Programación didáctica de Seguridad y Alta Disponibilidad

Administración de Sistemas Informáticos en Red

Curso 2022-2023

Profesores: Francisco Soria López

Marisa Aguilera Marín

ÍNDICE

1. CONTEXTUALIZACIÓN.

El ciclo formativo de Administración de Sistemas Informáticos en Red tiene una duración total de 2000 horas, se trata de un ciclo de formación profesional de grado medio. Pertenece a la familia profesional de Informática y Comunicaciones y se engloba, dentro de la Clasificación Internacional Normalizada de la Educación (CINE), en el grupo CINE-5b.

RD 1629/2009, de 30 de octubre de enseñanzas mínimas del Título de Técnico Superior en Administración de Sistemas Informáticos en Red.

Esta programación está referida al módulo de "Seguridad y Alta Disponibilidad" del ciclo formativo "Administración de Sistemas Informáticos en Red" del centro I.E.S. Politécnico Jesús Marín en Málaga. Se imparte en el segundo curso del ciclo formativo de grado superior de ASIR. Dentro de las directivas educativas y de ordenación de los módulos en el Ciclo Formativo de Administración de Sistemas Informáticos y en Red, el módulo SAD tiene una duración de 84 horas a razón de 4 horas semanales. El grupo de 2º de ASIR que cursa dicho módulo, puede tener alumnos con sólo módulos de segundo o bien, de primero repetidores que completen horario con éste.

Véase programación del ciclo formativo.

MARCO LEGISLATIVO

Se detallan todos y cada una de las legislaciones por las que se rige esta programación didáctica.

Ley Orgánica de Educación (LOE) 2/2006, de 3 de mayo.

Ley de Educación de Andalucía (LEA) 17/2007, de 10 de diciembre.

Ley Orgánica 5/2002, de 19 de junio, de las Cualificaciones y de la Formación Profesional, por la que se establece la ordenación de un sistema integral de formación profesional, cualificaciones y acreditación, que responda con eficacia y transparencia a las demandas sociales y económicas a través de las diversas modalidades formativas.

El **Real Decreto 1538/2006**, de 15 de diciembre, establecía la ordenación general de la formación profesional del sistema educativo y fija la estructura de los títulos de formación profesional, que tendrán como base el Catálogo Nacional de las Cualificaciones Profesionales, las directrices fijadas por la Unión Europea y otros aspectos de interés social, dejando a la Administración educativa correspondiente el desarrollo de diversos aspectos contemplados en el mismo. Este real decreto queda derogado por el **RD 1147/2011**, 29 de Julio que es el que establece la ordenación general de la formación profesional del sistema educativo.

El **Decreto 436/2008**, de 2 de septiembre, por la que se regulan los aspectos generales y que establece la ordenación y las enseñanzas de la formación profesional inicial que forma parte del sistema educativo.

El **Real Decreto 1629/2009,** de 30 de octubre por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas, hace necesario que, al objeto de poner en marcha estas nuevas enseñanzas se desarrolle el currículo correspondiente a las mismas. Las enseñanzas correspondientes a este título se organizan en forma de ciclo formativo de grado superior, de 2.000 horas de duración, y están constituidas por los objetivos generales y los módulos profesionales del ciclo formativo.

La Orden de 19 de Julio de 2010 desarrolla su correspondiente currículo al módulo de Seguridad y Alta disponibilidad (SAD), para la comunidad autónoma de Andalucía, correspondiente al ciclo formativo de grado superior de Sistemas Informáticos en Red concretando el RD 1629/2009.

La orden de 29 de septiembre de 2010, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

2. OBJETIVOS.

2.1. COMPETENCIA GENERAL DEL TÍTULO.

Véase programación del ciclo formativo donde se recogen los objetivos generales de este ciclo formativo, recogidos en la Orden 19 de Julio de 2010.

2.2. OBJETIVOS GENERALES DEL CICLO Y LOS ASOCIADOS AL MÓDULO.

La formación del módulo contribuye a alcanzar los resultados de aprendizaje generales de este ciclo formativo que se relacionan a continuación:

a) Instalar y configurar el software de base, siguiendo documentación técnica y especificaciones dadas, para administrar sistemas operativos de servidor.

b) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.

c) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

d) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.

e) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.

f) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad analizando sus implicaciones en el ámbito de trabajo, para mantener el espíritu de innovación.

A continuación se mostrarán las competencias que se adquirirán en este módulo profesional y las relacionaremos con las competencias que se habrán adquirido una vez obtenido el título de Técnico Superior en Administración de Sistemas Informáticos en Red. RD 1629/2009, de 30 de octubre de enseñanzas mínimas del Título de Técnico Superior en Administración de Sistemas Informáticos en Red.

a) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.

b) Determinar la infraestructura de redes telemáticas elaborando esquemas y seleccionando equipos y elementos

c) Integrar equipos de comunicaciones en infraestructuras de redes telemáticas

determinando la configuración para asegurar su conectividad.

d) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.

e) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

f) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

g) Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.

h) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.

i) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.

j) Mantener la limpieza y el orden en el lugar de trabajo, cumpliendo las normas de competencia técnica y los requisitos de salud laboral.

k) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.

l) Mantener el espíritu de innovación y actualización en el ámbito de su trabajo para adaptarse a los cambios tecnológicos y organizativos de su entorno profesional.

m) Liderar situaciones colectivas que se puedan producir, mediando en conflictos personales y laborales, contribuyendo al establecimiento de un ambiente de trabajo agradable y actuando en todo momento de forma sincera, respetuosa y tolerante.

n) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.

o) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos

establecidos, definidos dentro del ámbito de su competencia.

p) Ejercer sus derechos y cumplir con las obligaciones derivadas de las relaciones laborales, de acuerdo con lo establecido en la legislación vigente.

2.3. OBJETIVOS ESPECÍFICOS ASOCIADOS AL MÓDULO.

La formación del módulo SAD contribuye a alcanzar las competencias profesionales, personales y sociales de este ciclo que se relacionan a continuación:

a) Administrar sistemas operativos de servidor, instalando y configurando el software, en condiciones de calidad para asegurar el funcionamiento del sistema.

b) Administrar aplicaciones instalando y configurando el software, en condiciones de calidad para responder a las necesidades de la organización.

c) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.

d) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

e) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

3. CONTENIDOS Y SU DISTRIBUCIÓN TEMPORAL

3.1. CONTENIDOS

0. **Preparación del entorno de trabajo.**
1. **Introducción a la seguridad informática.**
2. **Seguridad en redes corporativas.**
3. **Criptografía**
4. **Seguridad perimetral. Proxy y Cortafuegos.**
5. **Virtualización de servidores y Alta Disponibilidad.**
6. **Política de seguridad.**
7. **Aspectos éticos y legales.**

3.2. SECUENCIACIÓN DE UNIDADES DE TRABAJOS Y DISTRIBUCIÓN TEMPORAL

A continuación se desglosan los contenidos de cada una de las unidades de trabajo.

