MÓDULO:	**BASTIONADO DE REDES Y SISTEMAS**
CURSO ACADÉMICO:	2023/2024

DEPARTAMENTO	**INFORMÁTICA**
CURSO DE ESPECIALIZACIÓN EN	**CIBERSEGURIDAD EN ENTORNOS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN**
PROFESORES	**MANUEL JESÚS HIDALGO GALERA**

ÍNDICE

Índice de tablas

1. INTRODUCCIÓN

En el contexto del actual sistema educativo (LOMLOE, Ley Orgánica 3/2020, de 29 de diciembre), la programación es la planificación del proceso de enseñanza y el aprendizaje. Es decir, programar es planificar, concretar y secuenciar los distintos elementos curriculares, partiendo de la normativa propuesta por la administración educativa, en el marco de la autonomía pedagógica a través de la herramienta de planificación docente, reguladas por el Decreto 327/2010 (Plan de Centro: Proyecto Educativo, Proyecto de Gestión y ROF).

Una programación minimiza la necesidad de improvisación en el aula y evita el azar a la vez que atiende a las necesidades y características específicas del alumnado.

La eficacia de la programación didáctica como instrumento de planificación de la actividad en el aula dependerá de la adecuación al contexto, la concreción al currículo oficial, el nivel de flexibilidad que presenta y que sea factible, es decir, viable.

La finalidad de esta programación será la consecución de las capacidades propuestas en los objetivos del currículo y la adquisición de las competencias profesionales, personales y sociales. Por lo tanto, esta programación del "Curso de especialización en ciberseguridad en entornos de las tecnologías de la información", del módulo de "Bastionado de redes y sistemas", se ha realizado de acuerdo a los objetivos y contenidos de la normativa vigente. *Nota: en adelante, las siglas C.E. se usan para designar "Curso de especialización".*

La programación educativa se concreta en tres niveles denominados niveles de concreción curricular que, según la propuesta de César Coll (2012), son los siguientes:

- **Currículo:** Es dado por la administración educativa.
- **Programación Didáctica:** Se incluye en el Proyecto Educativo y hace referencia a las líneas generales de programación para el curso.
- **Programación de aula:** Es la concreción y secuenciación del currículo a nivel de aula, pormenoriza los elementos curriculares y establece los ejercicios, actividades y tareas a desarrollar.

En los distintos niveles de programación se debe tener en cuenta las fuentes epistemológica, sociológica, pedagógica y psicológica.

En esta programación didáctica se desarrollan objetivos, contenidos, competencias profesionales, personales y sociales, metodología, criterios de evaluación y resultados de aprendizaje evaluables, así como la atención a la diversidad y a las necesidades específicas de apoyo educativo.

1.1. PRESENTACIÓN DEL MÓDULO PROFESIONAL

Esta programación didáctica estructura la enseñanza correspondiente al módulo de "Bastionado de redes y sistemas" correspondiente al "Curso de especialización en ciberseguridad en entornos de las tecnologías de la información".

Este curso de especialización tiene una duración de 720 horas.

Este curso de especialización dispone de una organización modular. El módulo de "Bastionado de redes y sistemas" dispone de una carga lectiva de 150 **horas** que se distribuyen a razón de 5 **horas semanales**.

1.2. MARCO LEGISLATIVO

La Constitución Española de 1.978 establece en su artículo 27 el derecho universal a la educación que queda también regulado en la Ley Orgánica del Derecho a la Educación (LODE, 1985). Asimismo, el Estatuto Andaluz del 2007 garantiza a través del artículo 21 que esta educación será permanente y de carácter compensatorio. Sobre estas bases, el Sistema Educativo se ordena a través de la **Ley de Educación LOMLOE, Ley Orgánica 3/2020, de 29 de diciembre,** que se publicó en el BOE de 30 de diciembre de 2020 y por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo de Educación (LOE), modificada por la Ley Orgánica 8/2013 de Mejora de la Calidad Educativa (LOMCE). En el caso concreto de Andalucía, esta concreción se hace a través de la Ley de Educación de Andalucía (LEA 17/2007).

Esta programación se basa también en el **RD. 1147/11 por el que se establece la ordenación general de la formación profesional del sistema educativo** y en **la Ley Orgánica 5/2002, de 19 de junio, de Cualificaciones y Formación Profesional**, a través de las cuales se ha producido una reforma de la Formación Profesional. Además, se tendrán en cuenta el Decreto 436/2008, de 2 de septiembre, por el que se establece la ordenación y las enseñanzas de la Formación Profesional inicial que forma parte del sistema educativo, así como 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.

