
CATÁLOGO DE CURSOS



Las actualizaciones de este Catálogo están disponibles en:

www.LMdata.es/2017catLM.pdf

En sus 27 años de actividad continua, L&M Data Communications ha ido creciendo a la par que el mercado de las Tecnologías de la Información, las Comunicaciones y la Energía (TICE), gracias a su labor de investigación y asimilación de este entorno cambiante.

Actualmente nuestra empresa dispone de la oferta de cursos **más amplia en el mercado mundial de la formación** en las TICE, tanto por la extensión de los contenidos, como por la profundidad y el enfoque práctico con que son tratados. Hasta hoy llevamos impartidos, con gran éxito, más de **1.900 cursos a 25.000 profesionales**.

Nuestras señas de identidad son las siguientes:

• Profesionalidad y Experiencia

Todos los ponentes son profesionales de reconocido prestigio en el sector de las Comunicaciones de Datos, con gran capacidad pedagógica y experiencia profesional, que **imparten los cursos de los que son autores**. No ofrecemos cursos “enlatados” creados en otros países, que en la mayoría de los casos no describen nuestro entorno.

La formación se imparte íntegramente en español y se acompaña de una valiosa y completa documentación cuidadosamente revisada y actualizada, aportando a los asistentes los conocimientos necesarios para resolver los problemas reales que se presenten en su trabajo.

• Calidad

El control exhaustivo y constante de todos los cursos, la **preparación de los ponentes** y la adaptación de los temarios a nuestra realidad tecnológica, económica y de servicios, son nuestros **objetivos prioritarios**. La opinión de los asistentes, recogida a lo largo de todos los años en que venimos desarrollando nuestra actividad, indica el alto nivel de calidad que ofrece nuestra formación.

Los resultados de las últimas 3.000 encuestas, nos muestran los siguientes datos relevantes:

- **Ponentes: 8,8** (Valoración sobre 10)
- **Casos prácticos: 8,4** (Valoración sobre 10)
- **Fidelidad: 94,5%** (% empresas que repiten cursos con nosotros)
- **Recomendación: 99,8%** (% alumnos que recomiendan nuestros cursos)

• Rigor e Independencia

L&M Data Communications es la **única** empresa española que se dedica **exclusivamente** a la formación y asesoría en las TICs, con el objetivo de que los profesionales consigan implantarlas y mantenerlas con calidad y eficiencia.

El objeto de la empresa es exclusivamente la formación y la asesoría de alto nivel y no comercializa hardware ni software de ningún tipo, por ello está **desligada de intereses comerciales de productos o servicios**.

La formación impartida sigue criterios puramente técnicos y de mercado, como únicos condicionantes los derivados de la práctica y la experiencia profesional. Con ello se garantiza a los asistentes un conocimiento veraz y realista de estas técnicas, sin interferencias ni posicionamientos partidistas.

**Toda la información actualizada sobre nuestros
cursos, convocatorias y publicaciones en:**

www.LMdata.es

REDES Y EQUIPOS DE COMUNICACIONES	5
CURSO PRESENCIAL REDES DE DATOS Y EQUIPOS DE COMUNICACIONES	6
CURSO ON LINE REDES Y EQUIPOS DE COMUNICACIONES	7
INFRAESTRUCTURAS DE COMUNICACIONES	10
VOIP Y TELEFONÍA IP - SIP	11
IPV6: PARA CUÁNDO EL DÍA “D” ¿ESTÁ PREPARADA NUESTRA EMPRESA?	12
IPV6 CURSO PRÁCTICO	13
PROTOCOLOS DE TELECONTROL IEC 101/104 ANÁLISIS Y TROUBLESHOOTING.....	14
EL NUEVO ENTORNO DE CABLEADO EN COBRE Y FIBRA	15
SISTEMAS E INFRAESTRUCTURAS LAN DE FIBRA ÓPTICA.....	16
REDES ÓPTICAS Y DE TRANSPORTE	17
INTERNETWORKING EN TCP/IP Y ETHERNET	18
REDES MÓVILES LTE Y WI-FI DE NUEVA GENERACIÓN	19
SEGURIDAD EN REDES IP	20
ATAQUES EN REDES TCP/IP TÉCNICAS ANTI-HACKING EN COMUNICACIONES.....	21
SISTEMAS FIREWALLS	22
SISTEMAS Y PROTOCOLOS DE AUTENTICACIÓN EN TCP/IP	22
CERTIFICACIÓN DIGITAL Y TARJETAS INTELIGENTES	23
SEGURIDAD EN SISTEMAS TCP/IP	25
ATAQUES Y EXPLOITS EN LAS APLICACIONES TCP/IP	26
INDICADORES Y MÉTRICAS: CUADRO DE MANDOS DE SEGURIDAD	27
CONTINUIDAD Y PLANES DE CONTINGENCIA.....	28
ANÁLISIS Y GESTIÓN DE REDES	29
TROUBLESHOOTING Y SEGURIDAD EN IPV6 CURSO PRÁCTICO	30
WIRESHARK V.2: ANÁLISIS DE PROTOCOLOS Y REDES	31
WIRESHARK V.2: DETECCIÓN DE ATAQUES EN RED.....	32
SNMP: GESTIÓN Y SUPERVISIÓN DE SISTEMAS Y REDES	33
METODOLOGÍA DE GESTIÓN DE REDES. BUENAS PRÁCTICAS	34
ANÁLISIS DE PRESTACIONES Y SEGURIDAD DE REDES”	35
OTROS CURSOS DISPONIBLES	36
MPLS Y MPLS-TP	37
ROUTING EN REDES IP (v4/v6): RIP, IS-IS, OSPF, EIGRP, BGP	38
REDES DE ALMACENAMIENTO: SAN/NAS/DAS.....	39
IMS: CONVERGENCIA MULTIMEDIA EN REDES FIJAS Y MÓVILES	40
CLOUD COMPUTING: VIRTUALIZACIÓN EN LA “NUBE”	41
CÓMO IMPLANTAR SERVICIOS EN CLOUD ASPECTOS TECNOLÓGICOS, LEGALES Y DE NEGOCIO.....	42
EXPERTO EN EVIDENCIAS ELECTRÓNICAS	43
DESARROLLO DE APLICACIONES MÓVILES CON HTML5 CURSO PRÁCTICO	44
FIBRE CHANNEL	45
ULTRA HIGH PERFORMANCE INTERNET APPLICATIONS.....	46
REGULACIÓN Y SERVICIOS DE LAS TELECOMUNICACIONES EN ESPAÑA	47
OPTIMIZACIÓN DE SERVIDORES, VIRTUALIZACIÓN Y COMUNICACIONES	48
CERTIFICADOS	49
CERTIFICADOS OFICIALES CCTT DE FLUKE	50
Formación “a Medida” e “in-Company”	51
Documentación de Cursos	52

NIVELES

Iniciación: Cursos que no requieren conocimientos previos sobre los temas tratados.

Básico: Cursos de dificultad baja. Están dirigidos a Profesionales con conocimientos generales de informática. Es recomendable tener experiencia en comunicaciones.

Medio: Cursos de dificultad media. Están dirigidos a Profesionales con experiencia previa en comunicaciones.

Avanzado: Cursos de dificultad alta. Están dirigidos a Profesionales con bastante experiencia en comunicaciones. Requiere tener conocimientos previos sobre la materia básica en la que se va a profundizar

Experto: Cursos de dificultad muy alta. Están dirigidos a Expertos en comunicaciones que deseen ampliar sus conocimientos sobre nuevas tecnologías altamente especializados

Evalúe su nivel en nuestra aula virtual: www.LMdata.es/aulav.htm

LA OFERTA DE MAYOR CALIDAD DEL MERCADO

Al valorarla, tenga en cuenta que:

- ❖ **Disponemos de la oferta más rigurosa y completa del mercado**
 - Nuestro conjunto de Programas y Cursos es único en el mundo
 - En total disponemos de más de 700 horas de formación totalmente actualizados, de alto nivel en Comunicaciones de Datos (33 Cursos, 6 Áreas de formación específica y formación “online”).
- ❖ **Nuestros Ponentes son profesionales del máximo nivel, con amplia experiencia práctica (de 10 a 30 años) y autores de los cursos que explican.**
 - No tenemos profesores desconocidos, que “leen” transparencias de cursos “enlatados”
 - No tenemos traducciones de cursos, hechos en otros lugares y en otros idiomas, que describen un contexto que no es el nuestro.
 - Ofrecemos **exclusivamente** formación **independiente** de **alto nivel** y **calidad**
- ❖ **Tratamos sobre tecnologías, no sobre productos concretos, con total independencia de criterios, basados exclusivamente en la experiencia práctica**
 - Nuestros cursos no son un acumulo de presentaciones inconexas, ni damos información tendenciosa o parcial, pues somos una empresa autónoma y desligada de intereses comerciales relacionados con productos o servicios
 - El valor que diferencia nuestra formación reside en las experiencias y opiniones de los ponentes de nuestros cursos, que enriquecen la enseñanza impartida con sus conocimientos adquiridos a lo largo de los años
- ❖ **El interés que nos mueve es ofrecer la máxima calidad y el mejor servicio para usted y su organización, pues nuestro activo son los clientes satisfechos que asisten asiduamente a nuestros cursos**
 - Hoy en día es prácticamente imposible disponer de instructores, como es nuestro caso, con más de treinta años de experiencia real y dedicación continua a las comunicaciones y redes de datos

REDES Y EQUIPOS DE COMUNICACIONES

Curso "online"

OBJETIVOS:

- Ofrecer una sólida base y una amplia panorámica del estado del arte y situación real del entorno de las Comunicaciones de Datos y las Telecomunicaciones, presentando los conceptos necesarios y suficientes, de modo práctico y realista, para desarrollar de forma estructurada los conocimientos fundamentales que permiten construir sólidos sistemas de comunicaciones.
- "Refrescar" y "readquirir" informaciones "ya sabidas" para aclarar, ampliar y corregir conceptos "viciados" y descubrir los misterios que se ocultan detrás de los enrevesados tecnicismos, acrónimos y argot empleados en estas técnicas.

DURACIÓN:

La duración de este curso es de 66 horas a desarrollar en un máximo de tres meses. Recomendamos realizar el curso en un plazo no inferior a dos meses.

DIRIGIDO A:

- Todos aquellos que necesiten iniciarse en las Comunicaciones de Datos o asentar y aclarar conocimientos previos
- Directores de Informática y Ejecutivos con responsabilidad en la adquisición de productos de comunicaciones
- Directores, Jefes y Responsables de Comunicaciones, Redes Locales y Microinformática
- Personal Técnico de Departamentos de Comunicaciones, Gestión de Red, Centros I+D y Universidad
- Suministradores de Servicios de Telecomunicaciones, Fabricantes, Distribuidores, Instaladores e Integradores
- Particulares que deseen potenciar su carrera profesional

DOCUMENTACIÓN:

Los asistentes recibirán la documentación del curso; y dependiendo de cada uno: manuales complementarios, cuadernos de prácticas y material adicional. También se facilitará una clave para el acceso a la **Enciclopedia Virtual**, en la que información complementaria de este Area.

CURSO PRESENCIAL REDES DE DATOS Y EQUIPOS DE COMUNICACIONES

Nivel: INICIACIÓN - Duración: 2 días - Curso: Presencial

Este curso proporciona la base para entender las actuales tecnologías de comunicaciones, aportando una amplia visión del entorno de redes y equipos de comunicaciones. Los conocimientos adquiridos son fundamentales para poder profundizar en esta área. “Refrescar” y “Readquirir” informaciones “ya sabidas” para aclarar, ampliar y corregir conceptos “viciados” y descubrir que ocultan los enrevesados tecnicismos, acrónimos y argot empleados en Telecomunicaciones.

1. ARQUITECTURA DE LAS COMUNICACIONES

Organismos de Normalización
Arquitecturas y Modelo de Referencia
Arquitectura Genérica
Niveles, Servicios, Protocolos
Unidades de Datos, Mensajes

2. REDES DE DATOS: TÉCNICAS BÁSICAS

Transmisión y Conmutación
Circuitos Físicos, Virtuales y Datagramas
Servicios de Red en modo conectado
Sistemas en modo no-conectado
Bridging , Routing y Switching

3. EQUIPOS DE COMUNICACIONES

Repetidores y Bridges
Conmutación: Switches
Routers y Gateways

4. REDES LOCALES ETHERNET

Componentes Físicos y Lógicos
Formato de Tramas, Direcciones
Fast, Gigabit y 10G Ethernet
Topologías de Red y Prestaciones

5. ARQUITECTURA Y PROTOCOLO IP

Normalización: ISOC, IETF y RFCs
Elementos, protocolos y unidades de datos
Servicios de Red en Modo Datagrama IP
Servicios de Transporte TCP y UDP
Interfaces de programación y sockets
Datagramas y Protocolo IP
Protocolos auxiliares

ARP/RARP, ICMP
Direccionamiento IP
Direcciones de Broadcast y Red
Notación decimal de puntos
Direccionamiento público y privado
Direccionamiento de Subred
Representación de la máscara de subred
Asignación automática de direcciones
Protocolos: RARP, BOOTP, DHCP
Dispositivos NATS/NPATS
Servidores virtuales
Interconexión Internet -Intranet

6. PROTOCOLO TCP

Segmentos y Protocolo TCP
Conexiones, secuenciamiento, ACKs
Puertas y servicios
Redes TCP/IP: Operación
Control de error TCP
TCP Sliding Window
Mecanismos de aceptación

7. SERVICIOS Y APLICACIONES

DNS, Telnet, FTP, Correo Electrónico
Servidores proxy, Protocolo HTTP
Protocolos de Seguridad.

Objetivos: Dar a conocer los fundamentos de las redes y equipos basados en los protocolos TCP/IP de Internet.

Prerrequisitos: No se requieren conocimientos previos.

Metodología: Teórico con prácticas de Traces.

CURSO ON LINE

REDES Y EQUIPOS DE COMUNICACIONES

Nivel: BÁSICO/MEDIO - Duración: 66 horas lectivas - Curso: On-Line

Programa ampliado de Formación "on-line" del curso Redes y Equipos. El contenido del curso está dividido en 4 módulos, compuestos por lecciones independientes, con un test de evaluación al finalizar cada módulo.

MÓDULO 1 – LECCIÓN 1

ORGANISMOS DE NORMALIZACIÓN

- Organismos Internacionales
- Normativa IEEE 802
- Normativa IETF: RFCs (Request For Comments)

ARQUITECTURA DE COMUNICACIONES

- Servicios de Telecomunicaciones
- Modelo de Referencia Genérico
- Velocidad de Propagación y de Transmisión
- S. I. de unidades: Prefijos Normalizados
- Arquitectura y Modelo de Referencia de Internet IP
- Del ordenador de usuario al router de acceso
- Conmutación y Encaminamiento en la Red

MÓDULO 1 – LECCIÓN 2

NIVELES, SERVICIOS Y PROTOCOLOS

- Arquitectura Estratificada en Niveles
- Servicios y Protocolos. Primitivas de Servicio
- SAPs, SDUs y PDUs
- Delimitación de Protocolos (PDUs)
- Mensajes y Unidades de Datos de Protocolo

MODOS DE CONEXIÓN

- Topologías Básicas de Red
- Formas de Conexión

SEÑALES Y CÓDIGOS

- Códigos: Binario, Decimal y Hexadecimal
- Representación de los octetos
- Direccionamiento: Ethernet/MAC - IPv4 / IPv6

MÓDULO 1 – LECCIÓN 3

FIBRAS ÓPTICAS: CONCEPTO FUNDAMENTALES

- Estructura de la fibra óptica
- Multimodo (MMF) y Monomodo (SMF)
- Capacidades de la Fibra Óptica
- Espectro de Frecuencias y de pérdidas
- Las tres primeras ventanas
- Cobre y Fibra: Capacidad y Distancia

RED DE ACCESO DE FIBRA

- La fibra hasta la casa "FTTH"
- "FTTH" Pasiva y Activa
- Red de Acceso Óptica Pasiva: "PON"
- Red de Acceso Óptica Activa Ethernet "E-FTTH"

MULTIPLEXIÓN ÓPTICA (WDM)

- Multiplexión por División de Longitud de Onda
- WDM, CWDM & DWDM - ITU-T G.671
- CWDM vs DWDM

MÓDULO 1 – LECCIÓN 4

TÉCNICAS BÁSICAS DE CONMUTACIÓN

- Técnicas de Conmutación
- Estructura de la red de datos
- MODOS CONECTADO Y NO-CONECTADO
- Circuitos Físicos o Virtuales
- Multiplexión y Conmutación. Datagramas
- Router IP (v4/v6)

CONMUTACIÓN DE CIRCUITOS Y PAQUETES

- Circuitos vs Paquetes
- Conmutación de Circuitos Físicos
- Nodo de red de circuitos
- Conmutación y Nodo de red de paquetes

INTERCONEXIÓN DE SISTEMAS

- Normalización del "Internetworking": IEEE 802
- Interconexión con Repetidor. Bridge / Puente
- Normativa IEEE 802
- Switch de Nivel 2 (Bridge)
- Router Residencial / Pequeña Oficina

