



**Junta de Castilla
y León**

Delegación Territorial de Segovia
I.E.S. María Moliner



Módulo: Fundamentos de ciberseguridad

CICLO: Administración de Sistemas Informáticos y en Red
CURSO: 2025 / 2026
GRUPO: S2L
PROFESOR: Fernando Lozoya de Diego



ÍNDICE

ÍNDICE DE TABLA	3
1. INTRODUCCIÓN.....	4
1.1.CONTEXTO	5
2. COMPETENCIAS, OBJETIVOS Y CRITERIOS DE EVALUACIÓN.....	6
2.1.COMPETENCIA GENERAL	6
2.2.COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES	6
2.3.COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES ESPECÍFICAS	8
2.4.OBJETIVOS GENERALES	8
2.5.OBJETIVOS ESPECÍFICOS	9
2.6.RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN	10
3. CONTENIDOS	16
3.1.CONTENIDOS	16
3.2.UNIDADES DE TRABAJO	19
4. TEMPORALIZACIÓN	24
5. METODOLOGÍA	26
6. CRITERIOS DE CALIFICACIÓN	26
6.1.EVALUACIÓN Y CALIFICACIÓN	26
6.1.1.Procedimiento de evaluación.....	27
6.1.2.Criterios de calificación	28
6.1.3.Evaluación ordinaria	31
6.1.4.Evaluación extraordinaria.....	39
6.1.5.Instrumentos de evaluación	39
7. RECUPERACIÓN	40
8. ATENCIÓN A LA DIVERSIDAD	40
9. RECLAMACIONES.....	42
10. RECURSOS MATERIALES	45
11. BIBLIOGRAFÍA	46



ÍNDICE DE TABLA

Tabla 1: Temporalización.....	25
Tabla 2: Criterios de calificación: RA y peso nota	29
Tabla 3: Criterios de calificación: Unidades de trabajo y peso nota.....	30
Tabla 4: Criterios de calificación: Unidades de trabajo y RA	32
Tabla 5: Criterios de calificación: Unidades de trabajo y RA/actividades	34

1. INTRODUCCIÓN

Este módulo se encuadra dentro del segundo curso del Ciclo Formativo de Grado Superior, correspondiente al Título de Técnico Superior en Administración de Sistemas Informáticos en Red. Tiene una asignación de 54 horas lectivas divididas en 3 horas semanales.

La normativa curricular que regula este ciclo es:

- 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. (España, 2009)
- Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional. (España, 2023b)
- Real Decreto 500/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen títulos de Formación Profesional de grado superior y se fijan sus enseñanzas mínimas. (España, 2024)
- Real Decreto 658/2024, de 9 de julio, por el que se modifican el Real Decreto 132/2010, de 12 de febrero, por el que se establecen los requisitos mínimos de los centros que impartan las enseñanzas del segundo ciclo de la educación infantil, la educación primaria y la educación secundaria, y el Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional. (España, 2023a)
- DECRETO 24/2024, de 21 de noviembre, por el que se establece el currículo de los ciclos formativos de grado superior, correspondiente a la oferta de grado D y nivel 3 del Sistema de Formación Profesional, conducentes a la obtención del título de Técnico Superior, en la Comunidad de Castilla y León. (Consejería de Educación de Castilla y León, 2024b)
- ORDEN EDU/1287/2024, de 26 de noviembre, por la que se concretan los aspectos específicos del currículo del Ciclo Formativo de Grado Superior en Administración de Sistemas Informáticos en Red en la Comunidad de Castilla y León. (Consejería de Educación de Castilla y León, 2024c)

- ORDEN EDU/411/2025, de 15 de abril, por la que se concreta la optatividad en las enseñanzas de grado D, niveles 2 y 3 del Sistema de Formación Profesional y se establece el procedimiento de oferta y autorización de complementos de formación de los grados D y E, niveles 2 y 3 del Sistema de Formación Profesional, en la Comunidad de Castilla y León. (Consejería de Educación de Castilla y León, 2025a)

El desarrollo curricular del módulo se ajusta a las directrices que marca la "Documentación de apoyo al desarrollo curricular de los ciclos formativos". En base a ello, se considera la programación como un diseño abierto y adecuado a las características propias de cada entorno, por lo que se pretende acomodar la programación propuesta al desarrollo del curso.

El módulo no tiene asociada ninguna competencia de las que se encuentran recogidas en el 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, ni se fijan sus enseñanzas mínimas, las cuales son recogidas en el “*Artículo 6. Relación de cualificaciones y unidades de competencia del Catálogo Nacional de Cualificaciones Profesionales incluidas en el título*” (España, 2009), correspondiente al título, debido a que se ha implementado posterior al título del Ciclo Formativo siendo un módulo optativo y de nueva implementación en el curso vigente de esta programación. Para ser concretos se ha implementado en la ORDEN EDU/411/2025, de 15 de abril, la cual se ha indicado en líneas anteriores.

1.1. CONTEXTO

El Ciclo se imparte en la ciudad de Segovia, siendo el único centro de la provincia que ofrece esta enseñanza presencial. Por tanto, el alumnado proviene de cualquier punto de la ciudad, así como de poblaciones cercanas.

El grupo concreto está compuesto por 15 personas. No se aprecian problemas de socialización en el aula. Durante la evaluación inicial se hace patente una gran diversidad en el nivel de comprensión de los contenidos.

2. COMPETENCIAS, OBJETIVOS Y CRITERIOS DE EVALUACIÓN

2.1. COMPETENCIA GENERAL

La competencia general de este título es el cual se encuentra recogido en el 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 en el “Artículo 4. Competencia general” (España, 2009) y que la que se indica a continuación:

“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”.

2.2. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES

Las competencias profesionales, personales y sociales de este título es el cual se encuentra recogido en el 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, en el “Artículo 5. Competencias profesionales, personales y sociales” (España, 2009) y son las que se relacionan a continuación:

- a) *“Administrar sistemas operativos de servidor, instalando y configurando el software, en condiciones de calidad para asegurar el funcionamiento del sistema.*
- b) *Administrar servicios de red (web, mensajería electrónica y transferencia de archivos, entre otros) instalando y configurando el software, en condiciones de calidad.*
- c) *Administrar aplicaciones instalando y configurando el software, en condiciones de calidad para responder a las necesidades de la organización.*
- d) *Implantar y gestionar bases de datos instalando y administrando el software de gestión en condiciones de calidad, según las características de la explotación.*
- e) *Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.*

- f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.*
- g) Determinar la infraestructura de redes telemáticas elaborando esquemas y seleccionando equipos y elementos.*
- h) Integrar equipos de comunicaciones en infraestructuras de redes telemáticas, determinando la configuración para asegurar su conectividad.*
- i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.*
- j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.*
- k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.*
- l) Administrar usuarios de acuerdo a las especificaciones de explotación para garantizar los accesos y la disponibilidad de los recursos del sistema.*
- m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.*
- n) 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.*
- o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.*
- p) 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.*
- q) Liderar situaciones colectivas que se puedan producir, mediando en conflictos personales y laborales, contribuyendo al establecimiento de un ambiente de trabajo agradable y actuando en todo momento de forma sincera, respetuosa y tolerante.*
- r) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.*
- s) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.*
- t) Participar de forma activa en la vida económica, social y cultural con actitud crítica y responsable.*
- u) Crear y gestionar una pequeña empresa, realizando un estudio de viabilidad de productos, de planificación de la producción y de comercialización. ”*

2.3. COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES ESPECÍFICAS

Las competencias profesionales, personales y sociales específicas de este módulo, no se encuentran recogidas en el Real Decreto indicado en líneas anteriores, porque es un módulo optativo de nueva implementación en el Ciclo Formativo y aplicable en el curso procedente a esta programación.

