

PROGRAMACIÓN DEL MÓDULO:

NORMATIVA DE CIBERSEGURIDAD

PROFESOR/ES: <i>En caso de más de un profesor es necesario identificar al profesor coordinador y puede ser necesario calibración.</i>	Olga María Sánchez Gutiérrez
GRUPO/S Y CICLO/S:	CECETI
CURSO:	2020-2021

ÍNDICE

[INTRODUCCIÓN](#)

[OBJETIVOS](#)

[CONTENIDOS](#)

[DISTRIBUCIÓN TEMPORAL DE CONTENIDOS](#)

[CRITERIOS DE EVALUACIÓN](#)

[RELACIÓN CON OTROS MÓDULOS DEL CICLO](#)

[METODOLOGÍA DIDÁCTICA](#)

[PROCEDIMIENTOS DE EVALUACIÓN DEL APRENDIZAJE DE LOS ALUMNOS](#)

[CRITERIOS DE CALIFICACIÓN](#)

[ATENCIÓN A LA DIVERSIDAD](#)

[MATERIALES Y RECURSOS DIDÁCTICOS, HERRAMIENTAS Y EQUIPAMIENTOS](#)

[ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES](#)

[TEMAS TRANSVERSALES](#)

1. INTRODUCCIÓN

Este módulo se incluye 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 queda establecido y regulado por 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.

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.

Las competencias profesionales, personales y sociales de este curso de especialización son las que se relacionan a continuación:

- a) Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- b) Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- c) Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- d) Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- e) Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- f) Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- g) Implantar sistemas seguros de despliegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.

- h) Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- i) Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- j) Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
- k) Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.
- l) Adaptarse a las nuevas situaciones laborales, manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida.
- m) Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia, con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo.
- n) Generar entornos seguros en el desarrollo de su trabajo y el de su equipo, supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización.
- ñ) Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios.

2. OBJETIVOS

Los objetivos generales de este curso de especialización son los siguientes:

- a) Identificar los principios de la organización y normativa de protección en ciberseguridad, planificando las acciones que es preciso adoptar en el puesto de trabajo para la elaboración del plan de prevención y concienciación.
- b) Auditar el cumplimiento del plan de prevención y concienciación de la organización, definiendo las acciones correctoras que puedan derivarse para incluirlas en el plan de securización de la organización.

- c) Detectar incidentes de ciberseguridad implantando los controles, las herramientas y los mecanismos necesarios para su monitorización e identificación.
- d) Analizar y dar respuesta a incidentes de ciberseguridad, identificando y aplicando las medidas necesarias para su mitigación, eliminación, contención o recuperación.
- e) Elaborar análisis de riesgos para identificar activos, amenazas, vulnerabilidades y medidas de seguridad.
- f) Diseñar e implantar planes de medidas técnicas de seguridad a partir de los riesgos identificados para garantizar el nivel de seguridad requerido.
- g) Configurar sistemas de control de acceso, autenticación de personas y administración de credenciales para preservar la privacidad de los datos.
- h) Configurar la seguridad de sistemas informáticos para minimizar las probabilidades de exposición a ataques.
- i) Configurar dispositivos de red para cumplir con los requisitos de seguridad.
- j) Administrar la seguridad de sistemas informáticos en red aplicando las políticas de seguridad requeridas para garantizar la funcionalidad necesaria con el nivel de riesgo de red controlado.
- k) Aplicar estándares de verificación requeridos por las aplicaciones para evitar incidentes de seguridad.
- l) Automatizar planes de despliegado de software respetando los requisitos relativos a control de versiones, roles, permisos y otros para conseguir un despliegado seguro.
- m) Aplicar técnicas de investigación forense en sistemas y redes en los ámbitos del almacenamiento de la información no volátil, de los dispositivos móviles, del Cloud y de los sistemas IoT (Internet de las cosas), entre otros, para la elaboración de análisis forenses.
- n) Analizar informes forenses identificando los resultados de la investigación para extraer conclusiones y realizar informes.
- ñ) Combinar técnicas de *hacking* ético interno y externo para detectar vulnerabilidades que permitan eliminar y mitigar los riesgos asociados.
- o) Identificar el alcance de la aplicación normativa dentro de la organización, tanto internamente como en

relación con terceros para definir las funciones y responsabilidades de todas las partes.

