CICLO SUPERIOR

CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE TECNOLOGÍAS DE LA INFORMACIÓN

PROGRAMACIÓN ANUAL

Parte específica del módulo:
5022. Bastionado de Redes y Sistemas

Departamento de Familia Profesional de Informática

Curso: 2023-24
Nivel: N/A
Turno: tardes
Profesor: Alejandro Roca Alhama
Desdoble: no existe durante este curso

ESQUEMA DE CONTENIDOS

1 CARACTERÍSTICAS GENERALES DEL CURSO DE ESPECIALIZACIÓN EN CIBERSEGURIDAD EN ENTORNOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Se relacionan en la parte general de la programación del ciclo formativo.

2 DESCRIPCIÓN DEL MÓDULO

El módulo profesional de Normativa de ciberseguridad, al cual hace referencia esta programación didáctica, está enmarcado dentro de las enseñanzas del Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información.

3 UBICACIÓN, OBJETIVOS, CONTENIDOS Y DISTRIBUCIÓN TEMPORAL DEL MÓDULO

3.1 UBICACIÓN, DISTRIBUCIÓN TEMPORAL Y CARACTERÍSTICAS

El Real Decreto 479/2020, de 7 de abril, establece los aspectos básicos del currículo para este curso de especialización que cuenta con un total de 720 horas de duración, de las cuales al módulo profesional de *Bastionado de Redes y Sistemas* le corresponden 95 horas. Todo esto teniendo en consideración el Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

Para este módulo, se han asignado 5 horas semanales en el horario propuesto por la Consejería de Educación de la Región de Murcia que en el calendario actual lectivo de 2022-2023 para el municipio de murcia llegan a sumar 175 horas de clase y equivalentes sin embargo a 10 ECTS en el RD de Título.

3.2 OBJETIVOS/RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

De conformidad con lo regulado en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad, el módulo de *Bastionado de Redes y Sistemas* contribuye a alcanzar las siguientes **competencias profesionales** del curso de especialización:

c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.

d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.

e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.

k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.

m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.

n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.

ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

También contribuye a conseguir los siguientes **objetivos generales**:

e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.

f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.

g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.

h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.

i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.

j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.

q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.

r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.

s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.

t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.

u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».

v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

En cuanto a **resultados de aprendizaje y criterios de evaluación**, el módulo profesional de *Bastionado de Redes y Sistemas* está formado por una serie de resultados de aprendizaje descritos en términos de competencias y que el alumnado debe adquirir como resultado del proceso de enseñanza-aprendizaje. Con cada uno de estos resultados de aprendizaje se encuentran relacionados los criterios de evaluación, mediante los cuales se acredita la consecución de las competencias.

Criterios de evaluación:

RA1. Diseña planes de securización incorporando buenas prácticas para el bastionado de sistemas y redes.

Criterios de evaluación:

a) Se han identificado los activos, las amenazas y vulnerabilidades de la organización.

b) Se ha evaluado las medidas de seguridad actuales.

c) Se ha elaborado un análisis de riesgo de la situación actual en ciberseguridad de la organización

d) Se ha priorizado las medidas técnicas de seguridad a implantar en la organización teniendo también en cuenta los principios de la Economía Circular.

e) Se ha diseñado y elaborado un plan de medidas técnicas de seguridad a implantar en la organización, apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos de la organización.

f) Se han identificado las mejores prácticas en base a estándares, guías y políticas de securización adecuadas para el bastionado de los sistemas y redes de la organización.

RA2. Configura sistemas de control de acceso y autenticación de personas preservando la confidencialidad y privacidad de los datos.

Criterios de evaluación:

a) Se han definido los mecanismos de autenticación en base a distintos / múltiples factores (físicos, inherentes y basados en el conocimiento), existentes.

b) Se han definido protocolos y políticas de autenticación basados en contraseñas y frases de paso, en base a las principales vulnerabilidades y tipos de ataques.

c) Se han definido protocolos y políticas de autenticación basados en certificados digitales y tarjetas inteligentes, en base a las principales vulnerabilidades y tipos de ataques.

d) Se han definido protocolos y políticas de autenticación basados en tokens, OTPs, etc., en base a las principales vulnerabilidades y tipos de ataques.

e) Se han definido protocolos y políticas de autenticación basados en características biométricas, según las principales vulnerabilidades y tipos de ataques.

RA3. Administra credenciales de acceso a sistemas informáticos aplicando los requisitos de funcionamiento y seguridad establecidos.

Criterios de evaluación:

a) Se han identificado los tipos de credenciales más utilizados.

b) Se han generado y utilizado diferentes certificados digitales como medio de acceso a un servidor remoto.

c) Se ha comprobado la validez y la autenticidad de un certificado digital de un servicio web.

d) Se han comparado certificados digitales válidos e inválidos por diferentes motivos.

e) Se ha instalado y configurado un servidor seguro para la administración de credenciales (tipo RADIUS - Remote Access Dial In User Service).

RA4. Diseña redes de computadores contemplando los requisitos de seguridad.

