PROGRAMACIÓN DEL MÓDULO:

BASTIONADO DE REDES Y SISTEMAS

PROFESOR/ES: ***En caso de más de un profesor es necesario identificar al profesor coordinador y puede ser necesario calibración.***	Fréderic Sánchez García
GRUPO/S Y CICLO/S:	Curso de especialización en ciberseguridad en entornos de las tecnologías de la información
CURSO:	2020-2021

ÍNDICE

1. INTRODUCCIÓN

El módulo Bastionado de redes y sistemas se engloba en el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información, perteneciente a la Familia Profesional de Informática y Comunicaciones, que NO queda establecido NI regulado todavía para la Comunidad Autónoma de Extremadura y por lo tanto NO se establece el currículo del Curso de especialización en ciberseguridad en entornos de las tecnologías de la información, SÍ se establece a nivel nacional con 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 y se fijan los aspectos básicos del currículo.

Este módulo profesional contiene la formación necesaria para desempeñar la función de bastionado de los sistemas y redes de la organización.

La función de bastionado incluye aspectos como la administración de los sistemas y redes contemplando la normativa, tanto a nivel nacional como internacional, de ciberseguridad en vigor.

Las actividades profesionales asociadas a esta función se aplican en el diseño de planes de securización y en el diseño de las redes contemplando los requisitos de seguridad que apliquen a la organización.

2. OBJETIVOS

Según el Real Decreto 479/2020, de 7 de abril, los **Objetivos Generales** que este módulo ayuda a alcanzar son los siguientes:

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.

Las **competencias profesionales, personales y sociales** que este módulo contribuye a alcanzar son las siguientes:

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.

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.

Los **Resultados de Aprendizaje** de este módulo profesional, establecidos en el Real Decreto 479/2020, de 7 de abril, son los siguientes:

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.

Las líneas de actuación en el **proceso de enseñanza aprendizaje** que permiten alcanzar los objetivos del módulo 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.

3. CONTENIDOS

Unidad de Trabajo 0: Presentación del módulo y metodología de trabajo

0- Presentación del módulo.
1- Metodología de trabajo presencial, semipresencial y en línea.
2- Pruebas de capacidad de conexión y de los equipos del alumnado en el domicilio.
3- Recopilación de medios disponibles en el hogar.

Unidad de Trabajo 1: Diseño de planes de securización

1. Organismos nacionales.
2. Antecedentes.
3. ***Conceptos de activos, vulnerabilidades, amenazas e impacto. ¿Cómo se mide el nivel de riesgo? Ciclo de vida de una vulnerabilidad.***
4. ***Análisis de riesgo. Tratando y aceptando riesgos de seguridad de la información. Análisis de vulnerabilidades.***
5. La importancia del factor humano en ciberseguridad.
6. ***Seguridad Informática. Confidencialidad. Integridad. Disponibilidad.***
7. ***Bastionado de redes y sistemas. Aplicaciones y Servicios. Acceso remoto. Acceso local. Sistema Operativo. Redes.***
8. ***Buenas prácticas de seguridad.***

Unidad de Trabajo 2: Sistemas de control de acceso y autenticación de personas

1. ***Mecanismos de autenticación. Tipos de factores.***
2. ***AAA (Authentication, Authorization and Accountig).***
3. ***Tipos de sistemas de autenticación. Ataques de autenticación. Contraseñas. One-Time Password (OTP). Single Sign-On (SSO). Criptografía de clave simétrica. Criptografía de clave asimétrica. Firma digital. Autenticación biométrica. Tarjetas o dispositivos de identificación. Autenticación multi-factor.***
4. ***La importancia del proceso de autenticación.***
5. ***Control de acceso. Administración remota. Configuración de terminales. Configuración de acceso SSH.***
6. ***Control de acceso. Administración local. Cuentas de usuario. Política de contraseña.***
7. Protocolo RADIUS.

