959 830 780 / 640 798 742

info@inafe.es

MF0230_3 ADMINISTRACIÓN DE REDES TELEMÁTICAS (ONLINE)

350,00 € - 425,00 €

Este curso se ajusta a lo expuesto en el itinerario de aprendizaje perteneciente al Módulo Formativo MF0230_3 Administración de redes telemáticas, regulado por el Real Decreto 1531/2011, de 31 de diciembre, que permitirá al alumnado adquirir las competencias profesionales necesarias administrar la infraestructura de red telemática.

Categorías: Informática y Comunicaciones |

INFORMACIÓN

Duración	210 h
Modalidad	Online
Docencia	TUTOR PERSONAL
Prácticas	GESTIÓN DE PRÁCTICAS EN EMPRESAS
Método de pago	FINANCIACIÓN SIN INTERESES
Centro de empleo	AGENCIA DE COLOCACIÓN
Formación acreditada	CENTRO ACREDITADO POR EL SEPE
Precio	Particular, Empresa

DESCRIPCIÓN DEL PRODUCTO

MÓDULO 1. ADMINISTRACIÓN DE REDES TELEMÁTICAS

UNIDAD FORMATIVA 1. EQUIPOS DE INTERCONEXIÓN Y SERVICIOS DE RED

UNIDAD DIDÁCTICA 1. PROTOCOLO TCP/IP.

1. Arquitectura TCP/IP. Descripción y funciones de los distintos niveles:
2. - Nivel físico.
3. - Nivel de acceso a la red.
4. - Nivel de Internet.
5. - Nivel de transporte.
6. - Nivel de aplicaciones.
7. Análisis de la transmisión de datos: encapsulación y desencapsulación.
8. Correspondencia entre el modelo de referencia para la interconexión de sistemas abiertos (OSI) y la arquitectura TCP/IP.
9. Definición de red IP.
10. Ejemplificación de implementaciones de redes TCP/IP demostrativa de la gran variedad de las mismas.
11. Descripción y caracterización el protocolo IP: sin conexión, no confiable.
12. Análisis del formato del datagrama IP.

13. Descripción y caracterización el protocolo TCP: orientado a conexión, confiable.
14. Análisis del formato del segmento TCP.
15. Enumeración y ejemplificación de los distintos niveles de direccionamiento: direcciones físicas, direcciones lógicas, puertos, específicas de la aplicación (URL, email).
16. Análisis del direccionamiento IPv4.
17. - Estructura de una dirección IP.
18. - Clases de direcciones IP.
19. - Máscaras.
20. - Notaciones.
21. - Direcciones públicas y privadas.
22. - Direcciones reservadas y restringidas.
23. - Problemática del direccionamiento y subredes.
24. - Máscaras de subred de longitud variable (VLSM).
25. Mención de IPv6 como evolución de IPv4.
26. Explicación del uso de puertos y sockets como mecanismo de multiplexación.
27. Descripción y funcionamiento del protocolo de resolución de direcciones físicas ARP.
28. - Explicación de su objetivo y funcionamiento.
29. - Tipos de mensajes ARP.
30. - Tabla ARP.
31. - Protocolo de resolución de direcciones inverso (RARP) y BOOTP.
32. - Ejemplificación de comandos ARP en sistemas Windows y Linux.
33. Descripción y funcionamiento de ICMP.
34. - Explicación de sus objetivos.
35. - Tipos de mensajes ICMP.
36. - Ejemplificación de comandos ICMP en sistemas Windows y Linux.
37. Descripción y funcionamiento del protocolo de traducción de direcciones de red (NAT).
38. - Explicación de sus objetivos y funcionamiento.
39. - Ejemplificación de escenarios de uso de NAT.
40. - Tipos de NAT: estático y dinámico.
41. - NAT inverso o de destino (DNAT).
42. - Traducción de direcciones de puerto (PAT).
43. - Ejemplificación de configuración NAT en sistemas Linux con iptables.
44. - Descripción y usos de UDP.
45. - Comparación entre UDP y TCP.
46. - Descripción breve y función de algunos protocolos de nivel de aplicación: SNMP, DNS, NTP, BGP, Telnet, FTP, TFTP, SMTP, HTTP y NFS.

UNIDAD DIDÁCTICA 2. SERVICIOS DE NIVEL DE APLICACIÓN.