2.4. OBJETIVOS GENERALES

Los objetivos generales de este título es el cual se encuentra recogido en el 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, en el “Artículo 9. Objetivos generales” (España, 2009) y son las que se relacionan a continuación:

- a) *“Analizar la estructura del software de base, comparando las características y prestaciones de sistemas libres y propietarios, para administrar sistemas operativos de servidor.*
- b) *Instalar y configurar el software de base, siguiendo documentación técnica especificaciones dadas, para administrar sistemas operativos de servidor.*
- c) *Instalar y configurar software de mensajería y transferencia de ficheros, entre otros, relacionándolos con su aplicación y siguiendo documentación y especificaciones dadas, para administrar servicios de red.*
- d) *Instalar y configurar software de gestión, siguiendo especificaciones y analizando entornos de aplicación, para administrar aplicaciones.*
- e) *Instalar y administrar software de gestión, relacionándolo con su explotación, para implantar y gestionar bases de datos.*
- f) *Configurar dispositivos hardware, analizando sus características funcionales, para optimizar el rendimiento del sistema.*
- g) *Configurar hardware de red, analizando sus características funcionales y relacionándolo con su campo de aplicación, para integrar equipos de comunicaciones.*
- h) *Analizar tecnologías de interconexión, describiendo sus características y posibilidades de aplicación, para configurar la estructura de la red telemática y evaluar su rendimiento.*
- i) *Elaborar esquemas de redes telemáticas utilizando software específico para configurar la estructura de la red telemática.*

- j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.*
- k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.*
- l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.*
- m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.*
- n) Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios*
- o) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.*
- p) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.*
- q) 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.*
- r) Identificar formas de intervención en situaciones colectivas, analizando el proceso de toma de decisiones y efectuando consultas para liderar las mismas.*
- s) Identificar y valorar las oportunidades de aprendizaje y su relación con el mundo laboral, analizando las ofertas y demandas del mercado para gestionar su carrera profesional.*
- t) Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.*
- u) Reconocer sus derechos y deberes como agente activo en la sociedad, analizando el marco legal que regula las condiciones sociales y laborales para participar como ciudadano democrático.”*

2.5. OBJETIVOS ESPECÍFICOS

Los objetivos específicos de este módulo, no se encuentran recogidas en el Real Decreto indicado en líneas anteriores, porque es un módulo optativo de nueva implementación en el Ciclo Formativo y aplicable en el curso precedente a esta programación. Pero cabe indicar que en la Orden precedente a la implementación de este módulo se indica lo siguiente:

- *“Capacitar al alumnado para identificar y aplicar medidas de protección básicas frente a las principales amenazas de seguridad en sistemas, redes y aplicaciones informáticas.”*
(Consejería de Educación de Castilla y León, 2025a)

2.6. RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

Los Resultados de Aprendizaje (en adelante RA) y los Criterios de Evaluación (en adelante CE) de este módulo, son los que se encuentran recogidos en el 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, en el “*Anexo I*” (España, 2009) y son las que se relacionan a continuación:

1. *“Identifica las principales amenazas y vulnerabilidades en sistemas, redes y aplicaciones informáticas, relacionándolas con sus posibles consecuencias.”*

Criterios de evaluación:

- a) *Se han descrito las características y funciones de las principales amenazas informáticas, como malware, phishing, ransomware y ataques de denegación de servicio, entre otros.*
- b) *Se han clasificado las vulnerabilidades más comunes en sistemas operativos, redes y aplicaciones, justificando su impacto potencial en la seguridad.*
- c) *Se han relacionado las amenazas identificadas con las vulnerabilidades que explotan, explicando los mecanismos utilizados por los atacantes.*
- d) *Se han evaluado las consecuencias de las amenazas de seguridad sobre la confidencialidad, integridad y disponibilidad de los datos y servicios en casos específicos.*
- e) *Se han distinguido entre las diferentes categorías de ataques (internos, externos, dirigidos, masivos) según el contexto y los objetivos del atacante.*
- f) *Se han identificado las señales y síntomas que podrían indicar la presencia de amenazas o vulnerabilidades activas en un sistema o red.*

2. *Implementa medidas de protección básicas, como configuraciones seguras, control de accesos y políticas de gestión de contraseñas en sistemas operativos y redes.*

Criterios de evaluación:

- a) *Se han configurado sistemas operativos y redes aplicando configuraciones seguras, incluyendo la desactivación de servicios innecesarios y la actualización de software a versiones seguras.*
- b) *Se han aplicado políticas de gestión de contraseñas robustas, asegurando el uso de requisitos mínimos de longitud, complejidad y periodicidad de cambio.*
- c) *Se han establecido controles de acceso adecuados mediante la creación de roles y permisos, garantizando que los usuarios solo accedan a los recursos necesarios.*
- d) *Se han implementado reglas básicas de firewall para restringir el tráfico no deseado y proteger los sistemas frente a accesos no autorizados.*
- e) *Se han utilizado herramientas de monitoreo y auditoría para verificar el cumplimiento de las medidas de protección implementadas.*
- f) *Se han detectado configuraciones inseguras o inconsistentes, proponiendo y ejecutando las correcciones necesarias.*
- g) *Se han documentado los procedimientos seguidos para la implementación de las medidas de protección, incluyendo las configuraciones aplicadas y las herramientas utilizadas.*

3. *Analiza casos prácticos de incidentes de seguridad informática, proponiendo soluciones adecuadas para su prevención y mitigación.*

Criterios de evaluación:

- a) *Se han descrito los elementos clave de un incidente de seguridad, identificando las amenazas, las vulnerabilidades explotadas y las consecuencias del ataque.*
- b) *Se han clasificado los incidentes de seguridad analizados según su naturaleza, como ataques internos, externos, dirigidos o masivos, justificando la clasificación.*
- c) *Se han identificado los indicadores de compromiso (IoC) presentes en los casos prácticos, relacionándolos con los métodos y técnicas utilizadas por los atacantes.*

- d) *Se han propuesto soluciones viables para prevenir futuros incidentes, justificando las medidas de protección recomendadas.*
 - e) *Se ha evaluado el impacto de las soluciones propuestas en términos de mitigación de riesgos, costes y viabilidad.*
 - f) *Se han elaborado informes detallados sobre los incidentes analizados, destacando las causas, el impacto y las medidas correctivas.*
 - g) *Se han aplicado metodologías de análisis forense básicas para recopilar y documentar evidencias en los casos prácticos, respetando los principios éticos y legales.*
4. *Configura herramientas y tecnologías específicas de ciberseguridad, como cortafuegos, sistemas de detección de intrusos y software antivirus, asegurando su adecuado funcionamiento.*

