PROGRAMACIÓN DIDÁCTICA
F.P INFORMATICA
2022/23

CICLO	CFGM SISTEMAS MICROINFORMÁTICOS Y REDES
MÓDULO	0226 – Seguridad Informática
GRUPO	2º

ÍNDICE

1 CONTEXTUALIZACIÓN

PROFESOR	Ignacio Navarro Cuesta
Nº HORAS TOTALES	127
Nº HORAS SEMANALES	5
Nº HORAS PÉRDIDA DERECHO EVAL. CONTINUA	26

La legislación de este ciclo formativo está desarrollada en los siguientes documentos:

- Real Decreto 1691/2007, de 14 de diciembre, por el que se establece el Título de Técnico en Sistemas Microinformáticos y Redes, y se fijan las enseñanzas mínimas
- Decreto 107/2009, de 04/08/2009, por el que se establece el currículo del ciclo formativo de grado medio correspondiente al Título de Técnico o Técnica en Sistemas Microinformáticos y Redes, en la comunidad autónoma de Castilla-La Mancha

2 OBJETIVOS GENERALES

El **Real Decreto 1691/2007**, de 14 de diciembre, enumera los siguientes objetivos generales para este módulo:

a) Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
c) Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
d) Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de la red.
e) Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
g) Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
k) Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
l) Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.

3 PERFIL Y COMPETENCIA PROFESIONAL

El perfil profesional del título de **Técnico Medio en Sistemas Microinformáticos y Redes** queda determinado por su competencia general, sus competencias profesionales, personales y sociales, y por la relación de cualificaciones y, en su caso, unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales incluidas en el título.

3.1. COMPETENCIA GENERAL DEL CICLO

La competencia general de este título consiste en:

Instalar, configurar y mantener sistemas microinformáticos, aislados o en red, así como redes locales en pequeños entornos, asegurando su funcionalidad y aplicando los protocolos de calidad, seguridad y respeto al medio ambiente establecidos.

3.2. COMPETENCIAS PROFESIONALES DEL MÓDULO

Las competencias profesionales, personales y sociales según Real Decreto 1691/2007, de 14 de diciembre de este título son las que se relacionan a continuación:

a) Determinar la logística asociada a las operaciones de instalación, configuración y mantenimiento de sistemas microinformáticos, interpretando la documentación técnica asociada y organizando los recursos necesarios.

c) Instalar y configurar software básico y de aplicación, asegurando su funcionamiento en condiciones de calidad y seguridad.

i) Ejecutar procedimientos establecidos de recuperación de datos y aplicaciones ante fallos y perdidas de datos en el sistema, para garantizar la integridad y disponibilidad de la información.

j) Elaborar documentación técnica y administrativa del sistema, cumpliendo las normas y reglamentación del sector, para su mantenimiento y la asistencia al cliente.

l) Asesorar y asistir al cliente, canalizando a un nivel superior los supuestos que lo requieran, para encontrar soluciones adecuadas a las necesidades de este.

n) Mantener un espíritu constante de innovación y actualización en el ámbito del sector informático.

o) Aplicar los protocolos y normas de seguridad, calidad y respeto al medio ambiente en las intervenciones realizadas.

p) Cumplir con los objetivos de la producción, colaborando con el equipo de trabajo y actuando conforme a los principios de responsabilidad y tolerancia.

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

3.3 CUALIFICACIONES PROFESIONALES DEL CICLO:

CUALIFICACIONES PROFESIONALES COMPLETAS
a) Sistemas microinformáticos IFC078_2 (Real Decreto 295/2004, 20 febrero)
Unidades de Competencia
• UC0219_2: Instalar y configurar el software base en sistemas microinformáticos. • UC0220_2: Instalar, configurar y verificar los elementos de la red local según procedimientos establecidos. • UC0221_2: Instalar, configurar y mantener paquetes informáticos de propósito general y aplicaciones específicas. • UC0222_2: Facilitar al usuario la utilización de paquetes informáticos de propósito general y aplicaciones específicas.
b) Montaje y reparación de sistemas microinformáticos IFC298_2 (Real Decreto 1201/2007, 14 septiembre)
Unidades de Competencia
• UC0953_2: Montar equipos microinformáticos. • UC0219_2: Instalar y configurar el software base en sistemas microinformáticos. • UC0954_2: Reparar y ampliar equipamiento microinformático.
c) Operación de redes departamentales IFC299_2 (Real Decreto 1201/2007, 14 septiembre)
Unidades de Competencia
• UC0220_2: Instalar, configurar y verificar los elementos de la red local según procedimientos preestablecidos. • UC0955_2: Monitorizar los procesos de comunicaciones de la red local. • UC0956_2: Realizar los procesos de conexión entre redes privadas y redes públicas.
d) Operación de sistemas informáticos IFC300_2 (Real Decreto 1201/2007, 14 septiembre)
Unidades de Competencia
• UC0219_2: Instalar y configurar el software base en sistemas microinformáticos. • UC0957_2: Mantener y regular el subsistema físico en sistemas informáticos. • UC0958_2: Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación del cliente. • UC0959_2: Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

