidad Europea de Madrid
- Máster en Industria 4.0 por la Universidad Internacional de La Rioja (UNIR)
- Certificación profesional. SSCE0110: Docencia para la formación Profesional para el empleo

05

Estructura y contenido

Este Grand Master reúne una serie de módulos especializados que permitirán al informático profundizar en aspectos como la identificación digital, los sistemas de control de acceso, la arquitectura de seguridad de la información, la estructura del área de seguridad, los sistemas de gestión de la seguridad de la información en comunicaciones y operación software o el desarrollo del plan de continuidad del negocio asociado a la seguridad. A su vez, se abordan las técnicas más completas y actuales para el procesamiento de datos y la extracción de conocimiento, desde una perspectiva tanto teórica como práctica.





Todos los ámbitos de interés que necesitas dominar para trabajar con acierto en las ciencias de la computación, recopilados en un temario de máxima calidad"

Módulo 1. Fundamentos de programación

1.1. Introducción a la programación
- 1.1.1. Estructura básica de un ordenador
- 1.1.2. Software
- 1.1.3. Lenguajes de programación
- 1.1.4. Ciclo de vida de una aplicación Informática

1.2. Diseño de algoritmos
- 1.2.1. La resolución de problemas
- 1.2.2. Técnicas descriptivas
- 1.2.3. Elementos y estructura de un algoritmo

1.3. Elementos de un programa
- 1.3.1. Origen y características del lenguaje C++
- 1.3.2. El entorno de desarrollo
- 1.3.3. Concepto de programa
- 1.3.4. Tipos de Datos fundamentales
- 1.3.5. Operadores
- 1.3.6. Expresiones
- 1.3.7. Sentencias
- 1.3.8. Entrada y salida de Datos

1.4. Sentencias de control
- 1.4.1. Sentencias
- 1.4.2. Bifurcaciones
- 1.4.3. Bucles

1.5. Abstracción y modularidad: funciones
- 1.5.1. Diseño modular
- 1.5.2. Concepto de función y utilidad
- 1.5.3. Definición de una función
- 1.5.4. Flujo de ejecución en la llamada de una función
- 1.5.5. Prototipo de una función
- 1.5.6. Devolución de resultados
- 1.5.7. Llamada a una función: parámetros
- 1.5.8. Paso de parámetros por referencia y por valor
- 1.5.9. Ámbito identificador

1.6. Estructuras de Datos estáticas
- 1.6.1. *Arrays*
- 1.6.2. Matrices. Poliedros
- 1.6.3. Búsqueda y ordenación
- 1.6.4. Cadenas. Funciones de E/S para cadenas
- 1.6.5. Estructuras. Uniones
- 1.6.6. Nuevos tipos de Datos

1.7. Estructuras de Datos dinámicas: punteros
- 1.7.1. Concepto. Definición de puntero
- 1.7.2. Operadores y operaciones con punteros
- 1.7.3. *Arrays* de punteros
- 1.7.4. Punteros y *Arrays*
- 1.7.5. Punteros a cadenas
- 1.7.6. Punteros a estructuras
- 1.7.7. Indirección múltiple
- 1.7.8. Punteros a funciones
- 1.7.9. Paso de funciones, estructuras y *Arrays* como parámetros de funciones

1.8. Ficheros
- 1.8.1. Conceptos básicos
- 1.8.2. Operaciones con ficheros
- 1.8.3. Tipos de ficheros
- 1.8.4. Organización de los ficheros
- 1.8.5. Introducción a los ficheros C++
- 1.8.6. Manejo de ficheros

1.9. Recursividad
- 1.9.1. Definición de recursividad
- 1.9.2. Tipos de recursión
- 1.9.3. Ventajas e inconvenientes
- 1.9.4. Consideraciones
- 1.9.5. Conversión recursivo-iterativa
- 1.9.6. La Pila de recursión

1.10. Prueba y documentación
- 1.10.1. Pruebas de programas
- 1.10.2. Prueba de la caja blanca
- 1.10.3. Prueba de la caja negra
- 1.10.4. Herramientas para realizar las pruebas
- 1.10.5. Documentación de programas

Módulo 2. Estructura de datos

2.1. Introducción a la programación en C++
- 2.1.1. Clases, constructores, métodos y atributos
- 2.1.2. Variables
- 2.1.3. Expresiones condicionales y bucles
- 2.1.4. Objetos

2.2. Tipos abstractos de Datos (TAD)
- 2.2.1. Tipos de Datos
- 2.2.2. Estructuras básicas y TAD
- 2.2.3. Vectores y *Arrays*

2.3. Estructuras de Datos lineales
- 2.3.1. TAD Lista. Definición
- 2.3.2. Listas enlazadas y doblemente enlazadas
- 2.3.3. Listas ordenadas
- 2.3.4. Listas en C++
- 2.3.5. TAD Pila
- 2.3.6. TAD Cola
- 2.3.7. Pila y Cola en C++

2.4. Estructuras de Datos jerárquicas
- 2.4.1. TAD Árbol
- 2.4.2. Recorridos
- 2.4.3. Árboles n-arios
- 2.4.4. Árboles binarios
- 2.4.5. Árboles binarios de búsqueda

2.5. Estructuras de Datos jerárquicas: árboles complejos
- 2.5.1. Árboles perfectamente equilibrados o de altura mínima
- 2.5.2. Árboles multicamino
- 2.5.3. Referencias bibliográficas

2.6. Montículos y Cola de prioridad
- 2.6.1. TAD Montículos
- 2.6.2. TAD Cola de prioridad

2.7. Tablas *Hash*
- 2.7.1. TAD Tabla *Hash*
- 2.7.2. Funciones *Hash*
- 2.7.3. Función *Hash* en tablas *Hash*
- 2.7.4. Redispersión
- 2.7.5. Tablas *Hash* abiertas

2.8. Grafos
- 2.8.1 TAD Grafo
- 2.8.2 Tipos de Grafo
- 2.8.3 Representación gráfica y operaciones básicas
- 2.8.4 Diseño de Grafo

2.9. Algoritmos y conceptos avanzados sobre Grafos
- 2.9.1. Problemas sobre Grafos
- 2.9.2. Algoritmos sobre caminos
- 2.9.3. Algoritmos de búsqueda o recorridos
- 2.9.4. Otros algoritmos

2.10. Otras estructuras de Datos
- 2.10.1. Conjuntos
- 2.10.2. *Arrays* paralelos
- 2.10.3. Tablas de símbolos
- 2.10.4. *Tries*

Módulo 3. Algoritmia y complejidad

3.1. Introducción a las estrategias de diseño de algoritmos
- 3.1.1. Recursividad
- 3.1.2. Divide y conquista
- 3.1.3. Otras estrategias

3.2. Eficiencia y análisis de los algoritmos
- 3.2.1. Medidas de eficiencia
- 3.2.2. Medir el tamaño de la entrada
- 3.2.3. Medir el tiempo de ejecución
- 3.2.4. Caso peor, mejor y medio
- 3.2.5. Notación asintónica
- 3.2.6. Criterios de análisis matemático de algoritmos no recursivos
- 3.2.7. Análisis matemático de algoritmos recursivos
- 3.2.8. Análisis empírico de algoritmos

3.3. Algoritmos de ordenación
- 3.3.1. Concepto de ordenación
- 3.3.2. Ordenación de la burbuja
- 3.3.3. Ordenación por selección
- 3.3.4. Ordenación por inserción
- 3.3.5. Ordenación por mezcla (*Merge Sort*)
- 3.3.6. Ordenación rápida (*Quicksort*)

3.4. Algoritmos con árboles
- 3.4.1. Concepto de árbol
- 3.4.2. Árboles binarios
- 3.4.3. Recorridos de árbol
- 3.4.4. Representar expresiones
- 3.4.5. Árboles binarios ordenados
- 3.4.6. Árboles binarios balanceados

3.5. Algoritmos con *Heaps*
- 3.5.1. Los *Heaps*
- 3.5.2. El algoritmo *Heapsort*
- 3.5.3. Las colas de prioridad





3.6. Algoritmos con Grafos
- 3.6.1. Representación
- 3.6.2. Recorrido en anchura
- 3.6.3. Recorrido en profundidad
- 3.6.4. Ordenación topológica

3.7. Algoritmos *Greedy*
- 3.7.1. La estrategia *Greedy*
- 3.7.2. Elementos de la estrategia *Greedy*
- 3.7.3. Cambio de monedas
- 3.7.4. Problema del viajante
- 3.7.5. Problema de la mochila

3.8. Búsqueda de caminos mínimos
- 3.8.1. El problema del camino mínimo
- 3.8.2. Arcos negativos y ciclos
- 3.8.3. Algoritmo de Dijkstra