UNIDAD DE TRABAJO 0. Evaluación inicial. Virtualización, repaso linux y redes de primero. Preparación del entorno de trabajo. Metodología DevSecOps.

UNIDAD DE TRABAJO 1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA. ADOPCIÓN DE PAUTAS Y PRÁCTICAS DE TRATAMIENTO SEGURO DE LA INFORMACIÓN. DATACENTER. SAI. VIDEOVIGILANCIA.

Objetivos Didácticos	● Analizar la problemática general de la seguridad informática. ● Conocer los principios sobre los que se sustenta: Confidencialidad, Integridad y Disponibilidad. ● Conocer el significado de alta disponibilidad. ● Identificar las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas. ● Diferenciar la seguridad física y lógica, y la pasiva de la activa
Contenidos	1.1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA 1.2. FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD 1.2.1. Alta disponibilidad 1.3. Sistemas de Gestión de la Seguridad de la Información 1.3.1. Activos 1.3.2. Amenazas 1.3.3. Riesgos 1.3.4. Contramedidas 1.4. Alta disponibilidad Paradoja de la seguridad. 1.5. Amenazas y medidas de protección. 1.6. Seguridad física y ambiental. Datacenter. SAI (funcionamiento ininterrumpido) 1.7. Herramientas de fortaleza de contraseñas. ACL y permisos. 1.8. Servidores de autenticación 2FA. Autenticación single sing-on. 1.9. Herramientas de control de integridad, redundancia, alta disponibilidad y seguridad de datos. RAID. NAS. S ADOPCIÓN DE PAUTAS Y PRÁCTICAS DE TRATAMIENTO SEGURO DE LA INFORMACIÓN. 1.10. Ejemplo práctico Integridad: Herramientas rootkit (sfc y rkhunter). 1.11. Ejemplo práctico Disponibilidad: Bond y link aggregation 1.12. Elementos vulnerables en el sistema informático. Hardware, software y datos. 1.13. Análisis de las principales vulnerabilidades de un sistema informático. Amenazas.Tipos. 1.14. Medidas de seguridad: Seguridad Física/lógica, Seguridad Activa/Pasiva. 1.15. Primeras prácticas para asegurar (Buscar vulnerabilidades, Actualización de Paquetes, Estar siempre informado, etc.). Autenticación 2FA, Sing-on.

	1.16. ¿Cómo estar informado de todo lo relacionado con la seguridad? Canales de noticias. 1.17. Configuración RAID. 1.18. SEGURIDAD FÍSICA Y AMBIENTAL DE CPD Y PUESTOS DE TRABAJOS. 1.19. Ubicación y acondicionamiento de CPD. Elementos normalizados y seguridad de un armario. 1.20. Control de acceso físico al CPD. Sistemas biométricos. 1.21. Circuito videovigilancia. Cámaras IP. 1.22. - SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI/UPS). 1.23. Funciones de un SAI. 1.24. Tipos de SAI. SAI OFFLINE, SAI INLINE y SAI ONLINE. 1.25. Calculo de la potencia y monitorización en SAI.
Resultados de aprendizaje involucrados	1a, 1c, 1f, 1g, 1h, 1i, 2a, 2b, 2c, 2d, 2e, 2g, 2h, 2i, 3a, 3b, 3c

UNIDAD DE TRABAJO NÚMERO 2. SEGURIDAD EN REDES CORPORATIVAS.

Objetivos Didácticos	● Valorar los nuevos peligros derivados de la conexión a redes. ● Adoptar medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas. ● Analizar las principales vulnerabilidades de las redes inalámbricas. ● Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros. ● Conocer y emplear protocolos y aplicaciones seguras en comunicaciones.
Contenidos	2.1. Introducción a servicios de acceso remoto seguros. 2.2. Usando terminales seguros. Protocolo SSH. Generación de llaves usando criptografía asimétrica. 2.3. Túneles SSH. 2.4. Herramientas relacionadas con SSH y sistemas de archivos. 2.5. Segmentación de red. LAN, DMZ. Uso, funciones, ubicación y arquitectura de firewall. Zona DMZ. 2.6. Hardware perimetral. 2.7. VPN. Protocolos. Instalación con Virtual appliances y en linux desde cero. Clientes VPN. 2.8. Monitorización la red.

	2.9. Sistemas de log y auditorias. 2.10. Servidores de autenticación. Sistemas de cifrados. Autenticación Radius, PAM, BD… 2.11. Securizar la red LAN y WAN. Control por MAC-binding, Hostspots…. Ventajas diseño arquitectura de red y segmentación. VLAN. DMZ. 2.12. Control por MAC, MAC-binding. 2.13. Hotspots. Securizar redes WLAN. 2.14. Monitorización del tráfico de red. SNMP. 2.15. Servidores de autenticación. PAM, BD, RADIUS… 2.16. Servidores de logs. Auditorias. 2.17. Seguridad en redes inalámbricas.
Resultados de aprendizaje evaluables	1a, 1b, 1c, 1d, 1g, 1h, 1i, 2a, 2b, 2c, 2d, 2e, 2f, 2g, 2h, 2i, 3a, 3b, 3c, 3d, 3e, 3f, 3g, 4a, 4b, 4c, 4d, 4f, 4g, 4h, 5a, 5i, 6b, 6f, 6h, 7b

UNIDAD DE TRABAJO NÚMERO 3. CRIPTOGRAFÍA

Objetivos Didácticos	● Profundizar en aspectos de criptografía asociada a la confidencialidad de la información y de las comunicaciones. ● Garantizar la confidencialidad de la información. ● Garantizar la privacidad de las comunicaciones. ● Diferenciar ventajas e inconvenientes de la criptografía simétrica y asimétrica. ● Analizar nuevos procesos de identificación digital seguros mediante firma digital, certificado digital y DNI electrónico.
	3.1. Introducción 3.2. Principios e historia de la criptografía 3.3. Criptografía simétrica 3.4. Criptografía asimétrica 3.5 Algoritmos 3.5.1 DES 3.5.2 RSA 3.5.3 Híbrida

Contenidos	3.6 Mecanismos de autenticación 3.6.1 Firma digital 3.6.2 Certificados digitales 3.6.2.1 PKI 3.6.2.2 Terceras partes de confianza 3.6.2.3 DNIE 3.6.3 Autenticación simétrica Kerberos 3.6.4 Autenticación asimétrica 3.6.5 Huella digital. HASH y GPG. 3.6.6 Protocolos seguros. SSL y su uso en servicios de red. Conexiones seguras SSH, TLS/SSL, IPSec 3.6.7 Firma electrónica y certificado digital. Factura electrónica.
Resultados de aprendizaje involucrados	1a, 1g, 2f, 3c,

UNIDAD DE TRABAJO NÚMERO 4. SEGURIDAD PERIMETRAL. PROXY Y CORTAFUEGOS.