El "Curso de especialización en ciberseguridad en entornos de las tecnologías de la información" queda regulado a través del **Real Decreto 479/2020, de 7 de abril,** que en Andalucía se ordena a través de la **Resolución de 9 de Septiembre de 2022**.

Entre otras cosas, este Real Decreto nos muestra las Unidades de Competencia que se trabajarán en este C.E., de modo que se relacione de forma efectiva con el mundo laboral. Este es uno de los grandes objetivos del nuevo sistema de la Formación Profesional que pretende que la formación se entienda como una actividad que se desarrolla a lo largo de toda la vida y que se adapta a las situaciones concretas del individuo.

Este objetivo se instrumentaliza a través de la **Ley 5/2002 sobre las Cualificaciones y la Formación Profesional**, que basándose en el mercado laboral actual, construye las Cualificaciones Profesionales y las presenta en forma de las Unidades de Competencia necesarias para alcanzarla. Toda esta información junto con el contenido de la formación profesional asociada se organiza en un **Catálogo Nacional de Cualificaciones Profesionales regulado por el RD 1128/03**. Estas unidades de competencia se podrán conseguir desde el mundo laboral, a través de los certificados de profesionalidad o desde cualquiera de los subsistemas de la Formación Profesional: la formación profesional del sistema educativo, que es donde nosotros trabajamos, y la formación profesional para el empleo.

1.3. ENTORNO PROFESIONAL DEL TÍTULO

Las ocupaciones y puestos de trabajo más relevantes en los que desarrollarán su actividad profesional los alumnos/as que cursen este curso, según lo dispuesto en la normativa que lo regula son las siguientes:

Este profesional ejercerá su actividad en entidades de los sectores donde sea necesario establecer mecanismos y medidas para la protección de los sistemas de información y redes de comunicaciones.

Las ocupaciones y puestos de trabajo más relevantes son los siguientes:

a) Experto en ciberseguridad.

b) Auditor de ciberseguridad.

c) Consultor de ciberseguridad.

d) Hacker ético.

2. CONTEXTO

Una de las características de la ley educativa, es que se proporciona autonomía pedagógica a los centros educativos para adaptar la enseñanza de F.P. a la realidad social y económica del centro donde se impartirán.

Si bien el contexto socioeconómico se trata ampliamente en el Proyecto Educativo, se señala en este apartado el marco socioeconómico, así como el tipo de alumnado al que se dirige esta programación didáctica.

2.1. CONTEXTO SOCIOECONÓMICO

El actual modelo curricular, abierto y flexible, posibilita adecuar la programación didáctica a distintos contextos educativos teniendo en cuenta las características del entorno escolar del Centro y de los alumnos y alumnas.

Esta programación se ha elaborado considerando el siguiente contexto educativo: un centro docente donde se imparten los ciclos formativos de grado superior ASIR, DAM y DAW, situado en Jaén, una ciudad de aproximadamente 110.000 habitantes. El centro se encuentra en una zona habitada por una población de clase media/alta mayoritariamente.

Al tratarse de un tipo de enseñanza pos-obligatoria, en este centro se encuentran alumnos/as de otras poblaciones próximas de la ciudad, así como de zonas de la periferia de la misma.

La principal actividad económica en la ciudad proviene de los **sectores de servicios y de industria**. El centro educativo se sitúa en el centro de la ciudad. Fruto de la transformación digital en la que estamos inmersos no solo surgen nuevos sectores económicos, sino también nuevas profesiones que van ganando peso en la estructura organizativa de las compañías a medida que las nuevas tecnologías entran en todos sus departamentos. Es por ello que cada día más, las empresas situadas en las proximidades del centro educativo requieren de personal informático cualificado del que se forma en este centro.

3. PERFIL PROFESIONAL

3.1. COMPETENCIA GENERAL DEL TÍTULO

La competencia general de este curso de especialización consiste en definir e implementar estrategias de seguridad en los sistemas de información realizando diagnósticos de ciberseguridad, identificando vulnerabilidades e implementando las medidas necesarias para mitigarlas aplicando la normativa vigente y estándares del sector, siguiendo los protocolos de calidad, de prevención de riesgos laborales y respeto ambiental.