3.9. Algoritmos *Greedy* sobre Grafos
- 3.9.1. El árbol de recubrimiento mínimo
- 3.9.2. El algoritmo de Prim
- 3.9.3. El algoritmo de Kruskal
- 3.9.4. Análisis de complejidad

3.10. *Backtracking*
- 3.10.1. El *Backtracking*
- 3.10.2. Técnicas alternativas

Módulo 4. Diseño avanzado de algoritmos

4.1. Análisis de algoritmos recursivos y tipo divide y conquista
- 4.1.1. Planteamiento y resolución de ecuaciones de recurrencia homogéneas y no homogéneas
- 4.1.2. Descripción general de la estrategia divide y conquista

4.2. Análisis amortizado
- 4.2.1. El análisis agregado
- 4.2.2. El método de contabilidad
- 4.2.3. El método del potencial

4.3. Programación dinámica y algoritmos para problemas NP
- 4.3.1. Características de la programación dinámica
- 4.3.2. Vuelta atrás: backtracking
- 4.3.3. Ramificación y poda

4.4. Optimización combinatoria
- 4.4.1. Representación de problemas
- 4.4.2. Optimización en 1D

4.5. Algoritmos de aleatorización
- 4.5.1. Ejemplos de algoritmos de aleatorización
- 4.5.2. El teorema Buffon
- 4.5.3. Algoritmo de Monte Carlo
- 4.5.4. Algoritmo Las Vegas

4.6. Búsqueda local y con candidatos
- 4.6.1. *Garcient Ascent*
- 4.6.2. *Hill Climbing*
- 4.6.3. *Simulated Annealing*
- 4.6.4. *Tabu Search*
- 4.6.5. Búsqueda con candidatos

4.7. Verificación formal de programas
- 4.7.1. Especificación de abstracciones funcionales
- 4.7.2. El lenguaje de la lógica de primer orden
- 4.7.3. El sistema formal de Hoare

4.8. Verificación de programas iterativos
- 4.8.1. Reglas del sistema formal de Hoare
- 4.8.2. Concepto de invariante de iteraciones

4.9. Métodos numéricos
- 4.9.1. El método de la bisección
- 4.9.2. El método de Newton-Raphson
- 4.9.3. El método de la secante

4.10. Algoritmos paralelos
- 4.10.1. Operaciones binarias paralelas
- 4.10.2. Operaciones paralelas con Grafos
- 4.10.3. Paralelismo en divide y vencerás
- 4.10.4. Paralelismo en programación dinámica

Módulo 5. Programación avanzada

5.1. Introducción a la programación orientada a objetos
- 5.1.1. Introducción a la programación orientada a objetos
- 5.1.2. Diseño de clases
- 5.1.3. Introducción a UML para el modelado de los problemas

5.2. Relaciones entre clases
- 5.2.1. Abstracción y herencia
- 5.2.2. Conceptos avanzados de herencia
- 5.2.3. Polimorfismo
- 5.2.4. Composición y agregación

5.3. Introducción a los patrones de diseño para problemas orientados a objetos
- 5.3.1. ¿Qué son los patrones de diseño?
- 5.3.2. Patrón *Factory*
- 5.3.4. Patrón *Singleton*
- 5.3.5. Patrón *Observer*
- 5.3.6. Patrón *Composite*

5.4. Excepciones
- 5.4.1. ¿Qué son las excepciones?
- 5.4.2. Captura y gestión de excepciones
- 5.4.3. Lanzamiento de excepciones
- 5.4.4. Creación de excepciones

5.5. Interfaces de usuarios
- 5.5.1. Introducción a Qt
- 5.5.2. Posicionamiento
- 5.5.3. ¿Qué son los eventos?
- 5.5.4. Eventos: definición y captura
- 5.5.5. Desarrollo de interfaces de usuario

5.6. Introducción a la programación concurrente
- 5.6.1. Introducción a la programación concurrente
- 5.6.2. El concepto de proceso e hilo
- 5.6.3. Interacción entre procesos o hilos
- 5.6.4. Los hilos en C++
- 5.6.5. Ventajas e inconvenientes de la programación concurrente

5.7. Gestión de hilos y sincronización
- 5.7.1. Ciclo de vida de un hilo
- 5.7.2. La clase *Thread*
- 5.7.3. Planificación de hilos
- 5.7.4. Grupos hilos
- 5.7.5. Hilos de tipo demonio
- 5.7.6. Sincronización
- 5.7.7. Mecanismos de bloqueo
- 5.7.8. Mecanismos de comunicación
- 5.7.9. Monitores

5.8. Problemas comunes dentro de la programación concurrente
- 5.8.1. El problema de los productores consumidores
- 5.8.2. El problema de los lectores y escritores
- 5.8.3. El problema de la cena de los filósofos

5.9. Documentación y pruebas de software
- 5.9.1. ¿Por qué es importante documentar el software?
- 5.9.2. Documentación de diseño
- 5.9.3. Uso de herramientas para la documentación

5.10. Pruebas de software
- 5.10.1. Introducción a las pruebas del software
- 5.10.2. Tipos de pruebas
- 5.10.3. Prueba de unidad
- 5.10.4. Prueba de integración
- 5.10.5. Prueba de validación
- 5.10.6. Prueba del sistema

Módulo 6. Informática teórica

6.1. Conceptos matemáticos utilizados
- 6.1.1. Introducción a la lógica proposicional
- 6.1.2. Teoría de relaciones
- 6.1.3. Conjuntos numerables y no numerables

6.2. Lenguajes y gramáticas formales e introducción a las máquinas de Turing
- 6.2.1. Lenguajes y gramáticas formales
- 6.2.2. Problema de decisión
- 6.2.3. La máquina de Turing

6.3. Extensiones para las máquinas de Turing, máquinas de Turing restringidas y computadoras
- 6.3.1. Técnicas de programación para las máquinas de Turing
- 6.3.2. Extensiones para las máquinas de Turing
- 6.3.3. Máquinas de Turing restringidas
- 6.3.4. Máquinas de Turing y computadoras

6.4. Indecibilidad
- 6.4.1. Lenguaje no recursivamente enumerable
- 6.4.2. Un problema indecidible recursivamente enumerable

6.5. Otros problemas indecibles
- 6.5.1. Problemas indecidibles para las máquinas de Turing
- 6.5.2. Problema de correspondencia de Post (PCP)

6.6. Problemas intratables
- 6.6.1. Las clases P y NP
- 6.6.2. Un problema NP completo
- 6.6.3. Problema de la satisfacibilidad restringido
- 6.6.4. Otros problemas NP completos

6.7. Problemas co-NP y PS
- 6.7.1. Complementarios de los lenguajes de NP
- 6.7.2. Problemas resolubles en espacio polinómico
- 6.7.3. Problemas PS completos

6.8. Clases de lenguajes basados en la aleatorización
- 6.8.1. Modelo de la MT con aleatoriedad
- 6.8.2. Las clases RP y ZPP

6.8.3. Prueba de primalidad
6.8.4. Complejidad de la prueba de primalidad
6.9. Otras clases y gramáticas
6.9.1. Autómatas finitos probabilísticos
6.9.2. Autómatas celulares
6.9.3. Células de *McCulloch* y Pitts
6.9.4. Gramáticas de Lindenmayer
6.10. Sistemas avanzados de cómputo
6.10.1. Computación con membranas: sistemas P
6.10.2. Computación con ADN
6.10.3. Computación cuántica

Módulo 7: Teoría de autómatas y lenguajes formales

7.1. Introducción a la teoría de autómatas
7.1.1. ¿Por qué estudiar teoría de autómatas?
7.1.2. Introducción a las demostraciones formales
7.1.3. Otras formas de demostración
7.1.4. Inducción matemática
7.1.5. Alfabetos, cadenas y lenguajes
7.2. Autómatas finitos deterministas
7.2.1. Introducción a los autómatas finitos
7.2.2. Autómatas finitos deterministas
7.3. Autómatas finitos no deterministas
7.3.1. Autómatas finitos no deterministas
7.3.2. Equivalencia entre AFD y AFND
7.3.3. Autómatas finitos con transiciones €
7.4. Lenguajes y expresiones regulares (I)
7.4.1. Lenguajes y expresiones regulares
7.4.2. Autómatas finitos y expresiones regulares
7.5. Lenguajes y expresiones regulares (II)
7.5.1. Conversión de expresiones regulares en autómatas
7.5.2. Aplicaciones de las expresiones regulares
7.5.3. Álgebra de las expresiones regulares
7.6. Lema de bombeo y clausura de los lenguajes regulares
7.6.1. Lema de bombeo
7.6.2. Propiedades de clausura de los lenguajes regulares
7.7. Equivalencia y minimización de autómatas
7.7.1. Equivalencia de AF
7.7.2. Minimización de AF
7.8. Gramáticas independientes de contexto (GIC)
7.8.1. Gramáticas independientes de contexto
7.8.2. Árboles de derivación
7.8.3. Aplicaciones de las GIC
7.8.4. Ambigüedad en las gramáticas y lenguajes
7.9. Autómatas a Pila y GIC
7.9.1. Definición de los autómatas a Pila
7.9.2. Lenguajes aceptados por un autómata a Pila
7.9.3. Equivalencia entre autómatas a Pila y GIC
7.9.4. Autómata a Pila determinista
7.10. Formas normales, lema de bombeo de las GIC y propiedades de los LIC
7.10.1. Formas normales de las GIC
7.10.2. Lema de bombeo
7.10.3. Propiedades de clausura de los lenguajes
7.10.4. Propiedades de decisión de los LIC

