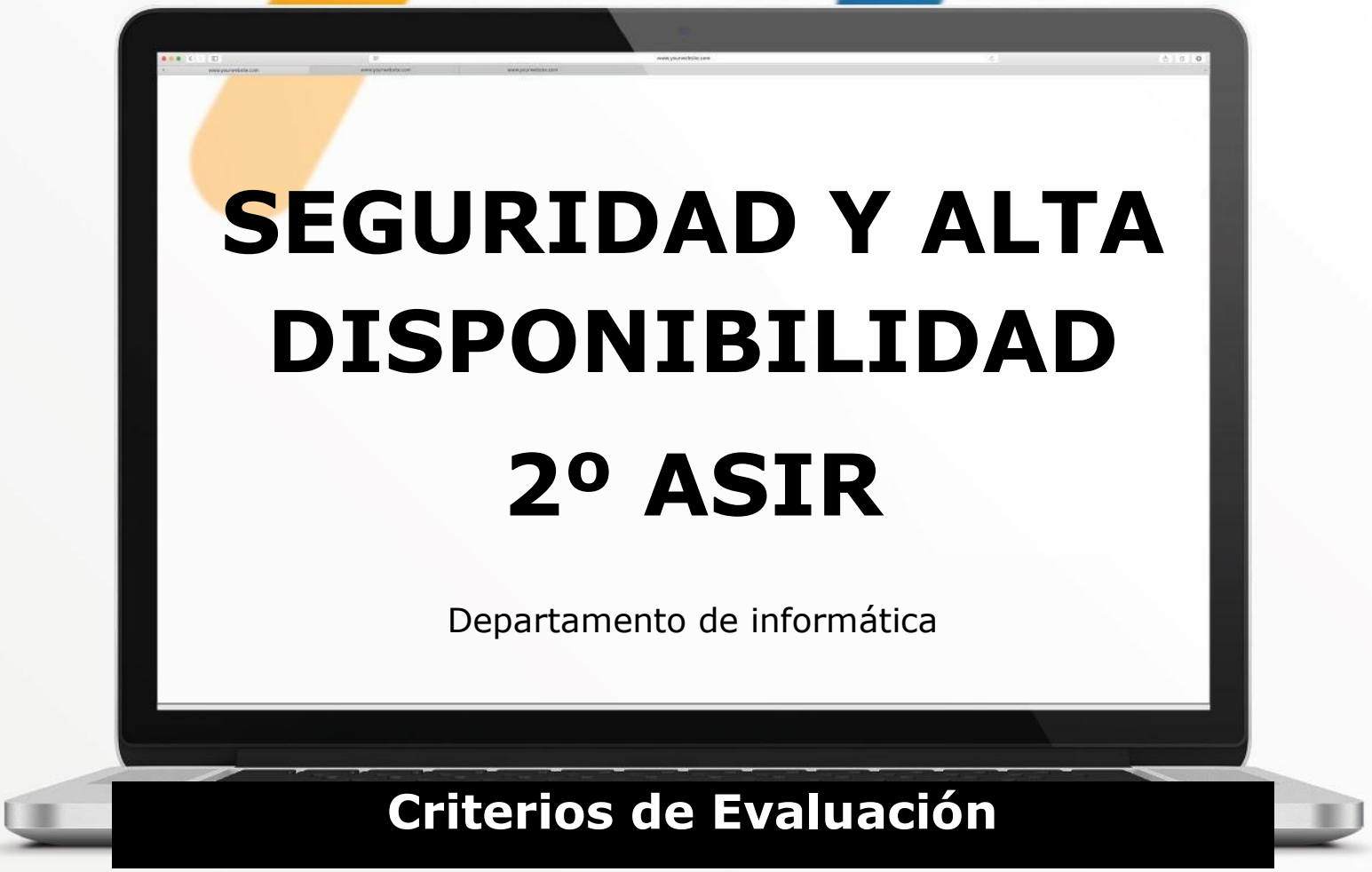
ies mutxamel

GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL

UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro



SEGURIDAD Y ALTA DISPONIBILIDAD

2º ASIR

Departamento de informática

Criterios de Evaluación

Curso: 2023/2024

David Alcaraz Pérez

Ficha identificativa del módulo

Referente Europeo	CINE 5b (Clasificación Internacional Normalizada de la Educación).						
Familia Profesional	Informática y Comunicaciones.						
Ciclo Formativo	Grado Superior	**Duración**	2000 horas	**Nº Cursos**	2		
Nombre del título	Técnico Superior en Administración de Sistemas Informáticos en Red						
Referencia Normativa Básica	- 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. - ORDEN 36/2012, de 22 de junio, de la Conselleria de Educación, Formación y Empleo, por la que se establece para la Comunitat Valenciana el currículo del ciclo formativo de grado superior correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red.						
Competencia General	La competencia general de este título consiste en configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente.						
Código y denominación del módulo	0378. Seguridad y Alta Disponibilidad						
Nº Trimestres	2	**Carga Lectiva**	100 horas	**Nivel**	2º Curso	**Curso Académico**	2023/2024
Modalidad	Presencial	**Docencia en Inglés**	No				
Horario Lectivo	5h a la semana						
Docente	David Alcaraz Pérez						
Cualificaciones Profesionales	IFC152_3, IFC156_3, IFC079_3, IFC154_3						
Unid. Competencia	UC0486_3						