Criterios de evaluación:

a) Se ha incrementado el nivel de seguridad de una red local plana segmentándola físicamente y utilizando técnicas y dispositivos de enrutamiento.

b) Se ha optimizado una red local plana utilizando técnicas de segmentación lógica (VLANs).

c) Se ha adaptado un segmento de una red local ya operativa utilizando técnicas de subnetting para incrementar su segmentación respetando los direccionamientos existentes.

d) Se han configurado las medidas de seguridad adecuadas en los dispositivos que dan acceso a una red inalámbrica (routers, puntos de acceso, etc.).

e) Se ha establecido un túnel seguro de comunicaciones entre dos sedes geográficamente separadas.

RA5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

Criterios de evaluación:

a) Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.

b) Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.

c) Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego.

d) Se han implementado contramedidas frente a comportamientos no deseados en una red.

e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

RA6. Configura dispositivos para la instalación de sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se ha configurado la BIOS para incrementar la seguridad del dispositivo y su contenido minimizando las probabilidades de exposición a ataques.

b) Se ha preparado un sistema informático para su primera instalación teniendo en cuenta las medidas de seguridad necesarias.

c) Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con fines de acceso ilegítimo.

d) Se ha instalado un sistema informático utilizando sus capacidades de cifrado del sistema de ficheros para evitar la extracción física de datos.

e) Se ha particionado el sistema de ficheros del sistema informático para minimizar riesgos de seguridad.

RA7. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Criterios de evaluación:

a) Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema.

b) Se han configurado las características propias del sistema informático para imposibilitar el acceso ilegítimo mediante técnicas de explotación de procesos.

c) Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.

d) Se ha instalado y configurado un Sistema de detección de intrusos en un Host (HIDS) en el sistema informático.

e) Se han instalado y configurado sistemas de copias de seguridad.

El citado **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", establece los siguientes objetivos, expresados como resultados de aprendizaje previsibles y sus correspondientes criterios de evaluación.

4 UNIDADES DE TRABAJO

De las Unidades de Trabajo vamos a prever, en lo posible, los objetivos y resultados de aprendizaje, contenidos, distribución temporal, metodología concreta y criterios de evaluación aplicables.

Contenidos de las Unidades de Trabajo:

UT.00. Introducción a la administración de sistemas Linux

Introducción a la virtualización. Laboratorio a utilizar.
Introducción intérprete comandos.
Admin. básica de sistemas Linux
Procesos
Sistemas de Ficheros.
Gestión de Usuarios.
Systemd.
Gestión de Software.
Configuración de red.

UT.01. Diseño de planes de securización

Conceptos básicos de seguridad.
Análisis de riesgos.
Principios de la Economía Circular en la Industria 4.0.
Plan de medidas técnicas de seguridad.
Políticas de securización más habituales.
Guías de buenas prácticas para la securización de sistemas y redes.
Estándares de securización de sistemas y redes.
Caracterización de procedimientos, instrucciones y recomendaciones.
Niveles, escalados y protocolos de atención a incidencias.

UT.02. Criptografía

Conceptos básicos.
Criptografía moderna.
Aleatoriedad.
Criptografía simétrica.
Funciones Hash.
Keyed Hashing y Authenticated Encryption.
Cifrando discos duros y dispositivos USB.

Criptografía asimétrica.
PKI: Public Key Infrastructure.
OpenSSL.

UT.03. Configuración de sistemas de control de acceso y autenticación

Introducción: identificación y autenticación.
- Identificación y autenticación.
- Factores de autenticación.
- Autenticación multifactor.

Métodos comunes de autenticación.
- Contraseñas.
- Autenticación biométrica.
- OTP: One-time password.
- Dispositivos criptográficos: HSM (Hardware Security Module).
- Estándares FIDO/FIDO2.

Métodos de autenticación: ejemplos prácticos.
- Políticas de contraseñas en Linux y en Windows.
- SSH: autenticación por claves criptográficas.
- Google Authenticator.
- Autenticación con la administración: DNIe, Cl@ve.

Autorización y auditoría.
- Permisos de ficheros en Linux.
- Control de acceso.
- ACL: listas de control de acceso en Linux y en Windows.
- Capacidades.
- Modelos de Control de Acceso.
  - DAC y MAC.
  - Rule-based, role-based, attribute-based, multilevel.
- Auditoría.

UT.04. Acceso a los Sistemas Informáticos

Servicios de directorio.
LDAP.
- OpenLDAP.
- Active Directory.

Gestión de Usuarios y Grupos.
- PAM.
- LDAP.
- Privilegios con sudo.

Single Sign-On.
- Kerberos.

Active Directory: Kerberos + LDAP + DNS.

UT.05. Redes Seguras

Ethernet. VLAN.
Redes TCP/IP.
Protocolos de Red Seguros.
- IPSec.
- TLS.
- SSH.

Seguridad en dispositivos de red.
- 802.1x.
- Seguridad en redes WiFi.
- Radius.
- Sistemas NAC (Network Access Control).

Redes privadas virtuales (VPNs).
- OpenVPN.

Cortafuegos.
- Segmentación de redes. DMZ.
- Cortafuegos en Linux.

Cortafuegos NextGeneration.
- Fortinet.
  - Identificación de aplicaciones.
  - Vinculación del uso de la aplicación a la identidad del usuario.
  - Prevención de amenazas.
  - Simplificación de la administración de políticas.
  - VPN.

Configuración segura de cortafuegos, enrutadores y proxies.

UT.06. Configuración de Dispositivos y Sistemas

Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall).
Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
Seguridad de entornos cloud. Soluciones CASB.
Seguridad del correo electrónico. Protección frente spam, phising y malware.
- Herramientas para el cifrado del correo.