4 LÍNEAS DE ACTUACIÓN

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

- La protección de equipos y redes informáticas
- La protección de la información transmitida y almacenada.
- La legislación y normativa vigente en materia de seguridad.

5 ORGANIZACIÓN Y METODOLOGÍA

- Se impartirán 5 horas semanales, en la siguiente distribución:
  - 2 horas los miércoles, de 10:20h a 12:10h
  - 1 hora los jueves, de 13:35h a 14:30h
  - 2 horas los viernes, de 8:30h a 10:20h
- Se pretende un aprendizaje basado en una metodología activa donde el alumno sea protagonista de su propio proceso de aprendizaje a partir de unos conocimientos previos hasta lograr los resultados de aprendizaje del módulo.
- La metodología a emplear en la impartición de este módulo profesional se encuadra dentro de los principios metodológicos establecidos para la **Formación Profesional Específica**:
  - Metodología activa y participativa.
  - Exposición por parte del profesor de contenidos seguida de su aplicación práctica.
  - Uso del ordenador, software y demás recursos ligados a las TIC para la realización de las prácticas propuestas.
  - Planteamiento de problemas y tareas próximos a la realidad de la materia.
  - Fomento del trabajo en grupo que complete el desarrollo individual.
  - Desarrollo de actividades de autoaprendizaje.
- Se utilizará el Aula Virtual para:
  - Publicación de fechas de exámenes y prácticas, calificaciones, entregas, etc.
  - Publicación de material escrito, enlaces, software, etc. para el desarrollo del módulo.
  - Publicación de otros recursos y materiales adicionales, relacionados con el módulo.
  - Publicación de prácticas, y recogida de las mismas.

6 MEDIDAS DE INCLUSIÓN EDUCATIVA

- Desde la enseñanza de la formación profesional específica, cuyos logros están marcados previamente por las capacidades terminales que han de alcanzar los alumnos, las posibilidades de atender esta diversidad están limitadas por la propia naturaleza del tipo de enseñanza. No obstante, sí existen una serie de recursos que pueden satisfacer en parte, estas necesidades de adaptación curricular.
- El profesor aceptará apoyos educativos, aplicará incentivos, corregirá fallos, y un seguimiento lo más individual posible para los alumnos. Es decir, podrán aplicarse pequeñas variaciones metodológicas, cambios en las actividades y recursos aplicados, todo ello según la disidencia que se pretenda compensar.
- Trataremos, en resumen, de detectar las características del grupo, las necesidades de éste y se facilitará que cada alumno pueda progresar por encima de un mínimo exigible a cada uno de ellos, en concordancia con las capacidades terminales fijadas previamente.
- Las adaptaciones curriculares en la FP podemos clasificarlas en dos tipos: no significativas (no afectan a los objetivos y capacidades mínimos) y de accesibilidad (mediante la modificación de las condiciones materiales o del puesto de trabajo).
- En cualquier, caso se debe contar con apoyos del profesorado y del personal especializado, del departamento de orientación, al objeto de proporcionar a estos alumnos/as los medios que le permitan desarrollar las capacidades terminales.

6.6.1. Actuaciones para el alumnado con discapacidad física

▫Los procesos de evaluación se adecuarán a las adaptaciones metodológicas de las que haya podido ser objeto el alumnado con discapacidad y se garantizará su accesibilidad a las pruebas de evaluación.

