Máster Título Propio
Telemática

tech universidad tecnológica

tech universidad tecnológica

Máster Título Propio
Telemática

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Acceso web: **www.techtitute.com/informatica/master/master-telematica**

Índice

01 Presentación — *pág. 4*

02 Objetivos — *pág. 8*

03 Competencias — *pág. 14*

04 Estructura y contenido — *pág. 18*

05 Metodología — *pág. 40*

06 Titulación — *pág. 48*

01

Presentación

La informática y la tecnología de la comunicación se combinan en la Telemática para dar respuesta al desarrollo e implantación de técnicas, procesos, conocimientos y dispositivos que permitan el envío y la recepción eficiente de datos. Este campo de trabajo y la constante incorporación de avances tecnológicos exigen una actualización permanente y muy amplia. Este estudio ofrece esa actualización o la especialización de calidad que el profesional necesita con un programa actualizado y de alta capacitación. Un recorrido de alta calidad que le permitirá avanzar en su profesión.

Completo, totalmente actualizado y adaptable a tu disponibilidad, este programa es una herramienta de alta calidad para el informático que busca ampliar sus competencias reales”

Los avances en las telecomunicaciones se suceden constantemente, ya que esta es una de las áreas de más rápida evolución. Por ello, es necesario contar con expertos en Informática que se adapten a estos cambios y conozcan de primera mano las nuevas herramientas y técnicas que surgen en este ámbito.

El programa en Telemática aborda la totalidad de temáticas que intervienen en este campo. Su estudio presenta una clara ventaja frente a otras Másteres que se centran en bloques concretos, lo que impide al alumno conocer la interrelación con otras áreas incluidas en el ámbito multidisciplinar de las telecomunicaciones. Además, el equipo docente de este programa ha realizado una cuidadosa selección de cada uno de los temas de esta capacitación para ofrecer al alumno una oportunidad de estudio lo más completa posible y ligada siempre con la actualidad.

Este programa está dirigido a aquellas personas interesadas en alcanzar un nivel de conocimiento superior sobre la Telemática. El principal objetivo es educar al alumno para que aplique en el mundo real los conocimientos adquiridos en este programa, en un entorno de trabajo que reproduzca las condiciones que se puede encontrar en su futuro, de manera rigurosa y realista.

Además, al tratarse de un programa 100% online, el alumno no está condicionado por horarios fijos ni por la necesidad de trasladarse a otro lugar físico, sino que puede acceder a los contenidos en cualquier momento del día, equilibrando su vida laboral o personal con la académica.

Esta **Máster Título Propio en Telemática** contiene el programa educativo más completo y actualizado del mercado. Sus características más destacadas son:

- El desarrollo de casos prácticos presentados por expertos en Telemática
- Los contenidos gráficos, esquemáticos y eminentemente prácticos con los que está concebido recogen una información científica y práctica sobre aquellas disciplinas indispensables para el ejercicio profesional
- Los ejercicios prácticos donde realizar el proceso de autoevaluación para mejorar el aprendizaje
- Su especial hincapié en metodologías innovadoras en Telemática
- 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

Incluye en tus competencias la capacidad de intervención en los diferentes ámbitos de la Telemática, con un recorrido de aprendizaje que impulsará tu desarrollo profesional"

Este programa es la mejor inversión que puedes hacer en la selección de un programa de actualización para poner al día tus conocimientos en Telemática"

El material didáctico con el que desarrollarás tu estudio es un compendio de alta calidad que te permitirá avanzar de forma cómoda y sencilla.

Este programa 100% online te permitirá compaginar tus estudios con tu labor profesional.

Incluye en su cuadro docente a profesionales pertenecientes al ámbito de la Informática de las telecomunicaciones, que vierten en esta capacitación 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 una capacitación inmersiva programada para entrenarse ante situaciones reales.

El diseño de este programa se centra en el Aprendizaje Basado en Problemas, mediante el cual el profesional 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 en Telemática y con gran experiencia.

02

Objetivos

El programa en Telemática tiene como objetivo ofrecer a los profesionales de la Informática un estudio completo y actualizado de todas las áreas que competen a la intervención en Telemática, Con la seguridad y la calidad de un programa creado con un criterio de excelencia total.

El objetivo de este programa es poner a disposición del profesional, un recorrido completo a través de los conocimientos teóricos y prácticos que necesitará en el ámbito de la Telemática"

Objetivo general

- Capacitar al alumno para que sea capaz de desarrollar aplicaciones telemáticas, analizar datos o llevar a cabo labores de seguridad digital, entre otros aspectos

Una oportunidad creada para los profesionales que buscan un curso intensivo y eficaz con el que dar un paso significativo en el ejercicio de su profesión"

Objetivos específicos

Módulo 1. Redes de computadores

- Adquirir los conocimientos esenciales sobre redes de computadores en Internet
- Comprender el funcionamiento de las distintas capas que definen un sistema en red, como son la capa de aplicación, de transporte, de red y de enlace
- Entender la composición de las redes LAN, su topología y sus elementos de red e interconexión
- Aprender el funcionamiento del direccionamiento IP y el subnetting
- Comprender la estructura de las redes inalámbricas y móviles, incluyendo la nueva red 5G
- Conocer los distintos mecanismos de seguridad en redes, así como los distintos protocolos de seguridad en Internet

Módulo 2. Sistemas distribuidos

- Dominar los principios básicos sobre sistemas distribuidos
- Aprender a caracterizar y clasificar los sistemas distribuidos en función de una serie de parámetros básicos
- Comprender los distintos tipos de modelos utilizados en los sistemas distribuidos
- Conocer las arquitecturas actuales que implementan el concepto de sistema de archivos distribuidos
- Ser capaz de analizar los algoritmos de sincronización de procesos y objetos, la definición de relojes lógicos y consistencia temporal de la información
- Comprender el sistema de nombres usado en Internet, conocido como DNS (Domain Name System)
- Aprender el funcionamiento del direccionamiento IP y el *subnetting*.

Módulo 3. Seguridad en sistemas y redes de comunicación

- Obtener una perspectiva global de la seguridad, la criptografía y los criptoanálisis clásicos
- Comprender los fundamentos de la criptografía simétrica y de la criptografía asimétrica, así como sus principales algoritmos
- Analizar la naturaleza de los ataques en redes y los distintos tipos de arquitecturas de seguridad
- Comprender las distintas técnicas de protección de sistemas y de desarrollo de código seguro
- Conocer los componentes esenciales de ***botnets*** y spam, así como del malware y del código malicioso
- Sentar las bases para el análisis forense en el mundo del software y de las auditorías informáticas

Módulo 4. Redes corporativas e infraestructuras

- Dominar aspectos avanzados de interconexión de infraestructuras, imprescindibles a la hora de diseñar y planificar redes de alta velocidad
- Conocer las principales características y tecnologías de redes de transporte
- Comprender las arquitecturas de WAN clásicas, All-Ethernet, MPLS, VPN
- Analizar los aspectos fundamentales de la evolución de las redes a Redes NGN (Redes de Próxima Generación)
- Comprender los requisitos avanzados de calidad de servicio, encaminamiento y control de congestión y fiabilidad
- Conocer y saber aplicar los estándares internacionales de redes

Módulo 5. Arquitecturas de seguridad

- Comprender los principios básicos de la seguridad informática
- Dominar los estándares de seguridad informática y procesos de certificación
- Analizar los fundamentos organizativos y criptográficos en los que se basan las tecnologías de seguridad
- Identificar las principales amenazas y vulnerabilidades de los distintos elementos involucrados en las TIC, así como sus causas
- Conocer en profundidad las herramientas para la seguridad en redes y sus funciones específicas
- Saber aplicar las tecnologías que conforman una arquitectura de Seguridad de las TIC, en sus distintas perspectivas

Módulo 6. Centros de datos, operación de redes y servicios

- Ser capaz de diseñar, operar, gestionar y mantener redes, servicios y contenidos proporcionados mediante un Data Center
- Conocer todos los elementos esenciales que componen un Data Center y los estándares y certificaciones existentes
- Analizar el impacto económico de una infraestructura de Data Center en términos de rendimiento y eficiencia
- Identificar en infraestructuras reales los elementos hardware de un Data Center
- Entender las implicaciones en seguridad de las diferentes soluciones para ofrecer servicios por los proveedores del mercado
- Conocer el funcionamiento del proceso de virtualización
- Entender las ventajas, beneficios y modelos de adopción de la nube (Cloud)

Módulo 7. Programación avanzada

- Profundizar en los conocimientos de programación, especialmente en relacion con 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 8. Ingeniería de sistemas y servicios de red

- Dominar los conceptos fundamentales de la ingeniería de servicios
- Conocer los principios básicos de gestión de configuración de sistemas software en evolución
- Conocer las tecnologías y herramientas para provisión de servicios telemáticos
- Conocer distintos estilos arquitectónicos de un sistema software, comprender sus diferencias y saber elegir el más adecuado de acuerdo a los requisitos del sistema.
- Comprender los procesos de validación y verificación y sus relaciones con otras fases del ciclo de vida
- Ser capaz de integrar sistemas de captación, representación, procesado, almacenamiento, gestión y presentación de información multimedia para la construcción de servicios de telecomunicación y aplicaciones telemáticas
- Conocer elementos comunes para el diseño detallado de un sistema software
- Adquirir capacidad de programación, simulación y validación de servicios y aplicaciones telemáticas, en red y distribuidas
- Conocer el proceso y las actividades de transición, configuración, despliegue y operación
- Comprender los procesos de gestión, automatización y optimización de red

Módulo 9. Auditoría de Sistemas de Información

- Dominar los principales conceptos, normas y metodologías de la auditoría de sistemas
- Estar al tanto de los elementos organizativos y el marco legal de las auditorías
- Obtener una guía de referencia para el diseño de nuevos sistemas de controles internos informáticos
- Comprender y determinar los riesgos que trae consigo el desarrollo tecnológico
- Detectar cómo los diferentes sistemas de información cumplen o no con los requisitos de seguridad deseados
- Ser capaces de llevar a cabo un proceso de mejora continua de la ciberseguridad

Módulo 10. Gestión de Proyectos

- Conocer los conceptos fundamentales de la dirección de proyectos y el ciclo de vida de la gestión de proyectos
- Entender las distintas etapas de la gestión de proyectos como son el inicio, la planificación, la gestión de los *stakeholders* y el alcance
- Aprender el desarrollo del cronograma para la gestión del tiempo, el desarrollo del presupuesto y la respuesta ante los riesgos
- Comprender el funcionamiento de la gestión de la calidad en los proyectos, incluyendo la planificación, el aseguramiento, el control, los conceptos estadísticos y las herramientas disponibles
- Entender el funcionamiento de los procesos de aprovisionamiento, ejecución, monitorización, control y cierre de un proyecto
- Adquirir los conocimientos esenciales relacionados con la responsabilidad profesional derivada de la gestión de proyectos

03

Competencias

Después de superar las evaluaciones del programa en Telemática, se habrá adquirido las competencias necesarias para intervenir de manera segura y actualizada en los diferentes campos de trabajo que la Telemática desarrolla. Un proceso de crecimiento competencial que marcará la diferencia en la trayectoria profesional.