Módulo 8. Procesadores de lenguajes

8.1. Introducción al proceso de compilación
8.1.1. Compilación e interpretación
8.1.2. Entorno de ejecución de un compilador
8.1.3. Proceso de análisis
8.1.4. Proceso de síntesis
8.2. Analizador léxico
8.2.1. ¿Qué es un analizador léxico?
8.2.2. Implementación del analizador léxico
8.2.3. Acciones semánticas

8.2.4. Recuperación de errores
8.2.5. Cuestiones de implementación
8.3. Análisis sintáctico
8.3.1. ¿Qué es un analizador sintáctico?
8.3.2. Conceptos previos
8.3.3. Analizadores descendentes
8.3.4. Analizadores ascendentes
8.4. Análisis sintáctico descendente y análisis sintáctico ascendente
8.4.1. Analizador LL (1)
8.4.2. Analizador LR (0)
8.4.3. Ejemplo de analizador
8.5. Análisis sintáctico ascendente avanzado
8.5.1. Analizador SLR
8.5.2. Analizador LR (1)
8.5.3. Analizador LR (k)
8.5.4. Analizador LALR
8.6. Análisis semántico (I)
8.6.1. Traducción dirigida por la sintaxis
8.6.2. Tabla de símbolos
8.7. Análisis semántico (II)
8.7.1. Comprobación de tipos
8.7.2. El subsistema de tipos
8.7.3. Equivalencia de tipos y conversiones
8.8. Generación de código y entorno de ejecución
8.8.1. Aspectos de diseño
8.8.2. Entorno de ejecución
8.8.3. Organización de la memoria
8.8.4. Asignación de memoria
8.9. Generación de código intermedio
8.9.1. Traducción dirigida por la síntesis
8.9.2. Representaciones intermedias
8.9.3. Ejemplos de traducciones
8.10. Optimización de código
8.10.1. Asignación de registros
8.10.2. Eliminación de asignaciones muertas
8.10.3. Ejecución en tiempo de compilación
8.10.4. Reordenación de expresiones
8.10.5. Optimización de bucles

Módulo 9. Informática gráfica y visualización

9.1. Teoría del color
9.1.1. Propiedades de la luz
9.1.2. Modelos de color
9.1.3. El estándar CIE
9.1.4. *Profiling*
9.2. Primitivas de salida
9.2.1. El controlador de vídeo
9.2.2. Algoritmos de dibujo de líneas
9.2.3. Algoritmos de dibujo de circunferencias
9.2.4. Algoritmos de relleno
9.3. Transformaciones 2D y sistemas de coordenadas y recorte 2D
9.3.1. Transformaciones geométricas básicas
9.3.2. Coordenadas homogéneas
9.3.3. Transformación inversa
9.3.4. Composición de transformaciones
9.3.5. Otras transformaciones
9.3.6. Cambio de coordenada
9.3.7. Sistemas de coordenadas 2D
9.3.8. Cambio de coordenadas
9.3.9. Normalización
9.3.10. Algoritmos de recorte
9.4. Transformaciones 3D
9.4.1. Translación
9.4.2. Rotación
9.4.3. Escalado

9.4.4. Reflexión
9.4.5. Cizalla
9.5. Visualización y cambio de coordenadas 3D
9.5.1. Sistemas de coordenadas 3D
9.5.2. Visualización
9.5.3. Cambio de coordenadas
9.5.4. Proyección y normalización
9.6. Proyección y recorte 3D
9.6.1. Proyección ortogonal
9.6.2. Proyección paralela oblicua
9.6.3. Proyección perspectiva
9.6.4. Algoritmos de recorte 3D
9.7. Eliminación de superficies ocultas
9.7.1. *Back-Face Removal*
9.7.2. *Z-Buffer*
9.7.3. Algoritmo del pintor
9.7.4. Algoritmo de Warnock
9.7.5. Detección de líneas ocultas
9.8. Interpolación y curvas paramétricas
9.8.1. Interpolación y aproximación con polinomios
9.8.2. Representación paramétrica
9.8.3. Polinomio de Lagrange
9.8.4. *Splines* cúbicos naturales
9.8.5. Funciones base
9.8.6. Representación matricial
9.9. Curvas Bézier
9.9.1. Construcción algebraica
9.9.2. Forma matricial
9.9.3. Composición
9.9.4. Construcción geométrica
9.9.5. Algoritmo de dibujo





9.10. *B-Splines*
- 9.10.1. El problema del control local
- 9.10.2. B-splines cúbicos uniformes
- 9.10.3. Funciones base y puntos de control
- 9.10.4. Deriva al origen y multiplicidad
- 9.10.5. Representación matricial
- 9.10.6. B-splines no uniformes

Módulo 10: Computación bioinspirada

10.1. Introducción a la computación bioinspirada
- 10.1.1. Introducción a la computación bioinspirada

10.2. Algoritmos de adaptación social
- 10.2.1. Computación bioinspirada basada en colonia de hormigas
- 10.2.2. Variantes de los algoritmos de colonias de hormigas
- 10.2.3. Computación basada en nubes de partículas

10.3. Algoritmos genéticos
- 10.3.1. Estructura general
- 10.3.2. Implementaciones de los principales operadores

10.4. Estrategias de exploración-explotación del espacio para algoritmos genéticos
- 10.4.1. Algoritmo CHC
- 10.4.2. Problemas multimodales

10.5. Modelos de computación evolutiva (I)
- 10.5.1. Estrategias evolutivas
- 10.5.2. Programación evolutiva
- 10.5.3. Algoritmos basados en evolución diferencial

10.6. Modelos de computación evolutiva (II)
- 10.6.1. Modelos de evolución basados en estimación de distribuciones (EDA)
- 10.6.2. Programación genética

10.7. Programación evolutiva aplicada a problemas de aprendizaje
- 10.7.1 Aprendizaje Basado en Reglas
- 10.7.2 Métodos evolutivos en problemas de selección de instancias

10.8. Problemas multiobjetivo
- 10.8.1. Concepto de dominancia
- 10.8.2. Aplicación de algoritmos evolutivos a problemas multiobjetivo

10.9. Redes neuronales (I)
- 10.9.1. Introducción a las redes neuronales
- 10.9.2. Ejemplo práctico con redes neuronales

10.10. Redes neuronales (II)
- 10.10.1. Casos de uso de las redes neuronales en la investigación médica
- 10.10.2. Casos de uso de las redes neuronales en la economía
- 10.10.3. Casos de uso de las redes neuronales en la visión artificial

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. Gestión de la seguridad IT

13.1. Gestión de la seguridad
- 13.1.1. Operaciones de seguridad
- 13.1.2. Aspecto legal y regulatorio
- 13.1.3. Habilitación del negocio
- 13.1.4. Gestión de riesgos
- 13.1.5. Gestión de identidades y accesos

13.2. Estructura del área de seguridad. La oficina del CISO
- 13.2.1. Estructura organizativa. Posición del CISO en la estructura
- 13.2.2. Las líneas de defensa
- 13.2.3. Organigrama de la oficina del CISO
- 13.2.4. Gestión presupuestaria

13.3. Gobierno de seguridad
- 13.3.1. Comité de seguridad
- 13.3.2. Comité de seguimiento de riesgos
- 13.3.3. Comité de auditoría
- 13.3.4. Comité de crisis

13.4. Gobierno de seguridad. Funciones
- 13.4.1. Políticas y normas
- 13.4.2. Plan director de seguridad
- 13.4.3. Cuadros de mando
- 13.4.4. Concienciación y formación
- 13.4.5. Seguridad en la cadena de suministro

13.5. Operaciones de seguridad
- 13.5.1. Gestión de identidades y accesos
- 13.5.2. Configuración de reglas de seguridad de red. *Firewalls*
- 13.5.3. Gestión de plataformas IDS/IPS
- 13.5.4. Análisis de vulnerabilidades