Objetivos Didácticos	● Valorar los peligros externos a las redes corporativas y conocer las medidas de seguridad perimetrales para hacerles frente. ● Comprender la importancia de los puertos de comunicaciones y su filtrado mediante cortafuegos o firewall. ● Aprender el significado de las listas de control de acceso (ACL) en routers y cortafuegos. ● Comprender la importancia y aprender a configurar servidores

Contenidos	4.1 Introducción 4.2 Tablas de enrutamiento 4.1.1 Route 4.1.2 Interfaces 4.1.3 Ip_forward 4.2 Cortafuegos 4.2.1 Tipos de cortafuegos 4.2.2 Capa de trabajo del cortafuegos 4.2.3 Topología de cortafuegos 4.2.3.1 Bastión 4.2.3.2 Screening router 4.2.3.3 Dual-Homed Host 4.2.3.4 Screened host 4.2.3.5 Screened Subnet 4.2.3.6 DMZ 4.2.4 Configuración Clasificación de “firewall” según ubicación de la aplicación, y según arquitectura de red. 4.2.5 Filtrado de paquetes de datos. Reglas de filtrado. 4.2.6 Instalación de cortafuegos mediante distribución Linux. Configuración. 4.2.7 Instalación de cortafuegos Dual Homed-Host Linux desde cero. 4.2.8 Firewall con dos tarjetas de red. Firewall dedicado para seguridad perimetral. 4.2.9 Pruebas de funcionamiento. Sondeo. Registro de sucesos de cortafuegos. 4.2.10 Casos prácticos con firewall de Windows, iptables y nftables. 4.3 Proxy

	4.4 Tipos de proxy. Características y funciones. 4.5 Instalación de proxy en distribuciones Linux. Configuración de clientes proxy. 4.6 Métodos de autentificación. Configuración de filtros. 4.7 Instalación de servidores Proxy-NAT en firewall Linux desde cero. 4.8 Autentificación en servidores proxy. 4.9 Control del ancho de banda en servidores proxy Web. 4.10 Usando TCP-Wrapper para controlar el acceso a servicios de red a nivel de hosts/redes.
Resultados de aprendizaje involucrados	4a, 4b, 4c, 4d, 4e, 4d, 4f, 4g, 4h, 5a, 5b, 5c, 5d, 5e, 5f, 5g, 5h, 5i

UNIDAD DE TRABAJO NÚMERO 5. VIRTUALIZACIÓN DE SERVIDORES, CLUSTER, BALANCEADORES, REPLICACIÓN Y OTRAS SOLUCIONES PARA ALTA DISPONIBLIDAD.

Objetivos Didácticos	● Analizar las distintas configuraciones seguridad y de alta disponibilidad utilizando herramientas de la metodología DevOps y DevSecOps. ● Valorar la importancia de realizar un buen análisis de riesgos potenciales en sistemas críticos y adoptar medidas para paliar sus posibles consecuencias. ● Aprender las diferencias, ventajas e inconvenientes entre los sistemas de almacenamiento redundante (RAID) y conocer sus opciones de configuración y prueba. ● Conocer las opciones de configuración y administración de balanceo de carga entre distintas conexiones de red. ● Realizar configuraciones de alta disponibilidad de servidores mediante virtualización de sistemas operativos, públicos, o de nube híbrida.

Contenidos	5.1 Soluciones de alta disponibilidad 5.1.1 RAID 5.1.2 Balanceadores de carga. 5.1.3 Virtualización de servidores. Virtualización con hipervisores de tipo 0 y 1, cloud computing, de nube privada, pública y mixta y virtualización ligera. 5.1.4 HA tarjetas de red y link aggregation. 5.1.5 Clusters. Kubernetes. Soluciones on premise y proxmox… 5.1.6 Replicación de servidores, de datos, almacenamiento distribuido y sincronización de directorios. 5.1.7 IaaC. 5.1.8 Métricas de HA. 5.1.9 Herramientas DevOps y DevSecOps. 5.1.10 Pruebas de carga.
Resultados de aprendizaje involucrados	1a, 1i, 2d, 2h, 2i, 6a, 6b, 6c, 6d, 6e, 6f, 6h, 6i

UNIDAD DE TRABAJO NÚMERO 6. POLÍTICA SE SEGURIDAD.

Objetivos Didácticos	● Valorar los nuevos peligros derivados de la conexión a redes. ● Adoptar medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas. ● Analizar las principales vulnerabilidades de las redes inalámbricas. ● Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros. ● Conocer y emplear protocolos y aplicaciones seguras en comunicaciones.

Contenidos	6.1 Implantación de una política de seguridad. 6.2 Identificar activos, ataques y atacantes. 6.3 Análisis de riesgos. 6.4 Planes de seguridad. 6.5 Planes de contingencia. 6.6 Tipos de ataques. Malware. Antivirus. Spam. Rookit, WLAN, suplantación SSID, ataque Dos, secuestro de sesión, man-in-the-middle…… 6.7 Herramientas de seguridad: 6.8 Escáner de vulnerabilidades. 6.9 Hardening (bastionado) de servidores Linux. Apache hardening. 6.10 Medidas de detección y recuperación. 6.11 Análisis forense. Auditorías. 6.12 Otras herramientas: NMAP, Snort, Nessus, Metaexploits…. 6.13 Amenazas y ataques. Patrones de ataque 6.13.1 Arp poisoning 6.13.2 Pharming 6.13.3 Man in the middle 6.13.4 Sniffing 6.13.5 Hijacking 6.14 Seguridad en WEB 6.14.1 HTTP Analyzer 6.14.2 Achilles 6.14.3 Forgeries 6.14.4 XSS (Cross site sripting) 6.14.5 Inyección SQL 6.14.6 Anonimato

	6.14.6.1 Bouncer 6.14.6.2 Proxies 6.15 IPS e IDS 6.15.1 NIDS 6.15.2 HIDS 6.15.3 Honeypot 6.16 Control de acceso 6.16.1 Tcpwrappers 6.16.2 Xinetd 6.17 AIDE 6.17.1 OSSEC HIDS 6.18 Seguridad en WEB 6.18.1 HTTP Analyzer 6.18.2 Achilles 6.18.3 Forgeries 6.18.4 XSS (Cross site sripting) 6.18.5 Inyección SQL 6.18.6 DooS. CDN. 6.18.7 Desboradamiento 6.18.8 Ataque por inyección 6.18.9 Anonimato 6.18.9.1 Bouncer 6.18.9.2 Proxies 6.19 Riesgos potenciales en los servicios de red 6.20 AIDE 6.20.1 OSSEC HIDS