Adquiere las competencias de un especialista en Telemática y comienza a intervenir en esta área con la visión de un profesional de vanguardia”

Competencia general

- Desarrollar aplicaciones telemáticas y realizar tareas de seguridad digital

Especialízate con los mejores y ponte en primera línea en la intervención profesional"

Competencias específicas

- Conocer toda la estructura de las redes de computadores
- Dominar los sistemas distribuidos y saber clasificarlos
- Realizar tareas de seguridad en sistemas y redes de comunicación
- Aplicar los estándares internacionales para las redes
- Dominar todos los procedimientos sobre seguridad informática
- Diseñar y gestionar centros de datos
- Realizar labores de programación, detectar posibles problemas y solventarlos
- Conocer todo el proceso del diseño de sistemas
- Realizar auditorías en los sistemas y mejorar la ciberseguridad
- Conocer todas las etapas de la gestión de proyectos y su ciclo de vida para saber dirigirlos

04

Estructura y contenido

La estructura de los contenidos ha sido diseñada por los mejores profesionales del sector de la Informática de telecomunicaciones. Un recorrido intensivo y completo que incluye todos los aspectos que el informático que trabaja en Telemática debe manejar con seguridad, desarrollados de manera estructurada y eficiente para el alumno.

Contamos con el programa más completo y actualizado del mercado. Buscamos la excelencia y que tú también la logres"

Módulo 1. Redes de computadores

1.1. Redes de computadores en Internet
- 1.1.1. Redes e Internet
- 1.1.2. Arquitectura de protocolos

1.2. La capa de aplicación
- 1.2.1. Modelo y protocolos
- 1.2.2. Servicios FTP y SMTP
- 1.2.3. Servicio DNS
- 1.2.4. Modelo de operación HTTP
- 1.2.5. Formatos de mensaje HTTP
- 1.2.6. Interacción con métodos avanzados

1.3. La capa de transporte
- 1.3.1. Comunicación entre procesos
- 1.3.2. Transporte orientado a conexión: TCP y SCTP

1.4. La capa de red
- 1.4.1. Conmutación de circuitos y paquetes
- 1.4.2. El protocolo IP (v4 y v6)
- 1.4.3. Algoritmos de encaminamiento

1.5. La capa de enlace
- 1.5.1. Capa de enlace y técnicas de detección y corrección de errores
- 1.5.2. Enlaces de acceso múltiple y protocolos
- 1.5.3. Direccionamiento a nivel de enlace

1.6. Redes LAN
- 1.6.1. Topologías de red
- 1.6.2. Elementos de red y de interconexión

1.7. Direccionamiento IP
- 1.7.1. Direccionamiento IP y *Subnetting*
- 1.7.2. Visión de conjunto: una solicitud HTTP

1.8. Redes inalámbricas y móviles
- 1.8.1. Redes y servicios móviles 2G, 3G y 4G
- 1.8.2. Redes 5G

1.9. Seguridad en redes
- 1.9.1. Fundamentos de la seguridad en comunicaciones
- 1.9.2. Control de accesos
- 1.9.3. Seguridad en sistemas
- 1.9.4. Fundamentos de criptografía
- 1.9.5. Firma digital

1.10. Protocolos de seguridad en Internet
- 1.10.1. Seguridad IP y Redes Privadas Virtuales (VPN)
- 1.10.2. Seguridad Web con SSL/TLS

Módulo 2. Sistemas distribuidos

2.1. Introducción a la computación distribuida
- 2.1.1. Conceptos básicos
- 2.1.2. Computación monolítica, distribuida, paralela y cooperativa
- 2.1.3. Ventajas, inconvenientes y desafíos de los sistemas distribuidos
- 2.1.4. Conceptos previos sobre sistemas operativos: procesos y concurrencia
- 2.1.5. Conceptos previos sobre redes
- 2.1.6. Conceptos previos sobre ingeniería del software
- 2.1.7. Organización de este manual

2.2. Paradigmas de computación distribuida y comunicación entre procesos
- 2.2.1. Comunicación entre procesos
- 2.2.2. Sincronización de eventos
  - 2.2.2.1. Supuesto 1: envío síncrono y recepción síncrona
  - 2.2.2.2. Supuesto 2: envío asíncrono y recepción síncrona
  - 2.2.2.3. Supuesto 3: envío síncrono y recepción asíncrona
  - 2.2.2.4. Supuesto 4: envío asíncrono y recepción asíncrona
- 2.2.3. Interbloqueos y temporizadores
- 2.2.4. Representación y codificación de datos
- 2.2.5. Clasificación y descripción de los paradigmas de computación distribuida
- 2.2.6. Java como entorno de desarrollo de sistemas distribuidos

2.3. API de *Sockets*
- 2.3.1. API de sockets, tipos y diferencias
- 2.3.2. Sockets de tipo datagrama
- 2.3.3. Sockets de tipo *Stream*
- 2.3.4. Solución a interbloqueos: temporizadores y eventos no bloqueantes
- 2.3.5. Seguridad en *Sockets*

2.4 Paradigma de comunicaciones cliente-servidor
- 2.4.1. Características y conceptos fundamentales de los sistemas distribuidos de tipo cliente-servidor
- 2.4.2. Proceso de diseño e implementación de un sistema cliente-servidor
- 2.4.3. Problemas de direccionamiento no orientado a conexión con clientes anónimos
- 2.4.4. Servidores iterativos y concurrentes
- 2.4.5. Información de estado y de sesión
  - 2.4.5.1. Información de sesión
  - 2.4.5.2. Información de estado global
- 2.4.6. Clientes complejos recibiendo respuestas asíncronas desde el lado servidor
- 2.4.7. Servidores complejos actuando como intermediadores entre varios clientes

2.5. Comunicación de grupo
- 2.5.1. Introducción a la multidifusión y usos comunes
- 2.5.2. Fiabilidad y ordenación en los sistemas multidifusión
- 2.5.3. Implementación Java de sistemas de multidifusión
- 2.5.4. Ejemplo de uso de la comunicación en grupo entre iguales
- 2.5.5. Implementaciones de multidifusión fiable
- 2.5.6. Multitransmisión a nivel de aplicación

2.6. Objetos distribuidos
- 2.6.1. Introducción a objetos distribuidos
- 2.6.2. Arquitectura de una aplicación basada en objetos distribuidos
- 2.6.3. Tecnologías de sistemas de objetos distribuidos
- 2.6.4. Capas software de Java RMI en el lado cliente y en el lado servidor
- 2.6.5. API Java RMI de objetos distribuidos
- 2.6.6. Pasos para construir una aplicación RMI
- 2.6.7. Uso de *Callback* en RMI
- 2.6.8. Descarga dinámica de resguardos de objetos remotos y gestor de seguridad RMI

2.7. Aplicaciones de Internet I: HTML, XML, HTTP
- 2.7.1. Introducción Aplicaciones de Internet I
- 2.7.2. Lenguaje HTML
- 2.7.3. Lenguaje XML
- 2.7.4. Protocolo de Internet HTTP
- 2.7.5. Uso de contenidos dinámicos: manejo de formularios y CGI
- 2.7.6. Manejo de datos de estado y sesión en Internet

2.8. CORBA
- 2.8.1. Introducción a CORBA
- 2.8.2. Arquitectura CORBA
- 2.8.3. Lenguaje de descripción de interfaz en CORBA
- 2.8.4. Protocolos de interoperabilidad GIOP
- 2.8.5. Referencias a objeto remoto IOR
- 2.8.6. Servicio de nombrado CORBA
- 2.8.7. Ejemplo en IDL Java
- 2.8.8. Pasos de diseño, compilación y ejecución en IDL Java

2.9. Aplicaciones de Internet II: Applets, Servlets y SOA
- 2.9.1. Introducción a Aplicaciones de Internet II
- 2.9.2. Applets
- 2.9.3. Introducción a los Servlets
- 2.9.4. Servlets HTTP y su funcionamiento
- 2.9.5. Mantenimiento de la información de estado en Servlets
  - 2.9.5.1. Campos ocultos de formularios
  - 2.9.5.2. *Cookies*
  - 2.9.5.3. Variables de Servlet
  - 2.9.5.4. Objeto Session
- 2.9.6. Servicios web
- 2.9.7. Protocolo SOAP
- 2.9.8. Breve reseña de la arquitectura REST

2.10. Paradigmas avanzados
- 2.10.1. Introducción a paradigmas avanzados
- 2.10.2. Paradigma MOM
- 2.10.3. Paradigma de agentes software móviles
- 2.10.4. Paradigma de espacio de objetos
- 2.10.5. Computación colaborativa
- 2.10.6. Tendencias futuras en computación distribuida

Módulo 3. Seguridad en sistemas y redes de comunicación

3.1. Una perspectiva global de la seguridad, la criptografía y los criptoanálisis clásicos
- 3.1.1. La seguridad informática: perspectiva histórica
- 3.1.2. Pero ¿qué se entiende exactamente por seguridad?
- 3.1.3. Historia de la criptografía
- 3.1.4. Cifradores de sustitución
- 3.1.5. Caso de estudio: la máquina Enigma

3.2. Criptografía simétrica
- 3.2.1. Introducción y terminología básica
- 3.2.2. Cifrado simétrico
- 3.2.3. Modos de operación
- 3.2.4. DES
- 3.2.5. El nuevo estándar AES
- 3.2.6. Cifrado en flujo
- 3.2.7. Criptoanálisis