3.2. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

Las **competencias profesionales, personales y sociales** describen el conjunto de conocimientos, destrezas y competencias, entendida éstas en términos de autonomía y responsabilidad, que permiten responder a los requerimientos del sector productivo, aumentar la empleabilidad y favorecer la cohesión social.

Las competencias profesionales, personales y sociales de este curso de especialiación vienen descritas en el currículo que regula título. Son un total de 15 y son las siguientes:

a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.

b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.

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.

f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.

g) Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.

h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.

i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.

j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.

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.

Concretamente, y tal y como se indica en el Real Decreto que regula este curso de especialización, de ese total de competencias profesionales, personales y sociales, el módulo que se está programando trabaja las indicadas en negrita: c), d), e), k), l), m), n) y ñ).

4. OBJETIVOS

Los objetivos educativos expresan el nivel de desarrollo que se espera alcance el alumnado como consecuencia de la intervención educativa y se expresan en términos de competencias, es decir, que la meta educativa no debe ser que el alumnado aprenda meros datos, sino que sean capaces de manejarse con ellos. Toda intervención educativa persigue en última instancia el desarrollo integral del individuo, por ello, el objetivo de la educación es el desarrollo de las competencias.

4.1. OBJETIVOS GENERALES DE ESTE C.E. QUE SE TRABAJAN EN EL MÓDULO

Los objetivos generales de este curso de especialización, según el R.D. que lo regula, son los que se indican a continuación:

a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.

b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan se securización de la organización.

c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.

d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.

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.

k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.

l) Automatizar planes de desplegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un desplegado seguro.

m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.

n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.

ñ) Combinar técnicas de hacking ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.

o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en relación con terceros para definir las funciones y responsabilidades de todas las partes.

p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.

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.

La formación de este módulo contribuye a alcanzar los objetivos generales de este curso de especialización, tal como se indica en el R.D que lo regula, son los indicados en negrita: e), f), g), h), i), j), q), r), s), t), u) y v) .

4.2. RESULTADOS DE APRENDIZAJE

Dentro de la programación, según el grado de concreción, se habla de objetivos a nivel del módulo que se pretenden conseguir durante el transcurso del mismo y los cuales vienen expresados en el correspondiente R.D. en términos de **resultados de aprendizaje**, que pasamos a citar:

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

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

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

4) Diseña redes de computadores contemplando los requisitos de seguridad.

5) Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad.

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

7) Configura sistemas informáticos minimizando las probabilidades de exposición a ataques.

Por otra parte, en cada una de las unidades didácticas en que queda dividida esta programación, se detallarán los objetivos específicos o didácticos de cada una.

5. CONTENIDOS

Los objetivos anteriormente planteados serán abordados a través de los contenidos que se describen a continuación. Se toman como fuentes para construir los contenidos: el Real Decreto y la Orden que establece este C.E. y el entorno socioeconómico del centro.

5.1. TEMPORALIZACIÓN DE CONTENIDOS

A continuación se esquematizan las unidades didácticas en las que se ha dividido el módulo.

UNIDADES DIDÁCTICAS	HORAS	TRIMESTRE
0. Presentación del Curso de especialización e introducción al módulo	4	1
1. Diseño de planes de securización	23	3
2. Configuración de sistemas de control de acceso y autenticación de personas	7	3
3. Administración de credenciales de acceso a sistemas informáticos	19	1
4. Diseño de redes de computadores seguras	22	1
5. Configuración de dispositivos y sistemas informáticos	40	1(15h) , 2(25h)
6. Configuración de dispositivos para la instalación de sistemas informáticos	12	2
7. Configuración de los sistemas informáticos	23	2(18) , 3(5)

Tabla 1: Temporalización de bloques de contenidos y unidades didácticas

La distribución horaria que tiene este módulo en mi horario lectivo, durante el presente curso escolar es:

1ª Evaluación			2ª Evaluación			3ª Evaluación			Total
Oct.	Nov.	Dic.	Ene.	Feb.	Mar.	Mar.	Abr.	May.	
25	20	15	20	20	15		25	10	
60			55			35 (fin 19 mayo)			150

Coincidiendo el total de horas con las 150 horas asignadas en el R.D. que regula este C.E.

5.2. SECUENCIACIÓN DE CONTENIDOS

En este apartado se pasan a esquematizar las unidades didácticas en las que se ha dividido el módulo. Para cada una de ellas se expresan sus contenidos didácticos específicos.