Criterios de evaluación:

- a) *Se han instalado y configurado cortafuegos, definiendo reglas de tráfico que limiten accesos no autorizados y protejan los sistemas frente a amenazas externas.*
- b) *Se han configurado sistemas de detección de intrusos (IDS) y/o sistemas de prevención de intrusos (IPS), ajustando parámetros para identificar y mitigar posibles ataques.*
- c) *Se han implantado software antivirus y antimalware, asegurando su actualización y definiendo políticas de escaneo adecuadas a las necesidades del sistema.*
- d) *Se han optimizado las configuraciones de las herramientas de ciberseguridad, comprobando su integración y compatibilidad con los sistemas existentes.*
- e) *Se han realizado pruebas funcionales para verificar el correcto funcionamiento de las herramientas configuradas, simulando escenarios de ataque y evaluando su efectividad.*
- f) *Se ha documentado el proceso de configuración de cada herramienta, incluyendo los parámetros establecidos, los cambios realizados y las recomendaciones de uso para su mantenimiento.*

5. *Aplica normativas y buenas prácticas en la gestión de la seguridad de la información, respetando los principios de confidencialidad, integridad y disponibilidad.*

Criterios de evaluación:

- a) *Se han identificado e interpretado las normativas y estándares internacionales más relevantes en ciberseguridad, como el RGPD (Reglamento General de Protección de Datos de la UE), ISO/IEC 27001 y ENS (Esquema Nacional de Seguridad), explicando su aplicación en distintos contextos.*
- b) *Se han analizado escenarios prácticos para evaluar si las medidas de seguridad implementadas cumplen con los principios de confidencialidad, integridad y disponibilidad de la información.*
- c) *Se han aplicado buenas prácticas de gestión de la seguridad de la información, como la clasificación de datos sensibles y la definición de políticas de acceso.*
- d) *Se ha evaluado la efectividad de las políticas y procedimientos implementados, proponiendo mejoras basadas en los principios de gestión de riesgos.*
- e) *Se ha elaborado documentación que describa los procedimientos utilizados para garantizar el cumplimiento normativo y las buenas prácticas, detallando los roles y responsabilidades asociados.*

Los resultados de aprendizaje que se realizaran en el periodo de formación en empresa u organismo equiparado, son los puntos de los resultados de aprendizaje números 2 y 5, en concreto el “2. *Implementa medidas de protección básicas, como configuraciones seguras, control de accesos y políticas de gestión de contraseñas en sistemas operativos y redes*” y “5. *Aplica normativas y buenas prácticas en la gestión de la seguridad de la información, respetando los principios de confidencialidad, integridad y disponibilidad*”. Dichos resultado de aprendizaje será evaluado en el centro educativo y en el centro de formación en empresa u organismo equiparado con un porcentaje de 90% en el centro educativo y 10% en el centro de formación en empresa u organismo equiparado.

Los porcentajes indicados referentes en el centro de formación en empresa u organismo equiparado, serán aplicados siempre que se cumpla lo que se recoge en la normativa vigente en el proceso de desarrollo de este documento, la cual el alumno que cumpla los requisitos recogidos en la siguiente normativa sean superados o bien cumplidos:

“Artículo 57. Organización de la formación.

3. La organización de la formación en empresa u organismo equiparado responderá, en todo caso, a las siguientes reglas:

- d) La formación en la empresa u organismo equiparado requerirá tener cumplidos los 16 años y haber superado la formación en prevención de riesgos laborales, que será impartida por los centros de formación profesional.*
- e) La formación en empresa se realizará en el momento adecuado en función de las características de la oferta de formación, la estacionalidad y la disponibilidad de plazas formativas en las empresas u organismo equiparado.” (España, 2022)*

“Artículo 9. Currículo y fase de formación en empresa u organismo equiparado.

6. La organización de la formación en empresa u organismo equiparado responderá a las siguientes reglas:

- d) Para iniciar la formación en la empresa u organismo equiparado el alumnado requerirá tener cumplidos los 16 años.*
- e) Las personas en formación que inicien su formación en empresa u organismo equiparado deben haber adquirido las competencias relativas a los riesgos específicos y las medidas de prevención de riesgos laborales en las actividades profesionales correspondientes al perfil profesional, según se requiera en la normativa vigente en materia de prevención de riesgos laborales.*

“Artículo 158. Requisitos para el periodo de formación en empresa u organismo equiparado.

El inicio de la estancia en la empresa u organismo equiparado requerirá:

- a) Tener cumplidos los dieciséis años.*
- b) Haber superado la formación en prevención de riesgos laborales, que será impartida por los centros del Sistema de Formación Profesional.” (España, 2023b)*

“Artículo 8. Evaluación inicial, sesiones parciales y evaluación previa a la fase de empresa u organismo equiparado.

- 3. Previamente a la incorporación de cada alumno o alumna a la fase de formación en empresa u organismo equiparado, se realizará una sesión de evaluación específica, que podrá ser coincidente con alguna de las parciales, en la que el equipo docente determinará la adquisición por parte del alumno o alumna, de las competencias relativas a los riesgos específicos y las medidas de prevención de riesgos laborales en las actividades profesionales correspondientes al perfil profesional, según se requiera en la normativa vigente en materia de prevención de riesgos laborales.*

Si en la sesión se acuerda que el alumno o alumna no tiene adquiridas dichas competencias, se adoptarán medidas de apoyo orientadas a su superación.

Esta sesión podrá realizarse en más de una ocasión para cada alumno o alumna, con el fin de que pueda realizar la fase de formación en empresa u organismo equiparado antes de la finalización del curso escolar.” (Consejería de Educación de Castilla y León, 2024d)

“Artículo 6. Requisitos para el inicio de la fase de formación en empresa u organismo equiparado.

- 1. De conformidad con el artículo 57.3.d) de la Ley 3/2022, de 31 de marzo, y con los artículos 9.6.d) y e), y 158, del Real Decreto 659/2023, de 18 de julio, para iniciar la fase de formación en la empresa u organismo equiparado, el alumnado deberá tener cumplidos dieciséis años, haber adquirido las competencias relativas a los riesgos específicos y las medidas de prevención de riesgos laborales en las actividades profesionales correspondientes al perfil profesional, según se requiera en la normativa vigente en materia de prevención de riesgos laborales, y haber superado la formación en prevención de riesgos laborales, que será impartida por los centros del Sistema de Formación Profesional.*

Los centros educativos verificarán el cumplimiento de los requisitos exigidos con carácter previo a la incorporación del alumnado a la empresa u organismo equiparado.” (Consejería de Educación de Castilla y León, 2025b)

Si por el contrario, el alumno no cumple lo que se recoge en la normativa vigente la cual se ha indicado en líneas anteriores, serán evaluados en el centro educativo de formación profesional. Además, cabe indicar que cuando se ha desarrollado este documento no se han cumplido los requisitos exigidos para la formación en empresa, puesto que dicho documento se ha redactado a lo largo del primer mes del

curso vigente, siendo imposible la aplicación de los porcentajes indicados en formación en empresa u organismo equiparado, por lo tanto, es asumido por el centro los RA indicados hasta que se haya comprobado que el alumno adquiriera las competencias relativas a materia de prevención de riesgos laborales, y haber superado la formación en prevención de riesgos laborales.