1. Análisis del protocolo servicio de nombres de dominio (DNS).
2. - Ejemplificación de los distintos niveles de direccionamiento: direcciones físicas, direcciones lógicas, puertos, específicas de la aplicación (URL, email).
3. - Necesidad, objetivos y características de DNS.
4. - Descripción de la estructura jerárquica de DNS.
5. - Tipos de servidores: primario, secundario y cache.
6. - Explicación de la delegación de autoridad. Subdominios.
7. - Enumeración de los tipos de registros SOA, NS, A, CNAME y MX.
8. - Ejemplificación del proceso de resolución de nombres.
9. - Descripción y elementos de la arquitectura cliente/servidor de DNS.
10. - Resolución inversa (reverse DNS lookup) .
11. - Ejemplificación de comandos DNS en sistemas Windows y Linux.
12. Implementación del servicio de nombres de dominio (DNS).
13. - Desarrollo de un supuesto práctico donde se muestre la instalación y configuración de un servidor DNS en un sistema Linux utilizando BIND (Berkeley Internet Name Domain), creando un ámbito y configurando rangos de direcciones y de reservas.
14. - Configuración de equipos clientes para la resolución de nombres.
15. Descripción y funcionamiento del protocolo de configuración dinámica de hosts (DHCP).
16. - Objetivos y funcionamiento.
17. - Descripción y elementos de la arquitectura cliente/servidor de DHCP.
18. - Descripción de los métodos de asignación de direcciones IP: estática, automática y dinámica.
19. - Conceptos de rangos, exclusiones, concesiones y reservas..
20. - Enumeración de los parámetros configurables por DHCP.
21. - Ejemplificación del proceso de asignación de configuración con DHCP.
22. - Comparación entre los protocolos DHCP y BOOTP.
23. Implementación del protocolo de configuración dinámica de hosts (DHCP).
24. - Instalación de un servidor DNS en un sistema Linux .
25. - Desarrollo de un supuesto práctico donde se muestre la instalación y configuración de un servidor DNS en un sistema Windows.
26. - Desarrollo de un supuesto práctico donde se muestre la instalación y configuración de un servidor DNS en un sistema Windows, incluyendo DNS Dinámico y el servicio DHCP para DNS.
27. - Configuración de equipos clientes DHCP.
28. Descripción y funcionamiento de un servidor proxy.
29. - Explicación del concepto genérico de proxy.
30. - Análisis de las ventajas e inconvenientes del uso de servidores proxy.

31. - Concepto de proxy transparente.
32. - Descripción y funcionamiento de un servidor proxy caché de web.
33. - Proxy inverso.
34. - Enumeración de servidores proxy para otros servicios: NAT, SMTP, FTP.
35. - Comparación de modo de funcionamiento y prestaciones entre un servidor proxy y un cortafuegos.
36. - Identificación y comparación de servidores proxy comerciales y de código abierto, destacando si ofrecen servicios de cortafuegos, NAT o caché.
37. Implementación de un servicio proxy.
38. - Desarrollo de un supuesto práctico donde se muestre la instalación de un proxy cache, configurando las distintas opciones: NAT, caché, cortafuegos.

UNIDAD DIDÁCTICA 3. CONFIGURACIÓN DE EQUIPOS DE INTERCONEXIÓN.

1. Repetidores (Hubs).
2. - Análisis de su influencia en los dominios de colisión y de broadcast.
3. - Enumeración de distintos usos.
4. Explicación de la técnica de segmentación y de sus ventajas.
5. Puentes (Bridges).
6. - Análisis de su influencia en los dominios de colisión y de broadcast.
7. - Enumeración de distintos usos .
8. - Ejemplificación de puentes interconectando redes 802.x iguales y/o distintas.
9. - Caracterización de un puente transparente y descripción del protocolo Spanning Tree.
10. - Caracterización de un puente remoto
11. Conmutadores (Switches).
12. - Análisis de su influencia en los dominios de colisión y de broadcast.
13. - Comparación de distintos tipos de conmutación: Cut-Through, Store-and-Forward y Fragment-free Switching..
14. - Comparación entre conmutadores y puentes.
15. - Mención a la conmutación de nivel 3 y 4.
16. - Enumeración de distintos usos .
17. Redes de área local virtuales (VLAN).
18. - Explicación del concepto y funcionamiento.
19. - Concepto de VLAN trunking.
20. - Análisis de su influencia en los dominios de colisión y de broadcast.
21. - Analizar las ventajas del uso de VLAN.
22. - Descripción y comparación de VLAN estáticas y dinámicas.
23. - Descripción y comparación de las técnicas de definición de VLANs agrupación de puertos y