	6.21 Redes Inalámbricas 6.21.1 Aircrack-ng 6.21.2 Wifiway 6.21.3 Wifislax 6.21.4 Sistemas de seguridad, como RADIUS.

Resultados de aprendizaje evaluables	1a, 1b, 1c, 1d, 1g, 1h, 1i, 2a, 2b, 2c, 2d, 2e, 2f, 2g, 2h, 2i, 3a, 3b, 3c, 3d, 3e, 3f, 3g, 4a, 4b, 4c, 4d, 4f, 4g, 4h, 5a, 5i, 6b, 6f, 6h, 7b

UNIDAD DE TRABAJO NÚMERO 7. Legislación y normas sobre seguridad.

Objetivos Didácticos	● Conocer la normativa española en materia de seguridad informática. ● Analizar la normativa y aplicaciones de la LOPD, en materia de seguridad de los datos de carácter personal. ● Analizar la normativa y aplicaciones de la LSSICE, en materia de comercio electrónico y actividades empresariales vía Internet. ● Valorar la importancia de la normativa como reguladora de derechos y obligaciones a ciudadanos y empresas.
Contenidos	7.1 Reglamento europeo de protección de datos 7.2 Principales modificaciones con el nuevo Reglamento Europeo de Protección de Datos 7.2.1 ¿Qué empresas estarán obligadas a cumplir con el RGPD? 7.2.2 Nuevas obligaciones 7.2.3 Notificación de violaciones de seguridad 7.2.4 Registro de las actividades de tratamiento 7.2.5 Responsabilidad proactiva. También llamado Accountability. 7.2.6 Evaluación de impacto de protección de datos 7.2.7 Delegado de Protección de Datos 7.2.8 ¿Cómo afecta a los ciudadanos y qué herramientas tienen para

	proteger sus datos personales? 7.2.9 Cambios en la obtención del consentimiento 7.2.10 Listas Robinson 7.2.11 Resumen 7.2.12 Facilita
Resultados de aprendizaje involucrados	7a, 7c, 7d, 7e, 7f, 7g

CRITERIOS DE EVALUACIÓN.

UNIDAD DE TRABAJO 0.

- Conocer la planificación global de desarrollo del módulo, así como a los miembros del grupo. Comprender los criterios que serán considerados y aplicados en el proceso formativo.
- Identificar los derechos y obligaciones como estudiante, en relación con el módulo.
- Comprender las principales interrelaciones que se dan entre las unidades didácticas del módulo y entre este y los demás que lo constituyen.
- Identificar los propios conocimientos en relación con los que se deben alcanzar en el módulo. Preparación y creación de las máquinas virtuales que serán necesarias a lo largo del módulo. Comprobar los objetivos alcanzados en módulos del primer año en temas relacionados con redes y Linux.
- Análisis de las relaciones existentes entre los módulos del ciclo y las de éste con las cualificaciones que le sirven de referente.
- Identificación y registro en el soporte adecuado de los aspectos, normas y elementos que se planteen en torno a cuestiones disciplinares, metodológicos, relacionales, etc.

UNIDAD DE TRABAJO 1.

- Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
- Se han descrito las diferencias entre seguridad física y lógica.
- Se han clasificado las principales vulnerabilidades de un sistema informático, según su

tipología y origen.

- Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
- Se han valorado las ventajas que supone la utilización de sistemas biométricos.
- Se ha valorado la importancia de herramientas de seguridad física como SAI y videovigilancia.
- Se ha puesto en marcha implementaciones de mecanismos de redundancia de datos y de tarjetas de red.
- Se han adoptado políticas de contraseñas.
- Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.
- Se ha descrito la funcionalidad de las ACL en la seguridad lógica.
- Se ha implantado un plan de copias de seguridad.
- Se han descrito herramientas para la seguridad y encriptación de los datos.

UNIDAD DE TRABAJO 2.

- Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.
- Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.
- Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.
- Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.
- Se ha reconocido la necesidad de establecer un plan integral de protección perimetral especialmente en sistemas conectados a redes públicas.
- Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.
- Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.
- Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
- Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.
- Se ha reconocido la necesidad de inventariar, monitorizar y controlar los servicios de red que se ejecutan en un sistema. Necesidad de implantación de herramientas SIEM.

UNIDAD DE TRABAJO 3.

- Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas y privadas.

UNIDAD DE TRABAJO 4.

- Se han identificado los tipos de proxy, sus características y funciones principales.
- Se ha instalado y configurado un servidor proxy-caché.
- Se han configurado los métodos de autenticación en el proxy.
- Se ha configurado un proxy en modo transparente.
- Se ha utilizado el servidor proxy para establecer restricciones de acceso web.
- Se ha n solucionado problemas de acceso desde los clientes al proxy.
- Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.
- Se ha configurado un servidor proxy en modo inverso.
- Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.
- Se han descrito las características, tipos y funciones de los cortafuegos.
- Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
- Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
- Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
- Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
- Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
- Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
- Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

UNIDAD DE TRABAJO 5.

- Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.
- Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.
- Se han evaluado las posibilidades de la virtualización de servidores para implementar soluciones de alta disponibilidad.
- Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.
- Se ha implantado un balanceador de carga a la entrada de la red interna.
- Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.
- Se ha evaluado la utilidad de los sistemas de clústeres para aumentar la fiabilidad y productividad del sistema.
- Se han implantado y utilizado conjunto de herramientas de metodología DevOps y DevSecOps para la implementación de redundancia, seguridad, y alta disponibilidad de servidores.
- Se han analizado soluciones de futuro para un sistema con demanda creciente.
- Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

UNIDAD DE TRABAJO 6.

- Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
- Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
- Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
- Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
- Se han implantado herramientas de ataque y defensa de la seguridad de un sistema informático.
- Se han identificado las fases del análisis forense ante ataques a un sistema.
- Se ha desarrollado un plan de seguridad.
- Se han probado diversas herramientas para la seguridad y escáner de vulnerabilidades.

UNIDAD DE TRABAJO 7.

- Se ha descrito la legislación sobre protección de datos de carácter personal.
- Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
- Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
- Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Se han contrastado las normas sobre gestión de seguridad de la información. Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

A continuación se plantea el calendario de ejecución de las unidades de trabajo ya descritas y el trimestre en el que se impartirán:

Unidad de Trabajo	Trimestre
U.T.0 y U.T. 1	1º
U.T. 2	1º
U.T. 3	1º
U.T. 4	1º
U.T. 5	2º
U.T. 6	2º
U.T. 7	2º

4. Competencias profesionales, personales y sociales del módulo.

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

COMP_1-> UC0486_3 Asegurar equipos informáticos.