3.3. Criptografía asimétrica
- 3.3.1. Orígenes de la criptografía de clave pública
- 3.3.2. Conceptos básicos y funcionamiento
- 3.3.3. El algoritmo RSA
- 3.3.4. Certificados digitales
- 3.3.5. Almacenamiento y gestión de claves

3.4. Ataques en redes
- 3.4.1. Amenazas y ataques de una red
- 3.4.2. Enumeración
- 3.4.3. Interceptación de tráfico: *Sniffers*
- 3.4.4. Ataques de denegación de servicio
- 3.4.5. Ataques de envenenamiento ARP

3.5. Arquitecturas de seguridad
- 3.5.1. Arquitecturas de seguridad tradicionales
- 3.5.2. Secure Socket Layer: SSL
- 3.5.3. Protocolo SSH
- 3.5.4. Redes Privadas Virtuales (VPN)
- 3.5.5. Mecanismos de protección de unidades de almacenamiento externo
- 3.5.6. Mecanismos de protección hardware

3.6. Técnicas de protección de sistemas y desarrollo de código seguro
- 3.6.1. Seguridad en operaciones
- 3.6.2. Recursos y controles
- 3.6.3. Monitorización
- 3.6.4. Sistemas de detección de intrusión
- 3.6.5. IDS de *Host*
- 3.6.6. IDS de red
- 3.6.7. IDS basados en firmas
- 3.6.8. Sistemas señuelos
- 3.6.9. Principios de seguridad básicos en el desarrollo de código
- 3.6.10. Gestión del fallo
- 3.6.11. Enemigo público número 1: el desbordamiento de búfer
- 3.6.12. Chapuzas criptográficas

3.7. Botnets y *Spam*
- 3.7.1. Origen del problema
- 3.7.2. Proceso del spam
- 3.7.3. Envío del spam
- 3.7.4. Refinamiento de las listas de direcciones de correo

3.7.5. Técnicas de protección
3.7.6. Servicios *Antispam* ofrecidos por terceros
3.7.7. Casos de estudio
3.7.8. Spam exótico
3.8. Auditoría y ataques web
3.8.1. Recopilación de información
3.8.2. Técnicas de ataque
3.8.3. Herramientas
3.9. Malware y código malicioso
3.9.1. ¿Qué es el malware?
3.9.2. Tipos de malware
3.9.3. Virus
3.9.4. Criptovirus
3.9.5. Gusanos
3.9.6. *Adware*
3.9.7. *Spyware*
3.9.8. *Hoaxes*
3.9.9. *Pishing*
3.9.10. Troyanos
3.9.11. La economía del malware
3.9.12. Posibles soluciones
3.10. Análisis forense
3.10.1. Recolección de evidencias
3.10.2. Análisis de las evidencias
3.10.3. Técnicas antiforenses
3.10.4. Caso de estudio práctico

Módulo 4. Redes corporativas e infraestructuras

4.1. Redes de transporte
4.1.1. Arquitectura funcional de las redes de transporte
4.1.2. Interfaz de nodo de red en SDH
4.1.3. Elemento de red
4.1.4. Calidad y disponibilidad de redes
4.1.5. Gestión de las redes de transporte
4.1.6. Evolución de las redes de transporte
4.2. Arquitecturas WAN clásicas
4.2.1. Redes de área extensa WAN
4.2.2. Normas WAN
4.2.3. Encapsulamiento WAN
4.2.4. Dispositivos WAN
4.2.4.1. Router
4.2.4.2. Módem
4.2.4.3. *Switch*
4.2.4.4. Servidores de comunicación
4.2.4.5. *Gateway*
4.2.4.6. *Firewall*
4.2.4.7. *Proxy*
4.2.4.8. NAT
4.2.5. Tipos de conexión
4.2.5.1. Enlaces punto a punto
4.2.5.2. Conmutación de circuitos
4.2.5.3. Conmutación de paquetes
4.2.5.4. Circuitos virtuales WAN
4.3. Redes basadas en ATM
4.3.1. Introducción, características y modelo de capas
4.3.2. Capa física de acceso a ATM
4.3.2.1. Subcapa dependiente del medio físico PM
4.3.2.2. Subcapa Convergencia de Transmisión, TC

4.3.3. Celda ATM
4.3.3.1. Encabezamiento
4.3.3.2. Conexión virtual
4.3.3.3. Nodo de Switching ATM
4.3.3.4. Control de flujo (carga del enlace)
4.3.4. Adaptación de celdas AAL
4.3.4.1. Tipos de servicios AAL
4.4. Modelos avanzados de colas
4.4.1. Introducción
4.4.2. Fundamentos de la teoría de colas
4.4.3. Teoría de colas sistemas básicos
4.4.3.1. Sistemas M/M/1, M/M/m y M/M/∞
4.4.3.2. Sistemas M/M/1/k y M/M/m/m
4.4.4. Teoría de colas sistemas avanzados
4.4.4.1. Sistema M/G/1
4.4.4.2. Sistema M/G/1 con prioridades
4.4.4.3. Redes de colas
4.4.4.4. Modelado de redes de comunicaciones
4.5. Calidad de servicio en redes corporativas
4.5.1. Fundamentos
4.5.2. Factores de QoS en redes convergentes
4.5.3. Conceptos de QoS
4.5.4. Políticas de QoS
4.5.5. Métodos para implementar QoS
4.5.6. Modelos de QoS
4.5.7. Mecanismos para el despliegue de DiffServ QoS
4.5.8. Ejemplo de aplicación
4.6. Redes corporativas e infraestructuras All-Ethernet
4.6.1. Topologías de la Red Ethernet
4.6.1.1. Topología en Bus
4.6.1.2. Topología en estrella
4.6.2. Formato de la trama Ethernet e IEEE 802.3
4.6.3. Red Ethernet Conmutada

4.6.3.1. Redes virtuales VLAN
4.6.3.2. Agregación de puertos
4.6.3.3. Redundancia de conexiones
4.6.3.4. Gestión de la QoS
4.6.3.5. Funciones de seguridad
4.6.4. Fast Ethernet
4.6.5. Gigabit Ethernet
4.7. Infraestructuras MPLS
4.7.1. Introducción
4.7.2. MPLS
4.7.2.1. Antecedentes al MPLS y evolución
4.7.2.2. Arquitectura MPLS
4.7.2.3. Reenvío de paquetes etiquetados
4.7.2.4. Protocolo de distribución de etiquetas (LDP)
4.7.3. VPN MPLS
4.7.3.1. Definición de una VPN
4.7.3.2. Modelos de VPN
4.7.3.3. Modelo de VPN MPLS
4.7.3.4. Arquitectura de VPN MPLS
4.7.3.5. *Virtual Routing Forwarding* (VRF)
4.7.3.6. RD
4.7.3.7. Route Target (RT)
4.7.3.8. Propagación de rutas VPNv4 en una VPN MPLS
4.7.3.9. Reenvío de paquetes en una red VPN MPLS
4.7.3.10. BGP
4.7.3.11. Comunidad extendida BGP: RT
4.7.3.12. Transporte de etiquetas con BGP
4.7.3.13. Route Reflector (RR
4.7.3.14. Grupo RR
4.7.3.15. Selección de rutas BGP
4.7.3.16. Reenvío de paquetes

4.7.4. Protocolos de *Routing* comunes en entornos MPLS
4.7.4.1. Protocolos de routing de tipo Vector Distancia
4.7.4.2. Protocolos de routing de tipo Estado de Enlace
4.7.4.3. OSPF
4.7.4.4. ISIS
4.8. Servicios de operador y VPN
4.8.1. Introducción
4.8.2. Requerimientos básicos de una VPN
4.8.3. Tipos de VPN
4.8.3.1. VPN de acceso remoto
4.8.3.2. VPN punto a punto
4.8.3.3. VPN interna (over LAN)
4.8.4. Protocolos usados en VPN
4.8.5. Implementaciones y tipos de conexión
4.9. NGN (Next Generation Networks)
4.9.1. Introducción
4.9.2. Antecedentes
4.9.2.1. Definición y características de la red NGN
4.9.2.2. Migración hacia las redes de nueva generación
4.9.3. Arquitectura NGN
4.9.3.1. Capa de conectividad primaria
4.9.3.2. Capa de acceso
4.9.3.3. Capa de servicio
4.9.3.4. Capa de gestión
4.9.4. IMS
4.9.5. Organizaciones normalizadoras
4.9.6. Tendencias regulatorias
4.10. Revisión de estándares ITU e IETF
4.10.1. Introducción
4.10.2. Normalización
4.10.3. Algunas organizaciones estándares
4.10.4. Protocolos y estándares de la capa física WAN
4.10.5. Ejemplos de protocolos orientados al medio

Módulo 5. Arquitecturas de seguridad

5.1. Principios básicos de seguridad informática
5.1.1. Qué se entiende por seguridad informática
5.1.2. Objetivos de la seguridad informática
5.1.3. Servicios de seguridad informática
5.1.4. Consecuencias de la falta de seguridad
5.1.5. Principio de defensa en seguridad
5.1.6. Políticas, planes y procedimientos de seguridad
5.1.6.1. Gestión de cuentas de usuarios
5.1.6.2. Identificación y autenticación de usuarios
5.1.6.3. Autorización y control de acceso lógico
5.1.6.4. Monitorización de servidores
5.1.6.5. Protección de datos
5.1.6.6. Seguridad en conexiones remotas
5.1.7. La importancia del factor humano
5.2. Estandarización y certificación en seguridad informática
5.2.1. Estándares de seguridad
5.2.1.1. Propósito de los estándares
5.2.1.2. Organismos responsables
5.2.2. Estándares en EE.UU
5.2.2.1. TCSEC
5.2.2.2. Federal Criteria
5.2.2.3. FISCAM
5.2.2.4. NIST SP 800
5.2.3. Estándares europeos
5.2.3.1. ITSEC
5.2.3.2. ITSEM
5.2.3.3. Agencia Europea de Seguridad de la Información y las Redes
5.2.4. Estándares internacionales
5.2.5. Proceso de certificación