agrupación de MACs.
24. - Descripción de la agregación de enlaces (Link trunk) y del etiquetado.
25. - Enumeración de distintos usos recomendados y no recomendados.
26. Puntos de acceso inalámbrico.
27. - Identificación y comparación de distintos estándares 802.11.
28. - Descripción y comparación de los modos de funcionamiento infraestructura y ad-hoc.
29. - Identificación y descripción de los principales riesgos de seguridad.
30. - Explicación de tecnologías y recomendaciones de buenas prácticas de seguridad en redes WiFi.
31. Desarrollo de un supuesto práctico donde se pongan de manifiesto.
32. - Distintas formas de conexión al conmutador para su configuración..
33. - Las técnicas de definición de VLANs por agrupación de puertos (en uno o varios conmutadores) y agrupación de MACs.
34. - Encaminadores (Routers).
35. - Ejemplificación de protocolos enrutables y no enrutables.
36. - Análisis de su influencia en los dominios de colisión y de broadcast.
37. - Estructura de la tabla de encaminamiento.
38. - Comparación de distintos modos de construcción de las tablas de encaminamiento: Hardware state, estáticas y dinámicas.
39. - Analizar las ventajas y limitaciones del encaminamiento estático.
40. - Descripción de CIDR como mejora en el manejo de direcciones IP.
41. - Comparación entre las dos técnicas básicas de encaminamiento: vector de distancia y estado del enlace.
42. - Definición de distancia administrativa, métrica y convergencia.
43. - Enumeración de los objetivos de los protocolos de encaminamiento.
44. - Descripción de las características y comparación de los tipos interior y exterior de protocolos de encaminamiento.
45. - Explicación de características y criterios de utilización de distintos protocolos de encaminamiento: RIP, IGRP, EIGRP, OSPF, BGP.
46. - Explicación de los conceptos unicast, broadcast y multicast.
47. - Instalación y configuración de un encaminador sobre un sistema Linux utilizando un producto software de código abierto.
48. - Descripción de las ventajas y desventajas de utilizar un router software frente a un router hardware.
49. Desarrollo de un supuesto práctico debidamente caracterizado donde se muestren las siguientes técnicas básicas de configuración y administración de encaminadores:
50. - Distintas formas de conexión al encaminador para su configuración inicial.

51. - Configuración del enrutamiento estático y ruta por defecto.
52. - Definición de listas de control de acceso (ACL).
53. - Establecimiento de la configuración de DHCP, si el router lo permite.

UNIDAD FORMATIVA 2. GESTIÓN DE REDES TELEMÁTICAS

UNIDAD DIDÁCTICA 1. CICLO DE VIDA DE LA REDES.

1. Explicación del ciclo de vida de una red usando el modelo PDIOO como referencia.
2. Descripción de las tareas y objetivos de las distintas fases.
3. - Planificar.
4. - Diseñar.
5. - Implementar.
6. - Operar.
7. - Optimizar.

UNIDAD DIDÁCTICA 2. ADMINISTRACIÓN DE REDES.

1. Explicación del concepto de administración de redes como el conjunto de las fases operar y optimizar del modelo PDIOO.
2. Recomendaciones básicas de buenas prácticas.
3. - Mantener una organización (NOC) responsabilizada con la administración de la red.
4. - Monitorizar la red para garantizar niveles de servicio en el presente y el futuro.
5. - Controlar, analizar, probar y registrar cambios en la red.
6. - Mantener y velar por la seguridad de la red.
7. - Mantener un registro de incidentes y solicitudes.
8. Visión general y procesos comprendidos.
9. - Gestión de la configuración..
10. - Gestión de la disponibilidad.
11. - Gestión de la capacidad.
12. - Gestión de seguridad.
13. - Gestión de incidencias.
14. El centro de operaciones de red.
15. - Explicación de sus funciones.
16. Gestión de la configuración.
17. - Explicación de los objetivos.
18. - Enumeración de las actividades.
19. - Identificación y comparación de herramienta comerciales y de código abierto.