Las competencias profesionales, personales y sociales de este módulo son las que se relacionan a continuación:

COMP_1-> Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.

COMP_2-> Evaluar el rendimiento de los dispositivos hardware

identificando posibilidades de mejoras según las necesidades de funcionamiento.

COMP_3-> Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.

COMP_4-> Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

COMP_5-> Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

COMP_6-> Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.

COMP_7-> Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.

COMP_8-> Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.

COMP_9-> Mantener el espíritu de innovación y actualización en el ámbito de su trabajo para adaptarse a los cambios tecnológicos y organizativos de su entorno profesional.

COMP_10-> Liderar situaciones colectivas que se puedan producir, mediando en conflictos personales y laborales, contribuyendo al establecimiento de un ambiente de trabajo agradable y actuando en todo momento de forma sincera, respetuosa y tolerante.

COMP_11-> Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.

COMP_12-> Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

Objetivos

La formación del módulo de Seguridad Informática y Alta Disponibilidad, en concreto, contribuye a alcanzar los siguientes objetivos generales del módulo:

OBJ_1_1-> Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.

OBJ_1_2-> Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.

OBJ_1_3-> Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.

OBJ_1_4-> Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

OBJ_1_5-> Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios

OBJ_1_6-> Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.

Otros objetivos que vienen expresados en términos de resultados de aprendizaje:

OBJ_2_1-> Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

OBJ_2_2-> Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

OBJ_2_3-> Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

OBJ_2_4-> Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

OBJ_2_5-> Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

OBJ_2_6-> Implanta soluciones de alta disponibilidad empleando técnicas de virtualización, metodología DevSecOps y configurando los entornos de prueba.

OBJ_2_7-> Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permitirán alcanzar los objetivos anteriores estarán relacionadas con:

OBJ_3_1-> El conocimiento de las prácticas y pautas adecuadas, relativas a la seguridad física y lógica en un sistema informático.

OBJ_3_2-> El conocimiento y análisis de técnicas y herramientas de seguridad activa, que actúen como medidas preventivas y/o paliativas ante ataques al sistema.

OBJ_3_3-> El análisis y aplicación de técnicas y herramientas de seguridad activa.

OBJ_3_4-> El análisis y aplicación de técnicas seguras de acceso remoto a un sistema.

OBJ_3_5-> El análisis de herramientas y técnicas de protección perimetral para un sistema.

OBJ_3_6-> La instalación, configuración y prueba de cortafuegos y servidores proxy como herramientas básicas de protección perimetral.

OBJ_3_7-> El análisis de los servicios de alta disponibilidad más comunes, que garanticen la continuidad de servicios y aseguren la disponibilidad de datos.

OBJ_3_8-> El conocimiento y análisis de la legislación vigente en el ámbito del tratamiento digital

5. CONTENIDOS DE CARÁCTER TRANSVERSAL.

Véase programación del ciclo formativo.

6. METODOLOGÍA.

Los aspectos metodológicos que se aplican en este módulo descansan en la idea de que el alumno se considere parte activa de la actividad docente. Con esto, se pretende involucrarlo en el proceso de asimilación de nuevos conceptos y adquisición de capacidades, no como un mero contenedor de éstas sino como un productor directo de estos conocimientos y habilidades en sí mismo. Se tratará de conseguir desarrollar progresivamente la autonomía y la autosuficiencia del alumno mediante la superación de las dificultades que vayan surgiendo y potenciando la iniciativa, la deducción lógica, la aplicación del método adecuado, la acumulación de experiencia y la capacidad de reacción ante nuevas situaciones. Además, se hará especial

hincapié en una formación en valores donde el respeto hacia el profesor, compañeros y material de clase será vital para poder realizar un aprendizaje correcto de la materia.

La metodología de trabajo en el aula se basa en un aprendizaje significativo que contemple las siguientes características:

- Asimilación de forma activa de los nuevos contenidos, relacionándolos con los conocimientos ya asimilados. La transmisión de los contenidos será el punto de partida, a través de una exposición oral por parte del profesor de forma asequible y adaptada al nivel de los alumnos.
- Construcción y organización de los conocimientos, estableciendo una visión previa general para luego profundizar en cada aspecto y reforzarlo con ejemplos y actividades. Implementación, por el profesor, de ejemplos prácticos, que clarifiquen los contenidos orales expuestos previamente.
- Implementación, por los alumnos, de ejemplos prácticos, para asimilar los contenidos de forma individual.
- Diferenciación de los contenidos de forma progresiva, estableciendo una organización y secuenciación de ellos.
- Solución de las dificultades de aprendizaje mediante las orientaciones del profesor y las actividades adicionales.
- Realización de actividades prácticas que constituirán la aplicación de los contenidos de cada unidad didáctica.
- Realización de actividades prácticas de profundización sobre los contenidos de cada unidad didáctica.
- Estas actividades estarán realizadas por los alumnos de forma individual y/o colectiva, y ayudándose de material de consulta apropiado.
- Actividades de investigación y búsqueda de documentación y soluciones a través de la web.

- Actividades de puesta en común y exposición de los resultados de trabajos e investigación, para adquirir una experimentación colectiva.
- Solución con trabajo en equipo, mediante actividades de grupo, para alcanzar un resultado individual y diferente, realizándose una exposición en clase de los problemas particulares encontrados y de las soluciones aplicadas, como base de una experiencia común.

Los medios que se implantarán en la medida de lo posible para conseguir estos fines son:

- Permitir a los alumnos que prefieran utilizar su propio portátil en lugar de los del aula. El Centro y las aulas cuentan con conexión wifi o cableada y con conexión a Internet.
- Utilización del proyector para realizar las explicaciones prácticas de software.
- Realización de actividades en grupo que permitan, de una forma próxima y fácil, el aporte de distintos puntos de vista sobre un tema concreto.
- Planteamiento de actividades creativas donde el alumno pueda aportar su criterio a los temas comentados.
- Búsqueda de información por parte del profesor acerca de cuáles son los intereses previos de los alumnos al matricularse en un curso de este tipo.
- La aplicación de los temas transversales al desarrollo de nuestro trabajo en el aula y fuera de ella, idónea para conseguir una mejora en la madurez individual, interpersonal, social, ética, moral, etc.
- Fomento del pensamiento crítico y constructivo sobre las actividades tecnológicas desarrolladas y en general, y las diversas propuestas comerciales que se pueden encontrar en el mercado.
- Ayudarles a seleccionar y manejar correctamente la documentación técnica y la información publicitaria.
- Fomentar el trabajo en grupo, en la medida en que las posibilidades del alumnado lo permitan.