13.6. Marco de trabajo de Ciberseguridad. NIST CSF
- 13.6.1. Metodología NIST
  - 13.6.1.1. Identificar
  - 13.6.1.2. Proteger
  - 13.6.1.3. Detectar
  - 13.6.1.4. Responder
  - 13.6.1.5. Recuperar

13.7. Centro de operaciones de seguridad (SOC). Funciones
- 13.7.1. Protección. *Red Team, Pentesting, Threat Intelligence*
- 13.7.2. Detección. SIEM, *User Behavior Analytics, Fraud Prevention*
- 13.7.3. Respuesta

13.8. Auditorías de seguridad
- 13.8.1. Test de intrusión
- 13.8.2. Ejercicios de *Red Team*
- 13.8.3. Auditorías de código fuente. Desarrollo seguro
- 13.8.4. Seguridad de componentes (*Software Supply Chain*)
- 13.8.5. Análisis forense

13.9. Respuesta a incidentes
- 13.9.1. Preparación
- 13.9.2. Detección, análisis y notificación
- 13.9.3. Contención, erradicación y recuperación
- 13.9.4. Actividad post incidente
  - 13.9.4.1. Retención de evidencias
  - 13.9.4.2. Análisis forense
  - 13.9.4.3. Gestión de brechas
- 13.9.5. Guías oficiales de gestión de ciberincidentes

13.10. Gestión de vulnerabilidades
- 13.10.1. Análisis de vulnerabilidades
- 13.10.2. Valoración de vulnerabilidad
- 13.10.3. Bastionado de sistemas
- 13.10.4. Vulnerabilidades de día 0. *Zero-Day*

Módulo 14. Análisis de riesgos y entorno de seguridad IT

14.1. Análisis del entorno
- 14.1.1. Análisis de la situación coyuntural
  - 14.1.1.1. Entornos VUCA
    - 14.1.1.1.1. Volátil
    - 14.1.1.1.2. Incierto
    - 14.1.1.1.3. Complejo
    - 14.1.1.1.4. Ambiguo
  - 14.1.1.2. Entornos BANI
    - 14.1.1.2.1. Quebradizo
    - 14.1.1.2.2. Ansioso
    - 14.1.1.2.3. No lineal
    - 14.1.1.2.4. Incomprensible
- 14.1.2. Análisis del entorno general. PESTEL
  - 14.1.2.1. Político
  - 14.1.2.2. Económico
  - 14.1.2.3. Social
  - 14.1.2.4. Tecnológico
  - 14.1.2.5. Ecológico/Ambiental
  - 14.1.2.6. Legal
- 14.1.3. Análisis de la situación interna. DAFO
  - 14.1.3.1. Objetivos
  - 14.1.3.2. Amenazas
  - 14.1.3.3. Oportunidades
  - 14.1.3.4. Fortalezas

14.2. Riesgo e incertidumbre
- 14.2.1. Riesgo
- 14.2.2. Gerencia de riesgos
- 14.2.3. Estándares de gestión de riesgos

14.3. Directrices para la gestión de riesgos ISO 31.000:2018
- 14.3.1. Objeto
- 14.3.2. Principios
- 14.3.3. Marco de referencia
- 14.3.4. Proceso

14.4. Metodología de análisis y gestión de riesgos de los sistemas de información (MAGERIT)
- 14.4.1. Metodología MAGERIT
  - 14.4.1.1. Objetivos
  - 14.4.1.2. Método
  - 14.4.1.3. Elementos
  - 14.4.1.4. Técnicas
  - 14.4.1.5. Herramientas disponibles (PILAR)

14.5. Transferencia del riesgo cibernético
- 14.5.1. Transferencia de riesgos
- 14.5.2. Riesgos cibernéticos. Tipología
- 14.5.3. Seguros de ciber riesgos

14.6. Metodologías ágiles para la gestión de riesgos
- 14.6.1. Metodologías ágiles
- 14.6.2. Scrum para la gestión del riesgo
- 14.6.3. *Agile Risk Management*

14.7. Tecnologías para la gestión del riesgo
- 14.7.1. Inteligencia artificial aplicada a la gestión de riesgos
- 14.7.2. *Blockchain* y criptografía. Métodos de preservación del valor
- 14.7.3. Computación cuántica. Oportunidad o amenaza

14.8. Elaboración de mapas de riesgos IT basados en metodologías ágiles
- 14.8.1. Representación de la probabilidad y el impacto en entornos ágiles
- 14.8.2. El riesgo como amenaza del valor
- 14.8.3. Re-evolución en la gestión de proyectos y procesos ágiles basados en KRIs

14.9. *Risk Driven* en la gestión de riesgos
- 14.9.1. *Risk Driven*
- 14.9.2. *Risk Driven* en la gestión de riesgos
- 14.9.3. Elaboración de un modelo de gestión empresarial impulsado por el riesgo

14.10. Innovación y transformación digital en la gestión de riesgos IT
- 14.10.1. La gestión de riesgos ágiles como fuente de innovación empresarial
- 14.10.2. Transformación de Datos en información útil para la toma de decisiones
- 14.10.3. Visión holística de la empresa a través del riesgo

Módulo 15. Criptografía en IT

15.1. Criptografía
- 15.1.1. Criptografía
- 15.1.2. Fundamentos matemáticos

15.2. Criptología
- 15.2.1. Criptología
- 15.2.2. Criptoanálisis
- 15.2.3. Esteganografía y estegoanálisis

15.3. Protocolos criptográficos
- 15.3.1. Bloques básicos
- 15.3.2. Protocolos básicos
- 15.3.3. Protocolos intermedios
- 15.3.4. Protocolos avanzados
- 15.3.5. Protocolos esotéricos

15.4. Técnicas criptográficas
- 15.4.1. Longitud de claves
- 15.4.2. Manejo de claves
- 15.4.3. Tipos de algoritmos
- 15.4.4. Funciones resumen. *Hash*
- 15.4.5. Generadores de números pseudoaleatorios
- 15.4.6. Uso de algoritmos

15.5. Criptografía simétrica
- 15.5.1. Cifrados de bloque
- 15.5.2. DES (*Data Encryption Standard*)
- 15.5.3. Algoritmo RC4
- 15.5.4. AES (*Advanced Encryption Standard*)
- 15.5.5. Combinación de cifrados de bloques
- 15.5.6. Derivación de claves

15.6. Criptografía asimétrica
- 15.6.1. Diffie-Hellman
- 15.6.2. DSA (*Digital Signature Algorithm*)
- 15.6.3. RSA (Rivest, Shamir y Adleman)
- 15.6.4. Curva elíptica
- 15.6.5. Criptografía asimétrica. Tipología

15.7. Certificados digitales
- 15.7.1. Firma digital
- 15.7.2. Certificados X509
- 15.7.3. Infraestructura de clave pública (PKI)

15.8. Implementaciones
- 15.8.1. Kerberos
- 15.8.2. IBM CCA
- 15.8.3. *Pretty Good Privacy* (PGP)
- 15.8.4. ISO *Authentication Framework*
- 15.8.5. SSL y TLS
- 15.8.6. Tarjetas inteligentes en medios de pago (EMV)
- 15.8.7. Protocolos de telefonía móvil
- 15.8.8. *Blockchain*

15.9. Esteganografía
- 15.9.1. Esteganografía
- 15.9.2. Estegoanálisis
- 15.9.3. Aplicaciones y usos

15.10. Criptografía cuántica
- 15.10.1. Algoritmos cuánticos
- 15.10.2. Protección de algoritmos frente a computación cuántica
- 15.10.3. Distribución de claves cuántica

Módulo 16. Gestión de identidad y accesos en seguridad IT

16.1. Gestión de identidad y accesos (IAM)
- 16.1.1. Identidad digital
- 16.1.2. Gestión de identidad
- 16.1.3. Federación de identidades

16.2. Control de acceso físico
- 16.2.1. Sistemas de protección
- 16.2.2. Seguridad de las áreas
- 16.2.3. Instalaciones de recuperación

16.3. Control de acceso lógico
- 16.3.1. Autenticación: tipología
- 16.3.2. Protocolos de autenticación
- 16.3.3. Ataques de autenticación

16.4. Control de acceso lógico. Autenticación MFA
- 16.4.1. Control de acceso lógico. Autenticación MFA
- 16.4.2. Contraseñas.Importancia
- 16.4.3. Ataques de autenticación

16.5. Control de acceso lógico. Autenticación biométrica
- 16.5.1. Control de acceso lógico. Autenticación biométrica
  - 16.5.1.1. Autenticación biométrica. Requisitos
- 16.5.2. Funcionamiento
- 16.5.3. Modelos y técnicas