- p) Revisar y actualizar procedimientos de acuerdo con normas y estándares actualizados para el correcto cumplimiento normativo en materia de ciberseguridad y de protección de datos personales.
- q) Desarrollar manuales de información, utilizando herramientas ofimáticas y de diseño asistido por ordenador para elaborar documentación técnica y administrativa.
- r) Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación, para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales.
- s) Desarrollar la creatividad y el espíritu de innovación para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal.
- t) Evaluar situaciones de prevención de riesgos laborales y de protección ambiental, proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo, para garantizar entornos seguros.
- u) Identificar y proponer las acciones profesionales necesarias para dar respuesta a la accesibilidad universal y al «diseño para todas las personas».
- v) Identificar y aplicar parámetros de calidad en los trabajos y actividades realizados en el proceso de aprendizaje, para valorar la cultura de la evaluación y de la calidad y ser capaces de supervisar y mejorar procedimientos de calidad.

3. CONTENIDOS

Previa a la impartición de los contenidos se realizará una unidad 0 en la que se explicará la metodología, los criterios y procedimientos de evaluación, incluyendo la eventualidad de tener que abandonar la enseñanza presencial por modelos semipresenciales o a distancia.

De forma frecuente se refrescará la metodología y se practicará con las herramientas a utilizar en caso de paso a enseñanza semipresencial o a distancia, algunas de las cuales se integrarán también en la clase presencial para facilitar una migración rápida y el seguimiento de las clases por parte del alumnado que no pueda asistir.

UNIDAD 1: Puntos principales de aplicación para un correcto cumplimiento normativo:

- Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales).
- Principios del buen gobierno y ética empresarial.
- Compliance Officer: funciones y responsabilidades.
- Relaciones con terceras partes dentro del Compliance.

UNIDAD 2: Diseño de sistemas de cumplimiento normativo:

- Sistemas de Gestión de Compliance.
- Entorno regulatorio de aplicación.
- Análisis y gestión de riesgos, mapas de riesgos.
- Documentación del sistema de cumplimiento normativo diseñado.

UNIDAD 3: Legislación para el cumplimiento de la responsabilidad penal:

- Riesgos penales que afectan a la organización.
- Sistemas de gestión de Compliance penal.
- Sistemas de gestión anticorrupción.

UNIDAD 4: Legislación y jurisprudencia en materia de protección de datos:

- Principios de protección de datos.
- Novedades del RGPD de la Unión Europea.
- Privacidad por Diseño y por Defecto.
- Análisis de Impacto en Privacidad (PIA), y medidas de seguridad.
- Delegado de Protección de Datos (DPO).

UNIDAD 5: Normativa vigente de ciberseguridad de ámbito nacional e internacional:

- Normas nacionales e internacionales.
- Sistema de Gestión de Seguridad de la Información (estándares internacionales) (ISO 27.001).
- Acceso electrónico de los ciudadanos a los Servicios Públicos.

UNIDAD 6: Esquema Nacional de Seguridad (ENS).

- Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301).
- Directiva NIS.
- Legislación sobre la protección de infraestructuras críticas.

UNIDAD 7: Ley PIC (Protección de infraestructuras críticas).

4. DISTRIBUCIÓN TEMPORAL DE CONTENIDOS

El orden de impartición de los contenidos y la duración planificada para cada uno de los bloques puede variar en función de las necesidades del grupo y de la eventualidad del paso a enseñanza semipresencial o a distancia. Dentro de cada bloque se impartirán contenidos de forma paralela, trabajando varios conceptos a la vez.

A pesar de que el número de horas asignadas al módulo es de **30**, ocurre que por cuestiones de calendario escolar y aspectos como el impacto de los días festivos respecto al horario generado para el módulo, el número total de horas exceda las **50**. La distribución temporal de los contenidos contemplará este hecho, dedicando ese excedente de horas a tareas de repaso, refuerzo y profundización de algunos de los contenidos vistos en el curso

El orden de impartición de los contenidos puede variar en función de las necesidades del grupo, así como la duración planificada para cada uno de los bloques.

EVALUACIÓN	TEMA, BLOQUE O UNIDAD DIDÁCTICA	FECHA INICIO ---- FECHA FIN <i>Diferenciar por grupo si son diferentes</i>	Nº HORAS LECTIVAS
1ª	UT0. Enseñanza de la metodología y de la plataforma en línea	16/11/2020 20/11/2020	2H
	UT1. Puntos principales de aplicación para un correcto cumplimiento normativo	21/11/2020 14/01/2021	8H
	UT2. Diseño de sistemas de cumplimiento normativo	15/01/2021 5/02/2021	7H
	UT3. Legislación para el cumplimiento de la responsabilidad penal	6/02/2021 8/03/2021	8H
% AVANCE EN CONTENIDOS			50%
2ª	UT4. Legislación y jurisprudencia en materia de protección de datos	9/03/2021 17/04/2021	9H
	UT5. Normativa vigente de ciberseguridad de ámbito nacional e internacional:	18/04/2021 07/05/2021	6H

	UT6. Esquema Nacional de Seguridad (ENS).	08/05/2021 02/06/2021	6H
	UT7. Ley PIC (Protección de infraestructuras críticas)	03/06/2021 18/06/2021	4H
% AVANCE EN CONTENIDOS			100%

5. CRITERIOS DE EVALUACIÓN

El profesorado evaluará los aprendizajes del alumnado, los procesos de enseñanza y su propia práctica docente. La evaluación en el curso de especialización se realizará teniendo en cuenta los resultados de aprendizaje y los criterios de evaluación establecidos en los módulos profesionales, así como los objetivos generales del curso de especialización.