5.3. Amenazas a la seguridad informática: vulnerabilidades y malware
- 5.3.1. Introducción
- 5.3.2. Vulnerabilidades de los sistemas
  - 5.3.2.1. Incidentes de seguridad en las redes
  - 5.3.2.2. Causas de las vulnerabilidades de los sistemas informáticos
  - 5.3.2.3. Tipos de vulnerabilidades
  - 5.3.2.4. Responsabilidades de los fabricantes de software
  - 5.3.2.5. Herramientas para la evaluación de vulnerabilidades
- 5.3.3. Amenazas de la seguridad informática
  - 5.3.3.1. Clasificación de los intrusos en redes
  - 5.3.3.2. Motivaciones de los atacantes
  - 5.3.3.3. Fases de un ataque
  - 5.3.3.4. Tipos de ataques
- 5.3.4. Virus informáticos
  - 5.3.4.1. Características generales
  - 5.3.4.2. Tipos de virus
  - 5.3.4.3. Daños ocasionados por virus
  - 5.3.4.4. Cómo combatir los virus

5.4. Ciberterrorismo y respuesta a incidentes
- 5.4.1. Introducción
- 5.4.2. La amenaza del ciberterrorismo y de las guerras informáticas
- 5.4.3. Consecuencias de los fallos y ataques en las empresas
- 5.4.4. El espionaje en las redes de ordenadores

5.5. Identificación de usuarios y sistemas biométricos
- 5.5.1. Introducción a la autenticación, autorización y registro de usuarios
- 5.5.2. Modelo de seguridad AAA
- 5.5.3. Control de acceso
- 5.5.4. Identificación de usuarios
- 5.5.5. Verificación de contraseñas
- 5.5.6. Autenticación con certificados digitales
- 5.5.7. Identificación remota de usuarios
- 5.5.8. Inicio de sesión único
- 5.5.9. Gestores de contraseñas
- 5.5.10. Sistemas biométricos
  - 5.5.10.1. Características generales
  - 5.5.10.2. Tipos de sistemas biométricos
  - 5.5.10.3. Implantación de los sistemas

5.6. Fundamentos de criptografía y protocolos criptográficos
- 5.6.1. Introducción a la criptografía
  - 5.6.1.1. Criptografía, criptoanálisis y criptología
  - 5.6.1.2. Funcionamiento de un sistema criptográfico
  - 5.6.1.3. Historia de los sistemas criptográficos
- 5.6.2. Criptoanálisis
- 5.6.3. Clasificación de los sistemas criptográficos
- 5.6.4. Sistemas criptográficos simétricos y asimétricos
- 5.6.5. Autenticación con sistemas criptográficos
- 5.6.6. Firma electrónica
  - 5.6.6.1. Qué es la firma electrónica
  - 5.6.6.2. Características de la firma electrónica
  - 5.6.6.3. Autoridades de certificación
  - 5.6.6.4. Certificados digitales
  - 5.6.6.5. Sistemas basados en el tercero de confianza
  - 5.6.6.6. Utilización de la firma electrónica
  - 5.6.6.7. DNI electrónico
  - 5.6.6.8. Factura electrónica

5.7. Herramientas para la seguridad en redes
- 5.7.1. El problema de la seguridad en la conexión a internet
- 5.7.2. La seguridad en la red externa
- 5.7.3. El papel de los servidores *Proxy*
- 5.7.4. El papel de los cortafuegos
- 5.7.5. Servidores de autenticación para conexiones remotas
- 5.7.6. El análisis de los registros de actividad
- 5.7.7. Sistemas de detección de intrusiones
- 5.7.8. Los señuelos

5.8. Seguridad en redes privadas virtuales e inalámbricas
- 5.8.1. Seguridad en redes privadas virtuales
  - 5.8.1.1 El papel de las VPN
  - 5.8.1.2 Protocolos para VPN
- 5.8.2. Seguridad tradicional en redes inalámbricas
- 5.8.3. Posibles ataques en redes inalámbricas
- 5.8.4. El protocolo WEP
- 5.8.5. Estándares para seguridad en redes inalámbricas
- 5.8.6. Recomendaciones para reforzar la seguridad

5.9. Seguridad en el uso de servicios de internet
- 5.9.1. Navegación segura en la web
  - 5.9.1.1. El servicio www
  - 5.9.1.2. Problemas de seguridad en www
  - 5.9.1.3. Recomendaciones de seguridad
  - 5.9.1.4. Protección de la privacidad en internet
- 5.9.2. Seguridad en correo electrónico
  - 5.9.2.1. Características del correo electrónico
  - 5.9.2.2. Problemas de seguridad en el correo electrónico
  - 5.9.2.3. Recomendaciones de seguridad en el correo electrónico
  - 5.9.2.4. Servicios de correo electrónico avanzados
  - 5.9.2.5. Uso de correo electrónico por empleados
- 5.9.3. El SPAM
- 5.9.4. El *Phising*

5.10. Control de contenidos
- 5.10.1. La distribución de contenidos a través de internet
- 5.10.2. Medidas legales para combatir los contenidos ilícitos
- 5.10.3. Filtrado, catalogación y bloqueo de contenidos
- 5.10.4. Daños a la imagen y reputación

Módulo 6. Centros de datos, operación de redes y servicios

6.1. data center: conceptos básicos y componentes
- 6.1.1. Introducción
- 6.1.2. Conceptos básicos
  - 6.1.2.1. Definición de un DC
  - 6.1.2.2. Clasificación e Importancia
  - 6.1.2.3. Catástrofes y pérdidas
  - 6.1.2.4. Tendencia evolutiva
  - 6.1.2.5. Costes de la complejidad
  - 6.1.2.6. Pilares y capas de redundancia
- 6.1.3. Filosofía de diseño
  - 6.1.3.1. Objetivos
  - 6.1.3.2. Selección de ubicación
  - 6.1.3.3. Disponibilidad
  - 6.1.3.4. Elementos críticos
  - 6.1.3.5. Evaluación y análisis de costes
  - 6.1.3.6. Presupuesto de IT
- 6.1.4. Componentes básicos
  - 6.1.4.1. Piso técnico
  - 6.1.4.2. Tipos de baldosas
  - 6.1.4.3. Consideraciones generales
  - 6.1.4.4. Tamaño del DC
  - 6.1.4.5. *Racks*
  - 6.1.4.6. Servidores y equipos de comunicación
  - 6.1.4.7. Monitorización

6.2. *Data Center*: sistemas de control
- 6.2.1. Introducción
- 6.2.2. Alimentación eléctrica
  - 6.2.2.1. Red eléctrica
  - 6.2.2.2. Potencia eléctrica

6.2.2.3. Estrategias de distribución eléctrica
6.2.2.4. UPS
6.2.2.5. Generadores
6.2.2.6. Problemas eléctricos
6.2.3. Control ambiental
6.2.3.1. Temperatura
6.2.3.2. Humedad
6.2.3.3. Aire acondicionado
6.2.3.4. Estimación calórica
6.2.3.5. Estrategias de refrigeración
6.2.3.6. Diseño de pasillos. Circulación del aire
6.2.3.7. Sensores y mantenimiento
6.2.4. Seguridad y prevención de incendios
6.2.4.1. Seguridad física
6.2.4.2. El fuego y su clasificación
6.2.4.3. Clasificación y tipos de sistemas de extinción
6.3. *Data Centers*: diseño y organización
6.3.1. Introducción
6.3.2. Diseño de red
6.3.2.1. Tipologías
6.3.2.2. Cableado estructurado
6.3.2.3. Backbone
6.3.2.4. Cables de red UTP y STP
6.3.2.5. Cables de telefonía
6.3.2.6. Elementos terminales
6.3.2.7. Cables de fibra óptica
6.3.2.8. Cable coaxial
6.3.2.9. Transmisión inalámbrica
6.3.2.10. Recomendaciones y etiquetado
6.3.3. Organización
6.3.3.1. Introducción
6.3.3.2. Medidas básicas
6.3.3.3. Estrategias para manejo y gestión del cableado
6.3.3.4. Políticas y procedimientos
6.3.4. Gestión del DC
6.3.5. Estándares en el *Data Center*
6.4. *Data Center*: modelos y montinuidad de negocio
6.4.1. Introducción
6.4.2. Optimización
6.4.2.1. Técnicas de optimización
6.4.2.2. *Data Centers* ecológicos
6.4.2.3. Desafíos actuales
6.4.2.4. *Data Centers* modulares
6.4.2.5. Housing
6.4.2.6. Consolidación de *Data Centers*
6.4.2.7. Monitorización
6.4.3. Continuidad de negocio
6.4.3.1. BCP. Plan de continuidad de negocios. Puntos claves
6.4.3.2. DR. Plan de recuperación ante desastres
6.4.3.3. Implementación de un DR
6.4.3.4. *Backup* y estrategias
6.4.3.5. *Data Center* de respaldo
6.4.4. Mejores prácticas
6.4.4.1. Recomendaciones
6.4.4.2. Utilización metodología ITIL
6.4.4.3. Métricas de disponibilidad
6.4.4.4. Control ambiental
6.4.4.5. Gestión de riesgos
6.4.4.6. Responsable del DC
6.4.4.7. Herramientas
6.4.4.8. Consejos de implantación
6.4.4.9. Caracterización

6.5. *Cloud Computing*: introducción y conceptos básicos
- 6.5.1. Introducción
- 6.5.2. Conceptos básicos y terminología
- 6.5.3. Objetivos y beneficios
  - 6.5.3.1. Disponibilidad
  - 6.5.3.2. Fiabilidad
  - 6.5.3.3. Escalabilidad
- 6.5.4. Riesgos y retos
- 6.5.5. Roles. Provider. Consumer
- 6.5.6. Características del Cloud
- 6.5.7. Modelos de entrega de servicios
  - 6.5.7.1. IaaS
  - 6.5.7.2. PaaS
  - 6.5.7.3. SaaS
- 6.5.8. Tipos de Cloud
  - 6.5.8.1. Pública
  - 6.5.8.2. Privada
  - 6.5.9.3. Híbrida
- 6.5.9. Tecnologías habilitadoras del Cloud
  - 6.5.9.1. Arquitecturas de red
  - 6.5.9.2. Redes de banda ancha. Interconectividad
  - 6.5.9.3. Tecnologías de Data Center
    - 6.5.9.3.1. *Computing*
    - 6.5.9.3.2. *Storage*
    - 6.5.9.3.3. *Networking*
    - 6.5.9.3.4. Alta disponibilidad
    - 6.5.9.3.5. Sistemas de *Backup*
    - 6.5.9.3.6. Balanceadores
  - 6.5.9.4. Virtualización
  - 6.5.9.5. Tecnologías web
  - 6.5.9.6. Tecnología Multitenant