8. Protocolo TACACS.
9. Protocolo KERBEROS.

Unidad de Trabajo 3: Configuración de dispositivos para la instalación de sistemas informáticos

0. ***Precauciones previas a la instalación.***
1. ***Seguridad en la BIOS.***
2. ***Protección GRUB en Linux. Impacto de un gestor de arranque no protegido. /boot/grub2/grub.cfg. /etc/default/grub. /etc/grub.d. Comandos. Proteger el acceso a GRUB. Ocultar el gestor de arranque. Bloquear el acceso a otros Sistemas Operativos o modos de arranque. Proceso de arranque.***
3. ***Seguridad en el arranque del sistema informático.***
4. ***Protección sistema de ficheros. Concepto de acceso a un sistema de ficheros. Cifrado de disco o particiones.***
5. ***Protección de archivos - Linux. Restringir las opciones de montaje de particiones. Restringir el montaje y desmontaje automático de unidades. Comprobaciones de permisos en archivos y directorios. Minimizar el uso de SUID root. Utilizar SUDO y SU. Programas de comprobación de Integridad (Tripwire, aide, etc). Cifrado de ficheros en Windows. Cifrado de ficheros en Linux.***
6. ***Protección de archivos - Windows***

Unidad de Trabajo 4: Diseño de redes de computadores seguras

1. ***Segmentación de redes.***
2. ***Subnetting.***
3. ***Redes virtuales (VLANs).***
4. ***Zona desmilitarizada (DMZ).***
5. ***Seguridad en redes inalámbricas (WPA2, WPA3, etc.).***
6. ***Protocolos de red seguros (IPSec, etc.).***

Unidad de Trabajo 5: Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad

1. Seguridad perimetral. Firewalls de Próxima Generación.
2. Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall).
3. Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware.
4. Seguridad de entornos cloud. Soluciones CASB.
5. Seguridad del correo electrónico
6. Soluciones DLP (Data Loss Prevention)
7. Herramientas de almacenamiento de logs.
8. Protección ante ataques de denegación de servicio distribuido (DDoS).
9. Configuración segura de cortafuegos, enrutadores y proxies.
10. Redes privadas virtuales (VPNs), y túneles (protocolo IPSec).
11. Monitorización de sistemas y dispositivos.
12. Herramientas de monitorización (IDS, IPS).
13. SIEMs (Gestores de Eventos e Información de Seguridad).
14. Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs

Unidad de Trabajo 6: Configura sistemas informáticos minimizando las probabilidades de

exposición a ataques

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

4. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

El inicio del curso será el día 16 de noviembre de 2020, y la finalización del mismo será el día 18 de junio de 2021. En base a esto, se ha planificado la siguiente distribución temporal de contenidos.

EVALUACIÓN	TEMA, BLOQUE O UNIDAD DIDÁCTICA	FECHA INICIO ---- FECHA FIN *Diferenciar por grupo si son diferentes*	Nº HORAS LECTIVAS
1ª	UT0. Presentación del módulo y metodología de trabajo	16/11/2020	1
	UT1. Diseño de planes de securización	17/11/2020 - 03/12/2020	16
	UT2. Sistemas de control de acceso y autenticación de personas	4/12/2020 - 02/02/2021	40
	UT3. Configuración de dispositivos para la instalación de sistemas informáticos	03/02/2021 - 03/03/2021	25
		% AVANCE EN CONTENIDOS	**46%**
2ª	UT4. Diseño de redes de computadores seguras	04/03/2021 - 22/04/2021	41

	UT5. Configura dispositivos y sistemas informáticos cumpliendo los requisitos de seguridad	23/04/2021 - 13/05/2021	21
	UT6. Configura sistemas informáticos minimizando las probabilidades de exposición a ataques	14/05/2021 - 18/06/2021	33
		% AVANCE EN CONTENIDOS	**100 %**

Destacar que esta planificación, realizada en base al calendario escolar del presente curso se podrá revisar a lo largo del mismo de forma periódica como consecuencia de la necesaria flexibilidad que suponen los distintos niveles de aprendizaje de contenidos que se presentan de forma natural en los distintos grupos de alumnos y también de otras circunstancias que puedan ocurrir de forma imprevista y que impida desarrollar de forma normal la impartición de estos contenidos.

Por otra parte, esta distribución puede no coincidir en número de horas totales respecto a lo que marca la ley (las puede superar o no llegar), ya que tiene que ir en función del calendario escolar oficial previsto para este curso.

5. CRITERIOS DE EVALUACIÓN

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

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.

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

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.

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

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)

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

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.

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

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

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

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.

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

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.