- Realización de actividades prácticas lo más actualizadas posible.
- Valoración del esfuerzo empleado en la comprensión y buena utilización de los sistemas operativos que se traten en los contenidos del módulo
- Por otra parte se plantea la necesidad de motivar e incentivar el interés del alumno por los temas referenciados en clase.
- Acercamiento de los temas didácticos al mundo real, aportando publicaciones y documentación de productos lo más conocidos y asequibles posible.
- Desmitificar la teoría más abstracta y convirtiéndola en cosas tangibles. Es decir, analizando el punto de vista práctico de los conceptos expresados en clase.
- Planteando ejemplos de aplicación de los trabajos en clase en el mundo laboral real (o lo más cercano posible) de forma que se vaya formando la imagen, en cada alumno, de su perfil profesional.
- Utilización de recursos TIC y carpetas compartidas en la nube para la distribución de material, entrega de las prácticas y seguimiento de fechas de interés.
- Realización de actividades en cada unidad didáctica de diferente nivel de dificultad.
- Creación de grupos de trabajo heterogéneos con alumnos que presenten diferentes niveles y destrezas, fomentando el cooperativismo entre ellos y planteando actividades que puedan ser desarrolladas por todos los miembros del grupo.
- Fomentar el que todos los alumnos tengan que preparar un tema que les guste o para el que presenten alguna habilidad especial y lo expongan en clase a sus compañeros.
- Fomentar la igualdad en clase, el respeto mutuo y la solidaridad.

7. CRITERIOS DE EVALUACIÓN Y RESULTADOS DE APRENDIZAJE.

La evaluación será continua, formativa y sumativa, considerándose además de las pruebas teórico-prácticas, el trabajo en clase, las prácticas, el progreso, el interés por el módulo, la atención, etc.

Los criterios y los procedimientos de evaluación tendrán en cuenta las competencias profesionales del título, los objetivos del ciclo, y la madurez del alumnado en relación con las características del sector productivo y su motivación frente a futuros aprendizajes y adaptaciones a los cambios tecnológicos propios del sector.

La evaluación del aprendizaje se realizará tomando como referencia las competencias profesionales, los objetivos, y los criterios de evaluación establecidos para el módulo profesional.

Los criterios de evaluación establecen el nivel aceptable de consecución de la capacidad correspondiente y, en consecuencia, los resultados mínimos que deben ser alcanzados en el proceso de enseñanza-aprendizaje.

Se muestran a continuación los criterios de evaluación:

Se desglosan los criterios de evaluación asociados a los resultados de aprendizaje según aparecen recogidos en la orden 19 de Julio de 2010.

- **Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.**

a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.
d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.
e) Se han adoptado políticas de contraseñas.
f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.
g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.
h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.

i) Se han identificado las fases del análisis forense ante ataques a un sistema.

- Implementa mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.

b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.

c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.

d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.

e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.

f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo

g) basado en el uso de redes públicas.

h) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.

i) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.

j) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

- Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.

b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.

c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.

d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.

e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.

f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.

g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.

- Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

a) Se han descrito las características, tipos y funciones de los cortafuegos.
b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.
c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.
d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.
e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.
f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.
g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.
h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.

- Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

a) Se han identificado los tipos de proxy, sus características y funciones principales.

b) Se ha instalado y configurado un servidor proxy-cache.

c) Se han configurado los métodos de autenticación en el proxy.

d) Se ha configurado un proxy en modo transparente.

e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web.

f) Se han solucionado problemas de acceso desde los clientes al proxy.

g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.

h) Se ha configurado un servidor proxy en modo inverso.

i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy

- Implanta soluciones de alta disponibilidad empleando diferentes técnicas de virtualización y configurando los entornos de prueba.

a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.

b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.

c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.

d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.

e) Se ha implantado un balanceador de carga a la entrada de la red interna.

f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.

g) Se ha evaluado e implantado sistemas de clúster para aumentar la fiabilidad y productividad del sistema.

h) Se han analizado soluciones de futuro para un sistema con demanda creciente.

i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad

j) Implanta soluciones de seguridad y alta disponibilidad empleando la metodología DevOps y DevSecOps.

- **Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.**
  - Se ha descrito la legislación sobre protección de datos de carácter personal.
- Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.

- Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.
- Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Se han contrastado las normas sobre gestión de seguridad de la información.
- Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

8. PROCEDIMIENTOS DE EVALUACIÓN.

Utilizando la observación y el análisis de los trabajos desarrollados, se utilizarán los siguientes instrumentos de evaluación:

1. El trabajo individual y en equipo del alumno.
2. Actitud abierta, constructiva y participativa en un ambiente de trabajo en grupo y relaciones ante usuarios. La investigación de los contenidos. Iniciativa propia en la búsqueda de soluciones a los problemas planteados.
3. Criterios actitudinales como la participación en clase, correcta utilización del material y equipos. Responsabilidad en su trabajo.
4. Orden y método en el trabajo desarrollado.
5. Realización y presentación de las prácticas solicitadas por el profesor. Exactitud, pulcritud y puntualidad en la documentación. Entrega en fecha de las prácticas obligatorias y trabajos optativos.
6. Participación y elaboración de los trabajos optativos.
7. Pruebas escritas, con contenidos teóricos y prácticos que cada alumno resolverá de forma individual.

Se considera que estos instrumentos de evaluación son adecuados para los criterios de evaluación de este módulo.

9. CRITERIOS DE CALIFICACIÓN.

Las calificaciones del módulo estarán sujetas a lo dispuesto en la Orden del 29 de Septiembre de 2010 por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de Formación Profesional Inicial que forma parte del Sistema Educativo en la Comunidad Autónoma de Andalucía (BOJA nº 102 del 15 de Octubre de 2010) y en el Real Decreto 1538/2006, de 15 de Diciembre, por el que se establece la ordenación general de la Formación Profesional del Sistema Educativo.

Dado el carácter práctico de la Formación Profesional, se establece una calificación mixta entre los contenidos evaluados en actividades teórico-prácticas por cada una de las evaluaciones parciales.

En cada una de las evaluaciones se calificarán los siguientes criterios:

- Evaluación de pruebas, individuales y colectivas, teórico-prácticas.

- Criterios actitudinales, a saber, trabajo en equipo, investigación de los contenidos, asistencia regular a clase y puntualidad, correcta utilización del material y equipos, participación continuada en clase, etc.

- Calificación de las prácticas. La calificación de cada uno de los proyectos se regirá por los criterios, entre otros:

    - Dificultad de los contenidos tratados.
    - La capacidad del grupo para buscar información y resolver problemas por él mismo
    - La calidad de su exposición y defensa y de la documentación

En cada una de las evaluaciones se calificarán los siguientes criterios:

- Prueba/s de contenido práctico-teórico y realización de prácticas de carácter obligatorio, una calificación entre 0 y 5. Es necesario haber entregado previamente todas las prácticas obligatorias solicitadas para poder hacer media.