6.5.9.7. Tecnología de servicios
6.5.9.8. Seguridad Cloud
6.5.9.8.1. Términos y conceptos
6.5.9.8.2. Integridad y autenticación
6.5.9.8.3. Mecanismos de seguridad
6.5.9.8.4. Amenazas de seguridad
6.5.9.8.5. Ataques de seguridad Cloud
6.5.9.8.6. Caso de estudio

6.6. *Cloud Computing*: tecnología y seguridad en la nube
6.6.1. Introducción
6.6.2. Mecanismos de Infraestructura Cloud
6.6.2.1. Perímetro de red
6.6.2.2. Almacenamiento
6.6.2.3. Entorno de servidores
6.6.2.4. Monitorización Cloud
6.6.2.5. Alta Disponibilidad
6.6.3. Mecanismos de Seguridad Cloud (parte I)
6.6.3.1. Automatización
6.6.3.2. Balanceadores de carga
6.6.3.3. Monitor de SLA
6.6.3.4. Mecanismos de pago por uso
6.6.4. Mecanismos de seguridad Cloud (parte II)
6.6.4.1. Sistemas de trazabilidad y auditoria
6.6.4.2. Sistemas de Failover
6.6.4.3. Hypervisor
6.6.4.4. Clusterización
6.6.4.5. Sistemas Multitenant

6.7. *Cloud Computing*: infraestructura. Mecanismos de control y seguridad
6.7.1. Introducción a mecanismos de gestión cloud
6.7.2. Sistemas de administración remota
6.7.3. Sistemas de gestión de recursos
6.7.4. Sistemas de gestión de acuerdos de nivel de servicios
6.7.5. Sistemas de gestión de la facturación
6.7.6. Mecanismos de Seguridad Cloud
6.7.6.1. Encriptación
6.7.6.2. *Hashing*
6.7.6.3. Firma digital
6.7.6.4. PKI
6.7.6.5. Gestión de accesos e identidades
6.7.6.6. SSO
6.7.6.7. Grupos de seguridad basados en cloud
6.7.6.8. Sistemas de bastionado

6.8. *Cloud Computing*: arquitecturas Cloud
6.8.1. Introducción
6.8.2. Arquitecturas cloud básicas
6.8.2.1. Arquitecturas de distribución de cargas de trabajo
6.8.2.2. Arquitecturas de uso de recursos
6.8.2.3. Arquitecturas escalables
6.8.2.4. Arquitecturas de balanceo de carga
6.8.2.5. Arquitecturas redundantes
6.8.2.6. Ejemplos
6.8.3. Arquitecturas cloud avanzadas
6.8.3.1. Arquitecturas de clúster de hipervisor
6.8.3.2. Arquitecturas virtuales de balanceo de carga
6.8.3.3. Arquitecturas *non-stop*
6.8.3.4. Arquitecturas de alta disponibilidad
6.8.3.5. Arquitecturas Bare metal
6.8.3.6. Arquitecturas redundantes
6.8.3.7. Arquitecturas híbridas

6.8.4. Arquitecturas cloud especializadas
6.8.4.1. Arquitecturas de acceso directo I/O
6.8.4.2. Arquitecturas de acceso directo LUN
6.8.4.3. Arquitecturas de red elástica
6.8.4.4. Arquitecturas SDDC
6.8.4.5. Arquitecturas especiales
6.8.4.6. Ejemplos
6.9. *Cloud Computing*: modelos de provisión de servicio
6.9.1. Introducción
6.9.2. Provisión de servicios cloud
6.9.3. Perspectiva del proveedor del servicio
6.9.4. Perspectiva del consumidor de esos servicios
6.9.5. Casos de estudio
6.10. *Cloud Computing*: modelos de contratación, métricas y proveedores de Servicio
6.10.1. Introducción a los modelos y métricas de facturación
6.10.2. Modelos de facturación
6.10.3. Métricas de pago por uso
6.10.4. Consideraciones de gestión de costes
6.10.5. Introducción a las métricas de calidad de servicio y SLA
6.10.6. Métricas de calidad de servicio
6.10.7. Métricas de rendimiento del servicio
6.10.8. Métricas de escalabilidad del servicio
6.10.9. SLA del modelo del servicio
6.10.10. Casos de estudio

Módulo 7. Programación avanzada

7.1. Introducción a la programación orientada a objetos
7.1.1. Introducción a la programación orientada a objetos
7.1.2. Diseño de clases
7.1.3. Introducción a UML para el modelado de los problemas
7.2. Relaciones entre clases
7.2.1. Abstracción y herencia
7.2.2. Conceptos avanzados de herencia
7.2.3. Polimorfismo
7.2.4. Composición y agregación
7.3. Introducción a los patrones de diseño para problemas orientados a objetos
7.3.1. ¿Qué son los patrones de diseño?
7.3.2. Patrón Factory
7.3.3. Patrón Singleton
7.3.4. Patrón Observer
7.3.5. Patrón Composite
7.4. Excepciones
7.4.1. ¿Qué son las excepciones?
7.4.2. Captura y gestión de excepciones
7.4.3. Lanzamiento de excepciones
7.4.4. Creación de excepciones
7.5. Interfaces de usuarios
7.5.1. Introducción a Qt
7.5.2. Posicionamiento
7.5.3. ¿Qué son los eventos?
7.5.4. Eventos: definición y captura
7.5.5. Desarrollo de interfaces de usuario
7.6. Introducción a la programación concurrente
7.6.1. Introducción a la programación concurrente
7.6.2. El concepto de proceso e hilo
7.6.3. Interacción entre procesos o hilos
7.6.4. Los hilos en C++
7.6.5. Ventajas e inconvenientes de la programación concurrente
7.7. Gestión de hilos y sincronización
7.7.1. Ciclo de vida de un hilo
7.7.2. La clase Thread
7.7.3. Planificación de hilos
7.7.4. Grupos hilos
7.7.5. Hilos de tipo demonio
7.7.6. Sincronización

7.7.7. Mecanismos de bloqueo
7.7.8. Mecanismos de comunicación
7.7.9. Monitores
7.8. Problemas comunes dentro de la programación concurrente
7.8.1. El problema de los productores consumidores
7.8.2. El problema de los lectores y escritores
7.8.3. El problema de la cena de los filósofos
7.9. Documentación y pruebas de software
7.9.1. ¿Por qué es importante documentar el software?
7.9.2. Documentación de diseño
7.9.3. Uso de herramientas para la documentación
7.10. Pruebas de software
7.10.1. Introducción a las pruebas del software
7.10.2. Tipos de pruebas
7.10.3. Prueba de unidad
7.10.4. Prueba de integración
7.10.5. Prueba de validación
7.10.6. Prueba del sistema

Módulo 8. Ingeniería de sistemas y servicios de red

8.1. Introducción a la ingeniería de sistemas y servicios de red
8.1.1. Concepto de sistema informático e ingeniería informática
8.1.2. El software y sus características
8.1.2.1. Características del software
8.1.3. La evolución del software
8.1.3.1. Los albores del desarrollo del software
8.1.3.2. La crisis del software
8.1.3.3. La Ingeniería del software
8.1.3.4. La tragedia del software
8.1.3.5. La actualidad del software
8.1.4. Los mitos del software
8.1.5. Los nuevos retos del software
8.1.6. Deontología profesional de la Ingeniería del software
8.1.7. SWEBOK. El cuerpo de conocimientos de la ingeniería del software
8.2. El proceso de desarrollo
8.2.1. Proceso de resolución de problemas
8.2.2. El proceso de desarrollo del software
8.2.3. Proceso software frente al ciclo de vida
8.2.4. Ciclos de vida. Modelos de proceso (tradicionales)
8.2.4.1. Modelo en cascada
8.2.4.2. Modelos basados en prototipos
8.2.4.3. Modelo de desarrollo incremental
8.2.4.4. Desarrollo rápido de aplicaciones (RAD)
8.2.4.5. Modelo en espiral
8.2.4.6. Proceso unificado de desarrollo o proceso racional unificado (RUP)
8.2.4.7. Desarrollo de software basado en componentes
8.2.5. El manifiesto ágil. Los métodos ágiles
8.2.5.1. Extreme Programming (XP)
8.2.5.2. Scrum
8.2.5.3. Feature Driven Development (FDD)
8.2.6. Estándares sobre el proceso software
8.2.7. Definición de un proceso software
8.2.8. Madurez del proceso software
8.3. Planificación y gestión de proyectos ágiles
8.3.1. ¿Qué es Agile?
8.3.1.1. Historia de Agile
8.3.1.2. Manifiesto Agile
8.3.2. Fundamentos de Agile
8.3.2.1. La mentalidad agile
8.3.2.2. La adecuación a Agile
8.3.2.3. Ciclo de vida del desarrollo de productos
8.3.2.4. El triángulo de hierro
8.3.2.5. Trabajar con incertidumbre y volatilidad

8.3.2.6. Procesos definidos y procesos empíricos
8.3.2.7. Los mitos de Agile
8.3.3. El entorno Agile
8.3.3.1. Modelo operativo
8.3.3.2. Roles Agile
8.3.3.3. Técnicas Agile
8.3.3.4. Prácticas Agile
8.3.4. Marcos de trabajo Agile
8.3.4.1. e-Xtreme Programming (XP)
8.3.4.2. Scrum
8.3.4.3. Dynamic Systems Development Method (DSDM)
8.3.4.4. Agile Project Management
8.3.4.5. Kanban
8.3.4.6. Lean software Development
8.3.4.7. Lean Start-up
8.3.4.8. Scaled Agile Framework (SAFe)
8.4. Gestión de configuración y repositorios colaborativos
8.4.1. Conceptos básicos de gestión de configuración del software
8.4.1.1. ¿Qué es la gestión de configuración del software?
8.4.1.2. Configuración del software y elementos de la configuración del software
8.4.1.3. Líneas base
8.4.1.4. Versiones, revisiones, variantes y *Releases*
8.4.2. Actividades de gestión de configuración
8.4.2.1. Identificación de la configuración
8.4.2.2. Control de cambios en la configuración
8.4.2.3. Generación de informes de estado
8.4.2.4. Auditoría de la configuración
8.4.3. El plan de gestión de configuración
8.4.4. Herramientas de gestión de configuración
8.4.5. La gestión de configuración en la metodología Métrica v.3
8.4.6. La gestión de configuración en SWEBOK