6. RELACIÓN CON OTROS MÓDULOS DEL CICLO

Para promover la integración y el aprendizaje significativo, los contenidos se presentarán con una estructura clara de las relaciones tanto a nivel de módulo como con otros módulos.
A continuación, se indican las diferentes relaciones que pueden establecerse entre el módulo de Bastionado de redes y sistemas y el resto de Módulos:

- **Incidentes de ciberseguridad**. El bastionado de redes y sistemas está íntimamente relacionado con los incidentes que pueden surgir tanto en la red, como en el sistema, por ello es necesario su conocimiento.
- **Puesta en producción segura**. Para implementar la producción segura de aplicaciones es necesario contar con un sistema y red seguro, sino de nada valdría.
- **Análisis forense informático**. El análisis forense está fuertemente relacionado con el bastionado, de esta forma influirá el análisis de en ficheros, sistema de archivos, discos duros... según el nivel de bastionado que hayamos realizado.
- **Hacking ético**. Permite comprobar el nivel de bastionado de nuestras redes y sistemas.
- **Normativa de ciberseguridad**. Es necesario conocer la normativa para poder realizar un bastionado de calidad adaptado a la legislación vigente.

7. METODOLOGÍA DIDÁCTICA

Durante el aprendizaje, gradual y controlado, debemos observar las dificultades colectivas e individuales para adoptar las medidas adecuadas a las necesidades de nuestros alumnos y así, poder reorientar el proceso. Debemos atender a la diversidad de los alumnos, lo que supone uno de los problemas más importantes a lo que el docente debe enfrentarse.

Deberemos favorecer la construcción de los aprendizajes significativos. La intervención educativa irá dirigida a garantizar la funcionalidad de los aprendizajes. La motivación aumentará cuando comprueben que su conocimiento es útil en situaciones reales.

Las sesiones permitirán que cada unidad incluya la presentación de actividades variadas, adaptadas a los

contenidos y al nivel de los alumnos.

El desarrollo de las sesiones se compondrá de dos fases, las cuales se llevarán a cabo de forma intercalada:

- **Teórica**: Se expondrá la necesidad del nuevo conocimiento y su relación con los conocimientos actuales del alumno.
- **Práctica**: El alumno deberá resolver problemas relacionados con el conocimiento adquirido en la fase teórica.

Para llevar a cabo esta programación hemos utilizado varios textos para la elaboración de las Unidades de Trabajo. El uso de esta diversidad contribuye a crear un programa para localizar y seleccionar los contenidos más interesantes y motivadores para los alumnos involucrados.

METODOLOGÍA EN CONDICIONES EXTRAORDINARIAS

En caso de imposibilidad de aplicación de la metodología presencial causadas por situaciones de carácter extraordinario, las líneas de actuación a seguir dependerán, en primer lugar, de las directrices de la Consejería de Educación de la Junta de Extremadura, contemplándose, además, la transformación del proceso de enseñanza/aprendizaje virtual.

En este contexto, se mantendría como vía de comunicación entre los pilares de la comunidad educativa la plataforma de Rayuela, el correo corporativo y como plataforma virtual de aprendizaje la utilizada en el aula, enfatizando, en mayor medida, el uso de recursos TIC, para la elaboración de contenidos. Además, se llevarán a cabo sesiones de videoconferencia con el alumnado de forma que puedan seguir el ritmo de aprendizaje de la forma más efectiva posible.

En este caso, se tomarán como contenidos básicos aquellos destacados en negrita y cursiva en la tabla de la distribución temporal de contenidos, por lo que serán tratados de forma preferente al resto.

8. PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS

Para llevar a cabo la evaluación del aprendizaje de los alumnos, se utilizarán los siguientes **instrumentos**:

- **Actividades**: Serán de una duración breve (15-20 minutos) y versarán sobre los contenidos estudiados. Se tendrá en cuenta el comportamiento de los alumnos, el interés y la motivación por la materia.
- **Exámenes**: El profesor informará sobre los Contenidos y Unidades de Trabajo sobre las que se trabajará. Serán exámenes teóricos y prácticos, que contendrán actividades similares a las realizadas en clase.

Al inicio de curso se realizará una evaluación inicial con el objetivo de conocer el nivel del alumnado en cuanto a aptitudes, capacidades y conocimientos básicos, de forma que el proceso sea individualizado.