3. CONTENIDOS

3.1. CONTENIDOS

Los contenidos de este módulo, son los que se encuentran recogidos en el 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, en el “*Anexo I*” (España, 2009) y son las que se relacionan a continuación:

1. Amenazas y vulnerabilidades informáticas:

- a. Introducción a las amenazas y vulnerabilidades informáticas: conceptos básicos, diferencias entre amenazas activas y pasivas y su impacto, principios de confidencialidad, integridad y disponibilidad.
- b. Clasificación y características de las principales amenazas informáticas: Tipos de malware. Técnicas de ingeniería social. Ataques a la red: (DoS y DDoS) y (Man-in-the-Middle). Exploits y ataques a aplicaciones web: Inyección SQL y Cross-Site Scripting (XSS).
- c. Clasificación de vulnerabilidades en sistemas, redes y aplicaciones. Vulnerabilidades en sistemas operativos, aplicaciones y redes. Redes inalámbricas sin cifrar o con cifrados obsoletos.
- d. Relación entre amenazas y vulnerabilidades. Mecánica de explotación: identificación de vulnerabilidades por los atacantes. Uso de Exploits y herramientas automatizadas. Ejemplos prácticos de explotación: ransomware en sistemas desactualizados e inyección SQL.
- e. Evaluación de las consecuencias de las amenazas y vulnerabilidades. Impacto sobre la confidencialidad, la integridad y la disponibilidad.
- f. Señales y síntomas de amenazas y vulnerabilidades activas. Detección de actividad sospechosa en sistemas. Señales de actividad maliciosa en redes.

2. Medidas de protección básicas:

- a. Importancia de las configuraciones seguras en la ciberseguridad. Conceptos básicos: servicios innecesarios, actualizaciones y vulnerabilidades conocidas. Procedimientos para desactivar servicios innecesarios en sistemas operativos. Herramientas para gestionar actualizaciones y parches de seguridad.
- b. Gestión de contraseñas robustas. Características de una contraseña segura. Políticas de gestión de contraseñas. Métodos de autenticación alternativos: autenticación Multifactor (MFA).
- c. Control de accesos y permisos. Principios de control de acceso. Gestión de roles y permisos en sistemas operativos. Configuración de accesos en redes.
- d. Implementación de reglas de firewall. Reglas básicas para controlar el tráfico: filtrado de puertos y protocolos y bloqueo de tráfico no autorizado. Configuración de cortafuegos en sistemas operativos y routers. Verificación y pruebas de las reglas implementadas.
- e. Herramientas de monitoreo y auditoría. Importancia del monitoreo en la ciberseguridad. Métodos para analizar registros y detectar incidentes o anomalías. Automatización del monitoreo mediante herramientas específicas.
- f. Corrección de configuraciones inseguras. Identificación de configuraciones inseguras o inconsistentes. Proceso de propuesta y ejecución de mejoras. Pruebas posteriores a la corrección para validar los cambios.
- g. Documentación de medidas de protección implementadas. Importancia de la documentación en la seguridad informática. Estructura recomendada para documentar configuraciones y procedimientos. Uso de plantillas para la documentación eficiente.

3. Análisis de los incidentes de seguridad:

- a. Concepto y clasificación de los incidentes de seguridad. Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje. Elementos clave de un incidente: amenazas, vulnerabilidades y consecuencias.
- b. Clasificación de incidentes de seguridad. Tipos de incidentes: internos, externos, dirigidos y masivos. Criterios para clasificar los incidentes: naturaleza, alcance y objetivo.
- c. Indicadores de compromiso (IoC). Definición y tipos de IoC: basados en red, basados en sistema y basados en registros. Métodos para identificar IoC en sistemas y redes. Relación entre IoC y las técnicas de ataque utilizadas.

- d. Estrategias proactivas para prevenir incidentes de seguridad: configuración de firewalls y herramientas de detección de intrusos e implementación de controles de acceso y gestión de contraseñas. Justificación de las medidas propuestas.
- e. Evaluación del impacto de soluciones propuestas. Análisis de mitigación de riesgos. Consideraciones de coste-beneficio en las soluciones. Viabilidad técnica y operativa de las medidas implementadas.
- f. Elaboración de informes sobre incidentes. Herramientas y formatos para la redacción de informes. Buenas prácticas en la comunicación de hallazgos técnicos.
- g. Conceptos básicos del análisis forense: recopilación de evidencias digitales y preservación de la cadena de custodia. Técnicas fundamentales de análisis forense en sistemas y redes. Principios éticos y legales en la gestión de evidencias: cumplimiento normativo y privacidad y confidencialidad.

4. Herramientas y tecnologías de aplicación:

- a. Introducción a las herramientas de ciberseguridad. Concepto y tipos. Funciones principales de cortafuegos, IDS/IPS, y software antivirus. Importancia de la configuración adecuada para la protección de sistemas.
- b. Cortafuegos (firewalls). Tipos de cortafuegos: basados en red y cortafuegos basados en host. Instalación de cortafuegos: configuración básica y configuración avanzada. Pruebas funcionales.
- c. Sistemas de detección y prevención de intrusos (IDS/IPS). Diferencias entre IDS y IPS. Instalación de IDS/IPS. Configuración de parámetros básicos. Ajustes avanzados. Verificación del funcionamiento.
- d. Software antivirus y antimalware. Funciones y tipos de software antivirus. Instalación de software antivirus. Configuración inicial. Actualización de bases de datos y software. Validación del software antivirus: pruebas de detección y generación de informes.
- e. Optimización de configuraciones y compatibilidad. Integración de herramientas de ciberseguridad con sistemas operativos y redes. Ajuste de configuraciones para maximizar el rendimiento. Resolución de conflictos entre herramientas y sistemas existentes.
- f. Pruebas de efectividad de las herramientas configuradas. Métodos para simular escenarios de ataque. Evaluación de la respuesta de las herramientas ante amenazas simuladas. Identificación y resolución de configuraciones ineficientes o erróneas.

- g. Documentación del proceso de configuración. Elementos básicos de la documentación técnica. Uso de plantillas para registrar procedimientos de instalación y configuración. Recomendaciones de mantenimiento y actualización.

5. Normativa y buenas prácticas de uso:

- a. Concepto y objetivos de la seguridad de la información. Principios fundamentales: confidencialidad, integridad y disponibilidad. Importancia del cumplimiento normativo y las buenas prácticas en entornos profesionales.
- b. Normativas y estándares internacionales en ciberseguridad. Reglamento General de Protección de Datos (RGPD). ISO/IEC 27001. Esquema Nacional de Seguridad (ENS).
- c. Buenas prácticas en la gestión de la seguridad de la información. Clasificación de datos sensibles. Definición de políticas de acceso. Gestión del ciclo de vida de la información.
- d. Evaluación de medidas de seguridad en escenarios prácticos. Análisis de casos. Uso de herramientas de auditoría. Diagnóstico de fallos. Propuestas de mejora.
- e. Gestión de riesgos y mejora continua. Identificación de riesgos. Evaluación de riesgos. Desarrollo de planes de acción. Importancia de la revisión y actualización de las políticas de seguridad.
- f. Documentación de la gestión de la seguridad de la información. Elaboración de procedimientos y políticas. Registro de incidencias y cumplimiento normativo. Uso de plantillas y formatos estándares para la documentación. Comunicación efectiva de las políticas y procedimientos a los usuarios.