–Las medidas que tomaremos, en caso de ser necesario, durante el curso dependerán del tipo de discapacidad que sufra el alumno:

- *Discapacidad visual*: En el caso de la discapacidad visual dependerá a su vez de si esta es total o parcial, en el caso de ser parcial los sistemas operativos ya disponen de herramientas para facilitar su uso a personas con problemas de visión, pero en el caso de la discapacidad visual total sería necesario además el uso de hardware especial adaptado para este tipo de discapacidad del que no disponemos en el centro.
- *Discapacidad auditiva*: Igual que el caso anterior tendremos que distinguir entre discapacidad auditiva total y parcial, en el caso de la discapacidad auditiva parcial si el alumno posee algún dispositivo que le permita corregir esta falta no sería necesaria realizar ninguna acción especial, en el caso de sordera total tendremos que adaptar todo nuestro material con textos y subtítulos necesarios para su adecuada compresión.
- *Discapacidad móvil*: Si tuviésemos algún alumno con este tipo de discapacidad y que no pueda acceder a su aula de grupo, por ejemplo, que esté en silla de ruedas, se le proporcionará un espacio en la primera planta en la que el alumno pueda desarrollar las actividades necesarias para poder superar cada módulo.

7 RESULTADOS DE APRENDIZAJE

REFERENCIA			RESULTADO DE APRENDIZAJE			PONDERACIÓN
RA 1			**Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.**			**25%**
U.T.	**Referencia**		**Criterios de Evaluación**	**Contenidos básicos del RD**	**Calificador/ Ponderación**	**Instrumento de evaluación**
	Nombre	**Mínimo**				
UT 1	CE 1.a	☒	Se ha valorado la importancia de mantener la información segura.	– Ubicación y protección física de los equipos y servidores. – Sistemas de alimentación ininterrumpida.	Numérico: <5: no superado >=5 superado 100%	– Prueba escrita (60%) – Prácticas individuales y/o en grupo (40%) Imprescindible superar por separado tanto la prueba escrita como las prácticas (en su conjunto).
	CE 1.b	☒	Se han descrito las diferencias entre seguridad física y lógica.			
	CE 1.c	☒	Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.			
	CE 1.d	☒	Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.			
	CE 1.e	☒	Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.			
	CE 1.f	☒	Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.			
	CE 1.g	☒	Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.			
	CE 1.h	☒	Se ha valorado la importancia de establecer una política de contraseñas.			
	CE 1.i	☒	Se han valorado las ventajas que supone la utilización de sistemas biométricos.			

REFERENCIA			RESULTADO DE APRENDIZAJE			PONDERACIÓN
RA 2			**Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.**			**25%**
U.T.	**Referencia**		**Criterios de Evaluación**	**Contenidos básicos del RD**	**Calificador/ Ponderación**	**Instrumento de evaluación**
	Nombre	**Mínimo**				
UT 2	CE 2.a	☒	Se ha interpretado la documentación técnica relativa a la política de almacenamiento.	– Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad. – Almacenamiento redundante y distribuido. – Almacenamiento remoto y extraíble. – Criptografía. – Copias de seguridad e imágenes de respaldo. – Medios de almacenamiento	Numérico: <5: no superado >=5 superado 100%	– Prueba escrita (60%) – Prácticas individuales y/o en grupo (40%) Imprescindible superar por separado tanto la prueba escrita como las prácticas (en su conjunto).
	CE 2.b	☒	Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).			
	CE 2.c	☒	Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.			
	CE 2.d	☒	Se han descrito las tecnologías de almacenamiento redundante y distribuido.			
	CE 2.e	☒	Se han clasificado los principales tipos de criptografía			
	CE 2.f	☒	Se han seleccionado estrategias para la realización de copias de seguridad.			
	CE 2.g	☒	Se ha tenido en cuenta la frecuencia y el esquema de rotación.			
	CE 2.h	☒	Se han realizado copias de seguridad con distintas estrategias.			
	CE 2.i	☒	Se han identificado las características de los medios de almacenamiento remotos y extraíbles.			
	CE 2.j	☒	Se han utilizado medios de almacenamiento remotos y extraíbles.			
	CE 2.k	☒	Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.			
	CE 2.l	☒	Se han utilizado herramientas de chequeo de discos.			