MÓDULO 2 – LECCIÓN 1

REDES LOCALES ETHERNET

- Componentes de la Red Local
- Comunicaciones en la Red Local
- Redes Locales Ethernet – Medios Físicos
- Bridge (802.1) con Interfaces Ethernet (802.3)
- Normalización de Ethernet

SISTEMAS DE CABLEADO ESTRUCTURADO

- Estándares de cableado: Cobre y Fibra
- Sistemas de Cableado Estructurado (SCE)
- SCE - Canal y Enlace
- Categorías ANSI/EIS/TIA para Cobre
- Clases ISO/IEC para Cobre
- Cobre: Conector de 8 contactos - RJ-45 / ISO 8877
- Ethernet – Conectorización
- Designación de Fibras Ópticas según ANSI e ISO
- Conectores de fibra
- Fibras Ópticas - Código de Colores
- Pérdidas en conexiones sucias

MÓDULO 2 – LECCIÓN 2

ETHERNET: TECNOLOGÍAS BÁSICAS

- ¿Qué es Ethernet?
- IEEE 802.3
- Medios Físicos ETH
- Progresión Tecnológica
- De 10 a 100.000 Mbps ... y más allá
- FORMATO DE TRAMAS Y DIRECCIONES
- Mensajes y Unidades de Datos de Protocolo
- Características de las Tramas Ethernet
- Trama Ethernet Completa (sin CRC)
- Direcciones Destino (DA) y Origen (SA)
- Tipo/Longitud
- Datos-Cabecero IP y TCP
- Relleno (Pad/Trailer)

MÓDULO 2 – LECCIÓN 3

ETHERNET: TOPOLOGIAS

- IEEE 802.3 10Base-T
- Dominio de Colisión
- Ethernet FDX (Full-Duplex)
- Ethernet Half Duplex vs Full Duplex
- ETHERNET: FAST, GIGA, Y 10 GIGABIT
- Ethernet / Fast Ethernet: 10/100BASE-T
- Cable 10/100Base-T
- Giga ETH (802.3z / 802.3ab)
- 10 Gigabit ETH / 1000BASE-T / 10GBASE-T
- Cable 1000BASE-T / 10GBASE-T

ETHERNET: PRESTACIONES

- Evolución y Velocidades
- Evaluación de Prestaciones Ethernet
- Máximo teórico de pps

MÓDULO 2 – LECCIÓN 4

EQUIPOS DE COMUNICACIONES

- Interconexión de Sistemas. Repetidores
- Repetidor (MPR) vs Conmutador (SWITCH)
- Puentes/Bridges: Normativa IEEE 802.1
- Características del "Bridging"
- Puente (Bridge) Clásico 802.1 D
- Switch (Bridge) con múltiples Interfaces Ethernet

ROUTERS IP

- ¿Qué son realmente un "Host" y un "Router"?
- Ejemplo Routers IP. Routing IP (v4/v6)
- Tablas de Encaminamiento o de "Routing"

(continuación programa curso "online")

MÓDULO 3 - LECCIÓN 1

ARQUITECTURA TCP/IP
 Normalización del TCP/IP
 IANA - IETF (RFC)
 Definiciones TCP/IP
 Elementos de una Internet
 Arquitectura INTERNET-TCP/IP
 Unidades de datos del protocolo (PDUs)
 Nivel de Red: IP
 Nivel de transporte: TCP/UDP
 Comunicaciones INTERNET
 Sockets: Interfaces de programación
 Aplicaciones INTERNET-TCP/IP
 PROTOCOLO IP: Arquitectura
 Nivel IP
 Cabecero IP
 Campos cabecero
 Algunas Opciones IP

MÓDULO 3 - LECCIÓN 2

PROTOCOLO IP
 Estructura del Direccionamiento IPv4
 Clases IP
 Fragmentación y Reensamblado Datagramas IP
 Fragmentación: Funcionamiento
 Ejemplo fragmentación datagrama
 Encaminamiento en IP
 Protocolo ARP
 Tipo de operación y tipo de hardware (IANA)
 Trace ARP: Pregunta y Respuesta

MÓDULO 3 - LECCIÓN 3

PROTOCOLO ICMP
 Algunos Mensajes ICMP
 Ejemplos ICMP
 Trace ICMP
 DIRECCIONAMIENTO IPv4
 Tipos de direcciones IP
 MultiHoming y Multicasting
 Subdireccionamiento
 Ejemplos de máscaras y subaddressing
 Toma de decisiones en el host

MÓDULO 3 - LECCIÓN 4

DISPOSITIVOS NATs/NPATs
 NATs - PATs – ALGs
 Tipos de NPATs
 Protocolo DHCP
 Funcionamiento del DHCP
 El IPv6
 Formato PDU IPv6
 Cabecero IPv6
 Arquitectura Direccionamiento IPv6
 Representación textual direcciones IPv6

MÓDULO 3 - LECCIÓN 5

Prefijos reservados IPv6
 Direcciones Locales IPv6
 Direcciones MAC IEEE 802 EUI-48 y EUI-64
 Identificación del Interface
 Direcciones especiales
 Cabeceros Opcionales
 Datagrama ICMPv6
 Procesos y Mecanismos de Autoconfiguración
 Autoconfiguración Stateless
 Mensajes ICMPv6
 Autoconfiguración Stateful
 Envío de datagramas
 Algoritmo básico de envío
 Resumen ICMPv6

MÓDULO 4 – LECCIÓN 1

PROTOCOLO TCP
 Fundamentos
 Nivel de Transporte Internet
 Servicios en Internet: TCP
 Elementos Conexión TCP/IP
 Protocolo y Servicios TCP
 Puertas, Direcciones y Conexiones
 Conceptos de la Arquitectura Internet
 PAQUETES TCP – UDP: FORMATO DE CABECERO
 Tramas ETH, Datagramas IP y Paquetes TCP
 Formato cabecero TCP
 Formato cabecero UDP

MÓDULO 4 – LECCIÓN 2

PROTOCOLO TCP: CONEXIONES A TRAVÉS DE LA RED
 Apertura no simétrica "Three Way Handshaking"
 Diagrama de Estados del TCP
 Establecimiento de Conexión TCP
 Necesidad del Transporte Fiable
 Control Error TCP/IP
 Transferencia de Datos TCP
 "Ventana Deslizante" (Sliding Window)
 Finalización de conexión TCP

MÓDULO 4 – LECCIÓN 3

INTERNET - TCP/IP
 Nombres en Internet: DNS
 El espacio de nombres de dominio DNS
 DNS: Proceso de Resolución
 La Consulta DNS
 Formato del mensaje DNS
 Aplicaciones: TELNET, FTP
 FTP: File Transfer Protocol
 FTP: Comandos y Respuestas
 Aplicaciones: E-mail: correo electrónico
 Protocolos y Estándares correo TCP/IP
 POP3: Post office protocol (RFC 1939)
 WWW "La telaraña"
 Elementos WWW
 Ejemplo conexión Web
 Servidor PROXY
 HTTP (Hypertext Transfer Protocol)
 HTTP (Petición y Respuestas)
 Protocolos de seguridad en TCP/IP

Objetivos:

- Proporcionar la base para entender las actuales tecnologías de comunicaciones.
- Aportar una amplia visión del entorno de redes y equipos de comunicaciones. Los conocimientos adquiridos son fundamentales para poder profundizar en esta área.

Material Didáctico:

- El material didactico se compone de la documentación de cada módulo en formato electrónico, para que pueda seguir las lecciones multimedia "on line" y un libro sobre Redes de Comunicaciones, Protocolos TCP/IP e Internet, que sirve como material de estudio complementario.

Test de Evaluación:

- El curso tiene 4 test de cualificación "on-line", a realizar después de cada módulo.

Cuestionario de Evaluación:

- Cuando finalice todo el curso, por favor, rellene el cuestionario de evaluación, accesible a través del enlace localizado en la parte inferior de la página de contenidos del curso.

Duración:

- La duración de este curso es de 66 horas a desarrollar en un máximo de tres meses. Recomendamos realizar el curso en un plazo no inferior a dos meses.

Programa de Actividades

- A continuación ofrecemos la planificación orientativa para una duración del curso "on-line" de 9 semanas, con los tiempos estimados de cada actividad a realizar.

Primera Semana <i>Manejo plataforma (1 h.)</i> <i>Módulo 1 – lecciones 1 y 2 (5 h.)</i> <i>Estudio libro – capítulos 1 y 2 (1 h.)</i> <i>TOTAL Semana 7 horas</i>	Sexta Semana <i>Repaso módulo 3 – lección 1 y 2 (1 h.)</i> <i>Módulo 3 – lección 3 y 4 (6 h.)</i> <i>Estudio libro – capítulos 7 y 8 (1 h.)</i> <i>TOTAL Semana 8 horas</i>
Segunda Semana <i>Módulo 1 – lecciones 3 y 4 (5 h.)</i> <i>Repaso módulo 1 (1 h.)</i> <i>Test módulo 1 (1 h.)</i> <i>TOTAL Semana 7 horas</i>	Séptima Semana <i>Módulo 3 – lección 5 (3 h.)</i> <i>Repaso módulo 3 completo (2 h.)</i> <i>Revisión consultas módulo 3 (1 h.)</i> <i>Test módulo 3(1 h.)</i> <i>TOTAL Semana 7 horas</i>
Tercera Semana <i>Módulo 2 – lecciones 1 y 2 (5 h.)</i> <i>Revisión consultas módulo 1 (1 h.)</i> <i>Estudio libro – capítulos 3 y 4 (1 h.)</i> <i>TOTAL Semana 7 horas</i>	Octava Semana <i>Módulo 4 – lección 1 y 2 (6 h.)</i> <i>Estudio libro – capítulo 9 y 10 (1 h.)</i> <i>TOTAL Semana 7 horas</i>
Cuarta Semana <i>Módulo 2 – lecciones 3 y 4 (5 h.)</i> <i>Repaso módulo 1 y 2 (2 h.)</i> <i>Test módulo 2 (1 h.)</i> <i>TOTAL Semana 8 horas</i>	Novena Semana <i>Módulo 4 – lecciones 3 (3 h.)</i> <i>Repaso módulo 4 (1 h.)</i> <i>Lectura libro – capítulos 11 al final (1 h.)</i> <i>Revisión consultas módulo 4 (1h.)</i> <i>Test módulo 4 (1 h.)</i> <i>TOTAL Semana 7 horas</i>
Quinta Semana <i>Módulo 3 – lección 1 y 2 (6 h.)</i> <i>Lectura libro – capítulos 5 y 6 (1 h.)</i> <i>Revisión consultas módulo 2 (1 h.)</i> <i>TOTAL Semana 8 horas</i>	TOTAL CURSO 66 Horas

INFRAESTRUCTURAS DE COMUNICACIONES

OBJETIVOS:

- Cubrir los aspectos estratégicos y comerciales que le ayudarán en la toma de decisiones para la implantación de sistemas VoIP.
- Ofrecer una amplia panorámica de las tecnologías y estándares que actualmente se están aplicando para el Smart Grid, desarrollando, en un solo día, los protocolos de telecontrol utilizados en los sistemas eléctricos.
- Cómo implantar, mantener y optimizar las actuales infraestructuras de comunicaciones. Para ello se desarrollan aspectos que cubren desde los Sistemas de Cableado Estructurado en Cobre y Fibra, incluyendo la certificación de este tipo de instalaciones, hasta la electrónica de red empleada (switches y routers)
- Además se estudiará la nueva generación de redes de acceso basada en Ethernet (NEBA) y el nuevo IPv6.

DURACIÓN Y HORARIO:

Los cursos que están integrados en esta Área tienen una duración de uno, dos o tres días. Con horario de 9:30 a 15:00 horas

DIRIGIDO A:

- Todos aquellos que necesiten iniciarse en las Comunicaciones de Datos o asentar y aclarar conocimientos previos
- Directores de Informática y Ejecutivos con responsabilidad en la adquisición de productos de comunicaciones
- Directores, Jefes y Responsables de Comunicaciones, Redes Locales y Microinformática
- Personal Técnico de Departamentos de Comunicaciones, Gestión de Red, Centros I+D y Universidad
- Suministradores de Servicios de Telecomunicaciones, Fabricantes, Distribuidores, Instaladores e Integradores
- Particulares que deseen potenciar su carrera profesional

METODOLOGÍA:

Estos Cursos se imparten independientemente, siguiendo un orden lógico, espaciados en el tiempo con objeto de que las personas que desean asistir a varios cursos maduren los conocimientos adquiridos, de manera que puedan aclararse las dudas antes de iniciar la etapa siguiente. Para ello será posible consultar todas las dudas que surjan a través de Internet con el e-mail que se habilitará a tal efecto. La Metodología de estos cursos está basada en:

- Adquirir conocimientos teóricos, mediante el desarrollo de las sesiones impartidas
- Adquirir conocimientos prácticos, mediante el estudio de casos y pruebas de laboratorio

DOCUMENTACIÓN:

Los asistentes recibirán la documentación del curso; y dependiendo de cada uno: manuales complementarios, cuadernos de prácticas y material adicional. También se facilitará una clave para el acceso a la **Enciclopedia Virtual**, en la que información complementaria de este Área.

VOIP Y TELEFONÍA IP - SIP

Nivel: ALTO - Duración: 2 días

La tecnología VoIP integra gran cantidad de elementos, protocolos y arquitecturas de comunicaciones. Este curso muestra de forma ordenada, clara y rigurosa, todo lo necesario para entender este complejo entorno.

1. SEÑALIZACIÓN, CODIFICACIÓN Y DIGITALIZACIÓN

Tipos, Estandarización
Factores que afectan a la Calidad

2. CONCEPTOS FUNDAMENTALES VoIP

Funcionamiento VoIP
Encapsulados sobre IP
Señalización

3. PLANIFICACIÓN DE REDES VoIP

Integración Voz/Datos/Imagen
Modos de la telefonía IP
Técnicas de integración
Grado de servicio
Modelos de tráfico

4. DISEÑO E IMPLANTACIÓN

Requerimientos
Análisis económico y de capacidad
Características del transporte
Parámetros del servicio
Gestión de la voz

5. ARQUITECTURA SIP DEL IETF

Componentes Funcionales
Elementos de la Arquitectura
Sintaxis, SIP
Registros SRV y NAPTR
Servidores SIP
Procesos, Funcionamiento y Ejemplos

6. PROCESOS Y MENSAJES SIP

Visión General
Estructura de los Mensajes
Cabeceros SIP
Limitaciones de los Servidores Stateless
Registration Stateful Servers
El SDP

NAT Traversal
PATs o NPATS clásicas
NAT hairpinning
IETF: STUN, TURN, ICE
Análisis con WireShark

7. SERVICIOS Y APLICACIONES SIP

Capacidades de la movilidad SIP
Registros remotos y multietapa
Macro y micro movilidad
Posibilidades del SIP
QoS, Seguridad, Autenticación
Mensajería Instantánea, Presencia
Notificación de Eventos Aplicaciones
Media servers
Análisis de una llamada
Paso a través de NATs
Utilización de servidores STUN
Resolución de problemas

8. SEGURIDAD EN SIP

Orígenes de la Inseguridad
Contra medidas
Ejemplos de Ataques
S/MIME en SIP, SAML
Seguridad en los Streams
Validación de entrada
Análisis de Vulnerabilidades y Herramientas
Firewalling y NATs con SIP

Objetivos: Permite conocer cómo acometer sin sobresaltos un proyecto de integración VoIP. Para ello se analizan los protocolos que se utilizan en las redes VoIP, tanto fijas como móviles.

Prerrequisitos: Conocimientos del protocolo TCP/IP y de Seguridad en Redes y Sistemas.

Metodología: Teórico (90%) – Práctico (10%)..

IPV6: PARA CUÁNDO EL DÍA “D” ¿ESTÁ PREPARADA NUESTRA EMPRESA?

Nivel: BÁSICO - Duración: 1 día

Desde el lanzamiento a nivel mundial del nuevo protocolo de red IPv6, el día 6 de junio de 2012, muchos profesionales del sector de las Tecnologías de la Información y las Comunicaciones tienen la falsa percepción de que se ha hecho muy poco en el desarrollo y despliegue del IPv6. Curiosamente esto es rigurosamente cierto si observamos lo que está pasando en nuestro país, y completamente falso si nos fijamos a nivel mundial, sobre todo en países fuertemente desarrollados.

Para arrojar un poco de luz en estos temas, hemos desarrollado un curso donde trataremos los siguientes puntos:

El IPv6: ¿Qué es? ¿Qué ventajas aporta?

¿Dónde impacta el IPv6?

Implicaciones en los Sistemas de Información y Comunicaciones de la Empresa

Estado actual y despliegue del IPv6 en el mundo

¿Cuándo alcanzará el IPv6 la masa crítica para que el IPv4 pase a ser el protocolo “legacy”?

Últimos análisis y estudios sobre la penetración del IPv6 en el mercado de las TICs

¿Por qué durante el 2016, se ha duplicado el tráfico IPv6?

Redes móviles solo IPv6

Movimientos en los grandes “App stores” hacia aplicaciones IPv6

¿Qué pasa si mi App no soporta IPv6? ¿Funcionará?