16.6. Sistemas de gestión de autenticación
- 16.6.1. *Single Sign On*
- 16.6.2. Kerberos
- 16.6.3. Sistemas AAA

16.7. Sistemas de gestión de autenticación: Sistemas AAA
- 16.7.1. TACACS
- 16.7.2. RADIUS
- 16.7.3. DIAMETER

16.8. Servicios de control de acceso
- 16.8.1. FW - Cortafuegos
- 16.8.2. VPN - Redes Privadas Virtuales
- 16.8.3. IDS - Sistema de Detección de Intrusiones

16.9. Sistemas de control de acceso a la red
- 16.9.1. NAC
- 16.9.2. Arquitectura y elementos
- 16.9.3. Funcionamiento y estandarización

16.10. Acceso a redes inalámbricas
- 16.10.1. Tipos de redes inalámbricas
- 16.10.2. Seguridad en redes inalámbricas
- 16.10.3. Ataques en redes inalámbricas

Módulo 17. Seguridad en comunicaciones y operación software

17.1. Seguridad Informática en comunicaciones y operación software
- 17.1.1. Seguridad Informática
- 17.1.2. Ciberseguridad
- 17.1.3. Seguridad en la nube

17.2. Seguridad Informática en comunicaciones y operación software. Tipología
- 17.2.1. Seguridad física
- 17.2.2. Seguridad lógica

17.3. Seguridad en comunicaciones
- 17.3.1. Principales elementos
- 17.3.2. Seguridad de redes
- 17.3.3. Mejores prácticas

17.4. Ciberinteligencia
- 17.4.1. Ingeniería social
- 17.4.2. *Deep* Web
- 17.4.3. *Phishing*
- 17.4.4. *Malware*

17.5. Desarrollo seguro en comunicaciones y operación software
- 17.5.1. Desarrollo seguro. Protocolo HTTP
- 17.5.2. Desarrollo seguro. Ciclo de vida
- 17.5.3. Desarrollo seguro. Seguridad PHP
- 17.5.4. Desarrollo seguro. Seguridad NET
- 17.5.5. Desarrollo seguro. Mejores prácticas

17.6. Sistemas de gestión de la seguridad de la información en comunicaciones y operación software
- 17.6.1. GDPR
- 17.6.2. ISO 27021
- 17.6.3. ISO 27017/18

17.7. Tecnologías SIEM
- 17.7.1. Tecnologías SIEM
- 17.7.2. Operativa de SOC
- 17.7.3. SIEM *vendors*

17.8. El rol de la seguridad en las organizaciones
- 17.8.1. Roles en las organizaciones
- 17.8.2. Rol de los especialistas IoT en las compañías
- 17.8.3. Certificaciones reconocidas en el mercado

17.9. Análisis forense
- 17.9.1. Análisis forense
- 17.9.2. Análisis forense. Metodología
- 17.9.3. Análisis forense. Herramientas e implantación

17.10. La Ciberseguridad en la actualidad
- 17.10.1. Principales ataques informáticos
- 17.10.2. Previsiones de empleabilidad
- 17.10.3. Retos

Módulo 18. Seguridad en entornos *Cloud*

18.1. Seguridad en entornos *Cloud Computing*
- 18.1.1. Seguridad en entornos *Cloud Computing*
- 18.1.2. Seguridad en entornos *Cloud Computing*. Amenazas y riesgos seguridad
- 18.1.3. Seguridad en entornos *Cloud Computing*. Aspectos clave de seguridad

18.2. Tipos de infraestructura *Cloud*
- 18.2.1. Público
- 18.2.2. Privado
- 18.2.3. Híbrido

18.3. Modelo de gestión compartida
- 18.3.1. Elementos de seguridad gestionados por proveedor
- 18.3.2. Elementos gestionados por cliente
- 18.3.3. Definición de la estrategia para seguridad

18.4. Mecanismos de prevención
- 18.4.1. Sistemas de gestión de autenticación
- 18.4.2. Sistema de gestión de autorización: políticas de acceso
- 18.4.3. Sistemas de gestión de claves

18.5. Securización de sistemas
- 18.5.1. Securización de los sistemas de almacenamiento
- 18.5.2. Protección de los sistemas de base de Datos
- 18.5.3. Securización de Datos en tránsito

18.6. Protección de infraestructura
- 18.6.1. Diseño e implementación de red segura
- 18.6.2. Seguridad en recursos de computación
- 18.6.3. Herramientas y recursos para protección de infraestructura

18.7. Detección de las amenazas y ataques
- 18.7.1. Sistemas de auditoría, *Logging* y monitorización
- 18.7.2. Sistemas de eventos y alarmas
- 18.7.3. Sistemas SIEM

18.8. Respuesta ante incidentes
- 18.8.1. Plan de respuesta a incidentes
- 18.8.2. La continuidad de negocio
- 18.8.3. Análisis forense y remediación de incidentes de la misma naturaleza

18.9. Seguridad en *Clouds* públicos
- 18.9.1. AWS (Amazon Web Services)
- 18.9.2. Microsoft Azure
- 18.9.3. Google GCP
- 18.9.4. Oracle *Cloud*

18.10. Normativa y cumplimiento
- 18.10.1. Cumplimiento de normativas de seguridad
- 18.10.2. Gestión de riesgos
- 18.10.3. Personas y proceso en las organizaciones

Módulo 19. Seguridad en comunicaciones de dispositivos Iot

19.1. De la telemetría al IoT
- 19.1.1. Telemetría
- 19.1.2. Conectividad M2M
- 19.1.3. Democratización de la telemetría

19.2. Modelos de referencia IoT
- 19.2.1. Modelo de referencia IoT
- 19.2.2. Arquitectura simplificada IoT

19.3. Vulnerabilidades de seguridad del IoT
- 19.3.1. Dispositivos IoT
- 19.3.2. Dispositivos IoT. Casuística de uso
- 19.3.3. Dispositivos IoT. Vulnerabilidades

19.4. Conectividad del IoT
- 19.4.1. Redes PAN, LAN, WAN
- 19.4.2. Tecnologías inalámbricas no IoT
- 19.4.3. Tecnologías inalámbricas LPWAN

19.5. Tecnologías LPWAN
- 19.5.1. El triángulo de hierro de las redes LPWAN
- 19.5.2. Bandas de frecuencia libres vs. Bandas licenciadas
- 19.5.3. Opciones de tecnologías LPWAN

19.6. Tecnología LoRaWAN
- 19.6.1. Tecnología LoRaWAN
- 19.6.2. Casos de uso LoRaWAN. Ecosistema
- 19.6.3. Seguridad en LoRaWAN

19.7. Tecnología Sigfox
- 19.7.1. Tecnología Sigfox
- 19.7.2. Casos de uso Sigfox. Ecosistema
- 19.7.3. Seguridad en Sigfox

19.8. Tecnología celular IoT
- 19.8.1. Tecnología celular IoT (NB-IoT y LTE-M)
- 19.8.2. Casos de uso celular IoT. Ecosistema
- 19.8.3. Seguridad en celular IoT

19.9. Tecnología Wi-SUN
- 19.9.1. Tecnología Wi-SUN
- 19.9.2. Casos de uso Wi-SUN. Ecosistema
- 19.9.3. Seguridad en Wi-SUN

19.10. Otras tecnologías IoT
- 19.10.1. Otras tecnologías IoT
- 19.10.2. Casos de uso y ecosistema de otras tecnologías IoT
- 19.10.3. Seguridad en otras tecnologías IoT

Módulo 20. Plan de continuidad del negocio asociado a la seguridad

20.1. Plan de continuidad de negocio
- 20.1.1. Los planes de continuidad de negocio (PCN)
- 20.1.2. Plan de continuidad de negocio (PCN). Aspectos clave
- 20.1.3. Plan de continuidad de negocio (PCN) para la valoración de la empresa

20.2. Métricas en un plan de continuidad de negocio (PCN)
- 20.2.1. *Recovery Time Objective* (RTO) y *Recovery Point Objective* (RPO)
- 20.2.2. Tiempo máximo tolerable (MTD)
- 20.2.3. Niveles mínimos de recuperación (ROL)
- 20.2.4. Punto de recuperación objetivo (RPO)

20.3. Proyectos de continuidad. Tipología
- 20.3.1. Plan de continuidad de negocio (PCN)
- 20.3.2. Plan de continuidad de TIC (PCTIC)
- 20.3.3. Plan de recuperación ante desastres (PRD)

20.4. Gestión de riesgos asociada al PCN
- 20.4.1. Análisis de impacto sobre el negocio
- 20.4.2. Beneficios de la implantación de un PCN
- 20.4.3. Mentalidad basada en riesgos

20.5. Ciclo de vida de un plan de continuidad de negocio
- 20.5.1. Fase 1: análisis de la organización
- 20.5.2. Fase 2: determinación de la estrategia de continuidad
- 20.5.3. Fase 3: respuesta a la contingencia
- 20.5.4. Fase 4: prueba, mantenimiento y revisión