REFERENCIA			RESULTADO DE APRENDIZAJE			PONDERACIÓN
RA 3			**Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.**			**20%**
U.T.	**Referencia**		**Criterios de Evaluación**	**Contenidos básicos del RD**	**Calificador/ Ponderación**	**Instrumento de evaluación**
	Nombre	**Mínimo**				
UT 3	CE 3.a	☒	Se han clasificado y enumerado los tipos de amenazas.	– Identificación digital. Firma electrónica y certificado digital. – Seguridad en los protocolos para comunicaciones inalámbricas. – Utilización de cortafuegos en un sistema o servidor. – Listas de control de acceso. – Política de contraseñas. – Recuperación de datos. – Software malicioso. Clasificación. Herramientas de protección y desinfección.	Numérico: <5: no superado >=5 superado 100%	– Prueba escrita (60%) – Prácticas individuales y/o en grupo (40%) Imprescindible superar por separado tanto la prueba escrita como las prácticas (en su conjunto).
	CE 3.b	☒	Se han descrito los principales tipos de ataques.			
	CE 3.c	☒	Se han aplicado técnicas de auditoría de sistemas.			
	CE 3.d	☒	Se han seguido planes de contingencia para actuar ante fallos de seguridad.			
	CE 3.e	☒	Se han clasificado los principales tipos de software malicioso.			
	CE 3.f	☒	Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.			
	CE 3.g	☒	Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.			
	CE 3.h	☒	Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.			
	CE 3.i	☒	Se han aplicado técnicas de recuperación de datos.			

REFERENCIA			RESULTADO DE APRENDIZAJE			PONDERACIÓN
RA 4			**Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.**			**20%**
U.T.	**Referencia**		**Criterios de Evaluación**	**Contenidos**	**Calificador/ Ponderación**	**Instrumento de evaluación**
	Nombre	**Mínimo**				
UT 4	CE 4.a	☒	Se ha identificado la necesidad de inventariar y controlar los servicios de red.	− Métodos para asegurar la privacidad de la información transmitida. − Fraudes informáticos y robos de información. − Control de la monitorización en redes cableadas. − Seguridad en redes inalámbricas. − Sistemas de identificación: firma electrónica, certificados digitales y otros. − Cortafuegos en equipos y servidores	Numérico: <5: no superado >=5 superado 100%	− Prueba escrita (60%) − Prácticas individuales y/o en grupo (40%) Imprescindible superar por separado tanto la prueba escrita como las prácticas (en su conjunto).
	CE 4.b	☒	Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.			
	CE 4.c	☒	Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.			
	CE 4.d	☒	Se han aplicado medidas para evitar la monitorización de redes cableadas.			
	CE 4.e	☒	Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.			
	CE 4.f	☒	Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.			
	CE 4.g	☒	Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.			
	CE 4.h	☒	Se han instalado, configurado y utilizado herramientas de cifrado.			
	CE 4.i	☒	Se han descrito el uso de la tecnología de tarjetas inteligentes.			
	CE 4.j	☒	Se ha instalado y configurado un cortafuegos en un equipo o servidor.			

REFERENCIA			RESULTADO DE APRENDIZAJE			PONDERACIÓN
RA 5			**Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.**			**10%**
U.T.	**Referencia**		**Criterios de Evaluación**	**Contenidos básicos del RD**	**Calificador/ Ponderación**	**Instrumento de evaluación**
	Nombre	**Mínimo**				
UT 5	CE 5.a	☒	Se ha descrito la legislación sobre protección de datos de carácter personal	– Legislación sobre protección de datos. – Legislación sobre los servicios de la sociedad de la información y correo electrónico	Numérico: <5: no superado >=5 superado 100%	– Prueba escrita (60%) – Prácticas individuales y/o en grupo (40%) Imprescindible superar por separado tanto la prueba escrita como las prácticas (en su conjunto).
	CE 5.b	☒	Se ha determinado la necesidad de controlar el acceso a la información personal almacenada			
	CE 5.c	☒	Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos			
	CE 5.d	☒	Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen			
	CE 5.e	☒	Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico			
	CE 5.f	☒	Se han contrastado las normas sobre gestión de seguridad de la información			