¿Por qué ha crecido tanto el despliegue del IPv6 en EE.UU.?

Situación en España ¿Es posible mantenerse indefinidamente en IPv4?

¿Qué riesgos y consecuencias estamos asumiendo? ¿Qué alternativas reales existen?

No hacer nada ¿Es una alternativa o una fuente de problemas futuros?

¿Qué debemos hacer? Implantación gradual de IPv6

IPv6

CURSO PRÁCTICO

Nivel: AVANZADO - Duración: 2 días

Aporta una visión completa y detallada de la arquitectura y el protocolo IPv6. Desarrolla la planificación necesaria para la correcta transición y coexistencia con el IPv4, revisando en profundidad todos los mecanismos que se pueden utilizar, indicando donde aplicar cada uno de ellos.

1. ARQUITECTURA y PROTOCOLO IPv6

- Componentes, Formato y Características IPv6
- Cabecero y direccionamiento IPv6
- Arquitectura direccionamiento IPv6
- Representación textual, sintaxis correcta
 - Esquemas de direcciones IPv6
 - IPv4 embebida en IPv6
 - Política de asignación direcciones IPv6
 - Direcciones locales IPv6
 - Direcciones MAC IEEE 802 EUI-48 y EUI-64
- Multicast N3 - N2 (IPv6)
- Opciones
 - Hop-by-Hop, Fragmentación, Routing
 - Seguridad y Autenticación, Movilidad
 - Destination
 - Orden de las opciones
- Protocolo ICMPv6
 - Procesos de autoconfiguración
 - Configuración direcciones
 - Mecanismos de autoconfiguración
 - Autoconfiguración stateless y stateful
 - Mensajes ICMPv6 (routers)
 - Respuesta/anuncio router ICMPv6
 - Protocolo NDP
 - Dialogo con los routers, Envío de datagramas
 - Solicitud/respuesta vecinos ICMPv6
- Multicast N3 - N2
- Multihoming IPv6
 - Shim6 - site multihoming
 - Arquitectura multihoming hosts
- Impacto sobre otros protocolos

2. TRANSICIÓN Y COEXISTENCIA IPv4 - IPv6

- Problemática general del IPv6
- Estado actual de la coexistencia IPv4 - IPv6
- Planificación de la transición
- Fases previstas durante la transición
- Estrategia de transición
 - Aspectos a considerar y Opciones
 - Qué es necesario hacer
- Impacto sobre las Aplicaciones, equipos, infraestructura
- Implicaciones del IPv6 en las aplicaciones
 - Aplicaciones Aware, Unaware, cliente, servidor, conectividad
- Efectos de la coexistencia
 - Seguridad, impacto sobre "la nube"
 - Interoperabilidad IPv6/IPv4

3. MECANISMOS DE TRANSICIÓN / COEXISTENCIA

- Soluciones iniciales
 - Dual stack y Técnicas de túnel
- Soluciones mejoradas
 - Traductores/conversores IPv4/IPv6
 - Direccionamiento IP6 en los traductores
 - Tunnel broker
 - 6to4: Arquitectura, Funcionamiento
 - Teredo: Flujos y Formatos
 - ISATAP
- Soluciones avanzadas
 - Transporte para ISPs
 - Túneles ISP (troncales)
 - 6PE, 6Vpe, Softwires Mesh
- Accesos para usuarios finales
 - 6rd, Hibridaciones: 6rd + CGNAT44
 - Coexistencia para los usuarios
 - Dual- stack lite (DS-LITE)
 - CGNAT, NAT64, NAT44
 - DNS64 + NAT64
- Soluciones "all IPv6"
- Dónde aplicar cada solución
- Mapa de ruta del IPv6

4. SEGURIDAD Y TROUBLESHOOTING EN EL IPv6

- Problemática de la seguridad en el IPv6
- Implicaciones de la seguridad durante la coexistencia
- Protocolo SEND
- Algunas formas de ataque y defensa
- Herramientas disponibles
- Troubleshooting en entornos IPv6 - IPv4

5. PRÁCTICAS (A lo largo del curso)

Desarrollo de múltiples prácticas utilizando equipos cliente, routers, firewalls, DNS, en distintos entornos.

Objetivos: Aportar una visión detallada y profunda de las redes IPv6, y los servicios de Red necesarios. Revisa en profundidad las diferentes técnicas de coexistencia con el IPv4 y dónde aplicar cada una de ellas.

Prerrequisitos: Conocimientos generales de TCP/IP

Metodología: Teórico (70%) – Práctico (30%)..

PROTOCOLOS DE TELECONTROL IEC 101/104

ANÁLISIS Y TROUBLESHOOTING

Nivel: MEDIO - Duración: 2 días

Amplia panorámica de las tecnologías y los estándares que actualmente se están aplicando en las Redes Eléctricas y en la Smart Grid.

1. PROTOCOLOS DE TELECONTROL

Entornos de los Protocolos de Telecontrol
Niveles, Servicios y Protocolos
Arquitectura y Modelo de Referencia TCP/IP
Protocolos IEC 60870-5 101 y 104
Arquitectura de Comunicaciones IEC 101 y 104
IEC – APCI, ASDU y APDU

2. PROTOCOLO IEC 60870-5-101

Medios Físicos: Señales
EIA RS-232; ITU-T V.24/V.28
EIA RS-485 / TIA-485-A.222
Modo Asíncrono (Start/Stop)
Estructura IEC 60870-5-101
Nivel Físico IEC 60870-5-101
Nivel de Enlace IEC 60870-5-101
Modo de Transmisión No Balanceada y Balanceada
Campo de Control de Enlace
Iniciación Estación Controlada
Capa Aplicación IEC 60870-5-101
Ejemplos IEC 60870-5-101

3. PROTOCOLO IEC 60870-5-104

Arquitectura básica 104
Funciones asociadas a los ASDUs
Inicialización de la estación controlada
Aspectos diferenciados con respecto al 101
Formatos: APCI - ASDU – APDU
Tipos y formatos del campo de control de L APCI
Funcionamiento secuenciación (tramas I)
Parámetros IEC 60870-5-104
Temporizadores
Arquitectura de la ASDU
Objetos de información
Campos de la ASDU
Ejemplo de tipo ASDU y estructura
Tipos de identificación
Significado primitivas
Cualificador de estructura
Dirección común ASDU
Campos de los objetos de información

Elementos de información
Reset de aplicación
Ejemplos de APDUs
Ejercicios prácticos

4. ANALISIS Y TROUBLESHOOTING EN 101 y 104

Revisión de conceptos TCP/IP para troubleshooting
Comunicaciones TCP/IP
Nivel IP, Protocolo ICMP
Protocolo TCP
Metodología Bottom-Up
Arquitectura de comunicaciones
Troubleshooting: acciones
Troubleshooting de las Infraestructuras Físicas
Troubleshooting del Internetworking IP
Configuración básica del TCP/IP
Errores frecuentes
Comprobación de problemas
Algunas utilidades de diagnóstico
Diagnósticos avanzados TCP/IP
Comprobación de conectividad
Herramientas avanzadas de "campo"
Tráfico de la red y mapa físico
Troubleshooting especializado: Análisis de protocolos
Analizadores de red: WireShark
Utilización con switches: TAPS
Ejemplos y casos prácticos
Análisis de traces con WireShark
Detección y resolución de problemas

Objetivos: Desarrollar en detalle los Protocolos de Telecontrol IEC 60870-5-101 y 104 con el objetivo de poder resolver todos los problemas que aparecen en este tipo de instalaciones .

Dirigido a: Técnicos y Directivos de las Tecnologías de la Información, las Comunicaciones y la Energía.

Metodología: Curso Teórico-Práctico de Análisis y Troubleshooting 101/104.

EL NUEVO ENTORNO DE CABLEADO EN COBRE Y FIBRA

Nivel: MEDIO - Duración: 2 días

El aumento de velocidad hace que los Sistemas de Cableado sean un elemento crítico en las redes de empresa. Este curso aporta los conocimientos imprescindibles para implantar, mantener y optimizar estas infraestructuras.

1. ESTÁNDARES PARA INSTALACIONES DE COBRE

Normas internacionales y europeas
ISO & EN: Categorías y Clases
Los estándares TIA
Principios de Transmisión: Par múltiple, Full Duplex
Parámetros: Atenuación, Diafonías, Pérdida de Retorno
Categorías de cable: Cat 5e, 6, 6A, 7, 7A, 8

2. SISTEMAS DE CABLEADO ESTRUCTURADO

Canales y Enlaces Permanentes
Medidas de Rendimiento
Elementos de un SCE
Topologías: Edificios horizontales, verticales...
Cableado y Conectorización

3. COMPROBACIÓN Y CERTIFICACIÓN EN COBRE

Procedimientos de Certificación
Parámetros de Medida
Equipos de Certificación

4. SISTEMAS DE ALTA VELOCIDAD: 10GBASE-T

Desarrollo, Definiciones
Requisitos de cableado
Comprobación entre cables: AXtalk
Estrategia de muestreo

5. TECNOLOGÍA DE FIBRA ÓPTICA

¿Qué son? ¿Cómo funcionan?
Espectro de frecuencias
Ventanas de transmisión: longitudes de onda
Reflexión y refracción: ángulo crítico
Monomodo y Multimodo
Tipos de fibra y normativas
Secciones transversales de fibra óptica

6. EL ENLACE DE FIBRA

Principios de transmisión y operación
Fuentes y receptores de luz
LED vs Láser
Métodos de terminación de la fibra
Conectores, empalmes y fusiones
APC, UPC, Pigtails, BiMMF

7. MEDIDAS EN FIBRA ÓPTICA

Potencia y pérdida de potencia: atenuación
Dispersión: limitaciones de longitud/velocidad
Reflectancia y ORL
Fuentes de pérdidas
Conexiones sucias, material de la fibra
Acoplamiento y Dobladura del cable

8. COMPROBACIÓN Y CERTIFICACIÓN EN FIBRA

Estándares de instalación (ISO, TIA) y aplicación (IEEE)
Certificación Básica y Extendida
Limpieza e inspección de fibra: IEC 61300-3-35
Certificación de nivel 1: ISO 14763-3
Ejemplo para un enlace dúplex
Certificación de nivel 2: Traza OTDR
Fundamentos de OTDR
Eventos: Reflexiones, Pérdidas,...
Fibras de lanzamiento y recepción
Ejemplo de medición OTDR

Objetivos: Conocer los criterios para la correcta elección de los componentes del sistema de cableado de infraestructuras de comunicaciones, el diseño de la topología, las actividades de mantenimiento y las pruebas necesarias para su aceptación.

Prerrequisitos: Conocimientos básicos de Comunicaciones.

Metodología: Teórico (80%) – Práctico (20%).
Demostraciones prácticas de equipamientos y cableados de cobre y fibra.

SISTEMAS E INFRAESTRUCTURAS LAN DE FIBRA ÓPTICA

Nivel: MEDIO - Duración: 2 días

1. COMUNICACIONES ÓPTICAS

- Ancho de Banda
- Colores y Espectro de Frecuencias
- Ventanas de transmisión
- Reflexión y Refracción
- Índice de refracción
- El ángulo crítico

2. FIBRAS ÓPTICAS: TECNOLOGÍA

- ¿Qué son las fibras ópticas?
- Claves de la tecnología
- Fibras monomodo vs multimodo
- Atenuación del cable de fibra
- Tipos de fibras ópticas ITU-T
- Tipos de fibras según ISO 11801
- SCE (Sistemas de Cableado Estructurado)
- Redes de acceso: FTTH

3. EL ENLACE DE FIBRA

- Operación del sistema de fibra óptica
- Enlace de fibra
- Leds vs. Lasers
- Métodos de terminación de la fibra
- Conectores, empalmes y fusiones
- Reflectancia
- "ORL" (Optical Return Loss)
- Atenuación y Dispersión

4. MEDIDAS DE FIBRA ÓPTICA

- Potencia Óptica
- Midiendo la pérdida óptica
- Dispersión
- Pérdidas de conexiones sucias
- Fuentes de atenuación
- Perdidas acopladas
- Dobladura del cable de Fibra Óptica

5. HERRAMIENTAS DE TEST DE FIBRA

6. ESTÁNDARES DE CERTIFICACIÓN DE FIBRA

- Comprobación y Certificación de fibra
- Tipos de estándares y especificaciones
- Ejemplo de estándar de aplicación
- Especificaciones de comprobación: Nivel 1 y Nivel 2
- Inspección de Fibras
- Estándar 61300-3-35
- Límites ISO 14763-3
- Proyecto de certificación de fibra de nivel 1
- Medida de pérdida de fibra dúplex
- Configuración y Resultados del test
- Certificación de nivel 2: OTDR
- Fundamentos OTDR

7. EJEMPLOS Y CASOS

A lo largo del curso se realizarán diversas prácticas con herramientas de prueba y Certificación de Fibra Óptica.

REDES ÓPTICAS Y DE TRANSPORTE

Nivel: MEDIO/AVANZADO - Duración: 2 días

1. OTNs (Optical Transport Network).

Explosión del Ancho de Banda
 ¿El futuro es óptico?
 Dispositivos electrónicos vs ópticos
 Tecnologías Ópticas “Estado del Arte”
 Convergencia de Redes
 Redes Totalmente Ópticas
 Elementos de la Red Óptica
 Componentes Básicos y Equipos
 Amplificador basado en Erblio (EDFA)
 Amplificación asistida por Raman
 Regeneración Óptica ITU-T G.872
 CWDM, DWDM
 Multiplexión WDM y Transmisión WDM
 WWDM, CWDM & DWDM
 Plan de Multiplexión CWDM, DWDM
 Componentes DWDM. OADM, ROADM
 Conmutación Óptica
 Técnicas de Conmutación Óptica
 Conmutador Óptico DWDM
 Topologías malladas con Cross-Connects
 Estándares del Plano de Control
 ITU-T G.8080 ASON
 Global Optical Connection Control
 Red Óptica de Transporte
 Generic Framing Procedure (GFP)
 Modelo de Referencia OTN ITU-T G.709
 OTH (Optical Transport Hierarchy)
 Evolución tecnológica: PDH – SDH – ETH
 Soporte OTN para 40/100/400 GE

2. PTNs (Packet Transport Networks)

Componentes y Tecnologías PTNs
 Ethernet en las PTNs
 Estándares IEEE 802.3 vs 802.1
 Qué buscan los proveedores de servicios

Definición de los tipos de redes
 Visión de la NGN (ITU - T)
 Ethernet y Transporte de IP
 Infraestructuras actuales con Ethernet
 Estandarización: MEF - ITU – IETF
 Categorías de servicios Ethernet,
 Metro Ethernet Forum - MEF
 Modelo básico del servicio basado en ETH
 Ethernet Virtual Connection
 Limitaciones actuales del MEF
 Recomendaciones ITU-T
 Series G, Q, X, Y
 Ethernet sobre SDH/SONET
 IETF – RFCs

3. TECNOLOGÍAS CARRIER ETHERNET IEEE

Posicionamiento de los estándares IEEE
 IEEE 802.1ad, 802.1ah, 802.1aw, 802.1Qay
 Funcionamiento del QinQ
 Problemática del Bridging
 Funcionamiento del MAC-in-MAC
 Puente PBB
 Organización interna del subnivel MAC en 802.ah
 El bridging en la 802.1ah
 VLANs en 802.1ah
 Tipos de Puentes de Proveedor
 Interconexión redes 802.1ad y 802.ah

Objetivos: Analizar el estado de las redes de transporte de nueva generación para Operadoras, basadas en fibras ópticas y ethernet, su evolución y futuro dentro de los sistemas de transporte de alta velocidad.

Prerrequisitos: Conocimientos de Redes y Comunicaciones.

Metodología: Teórico

INTERNETWORKING EN TCP/IP Y ETHERNET

Nivel: MEDIO - Duración: 2 días

El objetivo es **sistematizar en un solo curso** todos los componentes que forman parte de los actuales sistemas y redes TCP/IP, así como, conocer en profundidad la arquitectura y los protocolos de las redes IP. La correcta interconexión de redes locales precisa del bridging, routing y switching. Este curso desarrolla en detalle todas estas tecnologías con el objetivo de lograr la máxima fiabilidad, operación y el **óptimo aprovechamiento de la Electrónica de Red.**

1. ARQUITECTURA TCP/IP

Normalización: ISOC, IETF y RFCs
 Protocolo IP y Auxiliares: ARP/RARP/ICMP
 Direccionamiento público y privado
 Dispositivos NATs/NPATs
 RARP/DHCP
 Extensiones de Subred y Super Red
 Máscaras: Utilización y Ejemplos
 Protocolo TCP y UDP
 Servicios y Aplicaciones

2. ANÁLISIS Y TROUBLESHOOTING TCP/IP

Nivel de transporte TCP/UDP
 Operación y optimización del TCP
 Control de ventana y congestión en TCP/IP
 Opciones: WS, SACK, TS
 Velocidad nominal, efectiva, neta y agregada
 Verificación del TCP/IP
 Comprobación conexiones TCP
 Diagnósticos: Aplicación y Dispositivos

3. SISTEMAS ETHERNET – IEEE 802.3

Normalización de Ethernet: IEEE 802.3
 IEEE 802.3 MAC - Direccionamiento
 Interfaces: de 1 a 400 Gbps
 Análisis de la trama Ethernet
 Componentes de la Red
 Cableado en Cobre y Fibra
 Entornos industriales
 EEE y PoE
 Control de flujo - 802.3x
 Link Integrity Test y Auto-Negociación
 Agregación de enlaces
 Gigabit Ethernet sobre fibra y cobre

4. SWITCHING Y ROUTING

Electrónica de Red
 El Bridging IEEE 802.1
 Spanning Tree y Rapid STA
 Recálculo de topologías
 Problemática de las Instalaciones
 Routing: Operación y funcionamiento
 Procesos y arquitecturas básicas
 Tablas de encaminamiento: búsquedas
 Internetworking con Routing y Bridging

5. TECNOLOGÍAS DE SWITCHING Y VLANS

Switching L2 y L3
 Tráfico multicast con switches: IGMP Snooping
 Redes Locales Virtuales
 Tipos, Arquitectura, VLANs y SVLANs
 Interconexiones marcadas y no marcadas
 Separación VLANs por STP
 MSTP 802.1s
 Tipos de VLANs: L1, L2, L3, L4
 Sistemas de autenticación
 PVLANS : Private VLANs
 VLANs EN WANS
 Protocolos MVRP

Objetivos: Entender cómo utilizar las tecnologías y soluciones para la construcción e interconexión de redes locales y equipos para formar una Red Corporativa. Revisar en detalle las técnicas de bridging, switching, routing y VLANs.