Soluciones DLP (Data Loss Prevention).
Herramientas de almacenamiento de logs.
Protección ante ataques de denegación de servicio distribuido (DDoS).
Monitorización de sistemas y dispositivos.
Herramientas de monitorización (IDS, IPS).
SIEMs (Gestores de Eventos e Información de Seguridad).
Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red:

NOCs y SOCs.

UT.07. Configuración de dispositivos para la instalación de sistemas informáticos

Precauciones previas a la instalación de un sistema informático.

Aislamiento.

Configuración BIOS y gestor de arranque.

Seguridad en el arranque del sistema informático.

BIOE/UEFI.

SecureBoot.

Seguridad de los sistemas de ficheros.

Particionado.

Cifrado.

Cuotas.

UT.08. Securización de sistemas

Bastionado sistemas Linux.

Tareas.

Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.

Bastionado sistemas Windows.

Tareas.

5 DISTRIBUCIÓN TEMPORAL

5.1 DISTRIBUCIÓN TEÓRICA PREVISTA

UT	Título	Horas	Ev
00	UT.00. Introducción a la administración de sistemas Linux	20	1
01	UT.01. Diseño de planes de securización	20	1
02	UT.02. Criptografía	20	1
03	UT.03. Configuración de sistemas de control de acceso y autenticación	20	2
04	UT.04. Acceso a los Sistemas Informáticos	20	2
05	UT.05. Redes Seguras	20	2
06	UT.06. Configuración de Dispositivos y Sistemas	10	3
07	UT.07. Configuración de dispositivos para la instalación de sistemas informáticos	20	3
08	UT.08. Securización de sistemas	25	3
	Total	**175**	

5.2 ANÁLISIS DE LA VIABILIDAD DEL CURRÍCULO PREVISTO

Los contenidos planificados se pueden impartir con bastante holgura ya que el módulo en el RD correspondiente consta de un asignación de 30 horas y en la distribución temporal realizada por la administración educativa de la Comunidad Autónoma de la Región de Murcia para 2022-2023 se le asigna un cómputo de 5 horas semanas que llegan a unas 175 horas anuales, ampliando la imputación horaria del RD.

6 METODOLOGÍA

6.1 CRITERIOS

Se trata en la parte general de la programación del ciclo formativo ASIR.

6.2 ASPECTOS CONCRETOS

Los aspectos metodológicos que se pretenden aplicar 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. De igual forma se pretende que el alumno respete al profesor y a sus compañeros, respectando igualmente el material de la clase.

Este módulo profesional contiene parte de la formación necesaria para desempeñar varias de las funciones de un profesional en el ámbito de la ciberseguridad.

La metodología a utilizar en este módulo estará orientada a promover en el alumnado:

- Su **participación** en los procesos de enseñanza y aprendizaje, de forma que mediante la metodología activa se desarrolle su capacidad de autonomía y responsabilidad personales, de creciente importancia en el mundo profesional.
  - Con este enfoque metodológico activo se evitará la presentación de soluciones únicas y exclusivas a los problemas o situaciones planteados, que quitan al alumnado la posibilidad del descubrimiento propio. De forma que cuando se integren profesionalmente, sepan intervenir activamente en procesos de decisión compartida de forma creativa y positiva, desarrollando un espíritu crítico constructivo y aportando soluciones alternativas.
  - Al ser el alumnado quien construye su propio aprendizaje, el profesor actuará como guía y mediador para facilitar la construcción de capacidades nuevas sobre la base de las ya adquiridas. También se contribuirá a que el alumnado descubra su capacidad potencial en relación con las ocupaciones implicadas en el perfil profesional correspondiente, reforzando y motivando la adquisición de nuevos hábitos de trabajo.
- El desarrollo de la capacidad para **aprender por sí mismos**, de modo que adquieran una identidad y madurez profesionales motivadoras de futuros aprendizajes y adaptaciones al cambio de las cualificaciones.
- El desarrollo de la capacidad para **trabajar en equipo**, por medio de actividades de aprendizaje realizadas en grupo, de forma que cuando en el ámbito profesional se integren en equipos de trabajo puedan mantener relaciones fluidas con sus miembros, colaborando en la consecución de los objetivos asignados al grupo, respetando el trabajo de los demás, participando activamente en la organización y desarrollo de tareas colectivas, cooperando

en la superación de las dificultades que se presenten con una actitud tolerante hacia las ideas de los compañeros, y respetando las normas y métodos establecidos.

En relación con la forma de organizar el aprendizaje significativo de los contenidos se han tenido en cuenta las siguientes orientaciones:

- Teniendo en cuenta que las actividades productivas o de creación de servicios requieren de la acción, es decir, del "**saber hacer**", los aprendizajes se han articulado fundamentalmente en torno a los procedimientos y tomando como referencia las capacidades profesionales asociadas al módulo.
- Además del "saber hacer", tiene una importancia cada vez más creciente en el mundo productivo el dominio del "saber estar", adquiriendo relevancia los aspectos actitudinales.
- Para que el aprendizaje sea eficaz, debe establecerse también una secuencia precisa entre todos los contenidos que se incluyen en el período de enseñanza-aprendizaje del módulo profesional.