8 CONTENIDOS, SECUENCIACIÓN Y TEMPORIZACIÓN

8.1. CONTENIDOS

U.T	CONTENIDOS del DOCM
UT 1 Introducción a la seguridad informática y aplicación de medidas de seguridad pasiva	• Ubicación y protección física de los equipos y servidores. • Control del acceso físico: Sistemas biométricos. • Sistemas de alimentación ininterrumpida. • Equipos redundantes o de reserva. • Control ambiental: Polvo, suciedad, calor, humedad, electricidad estática, emisiones de radiofrecuencia, interferencias electromagnéticas y otros. • Preparación frente a catástrofes.
UT 2 Gestión de dispositivos de almacenamiento y resguardo de información	• Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad. • Sistemas tolerantes a fallos: Almacenamiento redundante y distribuido, sustitución de sectores, arrays de disco, agrupamiento (clustering). • Almacenamiento remoto y extraíble. • Criptografía: Cifrado simétrico, asimétrico, híbrido. • Estrategias de copias de seguridad. • Copias de seguridad e imágenes de respaldo. • Mantenimiento de un registro de copias de seguridad. • Medios de almacenamiento. • Tareas de control y mantenimiento: Herramientas de chequeo de discos.
UT 3 Aplicación de mecanismos de seguridad activa del software	• Tipos de amenazas: interrupción, interceptación, modificación y fabricación. • Tipos de ataques. • Identificación digital. Firma electrónica, certificado digital, autoridades de certificación. • Seguridad en los protocolos para comunicaciones inalámbricas. • Seguridad en la Web. • Utilización de cortafuegos en un sistema o servidor. • Listas de control de acceso. • Política de contraseñas. • Recuperación de datos. • Software malicioso o Malware. Clasificación. Herramientas de protección y desinfección. • Políticas de auditoría de un sistema. • Medidas de estudio de ataques a sistemas. Análisis forense. Utilidades. • Actualización del sistema operativo. Parches de seguridad. Autenticidad y fiabilidad del software instalado.
UT 4 Aseguramiento de la privacidad en redes	• Métodos para asegurar la privacidad de la información transmitida. • Fraudes informáticos y robos de información. • Ingeniería social. • Control de la monitorización en redes cableadas. • Protocolos de Internet seguros. • Seguridad en redes inalámbricas. • Redes privadas virtuales. • Sistemas de identificación: firma electrónica, certificados digitales, servidores de certificados y otros. • Infraestructura de clave pública (PKI). • Utilización de herramientas de cifrado. • Tarjetas inteligentes. • Cortafuegos en equipos y servidores.
UT 5 Legislación sobre seguridad informática y protección de datos	• Legislación sobre protección de datos. • Legislación sobre los servicios de la sociedad de la información y correo electrónico.

8.2. TEMPORIZACIÓN, PONDERACIÓN Y SECUENCICIÓN

U.T	RA	PONDERACIÓN	EVALUACIÓN	Nº SESIONES (1 h.)
UT 1. Introducción a la seguridad informática y aplicación de medidas de seguridad pasiva	RA1	25 %	1ª	31
UT 2. Gestión de dispositivos de almacenamiento y resguardo de información	RA2	25 %	1ª	31
UT 3. Aplicación de mecanismos de seguridad activa del software	RA3	20 %	2ª	26
UT 4. Aseguramiento de la privacidad en redes	RA4	20 %	2ª	26
UT 5. Legislación sobre seguridad informática y protección de datos	RA5	10 %	2ª	13
TOTAL HORAS				**127**

Para establecer la nota de cada evaluación se le aplicará el porcentaje

Porcentaje Unidad: (%Unidad * 100) /% total evaluación

Por ejemplo, tal y como está en la tabla anterior, el porcentaje de la 1ª evaluación con respecto al total es 50%, con lo cual cada U.T. se calculará como sigue:

% UT1 = (25%) *100/(50%) = 50 %

% UT2 = (25%) *100/(50%) = 50 %

9 PROCEDIMIENTOS DE EVALUACIÓN

- Se realizará un proceso de evaluación continua.
- A lo largo del desarrollo de las unidades de trabajo, se emplearán **Instrumentos de Evaluación** adecuados para la correcta evaluación de cada Criterio de Evaluación (CE), según se han descrito anteriormente, y que se pueden resumir como sigue:
  - Prueba escrita, a realizar en clase, con un peso del 60% sobre la UT.
  - Prácticas individuales y/o grupales, con un peso total del 40% sobre la UT.