3.2. UNIDADES DE TRABAJO

Las unidades de trabajo (en adelante UT) están diseñadas para cubrir los puntos incluidos en los contenidos de este módulo. El desglose de esta asignatura es flexible, pudiéndose establecer variaciones de acuerdo con el interés y dificultades encontradas por los alumnos en las diferentes unidades. También hay que tener en cuenta que los días que son no lectivos por cuestiones de calendario escolar de la comunidad donde se encuentra la impartición del módulo que se indica en esta programación. Por ello, hay que contemplar esta situación ya que repercutirá en la temporalización de las clases.

Una primera división de los contenidos en unidades de trabajo sería la siguiente:

1. Introducción. Un nuevo horizonte de amenazas.
2. Ciberseguridad y cómo construir tu estrategia:
 - a. Vivimos en la nueva era digital.
 - b. Tecnología exponencial e hiperconectada.
 - c. Crecimiento exponencial tecnológico.
 - d. Tecnologías exponenciales.
 - e. Ley de Moore y ley de los rendimientos acelerados.
 - f. Internet of Things, Big Data, Inteligencia artificial, Tecnologías emergentes.
 - g. Ciberdelincuencia, un problema de trillones de euros.
 - h. ¿Qué es un hacker?, Filosofía hacker y argot, White hat, sneaker o hacker ético.
 - i. Conceptos básicos de ciberseguridad.
 - j. Conceptos básicos de seguridad: CIA.
 - k. Triángulo seguridad, funcionalidad y facilidad de uso.
 - l. Zero Trust (cero confianza).
 - m. ¿Qué es una estrategia de ciberseguridad?.
3. Entiende tu entorno de amenazas:
 - a. Prepararse para la adversidad.
 - b. Panorama actual de las ciberamenazas.
 - c. Principales amenazas por sector.
 - d. Threat Actors, Estado-nación, Ciberdelincuentes, Hacktivistas.
 - e. Grupos terroristas, Lobos solitarios, Amenazas de ciberseguridad, Malware y ransomware, Phishing e ingeniería social, Amenazas a los datos y filtraciones, Distributed Denial of Service o denegación de servicio distribuido.
 - f. Uso de credenciales robadas.
4. Dónde te encuentras. evalúate a ti mismo:
 - a. Por qué es importante evaluarse.
 - b. ¿Cómo nos vamos a evaluar? A través de un Cybersecurity Framework (CSF).
 - c. Tipos de Cybersecurity Frameworks.

- d. Dominios.
- e. Controles y defensas.
- f. Niveles de ciberseguridad.
- g. Define tu plan de ciberseguridad: AS-IS y TO-BE.

5. Organización y riesgos:

- a. Introducción.
- b. Defensas-Básicas.
- c. Estrategia de negocio y organización.
- d. Prioridades en la organización, organización de ciberseguridad y normativa de ciberseguridad.
- e. Seguridad en proveedores.
- f. Identifica a tus proveedores tecnológicos.
- g. Evaluación continua de la ciberseguridad de tus proveedores.
- h. Cultura cibersegura, para empleados y stakeholders.

6. Protección:

- a. Introducción.
- a. Protección de la red.
- b. Firewalls y firewalls de última generación.
- c. Sistemas de detección/prevenición de intrusos o IDS/IPS, VPN.
- d. Network Traffic Analyzer (NTA).
- e. Arquitecturas de seguridad.
- f. Protege tus redes wifi, segmentación de la red corporativa, configuraciones seguras en redes inalámbricas, redes de invitados y políticas de uso.
- g. Protección de sistemas y dispositivos de usuario.
- h. Protección frente amenazas, las comunicaciones y la información.
- i. Usuarios privilegiados locales y gestión de cuentas privilegiadas.
- j. Configuración segura de vulnerabilidades y análisis de vulnerabilidades.
- k. Protección de datos.
- l. Herramientas de seguridad: Data-centric, DAG, DLP, IRM, DAM/DAF, CASB.
- m. Protección de datos-Defensas, protección de las aplicaciones y denegaciones de servicio.

- n. Protección frente a bots, gestión de contraseñas robustas y rotación y uso de autenticación multifactor (MFA).
- o. Protección de las redes sociales, riesgos, buenas prácticas.
- p. Cómo implementar una estrategia en protección

7. Detección, respuesta y resiliencia:

- a. Más allá de la protección, principales retos a los que nos enfrentamos y mantener la calma en la crisis.
- b. Defensas-Básicas.
- c. Responde a los ciberincidentes.
- d. Feeds de información y brechas de seguridad.
- e. Defensas-Avanzadas.
- f. Monitorización continua de ciberseguridad.
- g. Gestión continua de vulnerabilidades y resiliencia.

8. Define tu plan de ciberseguridad

- a. ¿Dónde nos encontramos?.
- b. Define tu plan de ciberseguridad.
- c. Ejemplo de evaluación del dominio de Protección.
- d. Análisis inicial y estado final.
- e. Construyendo mi plan de ciberseguridad.
- f. Dominio de Organización y riesgos, dominio de Protección, dominio de Detección y respuesta y resiliencia.

9. Establece tu plan y evolucionalo:

- a. Documentemos la estrategia.
- b. Definición de la estrategia y sus programas.
- c. Ciclo de vida del plan.
- d. Procedimientos y políticas cyber.
- e. Gobernemos la estrategia.
- f. Evolucionemos la estrategia.

10. Ciberseguridad para emprendedores:

- a. Introducción.
- b. Riesgos y amenazas específicas.
- c. Sobre la organización y riesgos.
- d. Protege tus redes wifi, dispositivos y sistemas, correo electrónico, tus datos, tu página web, las credenciales de acceso y tus redes sociales.
- e. Sobre la detección, respuesta y resiliencia.
- f. Buenas prácticas en la actuación ante un ciberincidente.
- g. Concienciación.
- h. Mantener la privacidad personal y profesional.

11. Estrategia de ciberseguridad en cloud:

- a. Introducción.
- b. Los conceptos a conocer.
- c. Tipos de nube.
- d. Modelos de entrega.
- e. Responsabilidad compartida.
- f. Nube pública y riesgos.
- g. Amazon Web Services (AWS).
- h. Infraestructura IaaS de AWS como aspecto básico.
- i. Seguridad de la nube y seguridad para la nube.
- j. Microsoft Azure e infraestructura IaaS de Azure como aspecto básico.
- k. Seguridad de la nube y seguridad para la nube y Google Cloud Platform (GCP).
- l. Estrategia de seguridad y buenas prácticas de seguridad.
- m. Framework de controles y monitorización del cumplimiento.
- n. Certificación de servicios en nube.
- o. Protección de los datos en entornos SaaS.