Resultados de aprendizaje

A continuación, se enumeran los resultados de aprendizaje vienen expresados en el RD de Título siendo éstos las habilidades que el alumno debe ir adquiriendo a través del módulo para ir desarrollando las competencias necesarias para adquirir el título.

RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.

RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.

RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.

RA5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.

RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba

RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Objetivos

La competencia general del título describe las funciones profesionales más significativas del perfil profesional tomando como referente el conjunto de cualificaciones profesionales y las unidades de competencia incluidas.

La competencia general de este título consiste en configurar, administrar y mantener sistemas informáticos, garantizando la funcionalidad, la integridad de los recursos y servicios del sistema, con la calidad exigida y cumpliendo la reglamentación vigente.

A través del módulo de Administración de Sistemas Operativos vamos a contribuir a la competencia general del título de manera significativa dado el carácter interdisciplinar del módulo ya que integra los contenidos, habilidades y destrezas de la mayoría de los módulos que conforman el ciclo formativo.

El 1629/2009 por el que se establece el título de Técnico Superior de Administración de Sistemas Informáticos en Red y sus enseñanzas mínimas, en su artículo 9 establece los siguientes objetivos generales, teniendo en cuenta que los objetivos que se detallan a continuación son sólo aquellos a los que contribuye el módulo objeto de la presente programación (j, k, l, m, o, y p):

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

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

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

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

16. Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.

17. Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para resolver problemas y mantener una cultura de actualización e innovación.

Competencias profesionales, personales y sociales

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales e), f), i), j), k), m), n), o), r) y s) del título.

5. Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.

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

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

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

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

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

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

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

19. Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

20. Participar de forma activa en la vida económica, social y cultural con actitud crítica y responsable.

Contenidos

Para la elaboración de este apartado se han tenido en cuenta los contenidos curriculares para el módulo de Seguridad y Alta Disponibilidad establecidos en la Orden de 36/2012 de 22 junio de la Conselleria de Educación, Formación y Empleo, por la que se establece para la Comunitat Valenciana el currículo del ciclo formativo de grado superior correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red de la que se detallan a continuación:

Adopción de pautas de seguridad informática

Adopción de pautas de seguridad informática:

- Fiabilidad, confidencialidad, integridad y disponibilidad.
- Elementos vulnerables en el sistema informático: hardware, software y datos.
- Análisis de las principales vulnerabilidades de un sistema informático.
- Amenazas. Tipos:
  - Amenazas físicas.
  - Amenazas lógicas.
- Seguridad física y ambiental:
  - Ubicación y protección física de los equipos y servidores.
  - Sistemas de alimentación ininterrumpida.
- Seguridad lógica:
  - Criptografía.
  - Listas de control de acceso.
  - Establecimiento de políticas de contraseñas.
  - Políticas de almacenamiento.
  - Copias de seguridad e imágenes de respaldo.
  - Medios de almacenamiento.
- Análisis forense en sistemas informáticos:

Implantación de mecanismos de seguridad activa

- Ataques y contramedidas en sistemas personales:
  - Clasificación de los ataques.
  - Anatomía de ataques y análisis de software malicioso.
  - Herramientas preventivas. Instalación y configuración.
  - Herramientas paliativas. Instalación y configuración.
  - Actualización de sistemas y aplicaciones.
  - Seguridad en la conexión con redes públicas.
  - Pautas y prácticas seguras.
- Seguridad en la red corporativa:
  - Monitorización del tráfico en redes.
  - Seguridad en los protocolos para comunicaciones inalámbricas.
  - Riesgos potenciales de los servicios de red.
  - Intentos de penetración.

Implantación de técnicas de acceso remoto. Seguridad perimetral

- Elementos básicos de la seguridad perimetral.
- Perímetros de red. Zonas desmilitarizadas.
- Arquitectura débil de subred protegida.
- Arquitectura fuerte de subred protegida.
- Redes privadas virtuales. VPN.
- Beneficios y desventajas con respecto a las líneas dedicadas.
- Técnicas de cifrado. Clave pública y clave privada:
  - VPN a nivel de red. SSL, IPSec.

- VPN a nivel de aplicación. SSH.