  Es imprescindible aprobar por separado tanto la prueba escrita como las prácticas (en su conjunto).
- Todos estos instrumentos tendrán asociada una calificación de 0 a 10.
- La evaluación será formativa, informando a los alumnos de los puntos fuertes (para consolidarlos) y de los puntos débiles (para mejorarlos) en cada una de las entregas, preferiblemente por escrito través del Aula Virtual (en casos excepcionales se realizará de modo verbal en la clase).
- A la hora de calificar una actividad práctica, el profesor podrá solicitar al alumno que realice una **defensa** de la misma. El alumno tendrá que explicar cómo ha realizado la práctica y deberá contestar a las preguntas relacionadas con la práctica que le haga el profesor. En este caso, la calificación se hará en función de esta defensa.
- **No se recogerán entregas fuera de plazo**. En caso de que tengan relación con algún CE importante, se le informará al alumno sobre modo de proceder, que podrá ser:
  - Entregar de nuevo (pudiendo el profesor poner prácticas distintas a las ya entregas) y defensa de la misma el día asignado para recuperaciones.
  - Prueba escrita o práctica relacionada el día asignado para recuperaciones.
- **Consideraciones referentes a las pruebas escritas**:
  - Se realizará en cada trimestre al menos una prueba individual escrita (teórico y/o práctica) que permita evaluar los RRAA impartidos en ese tiempo y que el profesor indicará previamente.
  - La fecha será fijada con suficiente antelación.
  - No se repetirá ninguna prueba escrita que no sea de evaluación ordinaria si el alumno falta el día del examen, aunque dicha falta esté justificada.
  - En caso de ausencia debidamente justificada a la prueba escrita de una evaluación ordinaria, y siempre que el tiempo y los medios sean posibles, se programará una nueva fecha para la realización de dicha prueba.

10 PROCESO DE EVALUACIÓN DE ALUMNADO Y CRITERIOS DE CALIFICACIÓN

- El alumno dispone de **2 convocatorias** por curso:
  - Evaluación Primera Ordinaria, realizada en marzo
  - Evaluación Segunda Ordinaria, realizada en junio
- El número total de convocatorias ordinarias del módulo es de 4.
- El alumno podrá renunciar a la Evaluación Primera Ordinaria en el plazo establecido por Jefatura de Estudios. Si el alumno no se presenta a la Evaluación Segunda Ordinaria la renuncia de convocatoria se hace oficio, no haciendo falta solicitarla.
- Para aprobar el módulo se deben superar **TODOS los RRAA** (Resultados de Aprendizaje) que forman parte del mismo. Un R.A. se considera superado cuando se han superado todos los mínimos establecidos para dicho R.A.
- Una vez superado un Resultado de Aprendizaje (RA), que estará asociado a una o varias UT, éste estará aprobado para todo el curso, incluida la Convocatoria Segunda Ordinaria (realizada a finales del mes de junio).
- Si la evaluación de las tareas prácticas está suspensa en su conjunto (ya sea por estar mal realizadas o por no ser entregadas en plazo), el resultado de aprendizaje al que pertenezcan estará suspenso, aunque la nota que corresponde en ese mismo RA a los demás instrumentos de evaluación sea de aprobado.
- Cuando las prácticas estén suspensas, el alumno tendrá la oportunidad de realizar una nueva entrega (pudiendo el profesor poner prácticas distintas a las ya entregas).
- La nota de cada evaluación se calculará aplicándole el porcentaje (calculado del total) correspondiente a cada UT que se haya impartido en dicha evaluación.
- En la programación de aula se detallarán de cada Unidad de Trabajo los criterios de calificación de la misma.

11 PROCEDIMIENTO DE RECUPERACIÓN

- Se realizarán tareas de recuperación por cada Unidad de Trabajo que el alumno haya suspendido, tanto durante la Evaluación Continua como para la Evaluación Segunda Ordinaria.
- Las prácticas deben ser entregadas en forma y plazo, pudiendo ser distintas de las propuestas inicialmente.
- Para poder presentarse a la prueba escrita, las prácticas deben estar aprobadas.
- Tanto para la Evaluación Primera Ordinaria como para la Evaluación Segunda Ordinaria, el alumnado recuperará aquellas UT que tenga suspensas.

12 EVALUACIÓN DEL ALUMNADO CON PÉRDIDA DEL DERECHO A LA EVALUACIÓN CONTINUA

- La asistencia a clase es obligatoria y presencial. Aquellos alumnos cuyo número total de faltas injustificadas sea superior al 20% de la carga total del módulo (127 horas), es decir, 26 horas, no tendrá derecho a la evaluación continua.
- Los alumnos que pierdan la Evaluación Continua:
  - Deberá entregar en tiempo y forma las prácticas que se le indiquen, pudiéndosele exigir prácticas distintas al resto de alumnos.
  - Realizarán al final de curso una serie de pruebas escritas, que podrán ser distintas a las que realicen el resto de alumnos, y que versarán sobre los contenidos impartidos durante el curso.
- El plazo de entrega de las prácticas será establecido por el profesor, siempre antes del día de las pruebas indicadas anteriormente.