Prerrequisitos: Conocimientos básicos de Comunicaciones.

Metodología: Teórico / Práctico.

REDES MÓVILES LTE Y WI-FI DE NUEVA GENERACIÓN

Curso: Mañana - Duración: 2 días (12 horas)

Hoy en día vivimos inmersos en una revolución de la movilidad que está cambiando el panorama de los Sistemas de Comunicaciones con una rapidez sin precedentes, lo que supone un punto de inflexión tecnológica que va a afectar radicalmente a los ámbitos privado, empresarial y a los servicios de movilidad

DIA 1: LTE

1. Comunicaciones Móviles: De GSM a LTE

Sistema de comunicaciones móviles
Implementación de una red móvil
Arquitectura de la Red GSM-GPRS
Elementos, Generaciones, Características y Capacidades
La tercera generación 3GPP
Arquitectura de la red UMTS

2. Introducción a LTE

Evolución UMTS-LTE
Redes NGN
Elementos de la Red
Planos de Usuario y de Control
eSIM o SIM virtual
Interfaces Radio
Antenas MIMO
Celdas y Femtoceldas
Equipamiento de usuario
Modelo de cálculo del enlace LTE

3. Arquitectura LTE

Tecnologías en la Interfaz Aire
Frecuencias de Radio y Canales
Calidad de servicio
Hybrid-Automatic Repeat Request
Protocolos y Seguridad
Voz sobre IP

4. De LTE a 7G

LTE Advanced
Arquitectura LTE Advanced
Nuevas categorías de terminales
Li-Fi
Coexistencia Wi-Fi-LTE
LTE-H, LTE-U, eLTE
LTE Air-to-Ground Communications
P-LTE, LTE in a box
TLE-B
5G
6G y 7G

DIA 2: Wi-Fi

5. Las Nuevas Tecnologías Móviles/Inalámbricas

Evolución de las Redes Inalámbricas
WLAN vs Redes Móviles Celulares
Evolución de la Normativa IEEE 802.11 - WFA
Arquitectura Básica Wi-Fi
Entorno Wi-Fi con TCP/IP

6. El Universo Wi-Fi de Nueva Generación

Evolución de IEEE 802.11 / WFA Wi-Fi
Bandas de Frecuencia
Aumento de Prestaciones
Rendimiento: "Signalling Rate" vs "Data Throughput Rate"
Velocidad de datos y rango de transmisión

7. IEEE 802.11ac/ad: las Redes Gigabit

Compatibilidad Wi-Fi en la Nueva Generación
¿Qué es exactamente IEEE 802.11ac?
Prestaciones y Aplicaciones del 802.11ac
La nueva Banda de 60 GHz: 802.11ad
Características y Capacidades
802.11ad – Sectorización y Beamforming

8. Wi-Fi de Nueva Generación

Despliegues Wi-Fi en interior y exterior
Ampliación de las Bandas de Frecuencia
Extensiones de Largo Alcance
Eficiencia Energética: el próximo desafío de Wi-Fi
Wi-Fi en la Internet de las Cosas (IoT) y Smart Grids
Mejoras en Seguridad: IEEE 802.11i vs 802.11ai

Objetivos:

- Dar a conocer las nuevas comunicaciones móviles e inalámbricas de banda ancha.
- Ofrecer una panorámica realista de la situación tanto de mercado como tecnológica.
- Formar a profesionales capaces de aplicar en cada caso las diferentes soluciones existentes

Dirigido a:

- Directivos de las Áreas de Sistemas y Comunicaciones
- Responsables dptos. de Telecomunicaciones, Redes, Tecnologías y Servicios.
- Consultores, Auditores y Jefes de Proyectos de Arquitecturas de Telecomunicaciones.
- Técnicos de Comunicaciones y Redes

Ponentes: José Morales y Juan José Domínguez

SEGURIDAD EN REDES IP

OBJETIVOS:

- Conocer los puntos débiles de nuestros sistemas y redes, implantar métodos de protección, usar credenciales electrónicas, protocolos de autenticación y sobre todo detectar y evitar fallos de seguridad, serán los aspectos relevantes que se desarrollarán en los diferentes cursos de este programa, cuyo objetivo es sistematizar todos los componentes que forman parte de la seguridad de las redes TCP/IP.
- La gran proliferación y el elevado crecimiento de servicios en Internet/Intranet hacen reflexionar hasta qué punto debemos planificar correctamente las instalaciones y conocer un conjunto de herramientas de seguridad vitales para un mantenimiento satisfactorio de dichos sistemas. La utilización de firewalls como frente de choque en los ataques que se producen en las redes basadas en IP es la piedra angular utilizada por casi todas las empresas y organizaciones. Sin embargo, se suelen olvidar que existen técnicas adicionales que complementan y mejoran los aspectos relativos a la seguridad, críticos en este tipo de redes. Por ello, se describen con gran detalle los métodos orientados a obtener la necesaria privacidad en temas tan importantes como el correo electrónico, las transacciones a través de la red, identificación de los usuarios mediante credenciales electrónicas, ataques a las redes IP, y un largo etc...

DURACIÓN Y HORARIO:

Los cursos que están integrados en esta Área tienen una duración de uno, dos o tres días. Con horario de 9:30 a 15:00 horas

DIRIGIDO A:

- Todos aquellos profesionales que quieran acometer un proyecto de seguridad con criterios claros y de forma realista
- Profesionales de Empresas y Organismos Públicos involucrados en los sistemas informáticos y de comunicaciones
- Directivos y Técnicos de las empresas conectadas, o que tienen intención de conectarse a Internet
- Responsables y Profesionales del área de Informática o que trabajen con equipos informáticos
- Laboratorios I+D, Universidades, Fabricantes, Distribuidores e Instaladores
- Particulares con titulación superior o experiencia equivalente, que deseen potenciar su carrera profesional

METODOLOGÍA:

Estos Cursos se imparten independientemente, siguiendo un orden lógico, espaciados en el tiempo con objeto de que las personas que desean asistir a varios cursos maduren los conocimientos adquiridos, de manera que puedan aclararse las dudas antes de iniciar la etapa siguiente. Para ello será posible consultar todas las dudas que surjan a través de Internet con el e-mail que se habilitará a tal efecto. La Metodología de estos cursos está basada en:

- Adquirir conocimientos teóricos, mediante el desarrollo de las sesiones impartidas
- Adquirir conocimientos prácticos, mediante el estudio de casos y pruebas de laboratorio

DOCUMENTACIÓN:

Los asistentes recibirán la documentación del curso; y dependiendo de cada uno: manuales complementarios, cuadernos de prácticas y material adicional.

ATAQUES EN REDES TCP/IP

TÉCNICAS ANTI-HACKING EN COMUNICACIONES

Nivel: AVANZADO - Duración: 3 días

Se desarrolla en profundidad la problemática de seguridad que sufre el TCP/IP desde el punto de vista de las comunicaciones, analizando las vulnerabilidades tanto externas como internas de las redes IP.

1. TÉCNICAS DE HACKING DE COMUNICACIONES

Caracterización y tipos
Tipologías de Hacking de comunicaciones
Ataques más usuales
Contra medidas clásicas

2. PROCESOS DE ATAQUE Y DEFENSA

Fase de Reconocimiento
Procesos correlación por MAC (dispositivos móviles)
Proceso de descubrimiento con SNMP
Ataques a equipos de red:
Switches, routers, APs
Pharming de comunicaciones
Modificación de mensajes DNS
Ataques tipo DoS y DDoS
Ataques de N2
Ataques al TCP
Inundación UDP (VoIP)
Ataques de N3
Ataques de escalado de privilegios

3. HERRAMIENTAS DE HACKING

4. ACCESO AL HOST

La seguridad del Host
Vulnerabilidades TCP
Ataques al stack
Transiciones de estados
Obtención de las "firmas de ataque"
Ejemplos de huellas de S.O.

6. ATAQUES INTERNOS EN LA RED LOCAL

Elementos activos de la LAN
Inundación de las CAM
IRDP spoofing
Camuflajes: Como router, DNS, DHCP
ARP Poisoning
Robo puerta del switch
Defensas contra ARP
Ataques STP, RSTP
Ataques a las VLANs, 802.1q
Ataques MitM (Hombre en medio)
Identificación de sniffers
Defensas
Sistemas y Protocolos de Autenticación

7. SEGURIDAD EN REDES INALÁMBRICAS WI-FI

WPA y WPA2, TKIP y AES
Elementos y Niveles para la seguridad WiFi
Análisis de vulnerabilidades: DoS, WPA, WPS, MiM
802.1x en WiFi
Herramientas de Ataque
Herramientas de diagnóstico

8. ATAQUES DE NIVEL 3

Tráfico malicioso de routing
Descubrimiento de routers
Fases del ataque
Tipos de ataques
Bloqueo
Entradas en las tablas
Control del router
Intercepción y reinyección
Ataques tipo DoS :
bucles, tablas erróneas
Con RIP, Con OSPF
Interconexión BGP
Defensas de routing
Ataques IGMP

9. SOLUCIONES ANTI-HACKING

10. DESARROLLO DE UNA ESTRATEGIA EFICAZ ANTI-HACKING

Objetivos: Este curso desarrolla en profundidad la problemática de seguridad que sufre el TCP/IP desde el punto de vista de las comunicaciones, analizando las vulnerabilidades tanto perimetrales como internas de las redes IP.

Prerrequisitos: Conocimientos previos de seguridad en redes IP y Protocolos TCP/IP

Metodología: Teórico (70%) – Práctico (30%). Se realizarán demostraciones prácticas con diferentes herramientas de ataque y defensa a lo largo del curso.

SISTEMAS FIREWALLS

Nivel: AVANZADO - Duración: 1 día

Desarrollar en detalle las tecnologías de seguridad basadas en Firewalls, incluyendo los elementos, conceptos, estrategias y topologías a utilizar para hacer segura las redes IP.

1. CONCEPTOS DE SEGURIDAD

Firewalls y Sesiones TCP/IP
Inbound/Outbound/NATs

2. ELEMENTOS DE SEGURIDAD Y CONTROL

Arquitectura de Redes Seguras
Colocación idónea elementos de Seguridad

3. ESTRATEGIAS: TIPOLOGÍAS

Planteamiento estrategia
Firewalls
Modelos de decisión
Tipologías genéricas
Filtrados de paquetes
SPF
Panorama y Tendencias actuales

4. REGLAS

Recomendaciones
Reglas Avanzadas
Errores más comunes
Lectura y configuración de Logs

5. ARQUITECTURAS

Externa-Interna-DMZ
Arquitectura de 2 y 3 Niveles
Casos Prácticos
Configuraciones
Ataques
Protecciones

Objetivos: Desarrollar en detalle las tecnologías de seguridad basadas en Firewalls, incluyendo los elementos, conceptos, estrategias y topologías a utilizar para hacer segura las redes IP.

Prerrequisitos: Conocimientos básicos TCP/IP.

Metodología: Curso teórico con casos prácticos sencillos.

SISTEMAS Y PROTOCOLOS DE AUTENTICACIÓN EN TCP/IP

Nivel: AVANZADO - Duración: 1 día

Este curso nos muestra los protocolos que permiten implantar un sistema de autenticación en redes IP de usuarios, desarrollando las diferentes tecnologías existentes y la interoperación entre sus componentes.

1. SISTEMAS DE AUTENTICACIÓN

Elementos y Arquitecturas

2. PROTOCOLOS De AUTENTICACIÓN

CHAP, MS-CHAP, PAP
EAP-TTLS, EAP-SIM/USIM/ISIM

3. ARQUITECTURA PKIs

Fundamentos criptográficos de las PKI
Entidades de una PKI (Agencia Certificadora, Autoridad de registros, ... etc)
Servicio de manejo de certificados (generación, validación, distribución y revocación)
Uso de las PKIs
Ejemplo de uso en IPsec (túneles, negociación de claves, etc...)
Simple Certificate Enrollment Protocol (SCEP)

4. SISTEMAS AAA

RADIUS
Integración de RADIUS con LDAP y DHCP
TACAS+

5. 802.1x : AUTENTICACIÓN DE ACCESO A SWITCHES Y APs

Arquitectura y elementos
Protocolos de autenticación EAP
Interconexión con RADIUS

6. ENTORNOS VoIP

Session Border Controllers (SBC)
Encriptación TLS y SRTP
Otras alternativas

Objetivos: Este curso nos muestra los protocolos que permiten implantar un sistema de autenticación en redes IP de usuarios, desarrollando las diferentes tecnologías existentes y la interoperación entre sus componentes.

Prerrequisitos: Conocimientos TCP/IP y técnicas básicas de seguridad

Metodología: Curso teórico

CERTIFICACIÓN DIGITAL Y TARJETAS INTELIGENTES

Nivel: AVANZADO - Duración: 2 días

Durante el curso se presentarán las bases necesarias para entender las PKI, los roles que juegan las Autoridades de Certificación, Autoridades de Registro y el modelo de seguridad de extremo a extremo que plantean PKI. También se analizan **las debilidades explotadas por los atacantes**, vulnerabilidades ya conocidas pero que se pensaban teóricas, y se aportan medidas de control de daños ante estos eventos. Por último se tratarán modelos alternativos a las PKI clásicas.

1. VULNERABILIDADES DE LAS PKIs

Situación actual
Ataques e Infraestructuras PKIs
Por qué existen riesgos en las PKIs

2. INFRAESTRUCTURAS DE PKI

Usuarios
Autoridades de Certificación
Autoridades de Registro

3. SEGURIDAD EXTREMO A EXTREMO

Soluciones en comunicaciones end-to-end
SSL, DNSsec, TLS
Diffie-Hellman

4. CERTIFICADOS Y AUTENTICACIÓN

Autenticación con Certificados
Tokens de Seguridad
OTPs (One Time Password)

5. FIRMA DIGITAL

Formatos, Estructuras, Operativa
Estándares PKIX, PKCS, CMS, Otros
Firma digital de larga duración
Validación de las firmas

6. TARJETAS INTELIGENTES

Propiedades y Tipos de tarjetas
Arquitectura de Seguridad
Nuevos Sistemas de Tarjetas Inteligentes

7. RESPUESTA A INCIDENTES

Contabilidad, Auditoría
Autenticación
Uso de múltiples factores

8. LEGISLACIÓN ACTUAL

Firma digital segura y Firma digital reconocida
Dispositivos seguros de firma
DNI Electrónico

Objetivos: Ver la problemática de seguridad en el desarrollo del comercio electrónico, analizar en detalle los aspectos relevantes de los certificados y firmas digitales, su implantación en los sistemas informáticos, tarjetas inteligentes y aplicaciones avanzadas. Todo ello combinado con la realización de casos prácticos a lo largo del curso.

Prerrequisitos: Conocimientos básicos seguridad

Metodología: Teórico (50%) – Práctico (50%). Se realizarán prácticas sobre una maqueta con ordenadores personales portátiles que se entregarán a los asistentes (Instalación de certificados y tarjetas inteligentes en entornos Windows) Demostración sobre entorno Unix.

SEGURIDAD EN SISTEMAS TCP/IP

OBJETIVOS:

- Ofrecer las pautas y buenas prácticas para el mantenimiento de la seguridad en webs.
- Proteger a mi empresa de la mala utilización de las Redes Sociales, que puede afectar a la Seguridad de los Sistemas Informáticos.
- Conocer y definir las normas y estrategias necesarias para el mantenimiento y continuidad de negocio, aprendiendo a diseñar un Plan de Contingencia, realizando un análisis de impacto (BIA).
- Desarrollar un cuadro de Mandos de Seguridad, cuantificando los diferentes indicadores y sus métricas.