- Servidores de acceso remoto:
  - Protocolos de autenticación.
  - Configuración de parámetros de acceso.
  - Servidores de autenticación.

Instalación y configuración de cortafuegos

- Utilización de cortafuegos.
- Filtrado de paquetes de datos.
- Tipos de cortafuegos. Características. Funciones principales.
- Instalación de cortafuegos. Ubicación.
- Reglas de filtrado de cortafuegos.
- Pruebas de funcionamiento. Sondeo.
- Registros de sucesos de un cortafuegos.

Instalación y configuración de servidores «proxy»

- Tipos de «proxy». Características y funciones.
- Instalación de servidores «proxy».
- Instalación y configuración de clientes «proxy».
- Configuración del almacenamiento en la caché de un «proxy».
- Configuración de filtros.
- Métodos de autenticación en un «proxy».

Implantación de soluciones de alta disponibilidad

- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad.
  - Funcionamiento ininterrumpido.
  - Integridad de datos y recuperación de servicio.
  - Servidores redundantes.
  - Sistemas de «clusters».
  - Balanceadores de carga.
- Instalación y configuración de soluciones de alta disponibilidad.
- Virtualización de sistemas.
- Posibilidades de la virtualización de sistemas.
- Herramientas para la virtualización.
- Configuración y utilización de máquinas virtuales.
- Alta disponibilidad y virtualización.
- Simulación de servicios con virtualización.

Legislación y normas sobre seguridad

- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

Elementos transversales

Los elementos transversales son un conjunto de saberes basados en actitudes, valores y normas que dan respuesta a algunos problemas sociales existentes en la actualidad. Los objetivos que se pretenden alcanzar están recogidos en el Programa Educativo de Centro y se trabajarán de forma global y programada desde los módulos que conforman el título. A continuación, se detallan los resultados de aprendizaje transversales que se persiguen alcanzar a través del módulo objeto de la presente programación:

RAT1. Respeta la diversidad de las personas y opiniones y participa de forma activa en la resolución de conflictos, en el rechazo de la violencia, en el respeto a los demás y rechazando cualquier tipo de discriminación o comportamiento sexista.

RAT2. Realiza un uso correcto de las tecnologías de la información y comunicación y los medios audiovisuales previniendo situaciones de riesgo derivadas de su utilización inadecuada.

RAT3. Realiza tareas de forma autónoma y responsable tanto individualmente como en equipo, utilizando el autoaprendizaje, la capacidad crítica y la creatividad como elementos que le permitan adaptarse a la evolución de los procesos productivos y al cambio social.

RAT4. Trabaja en condiciones de seguridad previniendo riesgos derivados del trabajo y utiliza los recursos de forma responsable respetando el medio ambiente, previniendo la formación de residuos, reparando, reutilizando o gestionando su reciclaje al final de su vida útil.

Criterios de evaluación

Para poder llegar a realizar la evaluación de los resultados de aprendizaje, objetivos y competencias del módulo es necesario establecer unos criterios de evaluación que, de modo orientativo, vienen recogidos en el Real Decreto de título. Dentro de cada una de las unidades didácticas se expresarán los criterios de evaluación que se utilizarán concretados en forma de indicadores de evaluación. A continuación, se relacionan los criterios de evaluación:

Resultado de Aprendizaje	Criterios de Evaluación
RA1	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. i) Se han identificado las fases del análisis forense ante ataques a un sistema.
RA2	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.

	d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.
RA3	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna. b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
RA4	a) Se han descrito las características, tipos y funciones de los cortafuegos. b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico. c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.
RA5	a) Se han identificado los tipos de «proxy», sus características y funciones principales. b) Se ha instalado y configurado un servidor «proxy-cache». c) Se han configurado los métodos de autenticación en el «proxy». d) Se ha configurado un «proxy» en modo transparente. e) Se ha utilizado el servidor «proxy» para establecer restricciones de acceso Web. f) Se han solucionado problemas de acceso desde los clientes al «proxy». g) Se han realizado pruebas de funcionamiento del «proxy», monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor «proxy» en modo inverso. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores «proxy».
RA6	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal. e) Se ha implantado un balanceador de carga a la entrada de la red interna. f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de «clusters» para aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.

RA7	a) Se ha descrito la legislación sobre protección de datos de carácter personal. b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen. e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. f) Se han contrastado las normas sobre gestión de seguridad de la información. g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

También es necesario expresar los criterios de evaluación para evaluar el cumplimiento de los resultados de aprendizaje transversales.