8.5. Prueba de sistemas y servicios
- 8.5.1. Conceptos generales de la prueba
  - 8.5.1.1. Verificar y validar
  - 8.5.1.2. Definición de prueba
  - 8.5.1.3. Principios de las pruebas
- 8.5.2. Enfoques de las pruebas
  - 8.5.2.1. Pruebas de caja blanca
  - 8.5.2.2. Pruebas de caja negra
- 8.5.3. Pruebas estáticas o revisioneZs
  - 8.5.3.1. Revisiones técnicas formales
  - 8.5.3.2. *Walkthroughs*
  - 8.5.3.3. Inspecciones de código
- 8.5.4. Pruebas dinámicas
  - 8.5.4.1. Pruebas de unidad o unitarias
  - 8.5.4.2. Pruebas de integración
  - 8.5.4.3. Pruebas del sistema
  - 8.5.4.4. Pruebas de aceptación
  - 8.5.4.5. Pruebas de regresión
- 8.5.5. Pruebas alfa y pruebas beta
- 8.5.6. El proceso de prueba
- 8.5.7. Error, defecto y fallo
- 8.5.8. Herramientas de prueba automática
  - 8.5.8.1. Junit
  - 8.5.8.2. LoadRunner

8.6. Modelado y diseño de arquitecturas de redes
- 8.6.1. Introducción
- 8.6.2. Características de los sistemas
  - 8.6.2.1. Descripción de los sistemas
  - 8.6.2.2. Descripción y características de los servicios
  - 8.6.2.3. Requisitos de operabilidad

8.6.3. Análisis de requisitos
8.6.3.1. Requisitos de usuario
8.6.3.2. Requisitos de aplicaciones
8.6.3.3. Requisitos de red
8.6.4. Diseño de arquitecturas de red
8.6.4.1. Arquitectura de referencia y componentes
8.6.4.2. Modelos de arquitectura
8.6.4.3. Arquitecturas de sistemas y de red
8.7. Modelado y diseño de sistemas distribuidos
8.7.1. Introducción
8.7.2. Arquitectura de direccionamiento y *Routing*
8.7.2.1. Estrategia de direccionamiento
8.7.2.2. Estrategia de enrutamiento
8.7.2.3. Consideraciones de diseño
8.7.3. Conceptos de diseño de redes
8.7.4. Proceso de diseño
8.8. Plataformas y entornos de despliegue
8.8.1. Introducción
8.8.2. Sistemas de computadoras distribuidas
8.8.2.1. Conceptos básicos
8.8.2.2. Modelos de computación
8.8.2.3. Ventajas, inconvenientes y desafíos
8.8.2.4. Conceptos básicos de sistemas operativos
8.8.3. Despliegues de redes virtualizadas
8.8.3.1. Necesidad de un cambio
8.8.3.2. Transformación de las redes: de "todo-IP" a la nube
8.8.3.3. Despliegue de red en cloud
8.8.4. Ejemplo: arquitectura de red en Azure
8.9. Prestaciones E2E: retardo y ancho de banda. QoS
8.9.1. Introducción
8.9.2. Análisis del rendimiento
8.9.3. QoS
8.9.4. Priorización y gestión de tráfico
8.9.5. Acuerdos de nivel de servicio
8.9.6. Consideraciones de diseño
8.9.6.1. Evaluación del rendimiento
8.9.6.2. Relaciones e interacciones
8.10. Automatización y optimización de red
8.10.1. Introducción
8.10.2. Gestión de red
8.10.2.1. Protocolos de gestión y configuración
8.10.2.2. Arquitecturas de gestión de red
8.10.3. Orquestación y automatización
8.10.3.1. Arquitectura ONAP
8.10.3.2. Controladores y funciones
8.10.3.3. Políticas
8.10.3.4. Inventario de red
8.10.4. Optimización

Módulo 9. Auditoría de sistemas de información

9.1. Auditoría de sistemas de información. Normas de buenas prácticas
9.1.1. Introducción
9.1.2. Auditoría y COBIT
9.1.3. Auditoría de los sistemas de gestión en las TIC
9.1.4. Certificaciones
9.2. Conceptos y metodologías de la auditoría de sistemas
9.2.1. Introducción
9.2.2. Metodologías de evaluación de sistemas: cuantitativas y cualitativas
9.2.3. Metodologías de auditoría informática
9.2.4. El plan auditor
9.3. Contrato de auditoría
9.3.1. Naturaleza jurídica del contrato
9.3.2. Partes de un contrato de auditoría

9.3.3. Objeto del contrato de auditoría
9.3.4. El informe de auditoría
9.4. Elementos organizativos de las auditorías
9.4.1. Introducción
9.4.2. Misión del departamento de auditoría
9.4.3. Planificación de las auditorías
9.4.4. Metodología de la auditoría de SI
9.5. Marco legal de las auditorías
9.5.1. Protección de datos de caracter personal
9.5.2. Protección jurídica del software
9.5.3. Delitos tecnológicos
9.5.4. Contratación, firma y DNI electrónico
9.6. Auditoría del outsourcing y marcos de referencia
9.6.1. Introducción
9.6.2. Conceptos básicos del outsorcing
9.6.3. Auditoría del outsourcing de TI
9.6.4. Marcos de referencia: CMMI, ISO27001, ITIL
9.7. Auditoría de seguridad
9.7.1. Introducción
9.7.2. Seguridad física y lógica
9.7.3. Seguridad del entorno
9.7.4. Planificación y ejecución de la auditoría de la seguridad física
9.8. Auditoría de redes e internet
9.8.1. Introducción
9.8.2. Vulnerabilidades en redes
9.8.3. Principios y derechos en internet
9.8.4. Controles y tratamientos de los datos
9.9. Auditoría de aplicaciones y sistemas informáticos
9.9.1. Introducción
9.9.2. Modelos de referencia
9.9.3. Evaluación de la calidad de las aplicaciones
9.9.4. Auditoría de la organización y gestión del área de desarrollo y mantenimiento
9.10. Auditoría de los datos de carácter personal
9.10.1. Introducción
9.10.2. Leyes y reglamentos de protección de datos
9.10.3. Desarrollo de la auditoría
9.10.4. Infracciones y sanciones

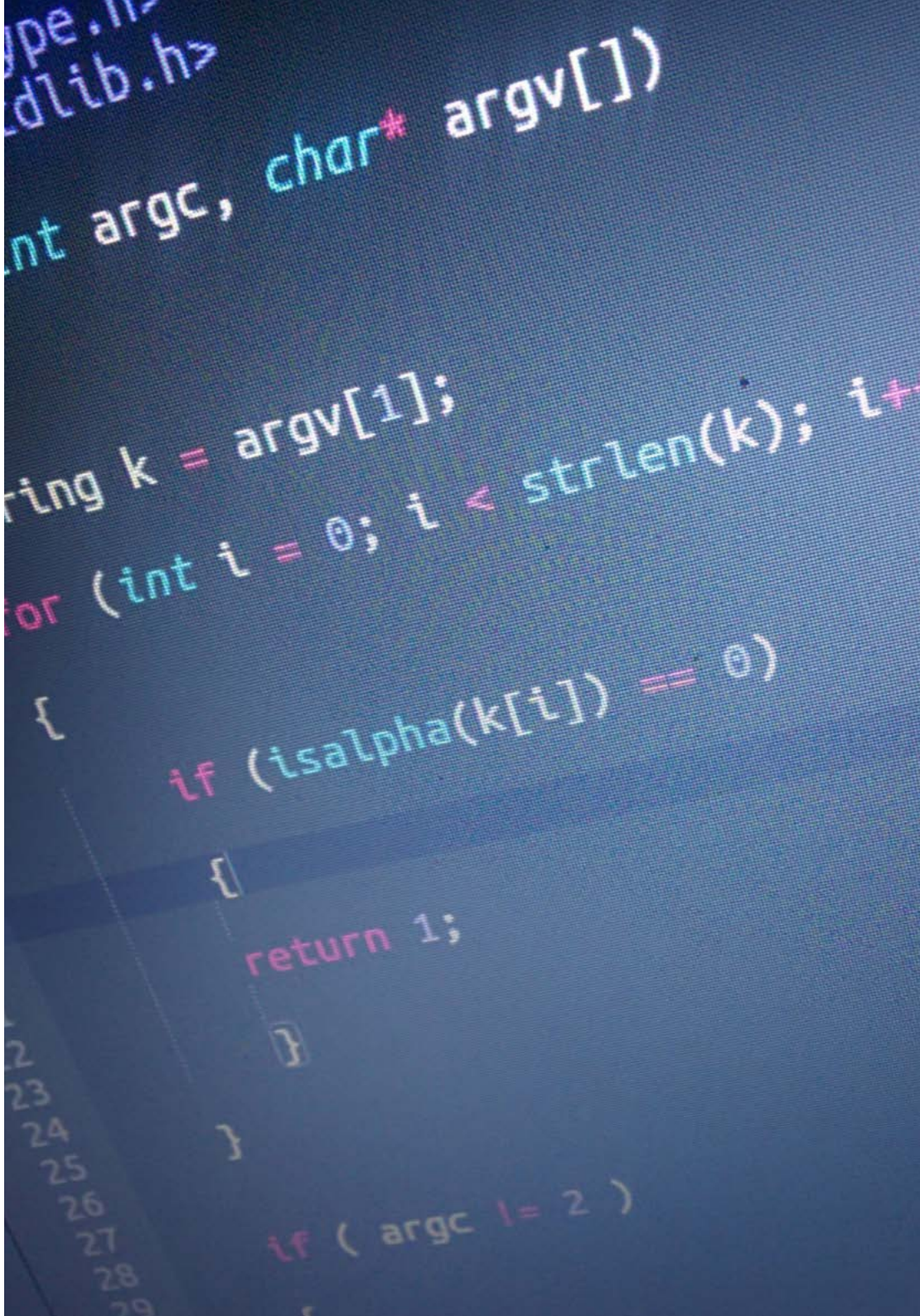
Módulo 10. Gestión de proyectos

10.1. Conceptos fundamentales de la dirección de proyectos y el ciclo de vida de la gestión de proyectos
10.1.1. ¿Qué es un proyecto?
10.1.2. Metodología común
10.1.3. ¿Qué es la dirección/gestión de proyectos?
10.1.4. ¿Qué es un plan de proyecto?
10.1.5. Beneficios
10.1.6. Ciclo de vida del proyecto
10.1.7. Grupos de procesos o ciclo de vida de la gestión de los proyectos
10.1.8. La relación entre los grupos de procesos y las áreas de conocimiento
10.1.9. Relaciones entre el ciclo de vida del producto y del proyecto
10.2. El inicio y la planificación
10.2.1. De la idea al proyecto
10.2.2. Desarrollo del acta de proyecto
10.2.3. Reunión de arranque del proyecto
10.2.4. Tareas, conocimientos y habilidades en el proceso de inicio
10.2.5. El plan de proyecto
10.2.6. Desarrollo del plan básico. Pasos
10.2.7. Tareas, conocimientos y habilidades en el proceso de planificación