20.6. Fase del análisis de la organización de un PCN
- 20.6.1. Identificación de procesos en el alcance del PCN
- 20.6.2. Identificación de áreas críticas del negocio
- 20.6.3. Identificación de dependencias entre áreas y procesos
- 20.6.4. Determinación del MTD adecuado
- 20.6.5. Entregables. Creación de un plan

20.7. Fase de determinación de la estrategia de continuidad en un PCN
- 20.7.1. Roles en la fase de determinación de la estrategia
- 20.7.2. Tareas de la fase de determinación de la estrategia
- 20.7.3. Entregables

20.8. Fase de respuesta a la contingencia en un PCN
- 20.8.1. Roles en la fase de respuesta
- 20.8.2. Tareas en esta fase
- 20.8.3. Entregables

20.9. Fase de pruebas, mantenimiento y revisión de un PCN
- 20.9.1. Roles en la fase de pruebas, mantenimiento y revisión
- 20.9.2. Tareas en la fase de pruebas, mantenimiento y revisión
- 20.9.3. Entregables

20.10. Normas ISO asociadas a los planes de continuidad de negocio (PCN)
- 20.10.1. ISO 22301:2019
- 20.10.2. ISO 22313:2020
- 20.10.3. Otras normas ISO e internacionales relacionadas

Módulo 21. Analítica del dato en la organización empresarial

21.1. Análisis de negocio
- 21.1.1. Análisis de negocio
- 21.1.2. Estructura del dato
- 21.1.3. Fases y elementos

21.2. Analítica del dato en la empresa
- 21.2.1. Cuadros de mando y KPI´s por departamentos
- 21.2.2. Informes operativos, tácticos y estratégicos
- 21.2.3. Analítica del dato aplicada a cada departamento
  - 21.2.3.1. Marketing y comunicación
  - 21.2.3.2. Comercial
  - 21.2.3.3. Atención al cliente
  - 21.2.3.4. Compras
  - 21.2.3.5. Administración
  - 21.2.3.6. RRHH
  - 21.2.3.7. Producción
  - 21.2.3.8. IT

21.3. Marketing y comunicación
- 21.3.1. KPI´s a medir, aplicaciones y beneficios
- 21.3.2. Sistemas de Marketing y *Data Warehouse*
- 21.3.3. Implementación de una estructura de analítica del dato en Marketing
- 21.3.4. Plan de Marketing y comunicación
- 21.3.5. Estrategias, predicción y gestión de campañas

21.4. Comercial y ventas
- 21.4.1. Aportaciones de analítica del dato en el área comercial
- 21.4.2. Necesidades del departamento de Ventas
- 21.4.3. Estudios de mercado

21.5. Atención al cliente
- 21.5.1. Fidelización
- 21.5.2. Calidad personal e inteligencia emocional
- 21.5.3. Satisfacción del cliente

21.6. Compras
- 21.6.1. Analítica del dato para estudios de mercado
- 21.6.2. Analítica del dato para estudios de competencia
- 21.6.3. Otras aplicaciones

21.7. Administración
- 21.7.1. Necesidades en el departamento de Administración
- 21.7.2. *Data Warehouse* y análisis de riesgo financiero
- 21.7.3. *Data Warehouse* y análisis de riesgo de crédito

21.8. Recursos humanos
- 21.8.1. RRHH y beneficios de la analítica del dato
- 21.8.2. Herramientas de analítica del dato en el departamento de RRHH
- 21.8.3. Aplicación de analítica del dato en los RRHH

21.9. Producción
- 21.9.1. Análisis de Datos en un departamento de Producción
- 21.9.2. Aplicaciones
- 21.9.3. Beneficios

21.10. IT
- 21.10.1. Departamento de IT
- 21.10.2. Analítica del dato y transformación digital
- 21.10.3. Innovación y productividad



Módulo 22. Gestión, manipulación de Datos e información para Ciencia de Datos

22.1. Estadística. Variables, índices y ratios
- 22.1.1. La Estadística
- 22.1.2. Dimensiones estadísticas
- 22.1.3. Variables, índices y ratios

22.2. Tipología del dato
- 22.2.1. Cualitativos
- 22.2.2. Cuantitativos
- 22.2.3. Caracterización y categorías

22.3. Conocimiento de los Datos a partir de medidas
- 22.3.1. Medidas de centralización
- 22.3.2. Medidas de dispersión
- 22.3.3. Correlación

22.4. Conocimiento de los Datos a partir de gráficos
- 22.4.1. Visualización según el tipo de dato
- 22.4.2. Interpretación de información grafica
- 22.4.3. Customización de gráficos con R

22.5. Probabilidad
- 22.5.1. Probabilidad
- 22.5.2. Función de probabilidad
- 22.5.3. Distribuciones

22.6. Recolección de Datos
- 22.6.1. Metodología de recolección
- 22.6.2. Herramientas de recolección
- 22.6.3. Canales de recolección

22.7. Limpieza del dato
- 22.7.1. Fases de la limpieza de Datos
- 22.7.2. Calidad del dato
- 22.7.3. Manipulación de Datos (con R)

22.8. Análisis de Datos, interpretación y valoración de resultados
- 22.8.1. Medidas estadísticas
- 22.8.2. Índices de relación
- 22.8.3. Minería de Datos

22.9. Almacén del dato (*Data Warehouse*)
- 22.9.1. Elementos
- 22.9.2. Diseño

22.10. Disponibilidad del dato
- 22.10.1. Acceso
- 22.10.2. Utilidad
- 22.10.3. Seguridad

Módulo 23. Dispositivos y plataformas IoT como base para la Ciencia de Datos

23.1. *Internet of Things*
- 23.1.1. Internet del futuro, *Internet of Things*
- 23.1.2. El consorcio de internet industrial

23.2. Arquitectura de referencia
- 23.2.1. La arquitectura de referencia
- 23.2.2. Capas
- 23.2.3. Componentes

23.3. Sensores y dispositivos IoT
- 23.3.1 Componentes principales
- 23.3.2. Sensores y actuadores

23.4. Comunicaciones y protocolos
- 23.4.1. Protocolos. Modelo OSI
- 23.4.2. Tecnologías de comunicación

23.5. Plataformas Cloud para IoT e IIoT
- 23.5.1. Plataformas de propósito general
- 23.5.2. Plataformas industriales
- 23.5.3. Plataformas de código abierto

23.6. Gestión de Datos en plataformas IoT
- 23.6.1. Mecanismos de gestión de Datos. Datos abiertos
- 23.6.2. Intercambio de Datos y visualización

23.7. Seguridad en IoT
- 23.7.1. Requisitos y áreas de seguridad
- 23.7.2. Estrategias de seguridad en IIoT

23.8. Aplicaciones de IoT
- 23.8.1. Ciudades inteligentes
- 23.8.2. Salud y condición física
- 23.8.3. Hogar inteligente
- 23.8.4. Otras aplicaciones

23.9. Aplicaciones de IIoT
- 23.9.1. Fabricación
- 23.9.2. Transporte
- 23.9.3. Energía
- 23.9.4. Agricultura y ganadería
- 23.9.5. Otros sectores

23.10. Industria 4.0
- 23.10.1. IoRT (*Internet of Robotics Things*)
- 23.10.2. Fabricación aditiva 3D
- 23.10.3. *Big Data Analytics*

Módulo 24. Representación gráfica para Análisis de Datos

24.1. Análisis exploratorio
- 24.1.1. Representación para análisis de información
- 24.1.2. El valor de la representación gráfica
- 24.1.3. Nuevos paradigmas de la representación gráfica

24.2. Optimización para ciencia de Datos
- 24.2.1. La gama cromática y el diseño
- 24.2.2. La Gestalt en la representación gráfica
- 24.2.3. Errores a evitar y consejos

24.3. Fuentes de Datos básicos
- 24.3.1. Para representación de calidad
- 24.3.2. Para representación de cantidad
- 24.3.3. Para representación de tiempo

24.4. Fuentes de Datos complejos
- 24.4.1. Archivos, listados y BBDD
- 24.4.2. Datos abiertos
- 24.4.3. Datos de generación continua

24.5. Tipos de gráficas
- 24.5.1. Representaciones básicas
- 24.5.2. Representación de bloques
- 24.5.3. Representación para análisis de dispersión
- 24.5.4. Representaciones circulares
- 24.5.5. Representaciones burbujas
- 24.5.6. Representaciones geográfias

24.6. Tipos de visualización
- 24.6.1. Comparativas y relacional
- 24.6.2. Distribución
- 24.6.3. Jerárquica

24.7. Diseño de informes con representación gráfica
- 24.7.1. Aplicación de gráficas en informes de Marketing
- 24.7.2. Aplicación de gráficas en cuadros de mando y Kpi´s
- 24.7.3. Aplicación de gráficas en planes estratégicos
- 24.7.4. Otros usos: ciencia, salud, negocio