A lo largo del curso se realizarán 2 sesiones de evaluación ordinarias, coincidiendo la última con lo que se denomina evaluación final ordinaria.

Para que el alumno supere el módulo, deberá haber alcanzado todos los resultados de aprendizaje asociados al módulo.

Los alumnos que no hayan superado el módulo en la convocatoria ordinaria de junio tendrán la posibilidad de hacerlo en la convocatoria extraordinaria, que se llevará a cabo en septiembre. Durante este periodo, realizarán actividades de recuperación.

RELACIÓN UNIDADES DE TRABAJO Y RESULTADOS DE APRENDIZAJE

A continuación, se indica la relación de cada una de las Unidades de Trabajo con los Resultados de Aprendizaje, además del porcentaje de contribución de la misma a la consecución de cada uno de ellos.

	RA 1	RA 2	RA 3	RA 4	RA 5	RA 6	RA 7
UT 1	100						
UT 2		100	100				
UT 3						100	
UT 4				100			
UT 5					100		
UT 6							100

9. CRITERIOS DE CALIFICACIÓN

PESOS DE LOS RESULTADOS DE APRENDIZAJE

Para llevar a cabo el cálculo de la calificación final del módulo, se tomarán las calificaciones de cada uno de los Resultados de Aprendizaje y se le aplicará la ponderación correspondiente según la tabla que se indica a continuación.

RA	RA 1	RA 2	RA 3	RA 4	RA 5	RA 6	RA 7
Peso	10	10	10	20	15	20	15

Como se ha indicado anteriormente, el alumno deberá superar todos los Resultados de Aprendizaje para poder dar por superado el módulo. En caso contrario, la calificación será como máximo 4.

ASPECTOS GENERALES

Atendiendo a los criterios de evaluación y procedimientos de evaluación descritos, la obtención de la calificación de cada Resultado de Aprendizaje en cada una de las Unidades de Trabajo se realizará teniendo en cuenta la siguiente ponderación:

- Exámenes: 70%
- Actividades: 30 %. En caso de no proponerse tareas, este porcentaje se sumará al de exámenes.

En caso de no diferenciarse el Resultado de Aprendizaje asociado en los exámenes y las actividades, la calificación de la Unidad de Trabajo se aplicará a cada uno de los Resultados de Aprendizaje asociados a la misma.

De acuerdo con los principios metodológicos del Proyecto Educativo de Centro, en los criterios de

calificación se tendrá en cuenta la corrección ortográfica, presentación estética de exámenes y ejercicios, trabajos, informes, memorias, etc.

NORMATIVA DE EXÁMENES Y ACTIVIDADES

- Los exámenes se realizarán en la fecha y hora indicadas por el profesor del módulo.
- La no asistencia a un examen supone la calificación de "0".
- Las actividades no realizadas serán calificadas con 0.
- Solo se considerarán justificantes válidos los emitidos por órganos oficiales que explícitamente indique que no es posible o recomendable la asistencia en la fecha y hora del examen. A los estudiantes que aporten tales justificantes de ausencia a examen se les propondrá otra fecha y hora de realización.
- En caso de detectar plagios en tareas y exámenes (sea de compañeros o de otras fuentes) la calificación del Resultado de Aprendizaje será 0, además del correspondiente apercibimiento por escrito.
- En los exámenes no se podrá hablar ni realizar preguntas en voz alta, ni comentarios o ruidos que distraigan a los demás compañeros. En el caso de que estos se produzcan se expulsará al alumno del aula, suponiendo la anulación del examen y la calificación de 0.

CALIFICACIÓN DE LA 1ª EVALUACIÓN

Debemos destacar que la calificación de esta evaluación es meramente informativa, y no supone haber superado los Resultados de Aprendizaje tratados en ella aunque la calificación sea mayor o igual a 5.
Para el cálculo de la primera evaluación, se tendrán en cuenta las calificaciones de los RA trabajados hasta el momento, ponderando sobre el 100% en función del peso de cada uno con respecto al total del curso.

CALIFICACIÓN DE LA EVALUACIÓN FINAL ORDINARIA

Tal y como se ha indicado anteriormente, la calificación del módulo será la suma de las calificaciones de cada uno de los RA ponderados.