- Una vez obtenido al menos un 2.5 en el punto anterior, se podrá tener en cuenta la realización de prácticas y proyectos para obtener los otros 5 puntos, donde se valorará la dificultad y calidad de los contenidos y calidad de la defensa.
- Posible realización de un trabajo individual final de módulo, de carácter obligatorio, que abarque contenidos relacionados con los contenidos descritos. Valoración de 0 a 10.
- Los criterios actitudinales necesarios para la adquisición de las competencias profesionales, será tenidos en cuenta para el redondeo de la calificación, por exceso o por defecto, al ser ésta un número entero sin decimales.

El alumno deberá superar cada una de las evaluaciones parciales del curso. La calificación final del módulo corresponde a la media aritmética de las calificaciones obtenidas en las dos evaluaciones parciales, en el caso de que todas ellas estén aprobadas.

Véase la programación del ciclo formativo en lo referente a la actuación a seguir respecto a las faltas de asistencia.

En el caso de que un alumno incurra en cualquier acto de deshonestidad académica como copiar exámenes o prácticas (serán culpables todas las partes implicadas, a no ser que se demuestre que el material ha sido obtenido por el copiador sin el consentimiento ni conocimiento del copiado), incumplimiento deliberado de las normas de seguridad e higiene en el aula de informática u otras indicadas en el ROF, destrozo voluntario de material del aula ya sea de forma física o mediante ataque con virus, troyanos o similares, sólo se evaluará al alumno atendiendo a la convocatoria ordinaria.

10. ACTIVIDADES DE RECUPERACIÓN Y EVALUACIÓN ORDINARIA.

Al final del segundo trimestre, se hará una recuperación para cada una de las evaluaciones no superadas. Si un alumno no superase una o varias evaluaciones, deberá recuperar todas las evaluaciones, superadas o no, en la prueba final que se realizará en la convocatoria ordinaria

En el examen final de la convocatoria ordinaria, el alumno deberá recuperar:

1. Todos los bloques y unidades didácticas vistas durante el curso escolar, independientemente de si hubiese superado alguna de ellas.
2. La calificación final se obtendrá a través de una prueba con contenido teórico-práctico. La calificación ha de oscilar entre 5 y 10 para aprobar el módulo. Asimismo, pueden requerirse con carácter obligatorio para aprobar el módulo, independiente de la calificación de la prueba teórico-práctica, la realización de prácticas relativas a las unidades trabajadas durante el curso escolar.

Los alumnos que, después de la primera convocatoria tengan el módulo no superado, accederán a la segunda convocatoria de otro curso académico, y se regirán por la misma programación y mismos criterios que aquellos alumnos matriculados en dicho módulo para ese nuevo curso académico.

Es responsabilidad del alumno preguntar y realizar el seguimiento de las explicaciones realizadas en clase, entrega de prácticas, fechas de pruebas teórico-prácticas, los días en que se ausente.

Aquellos alumnos que una vez conocida la nota de las evaluación parcial final al finalizar el segundo trimestre, y deseen subir nota, deberán de notificarlo por escrito a Jefatura de Estudios, asistir a las clases habilitadas en este período y realizar una prueba teórico-práctica en la convocatoria ordinaria de Junio. Podrán requerirse además de la prueba teórico-práctica, la elaboración de nuevos trabajos prácticos propuestos con carácter obligatorio.

11. MATERIAL DIDACTICO Y RECURSOS ESPECÍFICOS DEL MÓDULO.

Las clases se basarán principalmente en el uso del proyector y pizarra. Aunque estos elementos se utilizarán primordialmente para la exposición de los contenidos teóricos-prácticos del módulo.

Para la realización de los ejercicios prácticos el alumno contará con ordenador con S.O.

Windows, Linux, servidor, software de virtualización, software de simulación y seguridad de redes, conexión a Internet, apuntes y prácticas elaboradas por la profesora, manuales específicos, revistas de redes, enlaces web, y plataformas que permitan intercambio de documentación con el alumnado.

12. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES.

Véase programación del ciclo formativo.

Para el grupo S21AR, se realizará una actividad complementaria y evaluable en relación a los contenidos trabajados en la unidad de trabajo 3 (criptografía). Se trata de la participación de un proyecto coordinado por el Ayuntamiento de Málaga, a saber, TEME, donde en este caso concreto, los alumnos del grupo S21AR, pondrán de manifiesto los conocimientos adquiridos en dicha unidad de trabajo, al servicio de un grupo de mayores de la asociación de vecinos de la zona donde está ubicado el centro docente. El fin es que los alumnos les proporcionen las herramientas y conocimientos necesarios para poder usar la administración electrónica y acercarles a los beneficios hoy día de utilizarla.

13. SEGUIMIENTO Y AUTOEVALUACIÓN del profesorado.

La autoevaluación del profesorado está englobada en el Proyecto Educativo del Centro (según su plan de autoevaluación del centro), y se percibe como una forma de mejora y calidad de la enseñanza.

La autoevaluación del profesorado es una práctica constante y continua en el Departamento de Informática, que demuestra a lo largo de cada curso escolar una innovación de metodologías. Esta autoevaluación del trabajo docente suele ser un proceso interno, de reflexión intrínseca y de necesidad esencial en el trabajo del profesorado.

Sin embargo, siempre es conveniente realizar una reflexión del trabajo y quehacer de la labor del profesor, por ello una vez acabado la ter evaluación parcial, se facilitará un cuestionario

escrito anónimo al alumnado que permita al profesor reflexionar y mejorar su trabajo y otros aspectos de la metodología empleada. No sólo se realizará la evaluación de los alumnos. Al finalizar cada curso académico, el profesor pasará a los alumnos un cuestionario para que éstos evalúen, de forma anónima, la práctica docente y expresen libremente todas las deficiencias, sugerencias y mejoras que observen en el proceso de enseñanza-aprendizaje. En concreto, el cuestionario de evaluación de la práctica docente recogerá los siguientes aspectos:

- Claridad del profesor en las explicaciones de las diferentes unidades didácticas.
- Grado de cumplimiento de los objetivos marcados.
- Grado de adecuación de la metodología utilizada con los temas a explicar.
- Grado de estimulación de la participación en clase por parte del profesor.
- Grado de motivación a los alumnos por parte del profesor.
- Grado de amenidad de las clases.
- Grado de adecuación de las actividades propuestas con los temas tratados.
- Grado de adecuación del ritmo de las clases a los objetivos del módulo y nivel de los alumnos.
- Grado de adecuación de la evaluación realizada con el nivel trabajado en clase.
- Organización del aula, grupos de trabajo y tareas dentro de cada unidad didáctica

14. MATERIAL BIBLIOGRÁFICO.

Jesús Costas Santos. Seguridad y alta disponibilidad. Madrid. Ra-Ma.