DURACIÓN Y HORARIO:

Los cursos que están integrados en esta Área tienen una duración de uno, dos o tres días. Con horario de 9:30 a 15:00 horas

DIRIGIDO A:

- Todos aquellos profesionales que quieran acometer un proyecto de seguridad con criterios claros y de forma realista
- Profesionales de Empresas y Organismos Públicos involucrados en los sistemas informáticos y de comunicaciones
- Directivos y Técnicos de las empresas conectadas, o que tienen intención de conectarse a Internet
- Responsables y Profesionales del área de Informática o que trabajen con equipos informáticos
- Laboratorios I+D, Universidades, Fabricantes, Distribuidores e Instaladores
- Particulares con titulación superior o experiencia equivalente, que deseen potenciar su carrera profesional

METODOLOGÍA:

Estos Cursos se imparten independientemente, siguiendo un orden lógico, espaciados en el tiempo con objeto de que las personas que desean asistir a varios cursos maduren los conocimientos adquiridos, de manera que puedan aclararse las dudas antes de iniciar la etapa siguiente. Para ello será posible consultar todas las dudas que surjan a través de Internet con el e-mail que se habilitará a tal efecto. La Metodología de estos cursos está basada en:

- Adquirir conocimientos teóricos, mediante el desarrollo de las sesiones impartidas
- Adquirir conocimientos prácticos, mediante el estudio de casos y pruebas de laboratorio

DOCUMENTACIÓN:

Los asistentes recibirán la documentación del curso; y dependiendo de cada uno: manuales complementarios, cuadernos de prácticas y material adicional.

ATAQUES Y EXPLOITS EN LAS APLICACIONES TCP/IP

TÉCNICAS DE HACKING, ANÁLISIS DE VULNERABILIDADES Y CONTRAMEDIDAS

Nivel: MEDIO - Duración: 2 días

La Seguridad es uno de los aspectos más importantes que tanto desarrolladores como profesionales de TI deben tener en cuenta a la hora de planificar, desarrollar e implementar aplicaciones.

1. CARACTERIZACIÓN DE LOS TIPOS DE ATAQUES

Superficie de ataque (Attack Surface)
Ataques al servidor y al cliente
Ataque cruzados

2. TÉCNICAS COMUNES DE ATAQUE

SQL Injection
Cross Site Scripting (XSS)
Rotura de la autenticación y gestión de sesión
Cross Site Request Forgery CSRF
Remote/Local File Inclusion R/LFI
Insecure Direct Object References
Redirecciones y reenvíos no válidos
Data Exfiltration. Otros

3. MODELOS DE SEGURIDAD

Modelo FLI, Modelo RBAC/IRBAC, Modelo OWASP

4. CHECKLIST

Arquitectura y Diseño
Código, Acceso a Datos
Servicios a Empresas
Accesos Remotos, Servicios Web

5. INTEGRACIÓN DE LA SEGURIDAD EN EL PROYECTO

Modelo white box, Modelo black box, Modelo gray box

Metodología y medidas de footprinting
Information gathering, Social attacks
Hacking de sistemas CEH
Técnicas de análisis de pen-testing y herramientas
Problemáticas comunes

6. PROGRAMACIÓN E INTEGRACIÓN CONTINUA (CI)

Inclusión del modelo de seguridad en el testeo
Modelos de integración continua para la seguridad
Security Code Review
Análisis estático y dinámico de la aplicación
Herramientas
Análisis post deployment

7. SEGURIDAD EN LA CLOUD

Módulos de seguridad
Soft vs Appliances
Seguridad en las comunicaciones
Gestión de Redes con virtualización

8. SEGURIDAD EN HTML5

Introducción a las tecnologías de HTML5
Nuevo modelo de seguridad
Nuevos tipos de ataques
Web Storage Extraction - Blind Storage Enumeration

INDICADORES Y MÉTRICAS: CUADRO DE MANDOS DE SEGURIDAD

Nivel: MEDIO - Duración: 1 día

El cuadro de mandos, facilita su labor, al responsable de seguridad, permitiendo a la empresa conocer en cada momento su grado de seguridad y ayudando a la toma de decisiones tanto operativas como estratégicas, rentabilizando las inversiones.

1. SEGURIDAD GESTIONADA

Sistema de control interno
Políticas y Procedimientos.
Vulnerabilidades en la organización

2. MARCO METODOLÓGICO

Implantación de SGSI
NORMA UNE 71502:2004
Términos y definiciones UNE-71502
ISO/IEC17799, UNE 71501-x
Gestión de Riesgos
COBIT. Factor Crítico de Éxito
Ejemplos de Indicadores: KGIs, KPIs
Evaluaciones: MM, CSFs, KGIs, KPIs
Ejemplo de Informe y Buenas Prácticas

3. GOBIERNO

El Gobierno de Seguridad en TI.
Objetos de Alineamiento estratégico
STAKEHOLDERS
Factores críticos de Éxito (FCE): Metas
Propuesta de valor al cliente
Iniciativas estratégicas. UNE 66175
Diseño de indicadores y cuadro de mandos
Implantación del sistema de indicadores
Validación de indicadores
De la métrica al indicador

4. ALINEACION DE TI

Nexo del la TI con el Negocio
Valoración de las aplicaciones y de los recursos
Alineamiento de la Seguridad
Relación entre CMs de la organización

5. CUADRO DE MANDOS DE SEGURIDAD

Objetivos y Beneficios
Stakeholder, CMSTI
Arquitectura, Relación entre CM Filiales y Corporativo
Actividades de un CMSTI

6. DESARROLLO E IMPLEMENTACIÓN

Áreas de gestión y Tipos de indicadores
Gestión de procesos de Negocio
Soporte de métricas on-line
Normalización
Plan de proyecto de CMSTI

Objetivos: El cuadro de mandos descarga de trabajo al responsable de seguridad, facilita su labor, permite a la empresa conocer en cada momento su grado de seguridad (cuantificándolo) y ayuda a la toma de decisiones tanto operativas como estratégicas.

Prerrequisitos: Conocimientos de seguridad y su entorno de operación

Metodología: Curso teórico con ejemplos prácticos

CONTINUIDAD Y PLANES DE CONTINGENCIA

Nivel: MEDIO - Duración: 1 día (8 horas)

La **CONTINUIDAD** es una disciplina que intenta aumentar la capacidad de una organización para tolerar con flexibilidad situaciones límite y sobreponerse a ellas.

1. LA CONTINUIDAD DE NEGOCIO

- Introducción Continuidad de Negocio.
- Ventajas y beneficios del BCM
- Estándares y modelos de la continuidad de negocio
 - Norma BS 25999
 - Norma ISO 22031
- Sistemas de Gestión de Continuidad
- Diferencias entre DRP y BCM
- Continuidad Tecnológica
 - Norma BS25777

2. CONSTRUYENDO EL PLAN DE CONTINUIDAD DEL NEGOCIO

- Política de Continuidad
- Business Impact Analysis (Impacto de Análisis del Negocio).
- Risk Assesment (Evaluación o Valoración de Riesgos).
- Estrategias de Continuidad.
 - Análisis de factibilidad
 - Priorización de alternativas
 - Toma de Decisiones
- Estructura Organizacional para la Continuidad
 - Roles
 - Responsabilidades
 - Procedimientos
- Procesos y Procedimientos de Continuidad.
- Mantenimiento de los Planes

3. GESTIONANDO LA CRISIS, PLAN DE COMUNICACIÓN EN CRISIS

- Estrategias de comunicación
- Comunicación con los medios
- Uso de redes sociales

4. PROBANDO EL PLAN DE CONTINUIDAD DEL NEGOCIO

- Divulgación, concienciación y formación
 - Norma PD 25666:2010
- Escenarios de Pruebas
- Plan de Pruebas
- Ejecución de Pruebas
- Roles Play
 - Pruebas de recorrido o escritorio
- Análisis de Resultados

Objetivos: Conocer las diferentes normas acerca de Continuidad de Negocio. Definir las distintas estrategias de continuidad necesarias para el mantenimiento de su negocio. Aprender a construir un Plan de Continuidad de Negocio. Aprender a realizar un análisis de impacto (BIA). Conocer la manera en la que se realizan las pruebas a los planes de continuidad. Identificar los requerimientos mínimos para la puesta en marcha de un plan de continuidad de negocio.

ANÁLISIS Y GESTIÓN DE REDES

OBJETIVOS:

- Hoy en día es imprescindible un conocimiento práctico de los métodos y herramientas para el análisis y resolución de problemas (troubleshooting) en las Redes y Sistemas TCP/IP. Detectar, identificar y resolver rápidamente fallos en las actuales infraestructuras de comunicaciones es uno de los principales problemas de los departamentos de TI. Para ello esta área cubre el uso del WireShark como herramienta indispensable para la detección y resolución de problemas de networking.
- Conocer en detalle la optimización y resolución de problemas en instalaciones Wi-Fi.
- Analizar y estudiar la familia de protocolos SNMP para su aplicación en las instalaciones del usuario.
- Cómo implantar los procedimientos y la metodología para hacer que la gestión sea proactiva, anticipándose a los problemas. Ello hará el trabajo de los profesionales involucrados más grato, eficaz y productivo, aumentando al mismo tiempo la calidad de servicio y la satisfacción de los usuarios.

DURACIÓN Y HORARIO:

Los cursos que están integrados en esta Área tienen una duración de uno, dos o tres días. Con horario de 9:30 a 15:00 horas

DIRIGIDO A:

- Responsables de Gestión de Red y de Comunicaciones
- Directores de Informática/CPD y de Organización y Planificación
- Consultores, Auditores, Jefes de Proyectos y Consultores en Comunicaciones de Datos
- Responsables y Técnicos del área de Telecomunicaciones
- Responsables de los Sistemas de Información en Empresas y Organismos Públicos
- Laboratorios I+D, Universidades, Fabricantes, Distribuidores e Instaladores
- Suministradores de Servicios (Operadoras, Telefonía, GSM, Cables, Satélites y Radioenlaces, ISPs)
- Particulares con titulación superior o experiencia equivalente, que deseen potenciar su carrera profesional

REQUISITOS:

Los asistentes a estos Cursos deberán tener conocimientos en todos los aspectos fundamentales de las comunicaciones de datos: interfaces, protocolos, técnicas básicas de redes y arquitecturas de comunicaciones. No es aconsejable la asistencia de las personas que no cumplan estas condiciones, pues tendrán serias dificultades en el seguimiento de la materia

METODOLOGÍA:

Estos Cursos se imparten independientemente, siguiendo un orden lógico, espaciados en el tiempo con objeto de que las personas que desean asistir a varios cursos maduren los conocimientos adquiridos, de manera que puedan aclararse las dudas antes de iniciar la etapa siguiente. Para ello será posible consultar todas las dudas que surjan a través de Internet con el e-mail que se habilitará a tal efecto. La Metodología de estos cursos está basada en:

- Adquirir conocimientos teóricos, mediante el desarrollo de las sesiones impartidas
- Adquirir conocimientos prácticos, mediante el estudio de casos y pruebas de laboratorio

DOCUMENTACIÓN:

Los asistentes recibirán la documentación del curso, y dependiendo de cada uno: manuales complementarios, cuadernos de prácticas y material adicional.

TROUBLESHOOTING Y SEGURIDAD EN IPV6

CURSO PRÁCTICO

Nivel: AVANZADO - Duración: 2 días

1. GESTIÓN DE PROBLEMAS Y TROUBLESHOOTING EN IPV6

- Mapa de troubleshooting TCP/IPv6
- Metodología Bottom-Up
- Protocolos entorno IPv6
- Troubleshooting TCP/IPv6: Nivel Básico
- Internetworking IP: Problemáticas Frecuentes
- Utilidades de diagnostico básicas
- Comprobación preferencia de protocolo IPv4/IPv6
- Comprobación conexiones TCP
- Diagnosticos avanzados TCP/IPv6
- Utilizando herramientas semiautomáticas
- Herramientas avanzadas de "Campo"

2. TROUBLESHOOTING ESPECIALIZADO (TCP/IPv6)

- Analizadores de protocolos
- Capacidades y manejo del WireShark
- Análisis del internetworking IPv4/IPv6
- Análisis tráfico de trazes
- Troubleshooting y monitorización
- Performance: Localización de puntos de bajo performance
- Resolución de Problemas durante la Coexistencia IPv4/IPv6

- Resolución de trazes: Localización de problemas
- Recomendaciones para hacer un buen troubleshooting

3. PLANES DE DIRECCIONAMIENTO En IPV6

- Consideraciones generales
- Buenas Prácticas
- Agregación y Jerarquía
- Ejemplos de agrupación
- Tipos de Estrategías
- Asignación de direcciones: ISPs, Empresas, Particulares
- Ejemplos y casos

4. SEGURIDAD EN IPV6

- Aspectos a considerar
- Direccionamiento, ICMPv6, Firewalls, VPNs, DHCPv6
- Seguridad durante la Coexistencia y migración
- Ataques a equipos y servicios de Red
- Ataques a protocolos auxiliares
- Herramientas
- Conclusiones y Recomendaciones

EJEMPLOS Y CASOS PRÁCTICOS (a lo largo del curso)

WIRESHARK V.2: ANÁLISIS DE PROTOCOLOS Y REDES

Nivel: AVANZADO - Duración: 3 días

Hoy en día es imprescindible un conocimiento profundo de los métodos y herramientas para el análisis y resolución de problemas (troubleshooting) en las Redes y Sistemas TCP/IP. Detectar, identificar y resolver rápidamente fallos en las actuales infraestructuras de comunicaciones es uno de los principales problemas de los departamentos de TI.

Este curso está especialmente diseñado para cubrir esta necesidad de forma totalmente práctica y efectiva.

1. ANALIZADORES DE RED

Tipos y Funciones
Análisis base. Traces y Troubleshooting
Utilización en Switched LANs: SPAN ports, TAPs, etc...
Ejemplos de Aplicación

2. CAPACIDADES Y MANEJO DE WIRESHARK

Estudio detallado de todas las posibilidades del WireShark que permiten la resolución de problemas de comunicaciones
Manejo del analizador
Parametrización y Ajustes
Filtros, Capturas, Postfiltrado
Análisis básico, experto
Estadísticas, Gráficos I/O, Flujos
Análisis VoIP, Wireless WiFi
Gráficos Stream TCP, UDP, ..
Trucos de utilización
Optimización del WireShark
Cómo sacar el máximo rendimiento al WireShark

3. ANÁLISIS DEL PROTOCOLO IP (Traces)

Dónde, qué y cómo medir
Tráficos de Nivel IP, Ajustes
Sobrecargas en la Red
Análisis de Traces: Metodología
Detección y Aislamiento de Problemas
Cómo eliminar tráfico no deseado
Protocolos ARP, ICMP,

Análisis I/O avanzado
Descubrimiento de servicios de red

Identificación de comportamientos anómalos
Resolución de malas configuraciones
Detección de cuellos de botella
Casos y Ejercicios Prácticos

4. ANÁLISIS DEL PROTOCOLO TCP (Traces)

Metodología para el correcto análisis del TCP
Establecimiento y finalización de conexión
Errores, temporizadores y retransmisiones
Algoritmos de control de congestión
ACKs duplicados y Restransmisión Rápida
Escalado de ventana: funcionamiento
Aceptación Selectiva: SACK
Mejora de la eficiencia de las comunicaciones
Resolución de problemas de mal funcionamiento
Clientes, servidores y aplicaciones
Análisis gráfico de rendimiento de la transmisión
Detección, identificación y resolución de problemas
Aumento de la calidad de las comunicaciones

5. EJEMPLOS Y CASOS PRÁCTICOS

Medidas de Throughput, Retardos, Latencias
Aplicación - Comunicaciones - Equipo usuario
Cómo aislar los problemas
Cómo interpretar los traces
Detección de ataques de Red
Detección de anomalías
Análisis de aplicaciones y servicios de red:
DNS, FTP, telnet, HTTP, VoIP

WIRESHARK V.2: DETECCIÓN DE ATAQUES EN RED

Nivel: AVANZADO - Duración: 1 día

Este curso está basado en casos prácticos.

Para ello se analizan diferentes trases con problemas de seguridad. El objetivo es analizar, detectar e identificar el tipo de ataque que se está produciendo, quién lo está realizando y qué medidas correctivas tomar.

Es imprescindible que el asistente tenga conocimientos medio/avanzados en la utilización de Wireshark o en su caso que haya asistido a nuestro curso "Wireshark: Análisis de Protocolos y Redes".

Si no es así, el alumno tendrá dificultades para seguir adecuadamente el desarrollo de este curso.

1. El Wireshark como herramienta de análisis de Seguridad en Redes y Sistemas TCP/IP

- Herramienta de ayuda
- Configuración de dissectores para detectar ataques
- Análisis Experto
- Análisis Gráficos
- Análisis Estadísticos
- Generación de ACLs
- Telefonía y VoIP-SIP
- Perfiles de Seguridad

2. Detección y Análisis de Ataques con WireShark

- Detección de scaneos
- Análisis del ICMP
- Detección de IRDP
- Identificación de spoofing IP
- Detección de paquetes malformados
- Detección de ataques de hombre en medio
- Detección de fragmentación IP
- Detección de ataques DoS
- Detección de OS fingerprinting
- Utilización adecuada de la colorización en cada caso

3. Casos Prácticos basados en Trases

A lo largo del curso se verán diferentes trases con ataques de seguridad, con el objeto de que los alumnos se familiaricen en el uso del WireShark para estas labores.