12. Reglas de oro y guía de controles:

- a. Y el final es solo el principio.
- b. Las reglas de oro.
- c. Organización y riesgos.
- d. Estrategia de negocio y organización.

- e. Diseño tecnológico y gestión de activos.
- f. Gestiona tus ciberriesgos.
- g. Seguridad en proveedores.
- h. Cultura cibersegura.
- i. Protección.
- j. Copias de seguridad.
- k. Monitorización continua de ciberseguridad.

4. TEMPORALIZACIÓN

La programación del módulo que nos ocupa, se puede observar en el punto 3.2 UNIDADES DE TRABAJO, que se encuentra compuesta por 12 unidades de trabajo (UT en adelante), organizadas de manera que aseguran una progresión adecuada en el proceso de enseñanza-aprendizaje, cada unidad se apoya en los conceptos y herramientas presentados en líneas anteriores, sin invertir el orden.

Las horas que tiene asignado este módulo según el currículo del ciclo formativo de la Comunidad de Castilla y León (Consejería de Educación de Castilla y León, 2024c) al que pertenece este módulo, tiene una duración de 54 horas, las cuales la distribución de las horas semanales también recogidas en la normativa nombrada anteriormente es de 3 horas semanales siendo la distribución de estas de 2 horas los lunes y 1 hora los martes, formando un bloque 2-1. La duración real de cada una de las sesiones es de 50 minutos, según el horario del centro donde se imparte este módulo.

La planificación de las unidades de trabajo de los que se compone el módulo por trimestre podría ser la siguiente:

Evaluación	Contenidos del módulo	Horas asignadas
1ª Evaluación	Tema 1. Introducción. Un nuevo horizonte de amenazas.	3
	Tema 2. Ciberseguridad y cómo construir tu estrategia.	5
	Tema 3. Entiende tu entorno de amenazas.	4
	Tema 4. Dónde te encuentras. Evalúate a ti mismo.	4
	Tema 5. Organización y riesgos.	4
	Tema 6. Protección.	5
2ª Evaluación	Tema 7. Detección, respuesta y resiliencia.	5
	Tema 8. Define tu plan de ciberseguridad.	4
	Tema 9. Establece tu plan y evolucionalo.	4
	Tema 10. Ciberseguridad para emprendedores.	3
	Tema 11. Estrategia de ciberseguridad en cloud.	4
	Tema 12. Reglas de oro y guía de controles.	3
3ª Evaluación	Repaso por parte del profesor de las unidades de trabajo que se han suspendido en el primer y/o segundo trimestre, para preparar al alumno para la convocatoria de junio.	Se asigna el horario lectivo correspondiente durante el curso hasta finalizar el curso lectivo, correspondiendo a las horas de asignación de horario lectivo - docente.

Tabla 1: Temporalización

Fuente: Elaboración propia

La previsión que se ha indicado o distribución de contenidos por trimestres podrá variar teniendo en cuenta el ritmo de aprendizaje de los alumnos, sus intereses, la duración de las pruebas y días festivos. Contemplando lo anterior, si diera tiempo se destinarán algunas horas a profundizar en los contenidos y/o preparar exámenes.

5. METODOLOGÍA

Para la consecución de los objetivos señalados, se empleará una metodología activa y participativa desde el primer momento, así como de forma interdisciplinar.

Cada unidad didáctica comenzará con una explicación del profesor quien motivará al alumno a que pregunte todo aquello que estime oportuno relacionado con el módulo. Asimismo, sondeará los conocimientos del alumno sobre cada tema anterior para observar el grado de comprensión de este. Las explicaciones se complementarán por parte del alumno con el estudio individual y la resolución de forma individual o en grupo de cuestiones teóricas y ejercicios prácticos propuestos en clase.

Para facilitar el seguimiento de las clases, el profesor facilitará cuestiones y otros materiales extraídas de diferentes fuentes de información, que permitirán al alumno encontrar una guía de trabajo y buen material para seguir el desarrollo de la asignatura.

Se tratará de dar a la asignatura un matiz práctico, realizando el alumno ejercicios en aquellos puntos del temario en los que éste por su naturaleza y la disponibilidad de material del centro así lo permitan.

Dado que existen temas con un tratamiento básicamente teórico con contenidos conceptuales, y otros de marcado carácter práctico, se tratará en todo momento el intercalar unas unidades didácticas con otras.

La práctica con ordenador se irá simultaneando, siendo ésta de gran relieve en la consecución de las capacidades productivas que se persiguen. Para ello se constituirán grupos de trabajo de forma libre de tal manera que sean ellos mismos quienes lo establezcan.

Se tratará de coordinar esta asignatura con las restantes de informática.

El conjunto de actividades se desarrollará dentro de un amplio bagaje cultural que le permita al alumno su desarrollo como persona íntegra, libre de prejuicios racistas, sexistas o de cualquier otro tipo de discriminación injusta.

6. CRITERIOS DE CALIFICACIÓN

6.1. EVALUACIÓN Y CALIFICACIÓN

En la evaluación del módulo formativo que nos ocupa este documento se van a aplicar los Resultados de Aprendizaje que aparecen referenciados en el Real Decreto 1691/2007, de 14 de diciembre (España, 2008), con el fin de comprobar si se han asimilado los contenidos asociados y, en consecuencia, alcanzado los objetivos del módulo, así como las competencias profesionales, personales y sociales establecidas en la normativa vigente.

La asistencia a clase por parte de los alumnos es obligatoria (por ley) y en este módulo con más peso ya que tiene un elevado contenido práctico. Aquellos alumnos/as que obtengan un 15% de faltas de asistencia del total del módulo que es de 54 horas, las cuales si se encuentran sin justificar las cuales son 8,1 ~ 8 (redondeo de horas inferior) horas totales del módulo, es decir, no asistan como mínimo al 85% de las horas 45,9 ~ 46 (redondeo de horas superior) horas totales del módulo, no tendrán derecho a la evaluación continua, tal y como especifica en el propio Reglamento de Régimen Interno (en adelante RRI) en el “*CAPÍTULO V. ABSENTISMO ESCOLAR - Artículo 34. La obligatoriedad de asistir a clase - apartado b)*” (Consejo escolar, 2025) y también en la ORDEN EDU/1575/2024, de 23 de diciembre (Consejería de Educación de Castilla y León, 2024d), por la que se regula el proceso de evaluación del alumnado que curse enseñanzas de grados D y E del sistema de formación profesional en la Comunidad de Castilla y León, y deberán realizar un examen final de todo el módulo, con la misma estructura y valoración que la convocatoria extraordinaria.

6.1.1. Procedimiento de evaluación

La evaluación se realizará tomando como referencia los objetivos, expresados en RA, así como los objetivos generales del ciclo formativo.