Resultados de Aprendizaje Transversales	Criterios de evaluación
RAT1	● Se ha analizado, comprendido y tratado de conciliar e integrar posturas para lograr acuerdos en las situaciones de conflicto. ● Se ha evitado el enfrentamiento.
RAT2	● Se ha evitado el acceso a páginas web u correo electrónico no corporativo en el aula. ● Se ha concienciado de no utilizar el móvil en el aula.
RAT3	● Actúa de forma autónoma para gestionar su aprendizaje. ● Emplea la escucha activa y se muestra asertivo. ● Adecúa la comunicación verbal y no verbal a la situación e interlocutores. ● Asume las normas establecidas en el equipo de trabajo. ● Es responsable con las tareas asignadas y aúna los esfuerzos del grupo para lograr el objetivo. ● Analiza la relación entre el trabajo realizado por el equipo y los resultados obtenidos.
RAT4	● Se han analizado los riesgos derivados de su actividad laboral. ● Se ha realizado un uso eficiente de la energía. ● Se han analizado el consumo de recursos y los optimiza. ● Se ha adquirido una actitud positiva hacia el reciclaje.

Criterios de calificación

Se evaluará el grado de aprendizaje individual respecto a los objetivos mínimos propuestos para cada unidad didáctica. También serán evaluados, paralelamente, la práctica docente y el proceso de enseñanza.

Según los distintos tipos de contenidos, los porcentajes en cada uno de ellos serán los siguientes:

- 10% **Contenidos Actitudinales** (Saber ser): asistencia, puntualidad, interés, participación, responsabilidad, iniciativa, trabajo en equipo, persistencia, buena presentación en tiempo y forma, capacidad de planificación y organización y entrega de los ejercicios de clase. La asistencia a clase es obligatoria y necesaria en todos los niveles de enseñanza secundaria, y conviene hacerlo explícito en el ciclo formativo. Si la no asistencia a clase justificada o no, supera el 15% del total, el *'alumno perderá el derecho a realizar el examen ordinario, habiendo de presentarse en la convocatoria de junio'*. Se evaluarán en este apartado los ejercicios recogidos en clase.
- 30% **Contenidos Procedimentales** (Saber hacer): correcta realización de los ejercicios prácticos y trabajos propuestos en clase y también para ser realizados en casa (de forma excepcional).
- 60% **Contenidos Conceptuales** (Saber): evaluación de los conocimientos adquiridos a nivel global en cada unidad didáctica.

Para aprobar, el alumno **debe aprobar por separado** tanto los contenidos actitudinales, como los procedimentales y los conceptuales, es decir, los exámenes, los proyectos finales, las prácticas y los ejercicios recogidos por el profesor.

Para la aplicación del proceso de evaluación continua se requiere una asistencia regular a las clases y el desarrollo de las actividades previstas, siendo necesaria la asistencia al menos al 85% de las sesiones. Si se supera el 15% de inasistencia acreditada y justificada por Jefatura de Estudios supondrá la pérdida de evaluación continua y podrá suponer la anulación de matrícula por inasistencia.

Para poder superar cada una de las unidades didácticas es necesario que el alumno haya:

- Realizado y entregado todas las actividades planteadas en la unidad.
- Demostrado haber adquirido los mínimos exigibles
- Obtenido una nota igual o superior a 5 en las pruebas escritas/prácticas.
- Obtenido una nota positiva (igual o superior a 5) en la unidad didáctica.

Una práctica o trabajo copiado supondrá un cero en la nota, tanto para el alumno que copia como para el que ha permitido la copia. Ninguno de los dos tendrá derecho a recuperar esa práctica o trabajo, además de la sanción correspondiente tipificada en el RRI del centro. Si un alumno no asiste a clase de manera injustificada, la entrega de la práctica se calificará con un 0.

Las faltas graves de ortografía en prácticas o exámenes podrían llevar penalización de la nota.

Criterios ortográficos

Dentro del plan de mejora de escritura del alumnado, el departamento de informática ha acordado que en las actividades y exámenes de los alumnos se penalizarán los errores ortográficos. Penalización de 0,10 puntos por error ortográfico (0,05 por tilde), hasta un máximo de 2,5 puntos no acumulables.

Criterios de recuperación

Aquellos alumnos que no hayan superado alguna de las unidades didácticas tendrán la posibilidad de recuperarlas a través de unas actividades de refuerzo que serán planteadas a cada alumno por parte del profesor. Estas actividades se entregarán al alumno preferiblemente al finalizar la unidad, con una fecha límite de entrega, y su corrección se realizará de forma presencial junto con el profesor (el alumno deberá responder correctamente a las cuestiones relacionadas con las actividades planteadas por el profesor). La nota de las unidades didácticas recuperadas tendrá una calificación máxima de 5 puntos.

Se considerará superada la evaluación siempre y cuando se haya obtenido una calificación positiva (igual o superior a 5) en todas las unidades didácticas evaluadas en el trimestre. Se realizará una media ponderada de las unidades didácticas que formen parte de la evaluación. En caso de no superar alguna de las unidades tendrá que recuperar la evaluación correspondiente en convocatoria ordinaria.