Entre otros se analizan:

- Ataques DoS
- Ataques de hombre en medio
- Robo de stack
- Ataques en entornos Wi-Fi
- Detección de tráfico anómalo

SNMP: GESTIÓN Y SUPERVISIÓN DE SISTEMAS Y REDES

Nivel: MEDIO - Duración: 2 días

1. GESTIÓN Y SUPERVISIÓN DE RED

Áreas de Gestión "FCAPS"
Requerimientos del Usuario
La Gestión Corporativa
Elementos y Estructura de Gestión
Gestión SNMP - IETF STD15
Clientes, Servidores, Gestores SNMP

2. CONTROL Y ANÁLISIS DE PRESTACIONES

Control de calidad de la Red
Parámetros de prestaciones
Latencia vs Retardo de Red
Throughput vs Goodput
Influencia de las aplicaciones
Técnicas de Fiabilidad
Optimización
Terminología del IETF
Medidas de "throughput"
Parámetros
Valores de Referencia
Condiciones del Entorno
MTBF y MTTR
Redundancias y Dependencias
Efecto de las Interrupciones
Concepto de Nivel de Servicio

3. ARQUITECTURA SISTEMAS SNMP

Bases de información: Estructura de MIBs.
Sintaxis SMI, SMIv2, SMIng.
Contenido y Tipos de datos. MIBs.
Práctica: MIB browser.
Análisis de MIBs.
Problemática de la obtención de resultados de gestión a través de las MIBs.
Cálculos de parámetros de prestaciones.
Ejemplos prácticos MIB.

4. PROTOCOLO SNMP

Desarrollo del SNMP, Versiones, Arquitectura.
Funcionamiento.

Mensajes: Gets, Set, Traps, etc...
Seguridad SNMPv1: Problemas planteados.
Rendimiento del Sistema.
Correladores de eventos.
Análisis prácticos de traces SNMP.
Ejemplo de configuración.

5. MONITORIZACIÓN REMOTA: RMON

Servicios y funcionamiento.
Componentes, Descripción y análisis.
Tipos de productos, Funcionamiento.
Interoperabilidad, RMON 2.
Descripción de los grupos. Ventajas.
SMON para VLANs y SLANs.

6. SNMP v.3

Características y Operación.
Descripción de los nuevos mensajes.
Formatos del SNMPv3.
Ventajas, Coexistencia, Arquitectura y Seguridad, autenticación y privacidad.
Últimos desarrollos.

CASOS PRÁCTICOS

A lo largo de este curso se realizarán diversas prácticas sobre los temas tratados, utilizando diferentes herramientas tanto comerciales como de libre distribución.

Objetivos: Permite conocer las posibilidades reales que ofrece el estándar SNMP y su aplicación en la Gestión y Supervisión de Sistemas y Redes para conocer los parámetros más relevantes de nuestros sistemas de comunicaciones, que nos indica la "salud" de los Sistemas y Red Corporativa.

Prerrequisitos: Conocimientos de redes LAN, WAN e Internetworking

Metodología: Teórico – Práctico

METODOLOGÍA DE GESTIÓN DE REDES. BUENAS PRÁCTICAS

Nivel: MEDIO - Duración: 2 días

1. ANÁLISIS Y GESTIÓN DE RED

Procesos dinámicos de la Gestión
Bases Fundamentales
¿Cómo es mi gestión de Red?
Requisitos de La Gestión Corporativa
Estructura y elementos de Gestión
Auditoría y Proyecto de Red
Gestión SNMP

2. CONTROL Y ANÁLISIS DE PRESTACIONES

"Network Performance Testing"
¿Qué, cómo y cuándo debemos medir?
Métodos y Herramientas: Interpretación de resultados
Control de Calidad de la Red
Parámetros de Prestaciones
Acotación, Precisión y Tasa
Retardos, Throughput, Temporizadores, Errores
Influencia de las aplicaciones
Técnicas de Fiabilidad
Benchmarking: Metodología y Medidas

3. CONSTRUYENDO LA GESTIÓN: 1ª Parte

Introducción: Arquitectura gestión SNMP
Fases para la implantación de un CGR
Toma de datos previa
Herramientas
Verificación configuraciones
Descubrimiento y modelado de la red
Recomendaciones
Proceso de polling: ajuste de parámetros
Criticidad de los dispositivos
Gestión reactiva vs proactiva
Ejemplos

4. GESTIÓN DE PRESTACIONES

Parámetros y Valores de Referencia
Condiciones del Entorno
¿Qué parámetros adoptar?
Disponibilidad, Fiabilidad, Redundancias
Efecto de las Interrupciones
Aplicación práctica de las medidas de la Red
Visión global del Nivel de Servicio

Cómo asignar un único valor al Nivel de Servicio
Ejemplo Práctico

5. APLICACIÓN DE LA METODOLOGÍA

Evaluación de las Prestaciones
Valores de Referencia
Área de actuación para la Medida del Servicio
Fallos de Red en el Dominio Local y Global
Consideraciones y Fiabilidad
Tiempos de Interrupción
Ejemplos Prácticos de Aplicación
Informes de Gestión

6. CONSTRUYENDO LA GESTIÓN: 2ª Parte

Definición de parámetros por tecnología y tipo de dispositivo
Ejemplos y Tabla resumen
Origen de los Datos: Bases de gestión
Casos Prácticos
Buenas prácticas con SNMP para el origen de los datos
Acuerdos de Nivel de Servicio
SLAs y su entorno
Reporting
Casos Prácticos sobre SLAs

Objetivos: La Gestión de las Redes actuales tanto de proveedores de servicios, empresas de outsourcing como las Redes Corporativas de empresas, suele ser reactiva, con los inconvenientes que ello supone. Este curso describe en detalle cómo implantar los procedimientos y la metodología para hacer que la gestión sea proactiva, anticipándose a los problemas. También desarrolla en detalle todos los elementos necesarios para implantar y utilizar un entorno de Gestión Proactiva simple y eficaz.

Prerrequisitos: Conocimientos básicos de comunicaciones.

Metodología: Teórico – Práctico

ANÁLISIS DE PRESTACIONES Y SEGURIDAD DE REDES”

Nivel: MEDIO - Duración: 3 días

Aporta los conocimientos teórico-prácticos y las herramientas imprescindibles para planificar, analizar y resolver problemas y controlar las redes de datos y su seguridad.

1. ANÁLISIS DE PROTOCOLOS

Parametrización y ajustes
Análisis de traces: metodología

2. TROUBLESHOOTING DE LA RED ETHERNET

Revisión del tráfico de Red
Problemática del "broadcasting"
Situaciones de congestión

3. TROUBLESHOOTING DE LA INTERNET IP

Análisis avanzado del I/O
Detección de cuellos de botella

4. TROUBLESHOOTING DEL TRANSPORTE TCP

Estudio gráfico de prestaciones
Identificación y resolución de problemas

5. ANÁLISIS DE PRESTACIONES DE RED

Parámetros y medidas de Prestaciones
Análisis de interfaces, red, transporte
Evaluación de la infraestructura de red
Benchmarking, valores de referencia
Control con SNMP
Normalización: IETF STD15
Elementos, Áreas, Agentes y Gestores
Bases de Información: Estructura de MIBs
El Protocolo SNMP
Sintaxis, contenido y tipos de datos
Sondas RMON: Servicios y Componentes

6. SEGURIDAD EN REDES: ATAQUE Y DEFENSA

Técnicas de hacking de comunicaciones
Procesos de ataque y defensa, herramientas
Acceso al Host y ataques al Stack TCP/IP
Ataques de Red internos y externos
LANs Conmutadas, Routing, SNMP
Seguridad Inherente con UETS
Blindaje ante ataques internos y externos

7. EJEMPLOS Y CASOS PRÁCTICOS

Análisis base y troubleshooting
Interpretación de los traces
Medidas de throughput, retardos y latencias
Cómo aislar los problemas
Detección de ataques de red
Detección de anomalías
Análisis de aplicaciones
Servicios de Red de Nueva Generación

Objetivos: Adquirir, mediante experiencia práctica, las habilidades y conocimientos imprescindibles para la planificación, implantación, puesta en servicio, operación y resolución de problemas de sus redes actuales, así como conocer su estado real, y la mejora de capacidades y beneficios económicos que aportan las nuevas tecnologías.

Prerrequisitos: Conocimientos básicos de comunicaciones.

Metodología: Teórico – Práctico

OTROS CURSOS DISPONIBLES

Otros Cursos disponibles bajo demanda:

- **MPLS, GMPLS Y VPLS**
- **Redes de Acceso: XDSL, FTTH Y METROETHERNET**
- **Routing en Redes IP (V4/V6): RIP, IS-IS, OSPF, EIGRP, BGP**
- **Centros de Datos y Redes de Almacenamiento**
- **IMS: Convergencia Multimedia en Redes Fijas y Móviles**
- **Cloud Computing: Virtualización en la “NUBE”**
- **Cómo implantar Servicios en Cloud**
- **Experto en Evidencias Electrónicas**
- **Fibre Channel**
- **Ultra High Performance Internet**
- **Regulación y Servicios de las Telecomunicaciones en España**
- **Optimización Servidores (Virtualización/Comunicaciones)**

MPLS Y MPLS-TP

Nivel: MEDIO/AVANZADO - Duración: 2 días

1. ARQUITECTURA MPLS

Funcionamiento básico
 Arquitectura y tipos de routers
 Label Switched Path (LSP)
 Encapsulado de Etiquetas, FEC - NHLFE
 Funciones y Operación MPLS
 Ingeniería de Tráfico (TE) en MPLS
 Rutas explícitas. Rutas: off-line, on-line
 Cálculo de Rutas
 CSPF (Constrained Shortest Path First Algoritm)
 Ejemplo creación túneles
 Preemption, Reoptimización, Balanceo de carga
 Protección del tráfico
 Protocolos de Señalización en MPLS
 Funciones y tipos
 Distribución de etiquetas y creación de las tablas
 LDP, RSVP-TE, CR-LDP

2. SERVICIOS MPLS: PWE3 y VPNs

Alternativas PWE3 y MPLS/BGP-VPN
 El VPLS y la arquitectura PWE3
 Visión conceptual y elementos
 El Bridging, VPNs de N2 y el PWE3
 Operación VPN MPLS L2
 Configuración y señalización PWE3
 Etiquetas y Operación del PWE3
 Arquitectura VPLS
 Autodescubrimiento y Señalización MBGP
 VPNs MPLS L3
 Características
 Routing y Routers virtuales
 Operación y Funcionamiento

3. EL MPLS-TP

Posicionamiento y Elementos
 Terminología
 Requerimientos del Perfil de Transporte

MPLS-TP vs MPLS/IP
 Normalización
 Arquitectura y Áreas de Aplicación
 Distribución de las etiquetas
 Aprovisionamiento estático
 Requerimientos OAM RFC 5860
 Funciones OAM
 Mecanismos OAM
 Ejemplo LSP
 Canal asociado ACH
 OAM y stacks de etiquetas
 Gestión RFC 5951
 Protección: APS
 QoS
 Operación híbrida: ejemplo para servicios Ethernet

4. ARQUITECTURA GMPLS.

Transporte IP sobre múltiples tecnologías
 Extensiones del plano de control MPLS
 Propagación de Landas y tipos de Interfaces
 Componentes del GMPLS
 Plano de control GMPLS
 Protocolos de routing TE
 OXC: Componentes del plano de control
 Establecimiento de LSPs en GMPLS

5. RESUMEN EJECUTIVO

MPLS: Arquitectura y Funcionamiento
 MPLS-TP: Características y diferencias con el MPLS

Objetivos: Entender las técnicas de paquetes IP basadas en MPLS, incluyendo el plano de control GMPS y los nuevos servicios de LANs VPLS.

Prerrequisitos: Conocimientos de Redes y Comunicaciones.

Metodología: Teórico

ROUTING EN REDES IP (v4/v6): RIP, IS-IS, OSPF, EIGRP, BGP

Nivel: MEDIO/AVANZADO - Duración: 2 días

1. ENCAMINAMIENTO

Mecanismos de encaminamiento
Encaminamiento en IP
Tablas de encaminamiento
Tipos de entradas en una tabla
Procesos básicos de Routing
Convergencia y actualización tablas
Routing estático / dinámico
Tablas estáticas + routing dinámico
Procesos de búsqueda en las tablas
Routing "Hardware"
Supernetting, Summarization
Distancia Administrativa (da)

2. ENCAMINAMIENTO INTERIOR: RIP, OSPF, IS-IS, EIGRP

Routing Information Protocol (RIP)
Métricas RIP
Formato paquetes RIP-1 y RIP-2
Funcionamiento
RIP-2
Formato paquetes RIP-2 con SHA y HMAC
RIP ng para IPv6

3. ENCAMINAMIENTO INTERIOR: OSPF

Algoritmo EDGAR DIJKSTRA
Routing Jerárquico
LSAs - Áreas - S.A
Estructura PDUs OSPF
Tipos de Paquetes OSPF
Cabecero LSAs
Tipos y Formatos LSAs
Funcionamiento OSPF
Bases de datos y LSPs
Ejemplo de inundación fiable
Tipos de Áreas
OSPF para IPv6
Paquetes OSPFv3
LSAs OSPFv3
IS-IS: (Intermediate System- Intermediate System)

Equivalencias IS-IS OSPF
IS-IS vs OSPF
Integrated IS-IS PARA IPv6

4. PROTOCOLO EIGRP DE CISCO

EIGRP
Construcción Tablas EIGRP
Métricas
Conceptos Y DEFINICIONES EIGRP
Tabla TOPOLOGÍAS EIGRP
Protocolo DUAL
"Diffusing COMPUTATION"
Tipos de Paquetes EIGRP
Protocolo ENTRE VECINOS
Tabla de vecinos
Tipos de paquetes EIGRP

5. PROTOCOLO EXTERIOR: BGP

Interconexión de sistemas autónomos
Política de métricas
Tipos de sistemas autonomos BGP
Relación Proveedor-Cliente, Igual a Igual
Puntos neutros de Interconexión (IXP)
EBGP e IBGP
Evolución del BG,P
Formatos y Paquetes BGP
Algunos valores atributos Rutas
AS PATH
Problemática AS PATH
NEXT HOP, Local PREF, Community
AS PATH + Community
Atributo MED
Procesos de Routing BGP
Parametros BGP
MultiProtocol BGP4 para IPv6

Objetivos: Mostrar las técnicas y protocolos de routing en IP: RIPv2, OSPF, EIGRP, BGP.

Prerrequisitos: Conocimientos de Internetworking

Metodología: Teórico (70%) – Práctico (30%)..

REDES DE ALMACENAMIENTO: SAN/NAS/DAS

Nivel: MEDIO - Duración: 1 día

1. CENTROS DE DATOS Y ALMACENAMIENTO

Centralización y Consolidación de Datos.
Tecnologías de Almacenamiento
Infraestructura de Cableado.
Sistemas de Almacenamiento: Arquitectura

2. SAN, NAS y DAS

Direct Attached Storage "DAS"
Redes de almacenamiento "NAS" y "SAN"
Soluciones IP y Ethernet
SCSI – iSCSI
Fibre Channel
Componentes. Arquitectura
Topologías
Básicas: PP, BA y SF. Combinadas
Servicios y Operación
Aplicaciones en Sistemas SAN, NAS y DAS
Fibre Channel sobre Internet: iFCP, FCIP
FcoE: FCH over ETHERNET

Arquitectura y Protocolos FcoE
Modelo Enode. Modelo FCF
Data Center Bridging (DCB)
Normativa IEEE para Data Center
Control de flujo por prioridades
Notificación de congestión
Selección de Transmisión
Data Center bridging exchange

Objetivos: Conocer los conceptos básicos y terminología de los Centros de Datos, de los sistemas SAN/NAS y las características de las tecnologías empleadas en la actualidad en este entorno, como Fibre Channel, iSCSI, TCP/IP, IPFC, iFCP, FCIP o Gigabit Ethernet.

Prerrequisitos: Conocimientos básicos de Sistemas

Metodología: Curso teórico.