Este módulo tiene una carga lectiva de 150 horas que se distribuyen a razón de 5 horas semanales.

- **Unidad Didáctica 1:** Diseño de planes de securización.

Contenidos:

- 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.

- **Unidad Didáctica 2:** Configuración de sistemas de control de acceso y autenticación de personas.

Contenidos:

- Mecanismos de autenticación. Tipos de factores.
- Autenticación basada en distintas técnicas.

- **Unidad Didáctica 3:** Configuración de sistemas de control de acceso y autenticación de personas.

Contenidos:

- Gestión de credenciales.
- Infraestucturas de Clave Pública (PKI).
- Acceso por medio de Firma electrónica.
- Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red).
- Gestión de cuentas privilegiadas.
- Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros.

- **Unidad Didáctica 4:** Diseño de redes de computadores seguras.

Contenidos:

- Segmentación de redes
- Subnetting.
- Redes virtuales (VLANs).
- Zona desmilitarizada (DMZ).
- Seguridad en redes inalámbricas (WPA2, WPA3, etc.).
- Protocolos de red seguros (IPSec, etc.).

- **Unidad Didáctica 5:** Configuración de dispositivos y sistemas informáticos.

Contenidos:

- Seguridad perimetral. Firewalls de Próxima Generación.
- 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
- Soluciones DLP (Data Loss Prevention)
- Herramientas de almacenamiento de logs.
- Protección ante ataques de denegación de servicio distribuido (DDoS).
- Configuración segura de cortafuegos, enrutadores y proxies.

- Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
- 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.

- **Unidad Didáctica 6:** Configuración de dispositivos para la instalación de sistemas informáticos.

Contenidos:

- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros.
- Seguridad en el arranque del sistema informático, configuración del arranque seguro.
- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros.

- **Unidad Didáctica 7:** Configuración de los sistemas informáticos.

Contenidos:

- Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros.
- Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.).
- Eliminación de protocolos de red innecesarios (ICMP, entre otros).
- Securización de los sistemas de administración remota.
- Sistemas de prevención y protección frente a virus e intrusiones (antivirus, HIDS, etc.).
- Configuración de actualizaciones y parches automáticos.
- Sistemas de copias de seguridad.
- Shadow IT y políticas de seguridad en entornos SaaS.

5.3. ELEMENTOS TRANSVERSALES DEL CURRÍCULO

5.3.1. ÁREAS DE INTERÉS EN LA FP

Asimismo, se debe de prestar atención a las áreas prioritarias o de especial interés, existentes en la Formación Profesional: TIC, idiomas y prevención de riesgos laborales.

5.3.2. EDUCACIÓN EN VALORES

El Sistema Educativo incluye en el currículo una serie de saberes actualmente demandados por la sociedad: son los llamados temas transversales.

Se denominan transversales porque no surgen como un programa paralelo al desarrollo del currículo sino insertado en la dinámica diaria del proceso de enseñanza–aprendizaje. Son complementarios y deben impregnar la totalidad de actividades del centro.

La LOMLOE y, más concretamente la LEA refuerzan el uso en los currículos de las enseñanzas no universitarias de estos temas transversales.

En las diversas unidades, se trabajarán los siguientes temas transversales:

- Coeducación: Promoviendo la igualdad fundamentándola en el respeto a la diversidad.

- Educación para la vida en sociedad y convivencia: fomentando la empatía y la comprensión, sin echar la culpa del mal funcionamiento del equipo a compañeros de otro turno.
- Educación del consumidor: cuando vemos productos, comparando varios en aspectos como la energía consumida, el sobrecoste de productos de última generación; o el derroche de invertir en productos con tecnologías ya en desuso.
- Educación ambiental: este aspecto ya está incluido en el contenido de este módulo (Principios de la Economía Circular en la Industria 4.0).
- Educación para la salud: fomentando la prevención y el uso de medidas de protección.

6. METODOLOGÍA

6.1. LINEAS DE ACTUACIÓN

Las líneas de actuación en el proceso de enseñanza-aprendizaje vienen determinadas en el Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información, versarán sobre:

- El diseño de planes de securización de la organización.
- El diseño de redes de computadores.
- La administración de los sistemas de control de acceso.