10.3. La gestión de los *Stakeholders* y del alcance
- 10.3.1. Identificar a los interesados
- 10.3.2. Desarrollar el plan para la gestión de los interesados
- 10.3.3. Gestionar el compromiso de los interesados
- 10.3.4. Controlar el compromiso de los interesados
- 10.3.5. El objetivo del proyecto
- 10.3.6. La gestión del alcance y su plan
- 10.3.7. Recopilar los requisitos
- 10.3.8. Definir el enunciado del alcance
- 10.3.9. Crear la WBS (EDT)
- 10.3.10. Verificar y controlar el alcance

10.4. El desarrollo del cronograma
- 10.4.1. La gestión del tiempo y su plan
- 10.4.2. Definir las actividades
- 10.4.3. Establecimiento de la secuencia de las actividades
- 10.4.4. Estimación de recursos de las actividades
- 10.4.5. Estimación de la duración de las actividades
- 10.4.6. Desarrollo del cronograma y cálculo del camino crítico
- 10.4.7. Control del cronograma

10.5. El desarrollo del presupuesto y la respuesta a los riesgos
- 10.5.1. Estimar los costes
- 10.5.2. Desarrollar el presupuesto y la curva S
- 10.5.3. Control de costes y método del valor ganado
- 10.5.4. Los conceptos de riesgo
- 10.5.5. Cómo hacer un análisis de riesgos
- 10.5.6. El desarrollo del plan de respuesta



10.6. La gestión de la calidad
- 10.6.1. Planificación de la calidad
- 10.6.2. Aseguramiento de la calidad
- 10.6.3. Control de la calidad
- 10.6.4. Conceptos estadísticos básicos
- 10.6.5. Herramientas de la gestión de la calidad

10.7. La comunicación y los recursos humanos
- 10.7.1. Planificar la gestión de las comunicaciones
- 10.7.2. Análisis de requisitos de comunicaciones
- 10.7.3. Tecnología de las comunicaciones
- 10.7.4. Modelos de comunicación
- 10.7.5. Métodos de comunicación
- 10.7.6. Plan de gestión de las comunicaciones
- 10.7.7. Gestionar las comunicaciones
- 10.7.8. La gestión de los recursos humanos
- 10.7.9. Principales actores y sus roles en los proyectos
- 10.7.10. Tipos de organizaciones
- 10.7.11. Organización del proyecto
- 10.7.12. El equipo de trabajo

10.8. El aprovisionamiento
- 10.8.1. El proceso de adquisiciones
- 10.8.2. Planificación
- 10.8.3. Búsqueda de suministradores y solicitud de ofertas
- 10.8.4. Adjudicación del contrato
- 10.8.5. Administración del contrato
- 10.8.6. Los contratos
- 10.8.7. Tipos de contratos
- 10.8.8. Negociación del contrato

10.9. Ejecución, monitorización y control y cierre
- 10.9.1. Los grupos de procesos
- 10.9.2. La ejecución del proyecto
- 10.9.3. La monitorización y control del proyecto
- 10.9.4. El cierre del proyecto

10.10. Responsabilidad profesional
- 10.10.1. Responsabilidad profesional
- 10.10.2. Características de la responsabilidad social y profesional
- 10.10.3. Código deontológico del líder de proyectos
- 10.10.4. Responsabilidad vs. PMP®
- 10.10.5. Ejemplos de responsabilidad
- 10.10.6. Beneficios de la profesionalización

Un proceso de crecimiento profesional y personal que se convertirá en un impulso de enorme calidad para tu competitividad”

05

Metodología

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

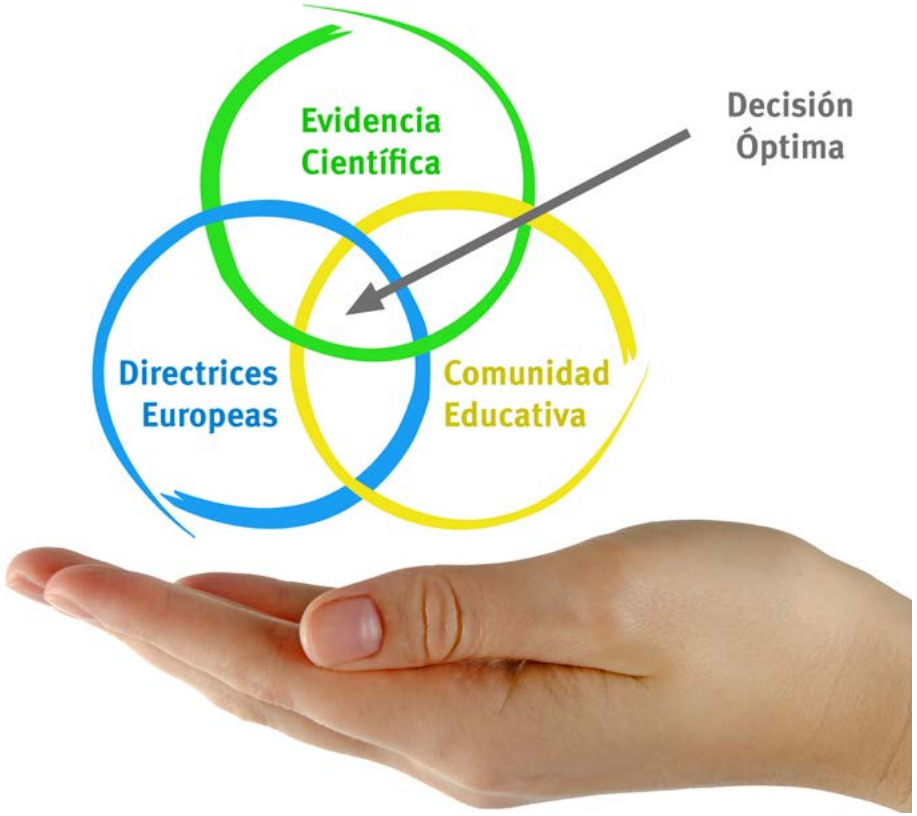
Este sistema de enseñanza es utilizado, por ejemplo, en las facultades de medicina más prestigiosas del mundo y se ha considerado uno de los más eficaces por publicaciones de gran relevancia como el ***New England Journal of Medicine.***

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

Estudio de Caso para contextualizar todo el contenido

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

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



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

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

Un método de aprendizaje innovador y diferente

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

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

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

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

Relearning Methodology

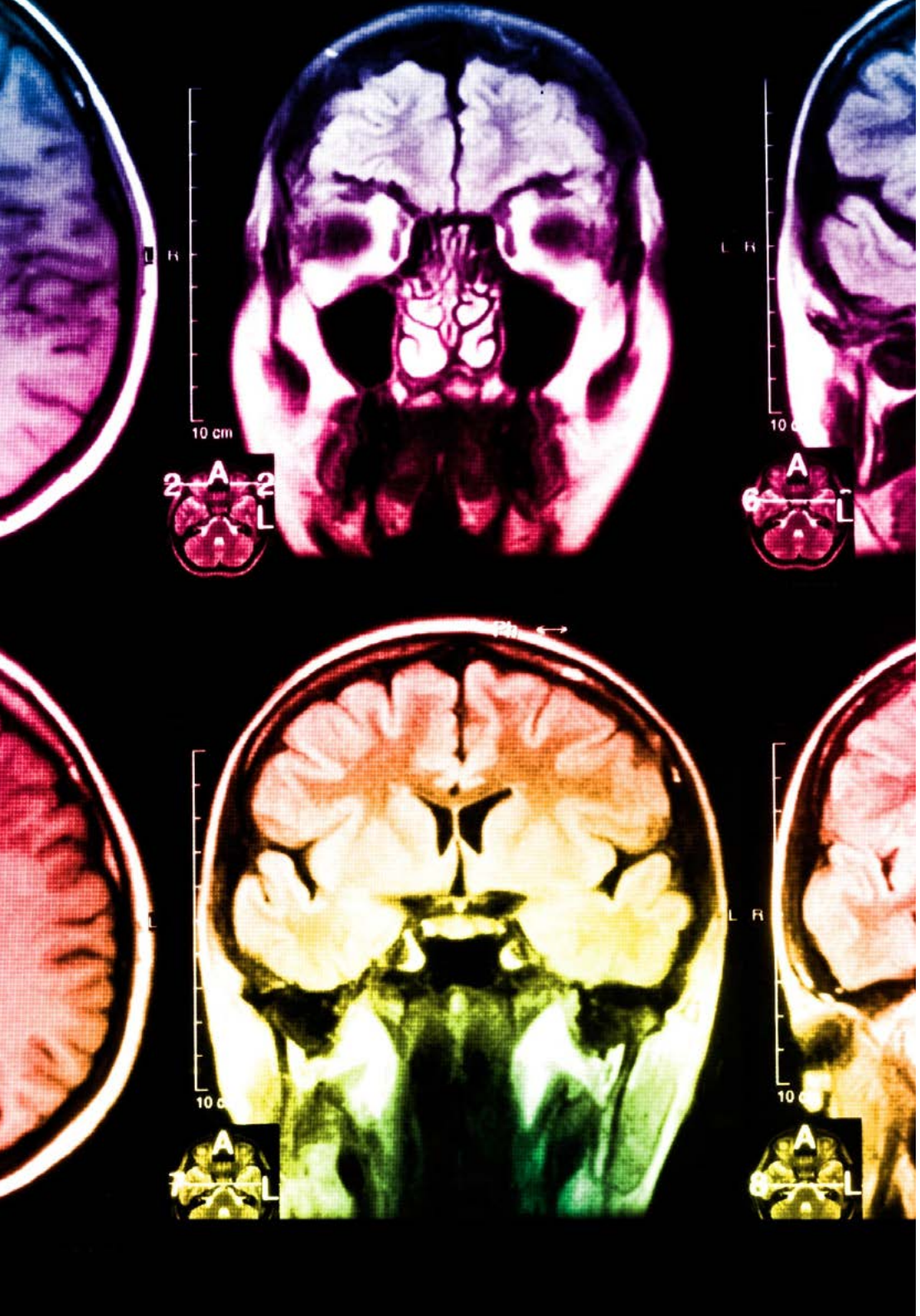
TECH aúna de forma eficaz la metodología del Estudio de Caso con un sistema de aprendizaje 100% online basado en la reiteración, que combina elementos didácticos diferentes en cada lección.