24.8. Narración gráfica
- 24.8.1. La narración gráfica
- 24.8.2. Evolución
- 24.8.3. Utilidad

24.9. Herramientas orientadas a visualización
- 24.9.1. Herramientas avanzadas
- 24.9.2. Software en línea
- 24.9.3. *Open Source*

24.10. Nuevas tecnologías en la visualización de Datos
- 24.10.1. Sistemas para virtualización de la realidad
- 24.10.2. Sistemas para aumento y mejora de la realidad
- 24.10.3. Sistemas inteligentes

Módulo 25. Herramientas de ciencia de Datos

25.1. Ciencia de Datos
- 25.1.1. La ciencia de Datos
- 25.1.2. Herramientas avanzadas para el científico de Datos

25.2. Datos, información y conocimiento
- 25.2.1. Datos, información y conocimiento
- 25.2.2. Tipos de Datos
- 25.2.3. Fuentes de Datos

25.3. De los Datos a la información
- 25.3.1. Análisis de Datos
- 25.3.2. Tipos de análisis
- 25.3.3. Extracción de información de un *Dataset*

25.4. Extracción de información mediante visualización
- 25.4.1. La visualización como herramienta de análisis
- 25.4.2. Métodos de visualización
- 25.4.3. Visualización de un conjunto de Datos

25.5. Calidad de los Datos
- 25.5.1. Datos de calidad
- 25.5.2. Limpieza de Datos
- 25.5.3. Preprocesamiento básico de Datos

25.6. *Dataset*
- 25.6.1. Enriquecimiento del *Dataset*
- 25.6.2. La maldición de la dimensionalidad
- 25.6.3. Modificación de nuestro conjunto de Datos

25.7. Desbalanceo
- 25.7.1. Desbalanceo de clases
- 25.7.2. Técnicas de mitigación del desbalanceo
- 25.7.3. Balanceo de un *Dataset*

25.8. Modelos no supervisados
- 25.8.1. Modelo no supervisado
- 25.8.2. Métodos
- 25.8.3. Clasificación con modelos no supervisados

25.9. Modelos supervisados
- 25.9.1. Modelo supervisado
- 25.9.2. Métodos
- 25.9.3. Clasificación con modelos supervisados

25.10. Herramientas y buenas prácticas
- 25.10.1. Buenas prácticas para un científico de Datos
- 25.10.2. El mejor modelo
- 25.10.3. Herramientas útiles

Módulo 26. Minería de Datos. Selección, preprocesamiento y transformación

26.1. La inferencia estadística
- 26.1.1. Estadística descriptiva vs Inferencia estadística
- 26.1.2. Procedimientos paramétricos
- 26.1.3. Procedimientos no paramétricos

26.2. Análisis exploratorio
- 26.2.1. Análisis descriptivo
- 26.2.2. Visualización
- 26.2.3. Preparación de Datos

26.3. Preparación de Datos
- 26.3.1. Integración y limpieza de Datos
- 26.3.2. Normalización de Datos
- 26.3.3. Transformando atributos

26.4. Los valores perdidos
- 26.4.1. Tratamiento de valores perdidos
- 26.4.2. Métodos de imputación de máxima verosimilitud
- 26.4.3. Imputación de valores perdidos usando aprendizaje automático

26.5. El ruido en los Datos
- 26.5.1. Clases de ruido y atributos
- 26.5.2. Filtrado de ruido
- 26.5.3. El efecto del ruido

26.6. La maldición de la dimensionalidad
- 26.6.1. *Oversampling*
- 26.6.2. *Undersampling*
- 26.6.3. Reducción de Datos multidimensionales

26.7. De atributos continuos a discretos
- 26.7.1. Datos continuos vs. Discretos
- 26.7.2. Proceso de discretización

26.8. Los Datos
- 26.8.1. Selección de Datos
- 26.8.2. Perspectivas y criterios de selección
- 26.8.3. Métodos de selección

26.9. Selección de instancias
- 26.9.1. Métodos para la selección de instancias
- 26.9.2. Selección de prototipos
- 26.9.3. Métodos avanzados para la selección de instancias

26.10. Preprocesamiento de Datos en entornos *Big Data*
- 26.10.1. *Big Data*
- 26.10.2. Preprocesamiento clásico vs.Masivo
- 26.10.3. *Smart Data*

Módulo 27. Predictibilidad y análisis de fenómenos estocásticos

27.1. Series de tiempo
- 27.1.1. Series de tiempo
- 27.1.2. Utilidad y aplicabilidad
- 27.1.3. Casuística relacionada

27.2. La serie temporal
- 27.2.1. Tendencia estacionalidad de ST
- 27.2.2. Variaciones típicas
- 27.2.3. Análisis de residuos

27.3. Tipologías
- 27.3.1. Estacionarias
- 27.3.2. No estacionarias
- 27.3.3. Transformaciones y ajustes

27.4. Esquemas para series temporales
- 27.4.1. Esquema (modelo) aditivo
- 27.4.2. Esquema (modelo) multiplicativo
- 27.4.3. Procedimientos para determinar el tipo de modelo

27.5. Métodos básicos de *Forecast*
- 27.5.1. Media
- 27.5.2. *Naïve*
- 27.5.3. *Naïve* estacional
- 27.5.4. Comparación de métodos

27.6. Análisis de residuos
- 27.6.1. Autocorrelación
- 27.6.2. ACF de residuos
- 27.6.3. Test de correlación

27.7. Regresión en el contexto de series temporales
- 27.7.1. ANOVA
- 27.7.2. Fundamentos
- 27.7.3. Aplicación práctica

27.8. Modelos predictivos de series temporales
- 27.8.1. ARIMA
- 27.8.2. Suavizado exponencial

27.9. Manipulación y análisis de series temporales con R
- 27.9.1. Preparación de los Datos
- 27.9.2. Identificación de patrones
- 27.9.3. Análisis del modelo
- 27.9.4. Predicción

27.10. Análisis gráficos combinados con R
- 27.10.1. Situaciones habituales
- 27.10.2. Aplicación práctica para resolución de problemas sencillos
- 27.10.3. Aplicación práctica para resolución de problemas avanzados

Módulo 28. Diseño y desarrollo de sistemas inteligentes

28.1. Preprocesamiento de Datos
- 28.1.1. Preprocesamiento de Datos
- 28.1.2. Transformación de Datos
- 28.1.3. Minería de Datos

28.2. Aprendizaje automático
- 28.2.1. Aprendizaje supervisado y no supervisado
- 28.2.2. Aprendizaje por refuerzo
- 28.2.3. Otros paradigmas de aprendizaje

28.3. Algoritmos de clasificación
- 28.3.1. Aprendizaje automático inductivo
- 28.3.2. SVM y KNN
- 28.3.3. Métricas y puntuaciones para clasificación

28.4. Algoritmos de regresión
- 28.4.1. Regresión lineal, regresión logística y modelos no lineales
- 28.4.2. Series temporales
- 28.4.3. Métricas y puntuaciones para regresión

28.5. Algoritmos de agrupamiento
- 28.5.1. Técnicas de agrupamiento jerárquico
- 28.5.2. Técnicas de agrupamiento particional
- 28.5.3. Métricas y puntuaciones para *Clustering*

28.6. Técnicas de reglas de asociación
- 28.6.1. Métodos para la extracción de reglas
- 28.6.2. Métricas y puntuaciones para los algoritmos de reglas de asociación

28.7. Técnicas de clasificación avanzadas. Multiclasificadores
- 28.7.1. Algoritmos de *Bagging*
- 28.7.2. Clasificador "*Random Forests*
- 28.7.3. "*Boosting*" para árboles de decisión

28.8. Modelos gráficos probabilísticos
- 28.8.1. Modelos probabilísticos
- 28.8.2. Redes bayesianas. Propiedades, representación y parametrización
- 28.8.3. Otros modelos gráficos probabilísticos

28.9. Redes neuronales
- 28.9.1. Aprendizaje automático con redes neuronales artificiales
- 28.9.2. Redes *Feedforward*

28.10. Aprendizaje profundo
- 28.10.1. Redes *Feedforward* profundas
- 28.10.2. Redes neuronales convolucionales y modelos de secuencia
- 28.10.3. Herramientas para implementar redes neuronales profundas

Módulo 29. Arquitecturas y sistemas para uso intensivo de Datos

29.1. Requisitos no funcionales. Pilares de las aplicaciones de Datos masivos
- 29.1.1. Fiabilidad
- 29.1.2. Adaptabilidad
- 29.1.3. Mantenibilidad