20. Gestión de la disponibilidad.
21. - Explicación de los objetivos.
22. - Enumeración de las actividades.
23. Gestión de la capacidad.
24. - Explicación de los objetivos.
25. - Enumeración de las actividades.
26. Gestión de la seguridad.
27. - Caracterización de la seguridad de la información como la garantía de su disponibilidad, integridad y confidencialidad.
28. - Explicación de los objetivos de la gestión de la seguridad.
29. - Referencia y explicación de los objetivos de control incluidos en el control 10.6 de la norma ISO27002.
30. - Enumeración de las actividades.
31. - Recomendaciones básicas de buenas prácticas.
32. - Sistemas de detección de intrusiones NIDS (Nessus, SNORT).
33. - Identificación y comparación de herramienta comerciales y de código abierto.
34. Gestión de incidencias.
35. - Explicación de los objetivos.
36. - Enumeración de las actividades.

UNIDAD DIDÁCTICA 3. PROTOCOLOS DE GESTIÓN DE RED.

1. Explicación del marco conceptual.
2. - Entidades que participan en la gestión.
3. - Estructuras de datos utilizadas.
4. - Protocolos de comunicación.
5. Componentes de la infraestructura y arquitectura.
6. - Entidad gestora.
7. - Dispositivos gestionados.
8. - Protocolos de gestión.
9. Grupos de estándares.
10. - CMISE/CMIP de OSI.
11. - SNMP de TCP/IP.

UNIDAD DIDÁCTICA 4. ANÁLISIS DEL PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP).

1. Objetivos y características de SNMP.

2. Descripción de la arquitectura.
3. - Dispositivos administrados.
4. - Agentes.
5. - Sistema de administración.
6. Comandos básicos.
7. - Lectura.
8. - Escritura.
9. - Notificación.
10. - Operaciones transversales.
11. Base de información de administración (MIB).
12. - Explicación del concepto.
13. - Organización jerárquica.
14. Explicación del concepto de TRAP.
15. Comparación de las versiones.
16. Ejemplificación de usos.

UNIDAD DIDÁCTICA 5. ANÁLISIS DE LA ESPECIFICACIÓN DE MONITORIZACIÓN REMOTA DE RED (RMON).

1. Explicación de las limitaciones de SNMP y de la necesidad de monitorización remota en redes.
2. Caracterización de RMON.
3. Explicación de las ventajas aportadas.
4. Descripción de la arquitectura cliente servidor en la que opera.
5. Comparación de las versiones indicando las capas del modelo TCP/IP en las que opera cada una.
6. Ejemplificación de usos.

UNIDAD DIDÁCTICA 6. MONITORIZACIÓN DE REDES.

1. Clasificación y ejemplificación de los tipos de herramientas de monitorización.
2. - Diagnóstico.
3. - Monitorización activa de la disponibilidad: SNMP.
4. - Monitorización pasiva de la disponibilidad: NetFlow y Nagios:
5. - Monitorización del rendimiento: cricket, mrtg, cacti.
6. Criterios de identificación de los servicios a monitorizar.
7. Criterios de planificar los procedimientos de monitorización para que tengan la menor incidencia en el funcionamiento de la red.
8. Protocolos de administración de red.
9. Ejemplificación y comparación de herramienta comerciales y de código abierto.

UNIDAD DIDÁCTICA 7. ANÁLISIS DEL RENDIMIENTO DE REDES.

1. Planificación del análisis del rendimiento.
2. - Propósito.
3. - Destinatarios de la información.
4. - Alcance.
5. Indicadores y métricas.
6. - Explicación de los conceptos.
7. Identificación de indicadores de rendimiento de la red .
8. - Capacidad nominal y efectiva del canal.
9. - Utilización del canal.
10. - Retardo de extremo a extremo.
11. - Dispersión del retardo (jitter).
12. - Pérdida de paquetes y errores.
13. Identificación de indicadores de rendimiento de sistemas.
14. - Disponibilidad.
15. - Memoria, utilización y carga de CPU.
16. - Utilización de dispositivos de entrada/salida.
17. Identificación de indicadores de rendimiento de servicios.
18. - Disponibilidad.
19. - Tiempo de respuesta.
20. - Carga.
21. Ejemplos de mediciones.
22. Análisis de tendencias y medidas correctivas.
23. Desarrollo de un supuesto práctico donde se muestren.
24. - El empleo de los perfiles de tráfico y utilización de la red para determinar como va a evolucionar su uso.
25. - El análisis de los resultados obtenidos por la monitorización con el fin de proponer modificaciones.