IMS:

CONVERGENCIA MULTIMEDIA EN REDES FIJAS Y MÓVILES

Nivel: ALTO - Duración: 2 días

1. VISIÓN GENERAL IMS

¿Qué es IMS?
 Convergencia Redes móviles/Fijas
 3GPP LTE/SAE
 Redes "ALL IP"
 Estado actual y evolución
 Estandarización
 Comités de Normalización
 TISPAN, OMA, 3GPPP, IETF, ITU-T
 Mapa de ruta de IMS
 Convergencia TISPAN, 3GPP, 3GPP2"
 Common" IMS

2. ARQUITECTURA

Características Funcionales
 Arquitectura IMS TISPAN y 3GPPP
 Plano de Transporte
 Plano de Control
 Plano de Servicios
 Características, descripción de cada plano
 Funciones y Procedimientos
 Protocolos y operativa
 Elementos Funcionales IMS:
 CSCF: P-CSCF, I-CSCF, S-CSCF
 Gateways, BGCF
 Servidores de Aplicaciones: Tipos
 MRFC
 Descripción, funcionamiento, operativa
 Protocolos: SIP, SDP
 Codecs
 Medios: RTP, RTCP, MSRP
 IMS Network to Network

3. SEGURIDAD

Requerimientos de seguridad
 Características IMS en seguridad
 Modelo de seguridad

Identidades
 Registro
 Inicio de sesiones
 Autenticación y acceso
 Mecanismos de Seguridad

4. EJEMPLO COMPLETO FLUJOS IMS

Caso Práctico

5. INTERWORKING EN IMS

Interworking con PSTN
 Interworking con redes WLAN
 Interworking con redes WWAN
 Soluciones de continuidad
 Continuidad de servicios de voz y de datos
 Movilidad
 Handover sin pérdida de sesión
 Retos

6. ARQUITECTURA DE SERVICIOS EN REDES IMS.

Desarrollo de servicios en IMS
 Presencia, Mensajería
 PoC, Telefonía Multimedia, RCS
 Gestión de políticas: QoS
 Componentes
 Gestión de políticas
 QoS con Acceso por Redes Fijas y Móviles
 Protocolos QoS
 RACS y NASS

Objetivos: Conocer esta arquitectura que permite la entrega de servicios Multimedia IP tanto en redes 3G, 3.5G y LTE como en redes fijas, qué es, qué aporta y cómo funciona IMS.

CLOUD COMPUTING: VIRTUALIZACIÓN EN LA “NUBE”

Nivel: MEDIO - Duración: 2 días

1. SISTEMAS DE CLOUD COMO SERVICIOS

Infraestructura como Servicio – IaaS
 Plataforma como Servicio – PaaS
 Software como Servicio – SaaS
 Ventajas competitivas
 ¿Que es lo que necesito? vs. ¿Que es lo que implemento?
 Implementación Público vs Privado

2. HERRAMIENTAS PARA EL CLOUD

Virtualización completa e híbrida
 Traducción binaria al vuelo
 Dominios lógicos
 Hipervisores, VMM y VMI
 Soporte Hardware para la Virtualización
 Procesadores, Entradas y Salidas, Memoria y DMA
 Virtualización en VMWare
 Intel VT y Vtd y AMD-v

3. INFRAESTRUCTURAS DE VIRTUALIZACIÓN

Maquinas Virtuales
 Discos Virtuales – SAN, iSCSI, NFS y AoE
 Tecnologías de Acceso
 Formatos de disco
 De-duplicación de datos
 Virtual Networking – Virtual Switching
 Módulos Ethernet Virtuales
 Módulos de Seguridad (Soft. vs Appliance)
 Nexus v1000 y Open vSwitch
 Redes lógicas virtuales y VxLAN
 Seguridad VLAN
 Gestión de Redes con Virtualización
 VXLAN y OpenFlow
 Topologías
 Virtualizadores
 VMWare Vsphere, VMWare ESX
 XEN, KVM

4. SOLUCIONES CLOUD IaaS: CLUSTER Y ESCRITORIOS

VMWare Cluster
 Creación de clusters
 Configuraciones de HA (Alta Disponibilidad)
 VDI: virtualización de escritorios
 Problemas de la virtualización de escritorios
 Densidad de escritorios
 Consolidación de escritorios

5. BUENAS PRÁCTICAS

¿Que Virtualizar?, ¿Donde comenzar?
 Estrategias de implementación
 ¿Que fabricantes de virtualización elegir?
 Consideraciones para la gestión
 Control de cambios
 Almacenamiento, recursos y limitaciones
 Consideraciones para el mantenimiento

EJEMPLOS Y DEMOS A LO LARGO DEL CURSO

Eucalyptus, Nimbus, OpenNebula, OpenStack, ESX, Xen, KVM, vSphere, vSwitch, dedup

Objetivos: En el curso se verá que es el Cloud Computing, distinguiendo entre IaaS, PaaS y SaaS, analizando las diferentes herramientas que existen y los diferentes tipos de despliegues que se pueden realizar. Se hará especial hincapié en las herramientas para el Cloud, en la tecnología sobre la que se apoya y en la virtualización, sin la que esta revolución de la computación no puede existir.

Prerrequisitos: Conocimientos básicos de Sistemas

Metodología: Curso teórico.

CÓMO IMPLANTAR SERVICIOS EN CLOUD

ASPECTOS TECNOLÓGICOS, LEGALES Y DE NEGOCIO

Nivel: MEDIO - Duración: 2 días

Este curso versa sobre uno de los aspectos de mayor actualidad y proyección en Internet: el cloud computing o computación en nube y sobre sus implicaciones tecnológicas, de negocio y la práctica legal.

Se analizará desde una dimensión tecnológica, legal y de negocio, sin perder de vista el planteamiento de casos prácticos, tanto europeos como norteamericanos.

1. ¿QUÉ ES LA COMPUTACIÓN EN NUBE?: INTRODUCCIÓN TECNOLÓGICA

La computación en nube en el desarrollo de Internet. Características de la nube. Modelos de servicio. Modelos de implantación. Proyección económica de la computación en nube. La interoperabilidad. Cloud computing y nuevos paradigmas tecnológicos.

2. LA REGULACIÓN DEL CLOUD COMPUTING. PRINCIPALES PROBLEMAS LEGALES

La infraestructura de la nube: calidad de servicio y neutralidad en cloud computing. Cloud y código: riesgos de parcelación de la nube y portabilidad de los datos. Cloud y contenidos: perspectiva general de la regulación legal del cloud. Problemas de jurisdicción aplicable al cloud computing

3. CONTRATACIÓN Y PRIVACIDAD EN EL ENTORNO DEL CLOUD COMPUTING

La contratación de servicios en nube. Contratos de adhesión, términos y condiciones de uso, los acuerdos de nivel de servicio y la capacidad de negociación. Elementos clave en la negociación de esta modalidad de servicios. El estatus jurídico del prestador de servicios en nube, del cliente y del consumidor.

La protección de datos en el entorno de la computación en nube. Los derechos ARCO. La denominada excepción doméstica. La transferencia internacional de datos. El acceso a los datos por autoridades públicas. La resiliencia. Las cláusulas de salida. La nube ante la propuesta de Reglamento Europeo de Protección de Datos.

Objetivos: Proporcionar nociones tecnológicas básicas que permitan conocer a los asistentes los fundamentos del cloud computing, imprescindibles para la ulterior comprensión de los asuntos legales y regulatorios. Estudiar los grandes retos empresariales y de negocio del cloud computing.

Comprender las grandes líneas de problemas regulatorios e iniciativas normativas planteadas por el cloud computing.

Señalar los principales aspectos a tener en cuenta a la hora de negociar este tipo de servicios.

Prerrequisitos: Conocimientos básicos de Sistemas

Metodología: Curso teórico.

EXPERTO EN EVIDENCIAS ELECTRÓNICAS

Nivel: ALTO - **Duración:** 2 días (9:00 a 17:00 horas)

1. MARCO GENERAL Y LÍNEAS

Definiciones
 La triple pareja de servicios de seguridad: Cómo asegurar la confianza en las evidencias de tu organización
 Pasos a seguir desde la información a la evidencia y de la evidencia a la prueba
 Normalización
 Generación, almacenamiento seguro y extracción:
 Sistemas de Gestión de las evidencias electrónicas
 Visión general de metodologías de análisis forense:
 CSIRT - CERTS.
 Análisis de sistemas vivos

2. ASPECTOS LEGALES

El sistema de pruebas y presunciones en España.
 ¿Cómo y qué presentar en un juicio?
 ¿Cómo redactar y presentar un informe pericial?
 Investigación del fraude en las empresas y sus problemas legales

3. HERRAMIENTAS TÉCNICAS

Controles sobre las evidencias electrónicas
 Metodología y procedimientos.
 Los sistemas de ficheros
 Métodos forenses y antiforenses
 Herramientas software y hardware: Adquiere
 Certificaciones hardware y software
 La estación forense
 Construyendo nuestro laboratorio forense

4. ANÁLISIS FORENSE

Network Forensic
 Trabajando en entornos virtuales
 Análisis de imágenes
 Análisis de información, técnicas de reducción
 Análisis temporal y relacional
 Dispositivos móviles:
 Pda
 Teléfonos inteligentes

Objetivos: Analizar, entender y estudiar los requerimientos para establecer un entorno de confiabilidad de las evidencias en formato electrónico. Identificar y gestionar las evidencias que cubran los procesos de los Sistemas de Información, que dan soporte a las actividades esenciales del Negocio, y a los riesgos jurídicos que afectan, de manera directa, a los activos de información en las organizaciones y a la gestión de la seguridad de la información. Analizar el soporte metodológico, técnico y legal, cubriendo el amplio espectro que va desde la evidencia a la prueba, y desde el soporte de las actividades al campo forense. Ser capaz de diseñar controles adaptados a las necesidades de cada organización. Realizar con éxito informes con finalidades tan dispares como: informes internos o periciales ante litigios como parte involucrada o como tercera parte.

DESARROLLO DE APLICACIONES MÓVILES CON HTML5

CURSO PRÁCTICO

Duración: 3 días

Las diferentes plataformas móviles como Android, iOS, Windows 10 y demás suponen un reto a la hora de desarrollar aplicaciones. Cada entorno posee APIs diferentes y formas de desarrollo diferentes.

HTML5 provee una estructura común y abierta para poder desarrollar aplicaciones para las plataformas móviles y entornos de escritorio, reduciendo el Time To Market cuando es necesario desarrollar para múltiples plataformas.

Durante el curso se eliminarán muchos de los mitos sobre el rendimiento de la Plataforma Web y se mostrará como utilizando correctamente el desarrollo HTML5, se puede conseguir el mismo rendimiento que una aplicación nativa con una mayor flexibilidad, facilidad y rapidez utilizando una sola base de código para todas las plataformas.

1. INTRODUCCIÓN

Native vs. HTML5
La WebView: iOS y Android
API Levels y soporte de HTML5
¿Que puedo utilizar?

2. HERRAMIENTAS DE DESARROLLO HTML5

Control del código – Git
Andamiaje – Yeoman
Ejecución de tareas y construcción – Grunt y Gulp
Gestión de Dependencias – Bower

3. TOOLKITS

Acceso a las capacidades nativas – Apache Cordova y PhoneGap
Intel XDK
Actualización de la WebView – CrossWalk

4. JAVASCRIPT Y ECMASCRIPT 6 – TOOLKITS DE DESARROLLO

Introducción a EC6
Patrones MVC: backbone.js, ember.js y Angular JS (1.4/2.0)
WebComponents
Custom Elements
Shadow DOM
HTML Templates
HTML Imports
Polymer y X-Tags

5. HTML5 DEBUGGING

Chrome Dev Tools
Safari Web Inspection Tools
Cross device Mobile Testing
UI Testing

6. HTML5 API

Location
Storage
Patrones de comunicaciones
Comunicaciones asíncronas
WebSockets
Push Messaging
WebRTC
Técnicas Offline First-Service Worker

7. INTERFAZ DE USUARIO

Responsive Design y Adaptative Design (RWD vs AWD)
Preprocesadores CSS y librerías
CSS3 y Animaciones a 60fps
HTML Canvas y SVG
WebGL y Shaders
Rendering Pipeline
UI Toolkits: Netflix Falkor, Facebook React, etc

8. PUBLICACIÓN DE LAS APLICACIONES

CORS
Content Security Policy
Integración nativa con el WebView
Publicación

PRÁCTICAS

Introducción a las herramientas
Construcción de una app usando Yeoman, WebComponents y Apache Cordova
Uso de capacidades nativas: GPS, notificaciones, giroscopio, brújula
Gestión de la cache
Comunicaciones remotas
Publicación

Requerimientos:

Entorno de desarrollo Eclipse, Atom y XCode
Las practicas se desarrollarán bajo Windows/Linux
Los despliegues para iOS se realizarán en modo demo debido a las restricciones de equipamiento.

Conocimientos previos:

Conocimientos de HTML y CSS
Programación en JavaScript
Object Oriented Programming
Conocimientos básicos de Java y ObjectiveC

Objetivos:

Conocer como estructurar, desarrollar y publicar aplicaciones híbridas multiplataforma para los entornos Android e iOS con tecnologías basadas en estándares abiertos de Internet y HTML5.

Dirigido a:

Desarrolladores de aplicaciones móviles, team managers, full stack developers, grupos devops.

FIBRE CHANNEL

Nivel: AVANZADO/EXPERTO - Duración: 1 día

1. FIBRE CHANNEL

- ¿Qué es Fibre Channel?
- Componentes
- Elementos de la Arquitectura
- Posibilidades
- Velocidades
- Estandarización
- Topologías
 - Básicas: PP, BA y SF
 - Combinadas
- Servicios y Operación
- Aplicaciones en sistemas SAN, NAS y DAS
- Arquitectura sobre IP
 - Fundamentos
 - Alternativas
 - Ejemplos de Red
- Fibre Channel sobre Internet
 - iFCP
- Fundamentos de Fibre Channel (FC).
- Arquitectura de FC.
- Topología y tipos de puertos de FC
- FC-0 (interfaces, velocidades (1 Gbps, 2 Gbps, 4 Gbps, 10 Gbps, etc.)
- FC-1 (código 8B/10B, etc.)

- FC-2 (tramado, señalización, tipos de servicio, control de flujo, intercambio, secuencia.)
- FC-3 servicios comunes
- FC-4 redes y canales (SCSI, HIPP, FICON)
- IPv4 e IPv6 sobre FC
- Proyectos en cursos FC
- Switch Fabric - Generation 4

2. FcoE: FIBRE CHANNEL over ETHERNET

- Virtualización en FC
- Arquitectura y Protocolos FcoE
- Modelo Enode
- Modelo FCF
- Enlaces Virtuales
- Aspectos de seguridad

Objetivos: Desarrollar en profundidad la Tecnología Fibre Channel, su arquitectura, posicionamiento, aplicaciones y últimos estándares de FCH sobre Ethernet.

Prerrequisitos: Conocimientos de Ethernet y TCP/IP.

Metodología: Curso teórico/práctico.

ULTRA HIGH PERFORMANCE INTERNET APPLICATIONS

IMPLEMENTACIÓN DE ARQUITECTURAS A GRAN ESCALA (DEVOPS)

Curso: Mañana y Tarde - Duración: 1 día

Con el traslado de los servicios y aplicaciones informáticas a la nube, cada vez es más crítico aumentar la velocidad y la capacidad para escalar todos estos servicios a más usuarios consiguiendo "downtimes" iguales a 0, todo ello con el mínimo coste.

Soportar 10.000 conexiones a la vez ya no es un problema, el problema es conseguir los 10.000.000 de conexiones simultaneas ..

1. Cloud Computing: nuevo paradigma

Del escalado vertical al horizontal

2. Comunicaciones

SDN e IPv6

Quitando el kernel de en medio

Utilizando stacks en espacio de usuario

Cuando el sistema operativo es el problema

Programación directa de red

10G en capa de Aplicación: PF_RING, DNA, NETMAP,

AF_SOCKETS y familia

3. Virtualización:

¿Buena o mala?

Cloud y virtualización: Ventajas y problemas

Hipervisores y red: Aumento del rendimiento

Cloud Orchestration

Virtualización más ligera: reduciendo el stack con Cloudius

osV, Capstan, Docker, etc.

4. Aplicaciones Web

REST y el ascenso de las WebApps

Porque cloud computing significa web

El navegador como plataforma

Medición y análisis de la latencia en las aplicaciones web:

Entorno PC y Móvil

Reducción de latencia en el stack y en el HTTP

Técnicas de reducción en HTTP 1.1 y el futuro

HTTP 2.0 (SPDY, QUIC, WS)

5. Aplicaciones Web: Programación

Programación sin estado, asíncrona

NodeJS, Scala, Python y otros derivados

Programación asíncrona de forma nativa

La programación funcional como paradigma

Reinicio de servicios sin downtime

Como HTML5 hace que parezca que nos hemos descargado Internet

Coloquio

Objetivos:

Revisar todo el stack de computación, desde que el paquete pasa por la red, hasta que los datos se le presentan al usuario, buscando el aumento del rendimiento de la aplicación..

Metodología:

Durante la Jornada se presentará una aplicación desarrollada con el modelo tradicional, y se analizará el rendimiento a medida que se aplica cada una de las nuevas técnicas, manteniendo la misma configuración de hardware

Ponente: Sean McCarthy

Socio-Director de Integra

REGULACIÓN Y SERVICIOS DE LAS TELECOMUNICACIONES EN ESPAÑA

Curso: Mañana - Duración: 2 días

Las redes de telecomunicaciones son esenciales en nuestra vida y todos estamos conectados a ellas, teniendo que tomar permanentemente decisiones para la elección de servicios y operadoras.

Pero, ¿conocemos bien qué son, quienes son los actores, como están regulados, cual es la cadena de valor y cómo evolucionan?

La nueva «Ley de Telecomunicaciones» aprobada el 9 de mayo pretende: "...facilitar el despliegue de redes de nueva generación tanto en telefonía móvil como fija y el fomento de las inversiones hasta alcanzar unos 25.000 millones..".