Se han planificado con mucho cuidado las actividades del proceso de enseñanza-aprendizaje de cada unidad de trabajo, teniendo en cuenta:

- Las capacidades que deben construir el alumnado y los contenidos que de ellas se derivan.
- Las capacidades conceptuales, procedimentales y actitudinales previas detectadas en el alumnado, relacionadas con las capacidades del currículo.
- Los recursos con los que cuenta el centro y las entidades colaboradoras del entorno.
- El tiempo disponible.

Generalmente en cada unidad de trabajo se comenzará con teoría y se pasará a la práctica en cualquier momento del proceso de enseñanza-aprendizaje. Las actividades de aprendizaje que desarrollen simularán ambientes reales.

Para promover la adquisición, por parte del alumnado, de una visión global y coordinada de los procesos a los que está vinculada la competencia profesional del título, se intentarán realizar actividades de carácter interdisciplinar para varios módulos del ciclo formativo.

Cuando se estime oportuno se fomentará el debate entre el grupo de alumnos, de tal forma que estos podrán reflexionar sobre la importancia de lo que se haya tratado.

7 MATERIALES, RECURSOS, ESPACIO DOCENTE

7.1 MATERIALES Y RECURSOS DIDÁCTICOS

Parte de este apartado se trata en la parte general de la programación del ciclo formativo ASIR.

Para la correcta marcha de este módulo cada alumno ha de disponer de su propio ordenador para el seguimiento de las clases, así como para la realización de las instalaciones y configuraciones de software. Es absolutamente negativo que dos o más personas compartan un mismo puesto de trabajo, por lo que en el caso de que el número de alumnos sea superior al de equipos en el aula, se propondrá un desdoble del grupo. Si no es posible el desdoble y el número de alumnos en el aula es superior a la capacidad nominal de estas aulas, se elevará a instancias superiores la necesidad de un profesor de apoyo, con el fin de conseguir una atención personalizada que, de otra forma, va a ser imposible de alcanzar.

En cuanto a otro material didáctico, se utilizará activamente la PDI (Pizarra Digital Interactiva), y el soporte de la instalación Moodle del IES Ingeniero de la Cierva, desarrollándose un curso Moodle específico para el módulo. El profesor imparte docencia directamente sobre un entorno similar al de los alumnos, es decir, un ordenador personal equipado con S.O. Linux. Se atenderá especialmente al uso de software libre mucho más adecuado al espíritu de la Comunidad y de la filosofía de distribuciones de Linux (como Ubuntu, Mint o Fedora), y casi la única opción que permite la actual situación de profunda penuria económica que aflige al sistema educativo público.

Se utilizarán pues:

- Apuntes elaborados por el Profesor.
- Artículos de revistas relacionados con los contenidos previstos.
- Todo tipo de documentación electrónica para ser utilizada como eje estructurador de la explicación de la materia. Será visualizada en forma interactiva por el alumno a la vez que se proyectan en pantalla mediante cañón.
- Supuestos para su resolución en clase y a domicilio.
- Bibliografía básica y complementaria.
- Sistemas informáticos adecuados con el software correspondiente que ser. fundamentalmente:
  - Distribuciones de Linux: Ubuntu, Mint, Debian y Fedora.
  - Sistemas propietarios como Windows.
  - Plataforma de e-learning Moodle que dará soporte a todos los materiales y actividades que se vayan trabajando/realizando. El módulo dispondrá de un curso completo Moodle que se irán actualizando permanentemente para que refleje la realidad del proceso docente.
  - Pizarra digital interactiva y software asociado: el docente desarrollar. sus tareas de explicación y ejemplificación de prácticas en una PDI. El material generado será exportado a pdf y colocado en la zona Moodle del curso.

Además de este equipamiento de uso directo, es imprescindible contar con:

- Hardware.
  - Cableado, conmutadores/routers, y tarjetas de red.
  - Equipos servidores de red.
  - Impresoras.
  - Firewalls físicos.
- Software.
  - Sistema operativo de red en servidores (Linux, Windows Server).
  - Sistema operativo adicional de estación (Linux, Windows).
  - Software de ofimática (LibreOffice).
  - Software de tratamiento de gráficos, de vídeo, de sonido, etc.
  - Software y entornos de desarrollo.
- Elementos auxiliares
  - Pizarra blanca.
  - Cañón para presentaciones.
  - Acceso a redes exteriores (Internet).

7.2 DISTRIBUCIÓN DEL ESPACIO Y EL TIEMPO DOCENTE

Se opta por la "organización tipo A" que se explica en la parte general de la programación del ciclo formativo.

Se solicita también la agrupación de las sesiones de clase en bloques de al menos 2 horas seguidas, pues está comprobado que en módulos de tipo informático agrupaciones de menor duración no son prácticas. La agrupación más adecuada sería un día 3 y otro dos de 2 períodos lectivos.

7.3 FUNCIONES DEL PROFESOR DE APOYO (DESDOBLE)

7.3.1 JUSTIFICACIÓN DEL APOYO

De acuerdo a la "Orden de 21 de junio de 2012, de la Consejería de Educación, Formación y Empleo, por la que se establecen criterios generales para la determinación de necesidades reales de profesorado en Institutos de Educación Secundaria", las circunstancias que determinan la necesidad de horas de desdoble para el presente módulo formativo según lo indicado en el artículo 15 sobre apoyos en módulos profesionales de formación profesional son:

a) Apoyo por atención educativa (AAE).