6.2. ACTIVIDADES DE ENSEÑANZA-APRENDIZAJE

Se va a impartir el temario proporcionado por diversos cursos realizados por el CEP e INCIBE, adaptados a los contenidos del módulo y versiones de Sistemas Operativos actualizados. Durante las clases se realizarán las siguientes actividades de enseñanza-aprendizaje:

- Exposiciones del contenido por parte del profesor
- Resolución de dudas
- Realización de ejemplos en clase
- Realización de ejercicios en clase
- Prácticas con diversas máquinas virtuales
- Pruebas de conceptos cortos
- Pruebas de resolución de ejercicios similares a los realizados en clase

6.3. ESTRATEGIAS DIDÁCTICAS

Se pretende llevar a cabo las siguientes estrategias didácticas:

- Aprendizaje basado en problemas. Se basa en la organización de pequeños grupos que buscan resolver problemas reales. Los estudiantes deberán buscar por sí mismos la información y debatir cuál es la mejor forma de solucionar el problema. El docente aportará los medios y la libertad para que encuentren la respuesta más adecuada y solamente intervendrá para resolver alguna duda que pueda surgir.

- Aprendizaje colaborativo. Se da cuando el alumno trabaja con otras personas, ya sean otros compañeros o el profesor, para adquirir nuevos saberes, competencias y capacidades. Además, aprenderán a socializar, cooperar, empatizar y llegar a un consenso.

- Aprendizaje activo. Se trata de aprender haciendo. Para ello, los alumnos interactuarán y experimentarán para comprender y desarrollar conceptos. Además, esta estrategia fomenta la escucha activa, para que se produzca un intercambio de saberes que ayude a reflexionar y aprender, fomentando el respeto mutuo.

- Fomento de la curiosidad: animando a los estudiantes a explorar más allá del plan de estudios y a investigar nuevas tecnologías y tendencias.

6.4. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Se consideran actividades complementarias las organizadas durante el horario escolar por los Centros, y que tienen un carácter diferenciado de las propiamente lectivas, por el momento, espacio o recursos que utilizan. Estas actividades son fundamentalmente las salidas y celebraciones y se organizarán de forma coordinada con los profesores del equipo docente.

6.5. MATERIALES Y RECURSOS DIDÁCTICOS

Todas las sesiones correspondientes a este módulo se desarrollarán en el aula-taller de informática de dotación de este curso de especialización. Además de los recursos tradicionales como la pizarra para explicaciones teóricas, se necesitarán los siguientes recursos tecnológicos en el aula:

- Cañón de proyección.
- Red de área local.
- Acceso a internet.
- Acceso a servidores y servicios del departamento
- Manuales, apuntes y tutoriales on-line.
- Routers Cisco 2801 o equivalentes.
- Switches Cisco Catalyst 2960 o equivalentes.
- Puntos de Acceso.
- Tarjetas de interfaz de red WiFi
- Equipos con capacidad suficiente para tener trabajando al menos una decena de máquinas en contenedores o virtualizadas.

6.6. BIBLIOGRAFÍA

6.6.1. BIBLIOGRAFÍA DE DEPARTAMENTO

- Máxima Seguridad en Windows: Secretos Técnicos. Editorial 0xWORD
- Hardening de servidores GNU/Linux. Editorial 0xWORD

6.6.2.BIBLIOGRAFÍA DE AULA

- Apuntes del profesor.
- Documentación en línea de aplicaciones software
- Documentación en línea de varios Sistemas Operativos
- Foros de resolución de dudas

7. EVALUACIÓN

La evaluación tendrá en cuenta el progreso del alumno/a respecto a la formación adquirida en los distintos módulos que componen el Ciclo Formativo. La superación del Ciclo Formativo requerirá la evaluación positiva de todos los módulos que lo componen.

La evaluación es **criterial** y **continua**. En primer lugar, es criterial, ya que a través del cumplimiento de los criterios de evaluación, se valida si se alcanzan las metas. En segundo lugar, se dice que es continua porque continuamente se está evaluando y cuando se detecta un problema en clase, se intenta solucionar. Por tanto, permite resolver el problema que tenga un alumno/a en un momento dado. Además, que la evaluación sea continua implica que sea formativa, puesto que permite cambiar aspectos determinados si se detectan fallos en el proceso de enseñanza.

7.1. ¿QUÉ, CUÁNDO Y CÓMO EVALUAR ?