¿Como nos afecta como usuarios y como parte del mercado?

¿Conseguirá reactivar el mercado e incrementar el PIB, como promete?.

1. La regulación. Conceptos básicos

¿Por qué se regula el mercado?, ¿Qué son los análisis de Mercado?. Concepto de escalera de inversión. ¿Qué es un agente con poder significativo?. Precios de interconexión regulados. Acceso a recursos escasos o de difícil replica. Los análisis de mercado que se han realizado y las conclusiones a las que se ha llegado.

La escalera de inversión. Reventa, Acceso indirecto, Acceso directo, Infraestructura propia. ¿Qué significa y ejemplos en cada paso?

2. La Regulación en España

El papel de la CNMC.

La regulación Europea ¿Cómo afecta a España?

La integración de la Comisión de defensa de la competencia y los reguladores de mercados, en el caso que nos ocupa la CMT. ¿Qué implica?

La precedencia de la regulación europea. Casos, roaming. Sentencias, multas.

3. La Ley General de Telecomunicaciones

La evolución de los objetivos de las distintas Leyes de Telecomunicación en España.

¿Qué Impacto puede tener esta nueva ley en el mercado?

Será capaz de generar empleo e inversión.

Será capaz de movilizar el sector.

¿Cómo afectará a las redes municipales y a las iniciativas autonómicas?

4. Impacto de los servicios regulados en el mercado

¿Puede la regulación afectar a la manera que se construyen los servicios?

Mediante los servicios de voz (interconexión por capacidad)

Mediante los servicios de datos (OBA)

La OIR. El factor diferencial español "la interconexión por capacidad". ¿En que ha afectado?

OBA, oferta de acceso al bucle de abonado. ¿Por qué contiene servicios que no son de bucle?

5. Servicios Mayoristas

Servicios fijos

Acceso directo (ULL)

Acceso indirecto (ADSL IP)

NEBA – MARCO - AMLT – ORLA - OIR

Se explicará y posicionara cada uno de ellos en la escalera de inversión.

Servicios Móviles

OMV Tipos que hay y por qué se desarrollan.

6. Servicios Minoristas

Residencial

Voz, Datos, TV. Conceptos de Dual Play y Triple Play.

Móvil (voz y datos)

Empaquetamiento de servicios, fijo mas móvil.

Las tarifas planas de voz, los servicios de tarificación adicional. ¿Por qué se asocia siempre la Banda Ancha (Datos) a tarifas planas de voz?

La TV sobre la Banda Ancha.

La voz en el móvil . Los datos, los paquetes de datos, las tarifas planas, el roaming.

¿Por qué se empaquetan servicios?

Empresas

Servicios de Datos. MPLS, Ethernet.

Servicios de Voz. Voz sobre IP, Centralitas Virtuales.

Servicios Móviles. M2M, MDM. Cloud

Los servicios de datos para empresas, interconexión de sedes en MPLS o en Ethernet. Separación entre acceso y transporte.

Servicios de voz, conceptos de red privada virtual (numeración corta sin tarificación interna). Integración fijo-móvil. La VoIP, en que casos es útil. Centralitas, gestión, centralitas virtuales de red.

M2M utilidad para las empresas, ejemplos. Flotas, almacenes, etc. MDM . Gestión de dispositivos móviles. La importancia para las empresas.

Los servicios en la nube. "Un subproducto de Google y Amazon".

12. Asesorías

OPTIMIZACIÓN DE SERVIDORES, VIRTUALIZACIÓN Y COMUNICACIONES

CONFIGURACIÓN Y AJUSTE DE PARÁMETROS DEL KERNEL LINUX Y RED TCP/IP

Curso: Mañana - Duración: 3 días

Con el uso intensivo de aplicaciones multimedia y el crecimiento exponencial del tráfico de voz es más crítico aumentar el rendimiento y la capacidad, tanto de los servidores como de la Red, para escalar estos servicios a más usuarios con el mismo coste y mantenimiento la calidad.

1. Arquitectura x64

- La arquitectura x64 es rápida, muy rápida
- Análisis de instrucciones y paralelización
- Gestión y Análisis de Memoria
- Paginación y Jerarquías de Cache y Memoria
- Sincronización y Coherencia
- Latencias y Ancho de Banda
- Buses de Datos
- Gestión para IO Eficiente
- Cuellos de botella
- Entornos de operación IPv4, IPv6 y SDN
- Data Plane vs Control Plane
- Optimizaciones a Nivel de Red
- Optimizaciones a nivel de Transporte y Aplicación
- Aplicaciones de Alta Velocidad
- Scalability vs Performance vs Throughput
- Flujo de datos
- Gestión del Plano de Datos
- NICs y TCP/IP

2. Optimización del kernel de Linux

- Funcionamiento del kernel
- Manejo de interrupciones
- Zero Copy
- Proceso de medición y ejemplos
- Observability
- Benchmarking
- Tuning
- Herramientas
- Linux Kernel Tunables y ejemplos
- Sistema de archivos
- Memoria, Procesador, Red
- Cuando el sistema operativo es el problema
- Programación directa de red
- Utilizando stacks TCP/IP en espacio de usuario
- 10G en capa de Aplicación
- Programación
- Estructuras de control y compresión de datos

- Threading
- Bloqueos y secciones críticas
- Atomic operations
- Lock Free Structures
- AsyncIO
- epoll
- Eliminación de Side-Effects
- Programación funcional: Java, Scala, Erlang

3. Análisis y Optimización del TCP/IP

- Análisis de Traces: Metodología
- Dónde, qué y cómo medir
- Tráficos de Nivel IP, Ajustes
- Detección y Aislamiento de Problemas
- Análisis I/O avanzado
- Identificación de comportamientos anómalos
- Optimización del TCP
- Protocolos TCP y UDP: Características
- Detección, identificación y resolución de problemas
- Análisis del protocolo TCP
- Gestión de ventanas y de buffers
- Mecanismo "Sliding Window"
- Control de congestión en TCP/IP
- Slow Start, Congestion Avoidance y Fast Retransmit
- Operación del TCP sobre "long, fat pipes"
- Llenado de ventana
- Problemática de la reordenación de segmentos
- Extensiones del TCP
- Windows Scale Option, SACK, RTTM
- Casos y Ejercicios Prácticos
- Ajustes y Transferencias TCP
- Análisis gráfico de rendimientos
- Rendimiento de la transmisión
- Rendimiento de servidores y aplicaciones
- Situaciones de congestión

Objetivos: Revisar en detalle todos los elementos involucrados, desde los servidores a la Red, buscando la optimización combinada de todo el sistema.

CERTIFICADOS

OBJETIVOS:

Estos PROGRAMAS DE CERTIFICACIÓN proporcionan un nivel “práctico” de formación en Tecnologías e Infraestructuras de Red. Ofreciéndole la posibilidad de presentarse al examen de certificación y obtener el certificado acreditativo correspondiente.

Los certificados, actualmente disponibles son:

- 1. CCTT de Cobre de Fluke Networks**
- 2. CCTT de Fibra de Fluke Networks**

DURACIÓN Y HORARIO:

Estos cursos tienen una duración de un día para cada CCTT.

DIRIGIDO A:

- Todos aquellos profesionales que deseen conocer en detalle las infraestructuras físicas (cobre y fibra óptica) y los elementos activos de internetworking (puentes, switches y routers).
- Ingenieros, arquitectos, instaladores, contratistas, inspectores, directores de instalación, administradores de red, técnicos de telecomunicaciones, personal de ventas y marketing y particulares que desarrollen su carrera profesional en entorno de las Tecnologías de la Información y las Comunicaciones.
- Todos los profesionales que estén trabajando en el área de la seguridad y quieran fijar y ampliar todos los elementos que conforman la seguridad en Redes y Sistemas TCP/IP.
- Todos aquellos que necesiten iniciarse en las comunicaciones de datos y diseñar sistemas de red, representantes de ventas y marketing, técnicos e instaladores y todos los interesados en conocer las funciones de las redes y su impacto en las Tecnologías de la Información y las Comunicaciones.
- Todos aquellos que necesiten iniciarse en las instalaciones de las redes celulares inalámbricas, jefes de proyecto de comunicaciones y aquellos interesados en el impacto y diseño de sistemas inalámbricos.
- Instaladores y Técnicos de redes corporativas que actualmente disponen de Analizadores DTX para cobre y Fibra (CCTT)

CERTIFICADOS OFICIALES CCTT DE FLUKE

Certificados CCTT en Cobre y Fibra para Versiv

Duración: 2 días - De 9:00 a 18:00 horas



La mayoría de fabricantes de Cableado exigen una Certificación correcta para que sea válida la garantía de todos los componentes de la instalación. Es por ello necesario obtener el certificado CCTT, cuyo periodo de vigencia viene limitado por Fluke Networks a dos años. Como empresa de formación oficial del CCTT de Fluke Networks ofrecemos los siguientes cursos para obtener o actualizar la Certificación:

Programa Cobre

- Introducción
- Límites de test en cobre/estándares
- Tipos de adaptadores
- Configuración del test, mediciones
- Nuevas medidas (Resist Unbalance, TCL)
- Diagnósticos del DSX: HDTDx, HDTDR
- Medidas, exportación, latiguillos,...
- Medición en campo de Alien Crosstalk
- Examen Final

Programa Fibra

- Fundamentos de Fibra Óptica
- Encircled flux
- Configuración del CertiFiber Pro
- Inspección de Fibra
- Medidas: ISO/IEC 14763-3, Referencia,
- Límites personalizados, enlaces simplex
- OTDR: Teoría, eventos, compensación,...
- OptiFiber Pro: Medidas, análisis, bidirecc.
- Examen Final



Formación “a Medida” e “in-Company”

¡Usted merece estar con los mejores!
22 años formando a más de 22.000 profesionales - 1.600 cursos impartidos

**Formación independiente de productos y servicios en
Tecnologías de la Información y las Comunicaciones**

Somos conscientes de que el conocimiento de las Tecnologías de la Información y las Comunicaciones (TICs), además de ser clave para el desarrollo de los profesionales, es un factor decisivo para ahorrar tiempo y dinero. Dicho ahorro se obtiene mediante la mejora en la resolución de problemas, la optimización de los recursos y la correcta toma de decisiones al realizar nuevas inversiones. Todo ello exige una formación de la máxima calidad y adecuada a su empresa. Con nuestra reconocida calidad y 23 años de experiencia nos ponemos a su disposición para ofrecerle la mejor formación, a un coste competitivo y con gran flexibilidad.

Somos expertos en ofrecer soluciones que permiten disminuir sus costes combinando la formación “In-Company” y nuestros cursos de calendario. Nos adaptamos, en función de sus necesidades, para conseguir el resultado más rentable y eficaz, incluso desarrollando, a través de nuestros expertos nuevas materias y temarios. De esta manera, la formación se adecua a los objetivos y características de su empresa y al perfil de los asistentes. Ayudamos a los departamentos de RR.HH., ofreciendo la formación que buscan, de forma que con nuestra decidida colaboración logren su objetivo de mejorar el talento de los profesionales de la empresa.

Estamos a su disposición para resolver sus dudas, ampliar esta información o estudiar sus necesidades.

Al considerar sus necesidades de formación, tenga en cuenta que disponemos de la oferta más completa y rigurosa del mercado.

- Nuestro conjunto de Cursos es único en el mundo, tanto por su amplitud -más de 700 horas de formación- como por la profundidad y amenidad con que son tratados los temas.
- Contamos con una amplia bibliografía que permite a los participantes de nuestros cursos estudiar y ampliar conocimientos de forma individual, después del curso.
- Todos Nuestros Ponentes son profesionales del máximo nivel, con amplia experiencia práctica (de 10 a 30 años), total independencia de criterios, y autores de los cursos que explican.
- El objetivo de todos nuestros cursos es enseñar a los asistentes como utilizar de la manera más eficiente las distintas tecnologías de comunicaciones, para mejorar rendimiento, reduciendo costes, tanto operativos como de inversiones.
- El valor diferenciador de nuestra formación reside en las experiencias y opiniones de los ponentes, basadas en su conocimiento, que enriquecen la enseñanza impartida.
- Nos adaptamos a sus necesidades presupuestarias, buscando siempre la mejor relación calidad/precio.

Otros servicios de formación

ENCICLOPEDIA VIRTUAL

¡¡ Servicio gratuito para nuestros alumnos !!

Este servicio “on-line” tiene como objetivo ofrecer información fiable y de calidad sobre tecnologías, productos y servicios de comunicaciones, de manera que los asistentes a nuestros cursos puedan posteriormente y de manera independiente ampliar conocimientos sobre los temas tratados. Más de 20.000 hiperenlaces organizados según nuestras áreas de formación. Acceso a través de nuestra web: www.lmdata.es/evc.htm

AUTOEVALUACIÓN

¡¡ Servicio gratuito!!

El objetivo de nuestra aula virtual para autoevaluación es poner en sus manos una herramienta “on-line” que le permitirá evaluar su nivel de conocimientos en las tecnologías de Redes de Comunicaciones y Telecomunicaciones, a través de varios test con distintos niveles de dificultad y finalmente le asesora sobre las materias que necesita profundizar.

¡Anímese y descubra su nivel de conocimientos en comunicaciones de datos!

Disponible en nuestra web: www.lmdata.es/aulav.htm

PLANES DE FORMACIÓN

¡¡ Servicio gratuito!!

Herramienta “on-line” que en función del perfil profesional de cada persona, experiencia y área de actividad de la empresa, genera un plan completo de desarrollo de competencias en el área de las Redes de Comunicaciones y Telecomunicaciones. Disponible en nuestra web: www.lmdata.es/plan.htm



Documentación de Cursos

Si usted está interesado en nuestros cursos, pero por cualquier razón no puede asistir, le ofrecemos la oportunidad de adquirir la documentación de cada uno de ellos.

¡¡ No pierda más tiempo y dinero buscando Información, nosotros le ofrecemos la más completa y rigurosa con nuestra garantía de calidad !!

Redes y Equipos de Comunicaciones	
<i>_ Redes y Equipos de Comunicaciones</i>	190 € + IVA
Infraestructuras de Comunicaciones	
<i>_ Experto en Tecnologías VoIP y SIP</i>	190 € + IVA
<i>_ IPv6 Avanzado</i>	190 € + IVA
<i>_ Smart Grid y Telecontrol IEC61850</i>	190 € + IVA
<i>_ Sistemas de Cableado en Cobre y Fibra</i>	190 € + IVA
<i>_ Nuevos Servicios Ethernet (NEBA)</i>	190 € + IVA
<i>_ Bridging, Routing, Switching y VLANs</i>	190 € + IVA
Seguridad en Redes TCP/IP	
<i>_ Experto de Seguridad en Redes TCP/IP</i>	190 € + IVA
<i>_ Ataque y Defensa en Redes IP</i>	190 € + IVA
<i>_ Sistemas Firewalls</i>	190 € + IVA
<i>_ Protocolos de Autenticación</i>	190 € + IVA
<i>_ Certificación Digital y PKIs</i>	190 € + IVA
Seguridad en Sistemas TCP/IP	
<i>_ Mantenimiento de la seguridad en la web</i>	190 € + IVA
<i>_ Seguridad en redes Sociales</i>	190 € + IVA
<i>_ Indicadores y Métricas: Cuadro de Mandos</i>	190 € + IVA
<i>_ Continuidad y Planes de Contingencia</i>	190 € + IVA
Análisis y Gestión de Redes	
<i>_ Network Troubleshooting con WireShark</i>	190 € + IVA
<i>_ Troubleshooting y Optimización Wi-Fi</i>	190 € + IVA
<i>_ Protocolos SNMP</i>	190 € + IVA
<i>_ Metodología de Gestión</i>	190 € + IVA
Otros Cursos	
<i>_ MPLS, GMPLS y VPLS</i>	190 € + IVA
<i>_ Redes de Acceso: xDSL, FTTH y MetroEthernet</i>	190 € + IVA
<i>_ Redes Ópticas y de Transporte: OTNs</i>	190 € + IVA
<i>_ Routing en Redes IP (v4/v6): RIP, IS-IS, OSPF, EIGRP, BGP</i>	190 € + IVA
<i>_ Centros de Datos y Redes de almacenamiento SAN/NAS</i>	190 € + IVA
<i>_ IMS: Convergencia multimedia en redes fijas y móviles</i>	190 € + IVA
<i>_ Redes Móviles 3,5 G y LTE</i>	190 € + IVA
<i>_ Movilidad IP en Redes 3,5 G y LTE</i>	190 € + IVA
<i>_ Wi-Fi y WiMax</i>	190 € + IVA
<i>_ Seguridad Wi-Fi/WiMax</i>	190 € + IVA
<i>_ Cloud Computing y Virtualización</i>	190 € + IVA
<i>_ Experto en Evidencias Electronicas</i>	190 € + IVA

SOLICITUD DE DOCUMENTACIÓN: (www.LMdata.es/public.htm)

Envíe este Boletín marcando la Documentación que desee recibir

Adjunto talón o transferencia (soliciten datos) a nombre de L&M Data Communications

Tarjeta (Visa American Express)

Nombre (como figura en la tarjeta):- _____

Nº _____

Caducidad _____