- **Evaluación continua.** Durante el desarrollo del módulo se realizan actividades y tareas que se encuentran relacionados con los RA para obtener el grado de asimilación de estos y comprobar que se está mejorando en el proceso de aprendizaje de forma continua. Esto se llevará a cabo mediante un registro de evidencias objetivas que cada alumno o alumna demostrará en el hecho de cumplir con los ejercicios / actividades individuales o colectivas, así como con trabajos que se soliciten.
- **Evaluación sumativa.** En el desarrollo del curso escolar donde se imparte dicho módulo se celebrarán tantas pruebas teóricas o prácticas por evaluación como se estime necesario para evaluar la adquisición de los RA. Además, se realizarán dos evaluaciones parciales, una por trimestre en las cuales se recogerán las calificaciones que serán el reflejo de los resultados obtenidos por el alumnado en las tareas o en las pruebas evaluables realizadas durante el periodo.
- **Evaluación final.** Esta evaluación se realiza en la finalización del régimen ordinario de periodo educativo de clase antes de realizar la formación en empresa u organismo equiparado, es decir, en marzo. En ella se podrá mejorar los resultados obtenidos quien así lo solicite, así como para

recuperar los RA no superados en evaluaciones anteriores. En la sesión de evaluación final del curso se expedirá una calificación que será reflejo del resultado conseguido por el alumno/a en el módulo.

- **Evaluación extraordinaria.** Esta evaluación se realiza en la finalización del régimen extraordinario de periodo educativo de clase, es decir, en junio. En ella se podrá mejorar los resultados obtenidos quien así lo solicite, así como para recuperar los RA no superados en evaluaciones anteriores. En la sesión de evaluación final extraordinaria del curso se expedirá una calificación que será reflejo del resultado conseguido por el alumno/a en el módulo.

6.1.2. Criterios de calificación

Los criterios de calificación se encuentran de acuerdo con la ordenación curricular vigente, la cual se procede a llevar a cabo con los Resultados de Aprendizaje (en adelante RA). Los RA se contemplan como bloques independientes desde el punto de vista de la evaluación y la calificación. Así, la superación del módulo exige la superación de cada uno y de forma independiente de los RA.

Para la consideración de superación de los RA correspondientes a cada evaluación producida, debe tener una nota mínima de 5 o superior. Si la nota obtenida en algún RA es inferior a ese valor, no solo se considera suspendido el RA, sino que además no se contempla en realización de la media de RA.

Una vez indicados los parámetros y nota mínima de superación de RA, se procede a indicar a nivel porcentual, el modo de obtención de cada RA se procede a indicar a continuación:

- Pruebas objetivas: las cuales son consideradas tanto pruebas teóricas (exámenes) como prácticas (desarrollo de ejercicios prácticos) y tienen los siguientes % referente a cada RA, los cuales sumando cada % sobre la nota es un valor de 70 % total.

RA	Unidades de trabajo	% sobre la nota final
1	<p>Tema 1: Introducción. Un nuevo horizonte de amenazas.</p> <p>Tema 3: Entiende tu entorno de amenazas.</p> <p>Tema 10: Ciberseguridad para emprendedores.</p>	9.76
2	<p>Tema 2: Ciberseguridad y cómo construir tu estrategia.</p> <p>Tema 5: Organización y riesgos.</p> <p>Tema 6: Protección.</p> <p>Tema 9: Establece tu plan y evolucionalo.</p> <p>Tema 10: Ciberseguridad para emprendedores.</p> <p>Tema 11: Estrategia de ciberseguridad en cloud.</p> <p>Tema 12: Reglas de oro y guía de controles.</p>	18.39
3	<p>Tema 7: Detección, respuesta y resiliencia.</p> <p>Tema 8: Define tu plan de ciberseguridad.</p> <p>Tema 12: Reglas de oro y guía de controles.</p>	12,02
4	<p>Tema 4: Dónde te encuentras. evalúate a ti mismo.</p> <p>Tema 6: Protección.</p> <p>Tema 7: Detección, respuesta y resiliencia.</p> <p>Tema 11: Estrategia de ciberseguridad en cloud.</p> <p>Tema 12: Reglas de oro y guía de controles.</p>	13,7
5	<p>Tema 2: Ciberseguridad y cómo construir tu estrategia.</p> <p>Tema 5: Organización y riesgos.</p> <p>Tema 8: Define tu plan de ciberseguridad.</p> <p>Tema 9: Establece tu plan y evolucionalo.</p> <p>Tema 10: Ciberseguridad para emprendedores.</p> <p>Tema 11: Estrategia de ciberseguridad en cloud.</p> <p>Tema 12: Reglas de oro y guía de controles.</p>	16,14
TOTAL		70

Tabla 2: Criterios de calificación: RA y peso nota

Fuente: Elaboración propia

- Ejercicios / actividades: este punto consiste en trabajos de investigación o bien ejercicios prácticos relacionados con los contenidos impartidos en cada RA descritos en el módulo, los cuales sumando cada % sobre la nota es un valor de 30 % total.

Unidades de trabajo	% final aproximado
1	2,3
2	2,8
3	2,25
4	4,5
5	2,75
6	2,5
7	2,25
8	1,8
9	2
10	1,6
11	2,1
12	3,15
TOTAL	30

Tabla 3: Criterios de calificación: Unidades de trabajo y peso nota

Fuente: Elaboración propia

Los porcentajes asignados a cada tema y actividad relacionados con los RA indicados en líneas anteriores, reflejan una planificación prevista a lo largo de la programación desarrollada en este documento. No obstante, el profesor (o docente) que imparte el módulo podrá, por motivos pedagógicos o de actualización del contenido, incorporar actividades adicionales, lo que podría modificar ligeramente los porcentajes indicados.

Todos los ejercicios / actividades que son planteadas por parte del docente, serán desarrolladas tanto en clase siempre y cuando el sistema implementado por los administradores de los equipos del aula, el curso que ocupa esta programación, se puedan realizar las instalaciones de los software por parte de los alumnos. Si por el contrario, no se pueden realizar los ejercicios / actividades en el aula, el alumno tendrá que desarrollar estas en su domicilio, pero la documentación que se exige de cada una de las tareas indicadas si que las pueden realizar en ambos lugares, no eximiendo esta parte por falta de software en el sistema de clase, ya que se puede realizar el desarrollo de la documentación de forma online.



6.1.3. Evaluación ordinaria

La evaluación ordinaria se encuentra formada por las evaluaciones continuas y la final. Para obtener esta calificación de la nota de cada evaluación ordinaria se tiene en cuenta el resultado de varias pruebas y ejercicios realizados durante los periodos a evaluar, los cuales serán puntuados desde 0 a 10.

A continuación, se expone el peso de las diferentes partes de las que forma parte la evaluación y obtención de la nota, las cuales se han indicado en líneas anteriores los pesos y desglose de estos:

- Pruebas objetivas: 70%.
- Ejercicios / actividades: 30%.

Para las pruebas objetivas que se han indicado en líneas anteriores se califican los RA, los cuales se pueden observar a continuación:

UNIDADES DE TRABAJO (UT)	RESULTADOS DE APRENDIZAJE (RA)				
	1	2	3	4	5
1	3,33 %	-	-	-	-
2	-	2,2 %	-	-	2,2
3	3,33 %	-	-	-	-
4	-	-	3 %	3 %	-
5	-	2,7 %	-	-	2,7 %
6	-	2,4 %	-	2,4 %	-
7	-	-	3 %	3 %	-
8	-	-	3,165 %	-	3,165 %
9	-	2,74 %	-	-	2,74 %
10	3,1 %	3,1 %	-	-	-
11	-	2,4 %	-	2,45 %	2,48 %
12	-	2,85 %	2,85 %	2,85 %	2,85 %
TOTAL	9,76 %	18,39 %	12,02 %	13,7 %	16,14 %
TOTAL RA	70 %				

Tabla 4: Criterios de calificación: Unidades de trabajo y RA

Fuente: Elaboración propia

Se establecen los siguientes conceptos de calificación de este punto, los cuales se exponen a continuación:

- Se realizarán tantas pruebas teóricas y prácticas por evaluación como se estime necesario para evaluar la adquisición de los distintos contenidos estudiados, generalmente una por unidad de trabajo (y resultado de aprendizaje) y mínimo una por trimestre.