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

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

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

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



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

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

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

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

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

Material de estudio

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

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

Clases magistrales

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

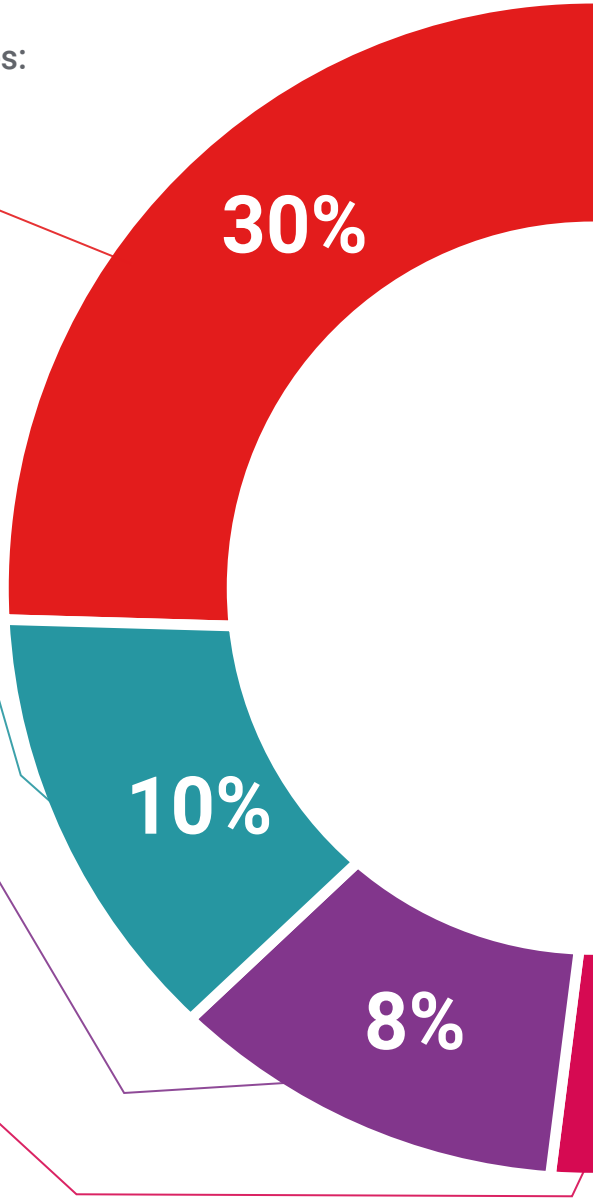
El denominado Learning from an Expert afianza el conocimiento y el recuerdo, y genera seguridad en las futuras decisiones difíciles.

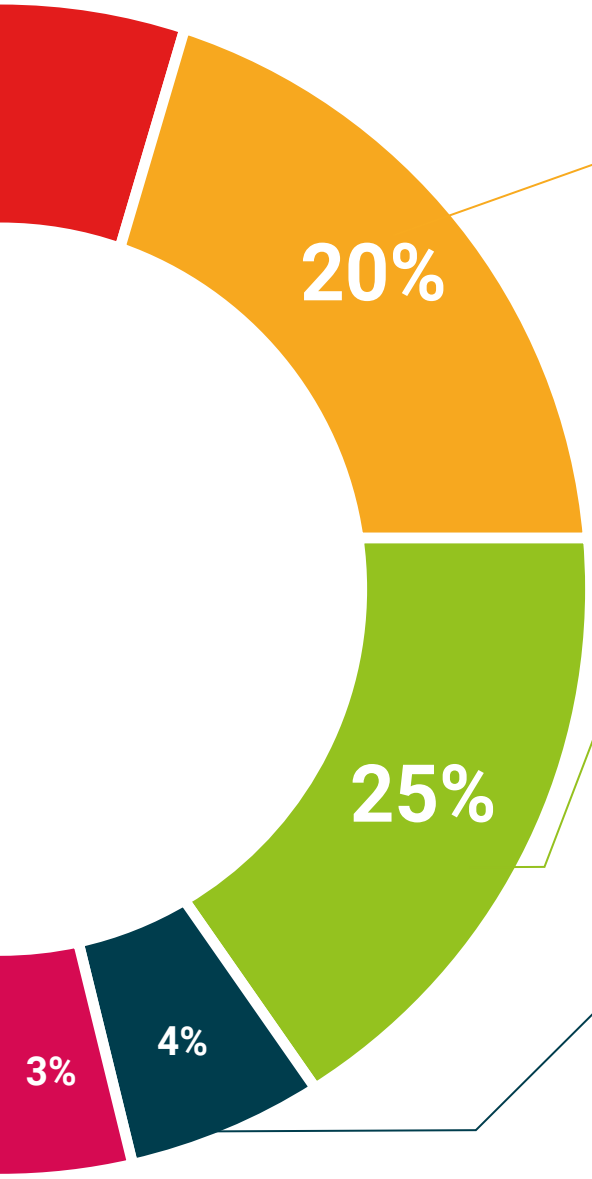
Prácticas de habilidades y competencias

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

Lecturas complementarias

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





Case studies

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

Resúmenes interactivos

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

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

Testing & Retesting

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

06

Titulación

El Máster Título propio en Telemática garantiza, además de la capacitación más rigurosa y actualizada, el acceso a un título de máster Propio expedido por TECH Universidad Tecnológica.

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

Esta **Máster Título Propio en Telemática** contiene el programa más completo y actualizado del mercado.

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

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

Título: **Máster Título Propio en Telemática**

N.º horas Oficiales: **1.500 h.**


tech universidad tecnológica

Otorga la presente

CONSTANCIA

a

C. _____, con documento de identificación nº_____

Por haber superado con éxito y acreditado el programa de

MÁSTER TÍTULO PROPIO

en

Telemática

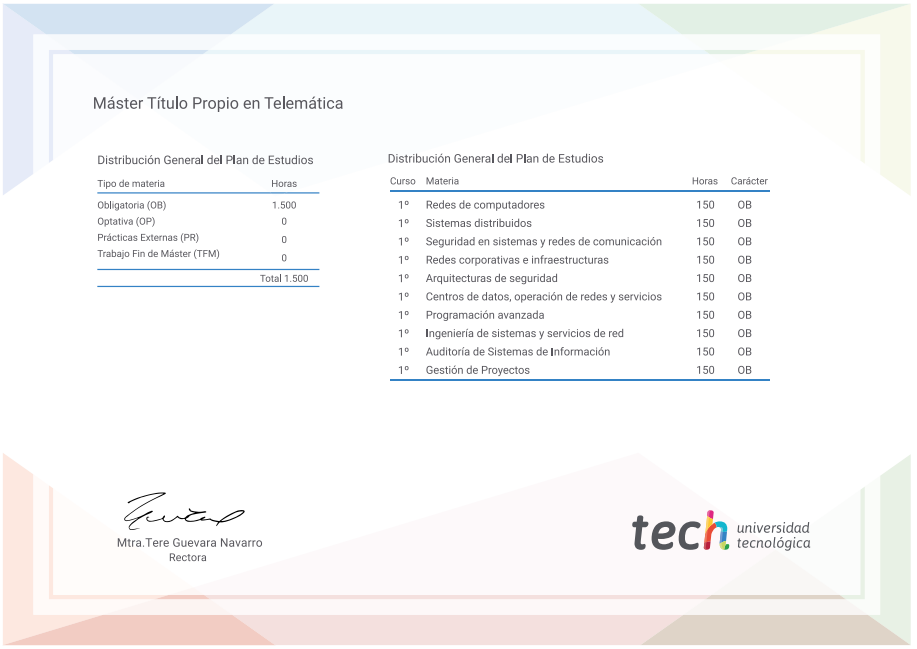
Se trata de un título propio de esta Universidad con una duración de 1.500 horas, con fecha de inicio dd/mm/aaaa y fecha de finalización dd/mm/aaaa.

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

A 17 de junio de 2020

Mtra.Tere Guevara Navarro
Rectora

código único TECH: AFWOR23S techtitute.com/titulos


Máster Título Propio en Telemática

Distribución General del Plan de Estudios

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

Distribución General del Plan de Estudios

Curso	Materia	Horas	Carácter
1º	Redes de computadores	150	OB
1º	Sistemas distribuidos	150	OB
1º	Seguridad en sistemas y redes de comunicación	150	OB
1º	Redes corporativas e infraestructuras	150	OB
1º	Arquitecturas de seguridad	150	OB
1º	Centros de datos, operación de redes y servicios	150	OB
1º	Programación avanzada	150	OB
1º	Ingeniería de sistemas y servicios de red	150	OB
1º	Auditoría de Sistemas de Información	150	OB
1º	Gestión de Proyectos	150	OB

Mtra.Tere Guevara Navarro
Rectora

tech universidad tecnológica

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

tech universidad tecnológica

Máster Título Propio

Telemática

- Modalidad: **online**
- Duración: **12 meses**
- Titulación: **TECH Universidad Tecnológica**
- Horario: **a tu ritmo**
- Exámenes: **online**

Máster Título Propio
Telemática

tech universidad tecnológica