El módulo formativo ISO tiene la peculiaridad de aspirar a obtener por parte del alumno unos resultados de aprendizaje que requieren un especial apoyo de otro profesor de la familia profesional para un mejor desarrollo pedagógico ya que las actividades requieren un trabajo individualizado a realizar por los alumnos en la utilización de equipos informáticos.

c y d) Apoyo por riesgo medio/bajo y alto:

El módulo formativo ISO requiere el acceso a taller en diferentes momentos, donde se realizarán tareas de montaje, mantenimiento y configuración de equipos informáticos que conlleva la utilización de diferentes de herramientas, además de estar interaccionando con componentes hardware desmontados y conectados a corriente eléctrica.

Algunas de estas actividades también son llevadas a cabo en el aula, trasladando el material necesario al aula.

Se procurará que los apoyos sean los días en que hay varias horas seguidas, dado que las prácticas pueden durar más de un periodo lectivo.

7.3.2 FUNCIONES Y OBJETIVOS DEL PROFESOR DE APOYO

La funciones y objetivos que se persigue por parte del profesor de apoyo son:

- Desarrollo de prácticas, preparando materiales y configurando equipos para ampliar la calidad y cantidad de los ejercicios con un mejor aprovechamiento de los recursos disponibles.

- El tipo de intervención del profesor de apoyo en general permitirá la potenciación del proceso formativo del alumno con actividades complejas, que requieren un tratamiento individualizado o en grupos reducidos. Realizará la supervisión del correcto desarrollo de las mismas.
- Aseguramiento de la calidad
- Reducción del peligro de riesgos laborales en las tareas de taller.

7.3.3 METODOLOGÍA EMPLEADA EN LOS APOYO

La metodología utilizada está marcada por las siguientes pautas:

El profesor de la asignatura impartirá en clase los conocimientos necesarios para poder desarrollar la práctica, pudiendo dedicar el principio de la hora en que se desarrolla el apoyo para recordar los aspectos más importantes de la misma, así como los aspectos relativos a la prevención de riesgos laborales asociados a la práctica en cuestión.

Ambos profesores supervisarán la realización de la misma, asesorando al alumnado en todos aquellos aspectos que necesiten.

Ambos profesores velarán por que los alumnos dispongan de los recursos necesarios para el correcto desarrollo de las prácticas, así como del correcto uso de los mismos.

7.3.4 EVALUACIÓN DE LAS ACTIVIDADES DE APOYO

La evaluación de las actividades que se desarrollen en la/s horas de apoyo será realizada según los mismos criterios de evaluación expresados en el apartado correspondiente de esta programación.

Periódicamente en las reuniones de departamento se analizará y evaluará la marcha de los apoyos.

Se utilizará una hoja de seguimiento compartida, entre los profesores del módulo, en la que se irán detallando las actividades de apoyo desarrolladas en cada sesión, así como las observaciones pertinentes sobre el desarrollo de la misma.

7.3.5 ACTIVIDADES REALIZADAS DURANTE LAS HORAS DE APOYO

Se intentará desarrollar las actividades que contengan mayores elementos procedimentales (normalmente las denominadas “prácticas de taller o laboratorio”) en las sesiones semanales establecidas como Apoyo, dado que son sesiones en las que se necesita incrementar la atención personalizada de los alumnos.

Los dos profesores están en el aula en la que se forma grupos de alumnos que realizaban la correcta realización de la práctica, comprobando su adecuada implementación.

Este curso NO EXISTE APOYO EN ESTE MÓDULO.

8 MEDIDAS PARA ESTIMULAR EL INTERÉS Y EL HÁBITO DE LECTURA Y LA CAPACIDAD DEL ALUMNO PARA EXPRESARSE CORRECTAMENTE

Este apartado se estudia en la parte general de la programación del ciclo.

9 CRITERIOS, PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

Además de lo indicado en la parte general, comentamos aquí los aspectos particulares del módulo.

Usaremos el Modelo 3 de la programación general con las siguientes concreciones.

La calificación del módulo profesional en la convocatoria ordinaria estará sujeta a las pruebas objetivas y ejercicios en clase con la siguiente **cuantificación**:

Participación	10%
Pruebas teórico/prácticas	55%
Ejercicios y prácticas	35%

Cada uno de los apartados anteriores comprende:

Participación	Tener iniciativa para la demanda de información. Aporte de información al aula para su estudio y análisis. Preocupación por organizar su propio trabajo y las tareas colectivas. Tenacidad y perseverancia en la búsqueda de soluciones a los ejercicios propuestos. Pulcritud personal en la realización del trabajo.
Pruebas teórico/prácticas	Pruebas escritas de desarrollo. Pruebas escritas de preguntas cortas. Pruebas escritas tipo test. Pruebas orales. Pruebas de cualquier otra naturaleza. Pruebas a desarrollar con el ordenador.
Ejercicios y prácticas	Ejercicios. Prácticas. Trabajos. Exposiciones/presentaciones. Proyectos.

Respecto a los ejercicios y prácticas y las pruebas objetivas, todas ellas tienen una fecha de entrega o realización que será improrrogable a excepción de una causa debidamente justificada. Las no realizadas o no entregadas en el plazo y forma estipuladas tendrán una calificación de 0 puntos.

Esta calificación de 0 puntos será incluida en el cálculo de la media ponderada en ambos elementos (Ejercicios/Prácticas y Pruebas Objetivas).