13 ATENCIÓN AL ALUMNO QUE APRUEBA EN PERIODO ORDINARIO

Los alumnos que hayan aprobado todos los RA, en el periodo que va desde la evaluación ordinaria hasta la evaluación extraordinaria, podrán realizar algunas de las actividades que se enumeran a continuación:

- Realizar actividades en los que los alumnos que han aprobado puedan ayudar a recuperar a los alumnos que hayan suspendido.
- Realizar grupos en los que los alumnos realicen trabajo de investigación relacionados con el módulo.
- Ampliar sus conocimientos trabajando los conceptos vistos a lo largo del curso con otros softwares.

14 ATENCIÓN AL ALUMNADO QUE SUSPENDE EN PERIODO ORDINARIO

Los alumnos que no superen alguno de los RA y por lo tanto, hayan suspendido en la convocatoria ordinaria, deberán de seguir los planes de trabajo que se enumeran a continuación:

- A cada alumno se le entregará un **plan de trabajo individualizado** donde se enumere los RA que debe recuperar.
- Para cada RA a recuperar se deberán realizar una serie de actividades propuestas, pero con un enunciado diferente a las ya vista en clase durante el curso, estas prácticas se realizarán de manera individual y se entregarán a través de la plataforma Google Classroom.

15 MATERIALES Y RECURSOS DIDÁCTICOS

- Material:
  - 1 ordenadores en red para cada alumno
  - Acceso a Internet

- Pizarra blanca y rotuladores
- Proyector

- Software:
  - Máquinas virtuales.
  - Programa de captura de equipos.
  - Procesador de Textos
  - Programa de manejo de transparencias
  - Herramientas de Google (Classroom, Meet…)
  - Aula Virtual
- Materiales de estudio suministrados por el profesor:
  - Apuntes y ejercicios (en formato electrónico).
  - Artículos de prensa y sitios web especializados.
  - Documentación y tutoriales de la Web.
- Libros recomendados:
  - Seguridad Informática. Editorial McGraw Hill
  - Seguridad informática. Editorial Editex
- Para alumnos avanzados se recomienda tener actividades que permiten profundizar más en los conceptos estudiados. Es el profesor quien, en función de las circunstancias, determinará qué actividades se consideran mínimas y cuáles son para profundizar.

16 NORMAS QUE EL ALUMNO DEBE RESPETAR

Serán las mismas que se han indicado en la programación del departamento. (Apartado 8)

16 NORMAS QUE EL ALUMNO DEBE RESPETAR

- Se exige puntualidad a la hora de entrar al aula.
- No se permitirá entrar o salir del aula una vez se haya iniciado la clase ni tampoco entre las horas de cada bloque horario, salvo que el motivo esté justificado y con el permiso del profesor. Sólo se saldrá en los períodos designados para ello (Recreo, de 12:10 a 12:40)
- En caso de que el alumno vaya a clase con su ordenador portátil, esto solo lo conectará a la red con el permiso del profesor y cuando éste lo estime oportuno.
- Los teléfonos móviles permanecerán desconectados y guardados durante las horas de clase.
- Cada alumno ocupará en el aula siempre el mismo sitio.
- Se deberá respetar el mobiliario y material informático del aula. Cada alumno o grupo será responsable de su puesto de trabajo (pc, mesa, etc.). Será el encargado de su buen estado (no rallar ni pintar mesas o equipos).
- Se deberá respetar la configuración original de los equipos.
- Está prohibido instalar programas en los equipos. Tampoco está permitida la descarga de programas o cualquier tipo de información, si no es con el permiso expreso del profesor.
- No está permitido el uso de chat o de correo electrónico para uso privado.
- Se deberá cuidar de no causar la pérdida de datos propios, de compañeros o del profesor.

EL INCUMPLIMIENTO DE ESTAS NORMAS SE CONSIDERARÁ COMO FALTA LEVE O GRAVE (SEGÚN PROPONGA EL DEPARTAMENTO DESPUÉS DE ESTUDIAR CADA CASO, CON LAS CONSIGUIENTES MEDIDAS QUE SE ESTIMEN OPORTUNAS).