UNIDAD DIDÁCTICA 8. MANTENIMIENTO PREVENTIVO.

1. Definición y objetivos de mantenimiento preventivo.
2. Gestión de paradas de mantenimiento.
3. - Periodicidad.
4. - Análisis de la necesidad.
5. - Planificación y acuerdo de ventanas de mantenimiento.
6. - Informes de realización.

7. Explicación de la relación entre el mantenimiento preventivo y los planes de calidad.
8. Ejemplificación de operaciones de mantenimiento indicadas en las especificaciones del fabricante de distintos tipos de dispositivos de comunicaciones.
9. El firmware de los dispositivos de comunicaciones.
10. - Definición del concepto de firmware.
11. - Explicación de la necesidad de actualización.
12. - Identificación y descripción de las fases del proceso de actualización de firmware.
13. - Recomendaciones básicas de buenas prácticas.
14. Desarrollo de supuestos prácticos de resolución de incidencias donde se ponga de manifiesto.
15. - La aplicación de los criterios de selección de equipos que pueden actualizar su firmware.
16. - La localización de las versiones actualizadas del firmware.
17. - La actualización del firmware.
18. - La comprobación del correcto funcionamiento del equipo actualizado.

UNIDAD FORMATIVA 3. RESOLUCIÓN DE INCIDENCIAS EN REDES TELEMÁTICAS

UNIDAD DIDÁCTICA 1. GESTIÓN DE INCIDENCIAS.

1. Definición del concepto de incidencia.
2. Enumeración de los objetivos de la gestión de incidencias.
3. Identificación y descripción de las actividades.
4. - Identificación.
5. - Registro.
6. - Clasificación.
7. - Priorización.
8. - Diagnóstico inicial.
9. - Escalado.
10. - Investigación y diagnóstico.
11. - Resolución y recuperación.
12. - Cierre.
13. Explicación y ejemplificación del flujo del proceso.
14. Ejemplificación de indicadores y métricas.
15. Recomendaciones básicas de buenas prácticas.
16. Sistemas de gestión de incidencias.
17. - Descripción de las funcionalidades.
18. - Ejemplificación y comparación de herramientas comerciales y de código abierto.

UNIDAD DIDÁCTICA 2. RESOLUCIÓN DE INCIDENCIAS.

1. Identificación y análisis de las distintas fases del proceso de resolución de incidencias.
2. - Definición del problema.
3. - Descripción del problema.
4. - Establecimiento de las posibles causas.
5. - Prueba de las causas más probables .
6. - Verificación de la causa real.
7. - Planificación de las intervenciones.
8. - Comprobación de la reparación.
9. - Documentación.
10. Descripción y ejemplificación del uso de los diagramas de causa / efecto (Ishikawa) en la solución de problemas.
11. Descripción de la funcionalidad y criterios de utilización de herramientas hardware de diagnóstico.
12. - Polímetro.
13. - Comprobador de cableado.
14. - Generador y localizador de tonos.
15. - Reflectómetro de dominio temporal.
16. - Certificador de cableado.
17. Descripción de la funcionalidad , criterios de utilización y ejemplificación de herramientas software de diagnóstico.
18. - Monitor de red.
19. - Analizador de protocolos.
20. - Utilidades TCP/IP: ping, traceroute, arp, netstat.
21. Desarrollo de supuestos prácticos de resolución de incidencias donde se ponga de manifiesto.
22. - La interpretación de la documentación técnica de los equipos implicados.
23. - La interpretación de la documentación técnica del proyecto.
24. - La elección de las herramientas de diagnostico en función del problema.
25. - La estimación de la magnitud del problema para definir la actuación.
26. Desarrollo de supuestos prácticos de resolución de incidencias donde se realice una captura de tráfico utilizando un analizador de tráfico.
27. - Analice la captura realizada y determine las variaciones con respecto a los parámetros de funcionamiento normal.
28. - Proponga, si es necesario, una solución justificada.