CALIFICACIÓN DE LA EVALUACIÓN FINAL EXTRAORDINARIA

Para la calificación de la evaluación extraordinaria, se tomarán las calificaciones de los Resultados de Aprendizaje evaluados en la evaluación extraordinaria (esta nota supondrá el 100% de la nota del Resultado de Aprendizaje evaluado) y las calificaciones de los Resultados de Aprendizaje superados en la evaluación ordinaria.
El cálculo de la calificación se realizará de idéntica forma a la evaluación final ordinaria.

ALUMNOS PENDIENTES

A los alumnos con el módulo pendiente de cursos anteriores, se les aplicarán idénticos Principios y Criterios de Evaluación y Calificación que al resto de alumnos.
Durante el curso 2020/21 no hay alumnos pendientes.

EVALUACIÓN ORDINARIA

Al acabar el curso, el último trimestre se celebrará la evaluación final ordinaria, en la que se valorará el grado de adquisición de los aprendizajes.

EVALUACIÓN EXTRAORDINARIA

Los alumnos que no superen el módulo, tendrán una convocatoria extraordinaria en el mes de septiembre, que abarca los contenidos teóricos y prácticos de cada uno de los Resultados de Aprendizaje no superados.

Si un alumno no se presenta a la prueba extraordinaria, la calificación en el correspondiente módulo será la de No Presentado, teniendo a todos los efectos, la consideración de calificación negativa.

CRITERIOS DE CORRECCIÓN

Son implícitos al instrumento de evaluación. Salvo en las pruebas escritas, donde necesariamente se detallarán los criterios de corrección, se intentará dar a conocer a priori, el criterio de corrección establecido para cada instrumento de evaluación antes de ponerlo en práctica.

SISTEMA DE RECUPERACIÓN DE RESULTADOS DE APRENDIZAJE PENDIENTES

Para la recuperación de los Resultados de Aprendizaje que el alumno no ha alcanzado, el profesor determinará para cada caso específico el sistema de recuperación, indicando a cada alumno, de forma personalizada, los puntos en los que falló y dependiendo del caso, realizando un nuevo examen y/o actividades.

10. ATENCIÓN A LA DIVERSIDAD

A la hora de abordar nuestra tarea docente, nos encontraremos con grupos heterogéneos, por lo que las estrategias de aprendizaje de los alumnos serán variadas. La metodología debe ser flexible para adaptarse a las distintas formas de aprendizaje de los alumnos del grupo.

Tal y como se indica en la Ley Orgánica 8/2013, deberemos prestar especial atención a los alumnos y alumnas con necesidad específica de apoyo educativo. Al encontrarnos en un Curso de especialización englobado dentro de la Formación Profesional, sólo podremos realizar adaptaciones no significativas. Son medidas parciales y transitorias. Se trata de actividades y materiales para conseguir un aprendizaje exitoso, pero que no implican cambios en los Objetivos, Resultados de Aprendizaje, Contenidos y Criterios de Evaluación establecidos en el Currículo.

El Decreto 228/2014, por el que se regula la respuesta educativa a la diversidad del alumnado en Extremadura, parte de la noción de que es necesario proporcionar respuestas diferenciadas y adaptadas a las características y necesidades de cada alumno, manteniendo altas expectativas sobre todos ellos y buscando el desarrollo de todo su potencial personal.

En el plano autonómico, la LEEx cita como principios para la organización de la atención a la diversidad del alumnado la prevención, inclusión, normalización, superación de desigualdades, coordinación y corresponsabilidad de toda la comunidad educativa, incidiendo en la apertura de los centros a su entorno.

El Plan de Atención a la Diversidad, incluido en la Programación General Anual, establece las líneas claves de actuación en los distintos niveles educativos y adaptadas a la realidad concreta del centro educativo.

Las **diferentes medidas** que adoptaremos para poder atender la diversidad del alumnado son:

- Refuerzo educativo: Se trata de una ayuda puntual por parte del profesor. Es una medida que tomamos con los alumnos que tienen dificultades para asimilar algunos contenidos. La metodología utilizada será variada para satisfacer sus necesidades de aprendizaje. Ofrecemos actividades con diferentes grados de dificultad para consolidar los conocimientos y siempre adaptado a las capacidades de nuestros alumnos. Enfatizaremos en el trabajo en grupos pequeños, teniendo

cuidado de mezclar alumnos de las diferentes necesidades en el mismo grupo.