Debido a que no todas las pruebas teórico/prácticas tienen el mismo grado de dificultad, todos las pruebas teórico/prácticas tendrán una ponderación según un número de créditos. Dicho número de créditos intenta ponderar las pruebas por volumen de contenido y por dificultad. La nota media de las pruebas teórico/prácticas será una nota media ponderada según ese numero de créditos.

Debido a que no todas los ejercicios y prácticas tienen el mismo grado de dificultad, todos los ejercicios y prácticas tendrán una ponderación según un número de créditos. Dicho número de créditos intenta ponderar los ejercicios y prácticas por tiempo de realización y dificultad. La nota media de los ejercicios y prácticas será una nota media ponderada según ese numero de créditos.

La calificación de cada evaluación será la media ponderada de cada una de las tres partes de la tabla superior, siendo condición necesaria el superar positivamente de forma separada las pruebas objetivas y los ejercicios y prácticas.

Ejemplo de calificación:

Examen 1 (12 créditos):	7,00
Examen 2 (8 créditos):	8,00
Examen 3 (20 créditos):	3,00
Práctica 1 (14 créditos):	6,00
Práctica 2 (20 créditos):	10,00
Práctica 3 (6 créditos):	7,00
Actitud (10%):	**7,35**
Pruebas (55%):	**5,20**
Prácticas (35%):	**8,15**
Nota Final:	**6,45**

Como la materia es eliminatoria, todas las pruebas teórico-prácticas contaran con otra prueba de recuperación, no así los ejercicios y prácticas. **Los ejercicios y prácticas no se pueden recuperar.**

Serán requisitos imprescindibles para la superación del módulo en evaluación continua:

- Que las faltas de asistencia a clase no superen las establecidas en el diseño curricular del Centro recogidas en el reglamento de régimen interior.
- Que la actitud personal del alumno hacia profesores y resto de compañeros sea correcta.
- Que la media ponderada de los tres elementos de la tabla anterior sea igual o superior a 5 y que se hayan superado por separado las pruebas objetivas y los ejercicios y prácticas.

La **calificación final del módulo** tendrá una cuantificación numérica entre 1 y 10, sin decimales. Se considerarán como positivas las comprendidas entre 5 y 10, y negativas las restantes. Se

calculará con la media aritmética de la obtenida en las 3 evaluaciones, siempre y cuando todas ellas tuvieran evaluación positiva. En cualquier otro caso, la calificación será negativa.

Proceso de recuperación.

Durante el curso, todas las pruebas teórico/prácticas contarán con un prueba de recuperación. El alumno tendrá la opción de presentarse a cada una de estas pruebas. Por el contrario, los ejercicios y prácticas no cuentan con una recuperación. Si la media de los ejercicios y prácticas no supera el 5, el alumno irá directamente a una prueba teórica/práctica final en junio.

En la fecha fijada para la convocatoria de junio, el alumno deberá realizar una prueba objetiva teórico-práctica en la que se comprueben la adquisición de las competencias profesionales del alumno sobre los contenidos del módulo, así como las capacidades terminales adquiridas. Debido a la amplitud de los contenidos la duración de esta prueba podrá oscilar entre 2 y 6 horas.

La calificación del módulo en la convocatoria de junio será la obtenida por el alumno en la Prueba Objetiva.

Procedimientos de recuperación extraordinaria

En la fecha fijada para la convocatoria de septiembre, el alumno deberá realizar una prueba objetiva teórico-práctica en la que se comprueben la adquisición de las competencias profesionales del alumno sobre los contenidos del módulo, así como las capacidades terminales adquiridas. Debido a la amplitud de los contenidos la duración de esta prueba podrá oscilar entre 2 y 6 horas.

La calificación del módulo en dicha convocatoria será la obtenida por el alumno en la Prueba Objetiva.

10 ATENCIÓN A LA DIVERSIDAD DEL ALUMNADO EN LOS CICLOS FORMATIVOS

Este apartado se estudia en la parte general de la programación del ciclo.

11 PREVENCIÓN DE RIESGOS LABORALES

Este apartado se estudia en la parte general de la programación del ciclo.

12 INTERDISCIPLINARIEDAD

En este caso, al tratarse de un módulo de contenidos eminentemente prácticos, centrado en el bastionado y securización de sistemas, surgen relaciones de interdisciplinariedad evidentes con el resto de módulos del curso.

13 TRANSVERSALIDAD

Se adopta todo lo que se indica en la parte general de la programación del ciclo.

14 ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se adopta todo lo que se indica en la parte general de la programación del ciclo.

15 USO DE LAS TICS

Este apartado se trata en la parte general de la programación del módulo.

16 BIBLIOGRAFÍA

16.1 BIBLIOGRAFÍA CERCANA AL CURRÍCULO OFICIAL

En este módulo no hay un libro de texto que se vaya a seguir de forma habitual. Los materiales de clase se irán depositando bien en el servidor Moodle del Centro, bien en un servidor FTP accesible al alumnado o indicándose el URL donde pueden ser accedidos.