Resultados de Aprendizaje y Criterios de Evaluación según recoge el Decreto 257/2011 de 7 de octubre:

1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.

Criterios de evaluación:

- Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.
- Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.
- Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones.
- Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.
- Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.

2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.

Criterios de evaluación:

- Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.
- Se han establecido las recomendaciones válidas para diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).
- Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).

d) Se ha documentado el sistema de cumplimiento normativo diseñado.

3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.

Criterios de evaluación:

- a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.
- b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.
- c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).
- d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).

4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación:

- a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.
- b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.
- c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.
- d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.
- e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos.
- f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.
- g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

5. Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación:

- a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.
- b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.
- c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.
- d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.

e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento normativo de las nuevas normativas. incluidas en el plan de revisiones.

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, ya para poder aplicar la mayoría de los contenidos del Curso de Especialización en Ciberseguridad en entornos de las tecnologías de la información es necesario tener en cuenta y adaptarse a las Normativas de Ciberseguridad.

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 el apartado tres 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.

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.

9. CRITERIOS DE CALIFICACIÓN

Se calificará a los alumnos/as en sesiones de evaluación una vez al final de cada trimestre.

La calificación de cada alumno/a se elaborará en base a:

- Serán evaluados los contenidos de la o las unidades, calificando de 0 a 10 puntos, de acuerdo a los siguientes elementos:
 - Pruebas teórico/práctica.
 - Prácticas o trabajos.
- La calificación obtenida en las pruebas teórico/prácticas realizadas en la evaluación estará comprendida entre los valores 0 y 10.
- La calificación obtenida en las prácticas y/o trabajos realizados en la evaluación estará comprendida entre los valores 0 y 10 o con la calificación APTO y NO APTO.

- Algunos criterios que se tienen en cuenta en la valoración de las prácticas y/o trabajos son:
 - Cumplir los plazos de entrega.
 - Formato y limpieza del documento.
 - La autoría del contenido por parte del alumno.
 - Que incluya las referencias bibliográficas (libros, páginas Web, documentos electrónicos, ...)
 - Entrega ordenada de todos los ficheros implicados en la práctica o proyecto.
- La práctica/trabajo se debe ajustar a los requisitos solicitados por el profesor, incluyendo todos los puntos solicitados y se ponga de manifiesto que el alumno ha asimilado los conceptos desarrollados en el trabajo.
- El porcentaje de cada parte irá en función del desarrollo de la evaluación y de las características de la materia a evaluar (hay evaluaciones con mayor contenido teórico y otras con mayor contenido práctico). Los porcentajes a aplicar serán:
 - Pruebas (teórico-prácticas): 70%.
 - Prácticas/Trabajos/Ejercicios: 30%.
- Al finalizar cada tema, y a criterio del profesor, se puede llevar a cabo una prueba parcial de los contenidos impartidos a lo largo de ese tema. Estas pruebas parciales se guardarían para el cálculo final de la nota de la evaluación y cada una de ellas tendría un peso del 20% sobre la parte de Prácticas/Trabajos/Ejercicios.
- En caso de detectar plagios en tareas y pruebas (sea de compañeros o de otras fuentes) la calificación de la tarea o prueba será de 0.
- Para poder aplicar los porcentajes descritos anteriormente es necesario obtener un mínimo de un 4 en cada uno de los apartados y que al calcular la calificación final resulte superior a un 5.
- La calificación final del módulo se calculará teniendo en cuenta las calificaciones de cada una de las evaluaciones, siendo requisito necesario y obligatorio el haber superado las dos evaluaciones para superar el curso. Se calculará aplicando la media aritmética de las calificaciones de las dos evaluaciones.

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 LEEEx 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 (LibreOffice 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

Se fomentará entre el alumnado la labor de investigación personal sobre los diferentes temas tratados a lo largo del curso y la realización de actividades complementarias que permitan conocer casos reales de implantación de los diversos aspectos abordados en el módulo.

A lo largo del curso se podrían organizar charlas de expertos, empresarios, trabajadores del sector y ex-alumnos para que aprendan cómo se desarrollará su profesión, la importancia de este módulo en el desempeño correcto de las labores encomendadas en su futuro puesto de trabajo y las últimas tendencias del sector.

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.