- Ampliación: De la misma forma que algunos alumnos presentan dificultades para asimilar algunos contenidos, podemos encontrarnos con alumnos que presentan altas capacidades intelectuales, o capacidades por encima de la media del aula, lo que les permite asimilar los conocimientos con mayor facilidad. A estos alumnos, se les propondrán actividades de profundización e investigación.
- Elementos curriculares de acceso: Se llevará a cabo una adaptación del centro y del aula a las condiciones del alumnado. Algunas medidas a tomar en este aspecto son:
    - Discapacidad visual: Se realizará una reordenación del aula para que el alumno encuentre los mínimos obstáculos posibles para su desplazamiento por ella. Se adoptarán las medidas necesarias en función de la discapacidad visual.
    - Discapacidad auditiva: El profesor hablará siempre de cara a los alumnos para que estos puedan leer sus labios y seguir el desarrollo de las clases de una forma más sencilla. Se proporcionará toda la información por escrito, que deberá estar adecuadamente estructurada para facilitar su comprensión, y aquellos alumnos con discapacidad auditiva se colocarán en las zonas más próximas al profesor.
    - Discapacidad motora: Dada la gran diversidad de tipos de discapacidad física, que afecta a distintas partes del cuerpo se estudiarán de forma independiente y se propondrán las medidas necesarias, como puede ser la adquisición de ayudas técnicas, reubicación del aula para facilitar desplazamientos por ella, etc.

Por último, hay que destacar las TICs en este aspecto, al facilitar el afianzamiento de los conocimientos con nuevas actividades o la continuación del proceso de enseñanza-aprendizaje de los alumnos que no puedan asistir temporalmente a clase.

11. MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS

La organización de los recursos debe tener en cuenta las directrices recogidas en el Proyecto Educativo del Centro y en el Proyecto Curricular del Ciclo. Gran parte de los recursos utilizados para el Ciclo Formativo son gestionados por el Departamento de la familia profesional a la que el Ciclo está adscrito, en este caso el Departamento de Informática, por lo que el profesor tratará que se incluyan en el Proyecto Curricular las bases para utilización por nuestra parte de los mismos.

Algunos materiales que utilizaremos en clase serán:

- Apuntes de clase y libros de consulta.
- Los manuales impresos y en línea, de todo el software instalado.
- Información obtenida en cursos de formación del profesorado.
- Publicaciones periódicas relacionadas con el mundo de la informática.
- La gran cantidad de información accesible vía Internet.
- Fotocopias, vídeos, etc.

En cuanto a recursos Hardware:

- Equipamiento del aula: ordenadores, periféricos.
- Cableado, hubs/conmutadores, y tarjetas de red.
- Red de área local.

- Intranet.
- Equipos servidores de red y estaciones de trabajo. Impresoras.
- Acceso a Internet.
- Manuales de instalación y configuración de todos los elementos.

En cuanto a recursos Software:

- Sistema operativo de red (preferentemente los de mayor uso en el mercado
- (Ubuntu, Debian, Windows Server).
- Sistema operativo en las estaciones de trabajo (Ubuntu, Debian, Windows).
- Software de Ofimática (LibreOficce y/o Microsoft Office).
- Software para acceso a Internet.

Elementos auxiliares:

- Sistemas de alimentación ininterrumpida (SAI) para servidores.
- Retroproyector y pantalla mural..

12. ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES

Debido a la situación de alerta sanitaria en la que nos encontramos por el COVID-19, según el protocolo de actuación del centro queda prohibido llevar a cabo actividades de este y cualquier otro tipo que suponga desplazamientos fuera del centro o interacción con agentes externos. No obstante, en caso de finalizar la situación de alerta y poder realizarse este tipo de actividades, se proponen las siguientes:

Actividades complementarias

- Charlas sobre las opciones (educativas y laborales) una vez obtenido el título.
- Visita a la Universidad de Extremadura, Escuela Politécnica, para observar parte de las instalaciones tecnológicas y tener conocimientos de los proyectos de Investigación que se llevan a cabo en ella.
- Visita al CETA-CIEMAT (Centro Extremeño de Tecnologías Avanzadas), ubicado en Trujillo.