Se realizará una evaluación inicial, basada en un test de preguntas cortas, que irá realizando el alumnado conforme se vaya incorporando presencialmente a clase, cuyo resultado servirá de base para la información suministrada en la sesión de evaluación inicial establecida por el centro.

Durante cada trimestre se realizarán varias pruebas que servirán de base para la nota asociada al trimestre.

La nota de la primera y segunda evaluación será la media ponderada de las distintas pruebas realizadas durante el trimestre correspondiente.

La nota de la tercera evaluación será la nota final, y se corresponderá con la media ponderada de todos los trimestres.

A continuación se indica los resultados de aprendizaje y criterios de evaluación del módulo

R.A 1: 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.

R.A 2: 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.

R.A 3: 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)

R.A 4: 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.

R.A 5: 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 cortafuegos. d) Se han implementado contramedidas frente a comportamientos no deseados en una red. e) Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.

R.A 6: 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.

R.A 7: 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.

Tabla 2: Resultados de aprendizaje y criterios de evaluación del módulo

7.2. CALIFICACIÓN Y CRITERIOS DE CALIFICACIÓN

Teniendo en cuenta la Orden de 29 de septiembre de 2010, la evaluación final de este módulo profesional el módulo se evaluará por resultados de aprendizaje, complementando con las competencias profesionales, personales y sociales.

7.2.1. CRITERIOS DE CALIFICACIÓN

Se utilizan los siguientes instrumentos de evaluación, con los pesos indicados:

- Pruebas del profesor: 70%
- Ejercicios/actividades evaluables: 30%

Por cada trimestre se obtendrá una nota ponderada de los elementos anteriores; dicha nota será directamente la nota en la primera y segunda evaluación; estas notas son orientativas.

Para la nota de la tercera evaluación, se realizará una media de las notas de los tres trimestres ponderas por la duración de cada trimestre.

En caso de que no se realicen "Pruebas del profesor", el 100% de la nota del trimestre se compondrá de las notas de los Ejercicios/actividades evaluables.

La nota final, coincidirá con la de la tercera evaluación.

7.3. RECUPERACIÓN Y MEJORA DE CALIFICACIÓN

La recuperación del módulo se llevará a cabo mediante la repetición de las pruebas y/o la realización de los ejercicios no finalizados. La nueva nota obtenida se aplicará para calcular la nota asociada a cada trimestre.

Para la mejora de la calificación, el alumnado tendrá que realizar de forma satisfactoria uno o varios cursos en línea, entre los que se pueden encontrar: "Cybersecurity Essentials (Conceptos

básicos de ciberseguridad)" de Cisco, "Cloud Foundations (Conceptos Básicos de la Nube)" de AWS Academy; si se supera/superan de forma satisfactoria, la calificación en la sesión de evaluación final de junio se incrementará en 1 punto sobre 10 a la obtenida en mayo.

8. ATENCIÓN A LA DIVERSIDAD

La diversidad está presente en todos los colectivos sociales. El reto de los centros educativos y del profesorado en relación con el alumnado que atienden, es proporcionar el desarrollo de las capacidades en función de sus características diferenciales.

Es una realidad que los alumnos/as del grupo-clase se diferencian en cuanto a sus capacidades, conocimientos previos, motivaciones e intereses. Por ello en el aula, existen alumnos/as que van a presentar distintas necesidades educativas.

La LOMLOE, entiende por alumnado con **necesidades específicas de apoyo educativo (NEAE)** a aquel alumnado, que requiera una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, TDAH, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar.

El alumnado con **necesidades educativas especiales**, es aquel alumnado con discapacidad o trastornos graves de conducta.

Los principios de actuación con estos alumnos/as son la no discriminación y la normalización educativa, a fin de lograr la igualdad de oportunidades para todos.

En este módulo se adoptan una serie de medidas para atender a las diferentes necesidades del alumnado:

- Flexibilidad en las entregas, permitiendo que los estudiantes entreguen tareas en diferentes momentos. Esto brinda flexibilidad a aquellos que pueden necesitar más tiempo para completar una tarea.
- Se proporcionará tiempo de sobra para completar los exámenes, ya que algunos estudiantes pueden necesitar más tiempo para procesar la información o para demostrar su comprensión.
- En el aula se fomenta la comunicación abierta con los estudiantes para que expresen sus necesidades y preocupaciones. Esto ayuda a adaptar el enfoque y ritmos de aprendizaje individual.