16.2 BIBLIOGRAFÍA COMPLEMENTARIA

La cantidad de material bibliográfico para un entorno académico como es la Administración de Sistemas es abrumadora, una lista de posibles libros interesantes podría ser:

- ALBITZ, P., LIU, C. **DNS and BIND.** Ed. O'Reilly. 4ªed. 2001.
- ALCALDE E. y GARCÍA M. **Informática básica.** Ed. Mcgraw-Hill. 1994.
- ALCALDE E. y MORERA J. **Introducción a los sistemas operativos.** Ed. Mcgraw-
- Hill. 1991.
- AHO A.V., SETHI R. y ULLMAN J.D. **Compiladores: principios, técnicas y**
- **herramientas.** Ed Addison-Wesley. 1990.
- ANDRESS, J. **Foundations of Information Security.** Ed. No Starch Press. 2019.
- AUMASSON, JP. **Serious Cryptography.** Ed. No Starch Press. 2018.
- BARRETT, D.J., SILVERMAN, R.E. y BYRNES R.G. **Linux Security Cookbook.** Ed.
- O'Reilly. 2003.
- BACON, J. **The Art of Community.** Ed. O'Reilly. 2009.
- BAUER, M.D. **Linux Server Security.** Ed. O'Reilly. 2ªed. 2005.
- BEEKMAN, G. **Introducción a la Informática.** Ed. Prentice Hall. 2005. 6aed
- BERKOUWER, S. **Active Directory Administration Cookbook.** Ed. Packt Publishing. 2ªed. 2022.
- BILLIMORIA, K. **Linux Kernel Programming.** Ed. Packt Publishing. 2021.
- BINNIE, C. **Linux Server Security.** Ed. Wiley. 2016.
- BUTCHER, M. **Mastering OpenLDAP.** Ed. Packt Publishing. 2007.
- CABALLERO, MA, CILLEROS, D. **El libro del Hacker, edición 2022.** Ed. Anaya. 2022.
- CARLING, M. **Administración de Sistemas LINUX.** Ed. Prentice Hall. 1999.
- CARRETERO J.,GARCÍA F., PÉREZ P.M. y PÉREZ F. **Sistemas Operativos. Una visión aplicada.** Ed. McGraw Hill. 2001.
- CARTER, G. **LDAP System Administration.** Ed. O'Reilly. 2003.
- COFFIN S. **Unix. Manual de referencia.** Ed. McGraw-Hill. 1989.
- CURTIS PRESTON, W. **Unix Backup & Recovery.** Ed. O'Reilly. 1999.
- DAKIC, V., y otros. **Mastering KVM Virtualization.** Ed. Packt Publishing. 2ªed. 2020.

- DAUTI. B. **Windows Server 2022 Administration Fundamentals.** Ed. Packt Publishing. 3ªed. 2022.
- FLICKENGER R. **Linux Server Hacks.** Ed. O'Reilly. 2003.
- FRANCIS. D. **Mastering Active Directory.** Ed. Packt Publishing. 3ªed. 2021.
- FRISCH A. **Essential System Administration.** Ed. O'Reilly. 2002.
- GARCÍA. J.L. **Ataques en redes de datos IPv4 e IPv6.** Ed. 0xWORD. 4ªed. 2021.
- GARMAN, J. **Kerberos. The Definitive Guide.** Ed.O'Reilly. 2003.
- GÓMEZ, J., BAÑOS, R. **Seguridad en Sistemas Operativos Windows y Linux.** Ed. Ra-Ma. 2006.
- GREGG, B. **Systems Performance.** Ed. Pearson. 2ªed. 2021.
- GRUBB, S. **How Cybersecurity Really Works.** Ed. No Starch Press. 2021.
- JULIAN, M. **Practical Monitoring.** Ed. O'Reilly. 2018.
- KEMP, J. **Linux System Administration Recipes.** Ed. Apress. 2009.
- LEE, T. **Windows Server Automation with PowerShell Cookbook.** Ed. Packt Publishing. 4ªed. 2021.
- LOCKHART A. **Network Security Hacks.** Ed. O'Reilly. 2004.
- LOUKIDES, M. **System Performance Tuning.** Ed. O'Reilly. 1992.
- LOVE, R. **Linux Kernel Development.** Ed. Addison Wesley. 3ªed. 2010.
- LOVE, R. **Linux System Programming.** Ed. O'Reilly. 2007.
- MANCILL, T. **Routers Linux.** 2aed. Ed. Prentice-Hall. 2003.
- MÁRQUEZ F.M. **Unix Programación avanzada.** Ed. Ra-Ma. 1996.
- MATOTEK, D., TURNBULL, J., LIEVERDINK, P. **Pro Linux system Administration.** Ed. Apress. 2ªed. 2017.
- MAUERER, W. **Linux Kernel Architecture.** Ed. Wrox. 2008.
- MICHAEL, R.K. **Mastering UNIX Shell Scripting.** Ed. Wiley. 2008.
- MILENKOVIC M. **Sistemas operativos, conceptos y diseño.** Ed. McGraw-Hill. 1994.
- NEGUS, C. Linux Bible. **The Comprehensive Tutorial Resource.** Ed Wiley. 10ªed. 2020.
- NEGUS, C., CAEN, F. **Ubuntu Linux Toolbox.** Ed Wiley. 2008.
- NEMETH, E., SNYDER, G., y otros. **UNIX and Linux System Administration Handbook.** Ed. Pearson. 5ªed. 2018.
- NEWHAM C., ROSENBLATT B. **Learning the bash Shell.** Ed. O'Reilly. 1998.
- OXER J., RANKIN, K. Y CHILDERS, B. **Ubuntu Hacks.** Ed. O'Reilly. 2006.
- PEEK J., O'REILLY T., LOUKIDES M. **UNIX Power Tools.** Ed. O'Reilly. 3ªed. 2002.
- PETRELEY N, BACON J. **Linux Desktop Hacks.** Ed. O'Reilly. 2005.
- PRIETO A., LLORIS A. y TORRES J.C. **Introducción a la Informática.** Ed. McGraw-Hill. 2002. 3aed.
- RANKIN, K. **Linux Multimedia Hacks.** Ed. O'Reilly. 2006.
- RANKIN, K., MAKO HILL, B. **The Official Ubuntu Server Book.** Ed. Prentice Hall. 2010.
- SANTOS, S. **Máxima Seguridad en Windows: Secretos Técnicos.** Ed. 0xWORD. 5ªed. 2020.
- SCHRODER C. **Curso de Linux.** Ed. O'Reilly/Anaya. 2005.