Actividades extraescolares

Se propondrán actividades que permitan al alumnado observar en primera persona la aplicación de los contenidos estudiados y los diferentes caminos que pueden tomar una vez obtenida la titulación. Se proponen las siguientes actividades:

- Visita a una de las empresas de base tecnológica existentes en la región.
- Visita a Cáceres para conocer: la factoría de software INSA, el campus universitario, el CIRL (Centro Internacional de Referencia Linux) y el CCMI (Centro de Cirugía de Mínima Invasión).
- Exploración de la red Eduroam en alguna de las sedes de la Universidad de Extremadura
- en Cáceres (ida y vuelta en el día).
- Visita a CPDs o empresas de gran tamaño como por ejemplo IBM, Telefónica, 112, o proveedor de servicios de internet en Madrid para conocer sus infraestructuras, recursos tecnológicos, así como el desarrollo de las distintas tareas informáticas realizadas. De esta forma los alumnos conocerán las instalaciones y el funcionamiento de una empresa líder en el sector informático y de las telecomunicaciones. Dirigido a alumnos de ciclos formativos.

Además, se colaborará en el resto de actividades propuestas por el departamento.

13. TEMAS TRANSVERSALES

De los temas transversales aconsejados por los departamentos de IyC y FOL para los módulos de la familia

profesional de Informática y Comunicaciones se trabajarán los siguientes:

Educación ambiental

El análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumno/a para decidir sobre los productos informáticos que debe adquirir y utilizar de la manera más apropiada, valorando de manera crítica las distintas ofertas, campañas de publicidad, etc.

Educación para la paz

Concienciando a los alumnos y alumnas de la importancia de mantener un clima de respeto y de cooperación en el aula.

Educación para la salud

Cuando se utilizan equipos informáticos uno de los objetivos es que los alumnos y alumnas conozcan unas normas básicas de higiene y seguridad en el trabajo, así como a tomar las debidas precauciones en el empleo de dichos equipos. Es necesario conocer unos principios de ergonomía en el puesto de trabajo, para que la actividad frente al ordenador no sea motivo de problemas físicos. Estos aspectos cobran especial importancia en la Prevención de riesgos laborales. Considerando que el ámbito laboral más común de los Técnicos va a ser las oficinas y centros de procesos de datos, habrá que insistir a diario en la existencia de los siguientes riesgos y de sus correspondientes medidas de prevención

Los aspectos básicos a trabajar en la educación para la salud en relación a COVID-19 son los aspectos de la enfermedad, cómo actuar ante la aparición de síntomas, medidas de distancia física y limitación de contactos, higiene de manos y resto de medidas de prevención personal, uso adecuado de la mascarilla, conciencia de la interdependencia entre los seres humanos y el entorno y fomento de la corresponsabilidad en la salud propia y en la salud de los otros, prevención del estigma.

Fomento de la capacidad emprendedora

La capacidad emprendedora se define como la capacidad de actuar con iniciativa y perseverancia, para modificar la realidad siendo un agente de cambio, junto a los que lo rodean, aportando soluciones innovadoras a organizaciones productivas y sociales desde su profesión. Debemos fomentar en nuestros alumnos esta capacidad inculcando en ellos valores tales como:

la autoconfianza, tener fe en nuestras posibilidades, sin olvidar que los objetivos marcados deben ser realistas.

la tolerancia a la frustración, saber sobreponerse a la frustración que suponen las expectativas no cumplidas, sabiendo extraer un análisis positivo de las situaciones negativas.

la gestión del riesgo, mediante un enfoque adecuado para manejar los posibles riesgos y mitigar su impacto.

la búsqueda de recursos, de todo aquello que puede contribuir a llevar un proyecto a buen término.

la productividad, saber explotar los recursos al máximo.

la creatividad, en un mundo cambiante, necesitamos plantear soluciones, formular hipótesis, tener iniciativas novedosas, y todo ello está íntimamente ligado con el proceso creativo.

Educación del consumidor

El análisis y la utilización de diferentes herramientas informáticas favorecen la capacidad del alumno/a para

decidir sobre los productos informáticos que debe adquirir y utilizar de la manera más apropiada, valorando de manera crítica las distintas ofertas, campañas de publicidad, etc.