29.2. Modelos de Datos
- 29.2.1. Modelo relacional
- 29.2.2. Modelo documental
- 29.2.3. Modelo de Datos tipo grafo

29.3. Bases de Datos. Gestión del almacenamiento y recuperación de Datos
- 29.3.1. Índices *Hash*
- 29.3.2. Almacenamiento estructurado en *Log*
- 29.3.3. Árboles B

29.4. Formatos de codificación de Datos
- 29.4.1. Formatos específicos del lenguaje
- 29.4.2. Formatos estandarizados
- 29.4.3. Formatos de codificación binarios
- 29.4.4. Flujo de Datos entre procesos

29.5. Replicación
- 29.5.1. Objetivos de la replicación
- 29.5.2. Modelos de replicación
- 29.5.3. Problemas con la replicación

29.6. Transacciones distribuidas
- 29.6.1. Transacción
- 29.6.2. Protocolos para transacciones distribuidas
- 29.6.3. Transacciones serializables

29.7. Particionado
- 29.7.1. Formas de particionado
- 29.7.2. Interacción de índice secundarios y particionado
- 29.7.3. Rebalanceo de particiones

29.8. Procesamiento de *Datos Offline*
- 29.8.1. Procesamiento por lotes
- 29.8.2. Sistemas de ficheros distribuidos
- 29.8.3. MapReduce

29.9 Procesamiento de Datos en tiempo real
- 29.9.1. Tipos de *Broker* de mensajes
- 29.9.2. Representación de bases de Datos como flujos de Datos
- 29.9.3. Procesamiento de flujos de Datos

29.10. Aplicaciones prácticas en la empresa
- 29.10.1. Consistencia en lecturas
- 29.10.2. Enfoque holístico de Datos
- 29.10.3. Escalado de un servicio distribuido

Módulo 30. Aplicación práctica de la ciencia de Datos en sectores de actividad empresarial

30.1. Sector sanitario
- 30.1.1. Implicaciones de la IA y la analítica de Datos en el sector sanitario
- 30.1.2. Oportunidades y desafíos

30.2. Riesgos y tendencias en sector sanitario
- 30.2.1. Uso en el sector sanitario
- 30.2.2. Riesgos potenciales relacionados con el uso de IA

30.3. Servicios financieros
- 30.3.1. Implicaciones de la IA y la analítica de Datos en el sector de los servicios financiero
- 30.3.2. Uso en los servicios financieros
- 30.3.3. Riesgos potenciales relacionados con el uso de IA

30.4. *Retail*
- 30.4.1. Implicaciones de la IA y la analítica de Datos en el sector del *Retail*
- 30.4.2. Uso en el *Retail*
- 30.4.3. Riesgos potenciales relacionados con el uso de IA

30.5. Industria 4.0
- 30.5.1. Implicaciones de la IA y la analítica de Datos en la Industria 4.0
- 30.5.2. Uso en la Industria 4.0

30.6. Riesgos y tendencias en Industria 4.0
- 30.6.1. Riesgos potenciales relacionados con el uso de IA

30.7. Administración Pública
- 30.7.1. Implicaciones de la IA y la analítica de Datos en la Administración Pública
- 30.7.2. Uso en la Administración Pública
- 30.7.3. Riesgos potenciales relacionados con el uso de IA

30.8. Educación
- 30.8.1. Implicaciones de la IA y la analítica de Datos en la Educación
- 30.8.2. Riesgos potenciales relacionados con el uso de IA

30.9. Silvicultura y agricultura
- 30.9.1. Implicaciones de la IA y la analítica de Datos en la silvicultura y agricultura
- 30.9.2. Uso en Silvicultura y Agricultura
- 30.9.3. Riesgos potenciales relacionados con el uso de IA

30.10. Recursos humanos
- 30.10.1. Implicaciones de la IA y la analítica de Datos en la gestión de recursos humanos
- 30.10.2. Aplicaciones prácticas en el mundo empresarial
- 30.10.3. Riesgos potenciales relacionados con el uso de IA

TECH pone a tu disposición el mejor programa para informáticos como tú que desean un cambio en su carrera para impulsar su trayectoria profesional”

07

Titulación

El Grand Master en Computer Science, Ciberseguridad y Análisis de Datos 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 Computer Science, Ciberseguridad y Análisis de Datos** 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 Computer Science, Ciberseguridad y Análisis de Datos**

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

Computer Science, Ciberseguridad y Análisis de Datos

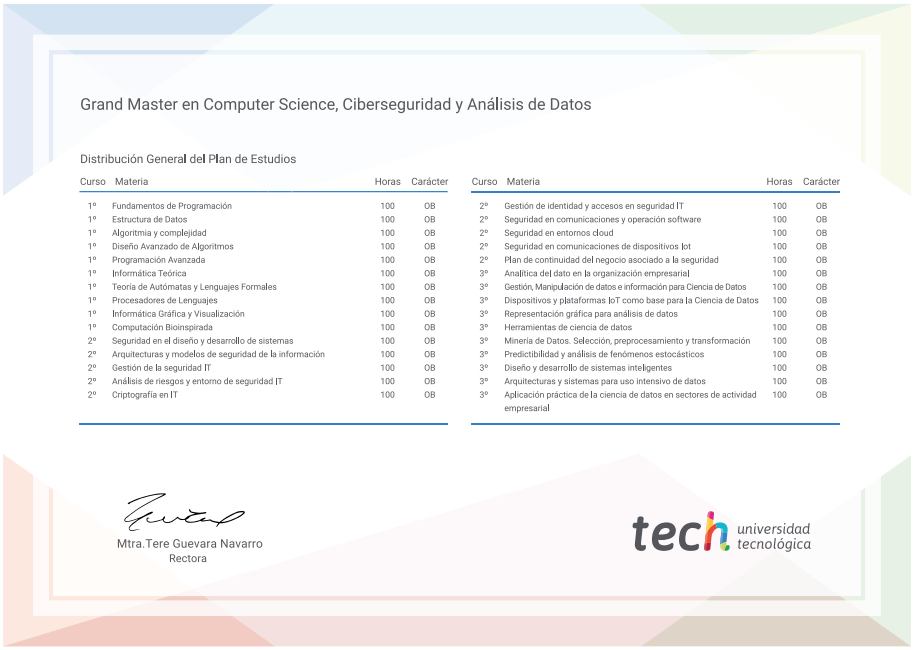
Se trata de un título propio de esta Universidad con una duración de 3.000 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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

Este título propio se deberá acompañar siempre del título universitario habilitante expedido por la autoridad competente para ejercer profesionalmente en cada país. código único TECH: AFWOR23S techtitute.com/titulos


Grand Master en Computer Science, Ciberseguridad y Análisis de Datos

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Fundamentos de Programación	100	OB
1º	Estructura de Datos	100	OB
1º	Algoritmia y complejidad	100	OB
1º	Diseño Avanzado de Algoritmos	100	OB
1º	Programación Avanzada	100	OB
1º	Informática Teórica	100	OB
1º	Teoría de Autómatas y Lenguajes Formales	100	OB
1º	Procesadores de Lenguajes	100	OB
1º	Informática Gráfica y Visualización	100	OB
1º	Computación Bioinspirada	100	OB
2º	Seguridad en el diseño y desarrollo de sistemas	100	OB
2º	Arquitecturas y modelos de seguridad de la información	100	OB
2º	Gestión de la seguridad IT	100	OB
2º	Análisis de riesgos y entorno de seguridad IT	100	OB
2º	Criptografía en IT	100	OB
2º	Gestión de identidad y accesos en seguridad IT	100	OB
2º	Seguridad en comunicaciones y operación software	100	OB
2º	Seguridad en entornos cloud	100	OB
2º	Seguridad en comunicaciones de dispositivos Iot	100	OB
2º	Plan de continuidad del negocio asociado a la seguridad	100	OB
3º	Analítica del dato en la organización empresarial	100	OB
3º	Gestión, Manipulación de datos e información para Ciencia de Datos	100	OB
3º	Dispositivos y plataformas IoT como base para la Ciencia de Datos	100	OB
3º	Representación gráfica para análisis de datos	100	OB
3º	Herramientas de ciencia de datos	100	OB
3º	Minería de Datos. Selección, preprocesamiento y transformación	100	OB
3º	Predictibilidad y análisis de fenómenos estocásticos	100	OB
3º	Diseño y desarrollo de sistemas inteligentes	100	OB
3º	Arquitecturas y sistemas para uso intensivo de datos	100	OB
3º	Aplicación práctica de la ciencia de datos en sectores de actividad empresarial	100	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

Computer Science, Ciberseguridad y Análisis de Datos

Modalidad: **Online**

Duración: **2 años**

Titulación: **TECH Universidad Tecnológica**

Horas lectivas: **3.000 h.**

Grand Master

Computer Science, Ciberseguridad y Análisis de Datos



tech universidad tecnológica