Triviño Mosquera, Ignacio. Seguridad y alta disponibilidad. Madrid. Síntesis. 2019.

Abad Domingo, Alfredo. Seguridad y alta disponibilidad Madrid. Garceta. 2018.

Costas Santos, Jesús. Hacking Linux Exposed. 3rd edition. Seguridad y Alta Disponibilidad. RA-MA.

Dauzon, Samuel. Git. Controles sus versiones. Ediciones ENI. 2018

Hacking Windows Exposed.

UNIX and Linux System Administration Handbook (4th edition) Pro Data Backup and Recovery

Practical UNIX and Internet Security Hacking Exposed. Malware and rootkits

Hacking Exposed. Network Security Secrets and Solutions Hacking. The next generation.

Foundations of security.

IT Security Interviews Exposed.

Webgrafia y recursos web necesarios para desarrollo, ampliación y refuerzo, aportados por la profesor@s.

ANEXO. CRITERIOS Y PROCEDIMIENTOS PREVISTOS PARA ORGANIZAR LA ATENCIÓN A LA DIVERSIDAD DE LOS ALUMNOS

Se realizarán las adaptaciones necesarias en los medios y procedimientos de evaluación para el alumnado con necesidades específicas de apoyo educativo, con el fin de garantizar su accesibilidad a las pruebas y que sea evaluado con los medios apropiados a sus posibilidades y características. No habrá adaptaciones significativas y el proceso y criterios de evaluación serán los mismos que para cualquier otro alumno.

Teniendo en cuenta la normativa Andaluza, en la Ley 17/2007, de 10 de diciembre, de Educación en Andalucía (LEA) en su artículo 113 (Principios de equidad) define alumnado con necesidades educativas específicas de apoyo educativo (n.e.a.e) como aquel que presenta necesidades educativas especiales debidas a diferentes grados y tipos de capacidades personales de orden físico, psíquico, cognitivo o sensorial; el que, por proceder de otros países o por cualquier otro motivo, se incorpore de forma tardía al sistema educativo, al alumnado con altas capacidades intelectuales, así como el alumnado que precise de acciones de carácter compensatorio.

Respecto a la formación profesional, en la LEA Artículo 69, se establece que la Administración educativa establecerá medidas de acceso al currículo, así como, en su caso, adaptaciones y exenciones del mismo, dirigidas al alumnado con discapacidad que lo precise en función de su grado de minusvalía.

En ningún caso, las adaptaciones curriculares supondrán la supresión o modificación de objetivos (competencias profesionales) relacionados con la competencia profesional básica característica de cada título. Por tanto, éstas solo afectarán a la metodología: actividades y temporización necesaria para la obtención de los objetivos.

Cada una de estas medidas son fundamentales a la hora de disminuir las dificultades de aprendizaje del alumnado, pero para ello es imprescindible una detección y atención temprana de las dificultades que presenta nuestro alumnado para poderle ofrecer una atención educativa eficaz y ajustada a sus necesidades. Durante el proceso de detección precoz y tratamiento de las dificultades juega un papel relevante los profesionales de orientación que junto con equipo educativo adaptarán los procesos de enseñanza-aprendizaje al alumnado. Todo esto intentando siempre integrar al alumno con el resto de compañeros.

Teniendo en cuenta lo anterior, en lo referido a la imposibilidad de disminuir la adquisición de objetivos que incidan en las competencias profesionales del título, podremos hacer un acercamiento del currículo al alumno, básicamente adaptando la metodología, la temporalización y los recursos, en los dos siguientes casos:

Con respecto a los alumnos que presenten alguna discapacidad física según sea ésta temporal o permanente se actuará de diferente forma. Para las discapacidades físicas permanentes se realizarán las adaptaciones curriculares que sean oportunas, basadas en la adaptación de los espacios, aspectos físicos, equipamiento y recursos. En el caso de discapacidades físicas temporales se realizará la adaptación que se considere más adecuada para cada caso particular durante el tiempo que dure la discapacidad. Cuando sea necesario, se facilitarán los medios materiales más apropiados para que estos problemas no impidan el normal seguimiento del módulo. Se podrán utilizar pantallas más grandes, mejor posición en el aula (primeras filas), teclados adaptados, etc. Algunas de estas necesidades educativas

especiales pueden requerir la aparición de nuevas personas que nos ayuden en el aula, por ejemplo un traductor de lenguaje de signos.

Para aquellos alumnos con un ritmo de aprendizaje más lento estableceremos un sistema de atención personalizada tratándoles de orientar hacia la realización de las actividades más básicas que cumplan los objetivos marcados para el módulo, ayudándoles en la resolución de problemas, dándoles más tiempo para la realización de ejercicios, prácticas, trabajos, y proponiéndoles actividades de refuerzo que les permitan la comprensión de los contenidos trabajados en clase. El objetivo es que sean capaces de alcanzar el nivel de sus compañeros y continúen el desarrollo normal de las clases sin perderse. Sobre estos alumnos recaerá la figura del ayudante del profesor como tutor de dichos alumnos y, en el caso de problemas más serios, se pedirá la ayuda del departamento de orientación o de alguna entidad especializada en el tema.

En el caso de alumnos extranjeros con problemas de comunicación asociados al lenguaje sería conveniente que se les dedicase alguna hora a la semanal para su más rápida compresión de la lengua. Esto podría ser llevado a cabo por profesorado del centro en las horas de libre configuración para poder normalizar en la lengua a este tipo de alumnado ayudado en la medida de lo posible por los profesores de las materias impartidas para que adapten sus materiales a la lengua nativa del alumno. Siempre que sea posible, se les remitirá a documentación o recursos que utilicen su idioma nativo para facilitar la comprensión de los conceptos. Se les orientará para que reflejen, en las actividades comunes, parte de la cultura del país de origen, facilitando así también la interculturalidad.

Para los alumnos con sobredotación, existirán una serie de ejercicios de ampliación y bibliografía avanzada, que promoverá que estos alumnos investiguen por su cuenta. Estas actividades profundizarán sobre las actividades que se desarrollan en clase, e intentarán despertar en el alumno el concepto de investigación y de superación.

También podrán implicarse en la ayuda a sus compañeros de clase como monitores en aquellas actividades en las que demuestren mayor destreza. Con esta medida se pretende además trabajar las habilidades sociales de los alumnos y alumnas, reforzando la cohesión del grupo y fomentando el aprendizaje colaborativo.

Véase también la programación del ciclo formativo.