- SCHRODER C. **Linux Networking Cookbook.** Ed. O'Reilly. 2007.
- SOBELL M.G. **A Practical Guide to Fedora and Red Hat Enterprise Linux.** Ed. Addison-Wesley Professional. 7ªed. 2013.
- SOBELL M.G. **A Practical Guide to Linux Commands.** Ed. Addison-Wesley Professional. 4ªed. 2017.
- SOBELL M.G. **A Practical Guide to Ubuntu.** Ed. Addison-Wesley Professional. 4ªed. 2015.
- STALLINGS W. **Operating Systems. Internals and Design Principles.** Ed. Pearson. 2017. 9ªed.
- STALLINGS W. **Data and Computer Communications.** Ed. Pearson. 10ªed. 2013.
- TANENBAUM A. S. **Structured Computer Organization.** Ed. Pearson. 6ªed. 2012.
- TAKEMURA, C., CRAWFORD, L.S. **The Book of Xen.** Ed. No Starch Press. 2010.
- TANENBAUM A. S. **Computer Networks.** Ed. Prentice Hall. 5ª ed. 2010.
- TANENBAUM A. S., BOS H. **Modern Operating Systems.** Ed. Pearson. 4ªed. 2016.
- TS, J., ECKSTEIN, R. y COLLIER-BROWN, D. **Using SAMBA.** Ed. O'Reilly. 2ªed. 2003.
- von HAGEN, W., JONES, B.K. **Linux Server Hacks. Volume II.** Ed. O'Reilly. 2006.
- van Vught, S. **Pro Ubuntu Server Administration.** Ed. Apress. 2009.
- WARD, B. **How Linux Works.** Ed. No Starch Press. 3ªed. 2021.
- ZIEGLER R. L. **Firewalls LINUX.** Ed. Prentice Hall. 2000.

16.3 WEBGRAFÍA

Enunciar aquí un conjunto de enlaces web relacionados con el módulo que nos ocupa podría ser tan interminable como inútil, dada la alta variabilidad de estos enlaces de Internet e incluso de los elementos de interés sobre los que se indican enlaces. No obstante hay algunos URL que podrían, a priori, destacar:

- **Apache Software Foundation.** https://apache.org/
- **Blog elhacker.NET.** https://blog.elhacker.net/
- **Cisco Networking Academy** https://www.netacad.com
- **danielmiessler.com.** https://danielmiessler.com/
- **DNS for Rockect Scientists.** https://www.zytrax.com/books/dns/
- **El Confidencia. Teknautas.** https://www.elconfidencial.com/tecnologia/
- **El Mundo. Tecnología.** https://www.elmundo.es/tecnologia.html
- **El País Tecnología.** https://elpais.com/tecnologia/
- **FreeBSD.** https://www.freebsd.org/es/
- **GNU.** https://www.gnu.org
- **Fedora Magazine.** https://fedoramagazine.org/
- **Google.** https://www.google.es
- **Hispasec. UnaAlDia.** https://unaaldia.hispasec.com/
- **It's FOSS.** https://itsfoss.com/
- **Krebs on Security.** https://krebsonsecurity.com/
- **Date followed: Aug 18 2022**

- **LDAP for Rockect Scientists.** https://www.zytrax.com/books/ldap/
- **Linux Debian.** https://www.debian.org
- **Linux Fedora.** https://getfedora.org/es/
- **Linux Mint.** https://linuxmint.com/
- **Linux Red Hat.** https://www.redhat.com/en
- **Linux Ubuntu.** https://ubuntu.com
- **Microsoft.** https://www.microsoft.com
- **MuyLinux.** https://www.muylinux.com/
- **nixCraft.** https://www.cyberciti.biz/
- **Phoronix. Linux Hardware Reviews, Benchmarking & Games.** https://www.phoronix.-com
- **SAMBA.** https://www.samba.org
- **Tecmint.** https://www.tecmint.com/
- **The Geek Stuff.** https://www.thegeekstuff.com/
- **The Linux Documentation Project.** https://www.tldp.org
- **The Linux Kernel Archives.** https://www.kernel.org
- **Threatpost | The first stop for security news.** https://threatpost.com/
- **Toms Hardware.** https://www.tomshardware.com
- **Un informático en el lado del mal.** http://www.elladodelmal.com/
- **Wikipedia.** https://www.wikipedia.org/