- Cada una de estas pruebas será valorada de 0 a 10 puntos, y la calificación obtenida deberá ser superior a 5 puntos para poder ser considerada a la hora de calcular la nota media de la evaluación. La nota de la evaluación se calculará como la media aritmética de las notas obtenidas en todas estas pruebas. En el caso de ser inferior a 5 la nota resultante, se considerará la evaluación no superada, y el alumno deberá realizar la correspondiente recuperación.
- Si un alumno o alumna copia en alguna de estas pruebas (con medios electrónicos u otros medios), la calificación en esa prueba será de 0 puntos para el que copia como el que ayuda en la copia y no tendrá derecho a realizar la media aritmética por lo que la calificación final de estas pruebas será de 0 puntos.
- Si por algún motivo el alumno/a no asiste a un examen, se aplicarán las siguientes medidas:
 - Si no se aporta justificando médico, supondrá un 0.
 - Si se aporta justificando médico y considera el profesor que es falso, se consulta a jefatura de estudios para informarse sobre qué medidas tomar y en determinación de lo indicado por jefatura se realiza acción sobre el examen pendiente.
 - Si se aporta justificando médico, el examen se realizará en una nueva fecha establecida por el profesor.

Para los ejercicios / actividades que se han indicado en líneas anteriores se califican los RA como se pueden observar a continuación:

UNIDADES DE TRABAJO (UT)	RESULTADOS DE APRENDIZAJE (RA) ACTIVIDADES				
	1	2	3	4	5
1	2,3 %	-	-	-	-
2	-	0,8 %	-	-	2
3	2,25 %	-	-	-	-
4	-	-	2,25 %	2,25 %	-
5	-	1,25 %	-	-	1,5 %
6	-	1,5 %	-	1 %	-
7	-	-	1,25 %	1 %	-
8	-	-	0,8 %	-	1 %
9	-	0,75 %	-	-	1,25 %
10	0,8 %	0,8 %	-	-	-
11	-	0,7 %	-	0,7 %	0,7 %
12	-	0,8 %	0,8 %	0,8 %	0,75 %
TOTAL	5,35 %	6,6 %	5,10 %	5,75 %	7,20 %
TOTAL RA	30 %				

Tabla 5: Criterios de calificación: Unidades de trabajo y RA/actividades

Fuente: Elaboración propia

Se establecen los siguientes criterios de calificación de este punto, los cuales se exponen a continuación:

- Este tipo de actividades (ejercicios, trabajos, prácticas, etc.) se realizarán con el ordenador y materiales disponibles, y el profesor evaluará el desarrollo de cada práctica en función del grado de consecución de los resultados esperados.
- Todas las actividades tienen una fecha tope de entrega puesta por parte del profesor. Si una actividad no se ha entregado dentro de la fecha tope y forma indicado por el profesor, o la copia de estos por parte del alumno/a, supondrá una calificación de 0 puntos y no tendrá derecho a realizar la media aritmética por lo que la calificación final de las actividades será de 0 puntos.
- Los trabajos desarrollados, tanto de forma individual como en grupo, se calificarán de 1 a 10 puntos. Si el trabajo se desarrolla en grupo, todos los miembros del grupo pueden no tener la misma nota, valorando el profesor la implicación de cada componente en el desarrollo del trabajo, el esfuerzo realizado en la presentación, etc.
- Cada uno de los trabajos desarrollados, tanto de forma individual como en grupo, se tendrán en cuenta las indicaciones recogidas en cada uno de los enunciados de cada uno de los trabajos solicitados, siendo corregidos a través de diferentes métodos de evaluación a consideración del docente que ha solicitado estos documentos.
- La nota final será la media aritmética de las actividades.

La evaluación de la situación de clase por parte del alumnado el cual es considerado un parámetro de apreciación personal del profesor, en relación con los factores que se enumeran a continuación:

- Asistencia y puntualidad.
- Educación.
- Colaboración en el trabajo en equipo.
- Actitud general frente al módulo.
- Participación en clase.
- Autonomía.

- Colaboración con el profesor y el resto de los alumnos en el buen uso del aula, equipos y programas informáticos.
- Cuidado del material.

Cualquiera de los incumplimientos indicados en líneas anteriores durante el desarrollo del trimestre, será penalizado en la nota de cada evaluación con -0.2. También se tendrán en cuenta otras apreciaciones como son las siguientes, las cuales serán penalizadas en la nota del trimestre con un -0.5 cada vez que se produzca una de ellas y además, serán se producirá la aplicación de las normas del RRI del centro. Los comportamientos a los que se hacen referencia son los siguientes:

- No respeten la dignidad, integridad, libertad y demás derechos de los profesores, alumnos, así como el resto de la comunidad escolar.
- Instalen, realicen descargas o utilizar programas distintos de los permitidos.
- Manipular a sabiendas de forma incorrecta los equipos o programas informáticos.
- Intentar deliberadamente burlar la seguridad de la red, especialmente si es con intención de causar daño.
- Utilizar Internet sin permiso. No se podrá chatear, ni utilizar el correo, ni descargar música, videos, etc.
- Utilizar en clase el teléfono móvil, auriculares, ni cualquier otro dispositivo sin previa autorización del profesor.
- Los materiales educativos que cualquier profesor de este departamento proporcione a los alumnos, subiéndolos al Aula Virtual o por cualquier otro medio, sólo se podrán utilizar dentro del ámbito educativo y siempre que el alumno previamente pida por escrito la autorización expresa al profesor que se los ha facilitado.
- Las manifestaciones expresas contrarias a los valores y derechos democráticos legalmente establecidos.
- Las acciones de desconsideración, imposición de criterio, amenaza, insulto y falta de respeto, en general, a los miembros de la comunidad educativa, siempre que no sean calificadas como faltas.

- No acatar las indicaciones del profesorado o contradecir sus órdenes, dificultando la marcha de la clase.
- El incumplimiento del deber de estudio durante el desarrollo de la clase, dificultando la actuación del profesorado y del resto de los alumnos.
- El deterioro de las dependencias e instalaciones del centro, de su material o de pertenencia de otros alumnos, realizado de forma negligente o intencionada.
- La falta de respeto, indisciplina, acoso, amenaza y agresión verbal o física, directa o indirecta, al profesorado, a cualquier miembro de la comunidad educativa.
- Las conductas que atenten contra la dignidad personal de otros miembros de la comunidad educativa, que tengan como origen o consecuencia una discriminación o acoso basado en el género, la orientación o identidad sexual, o un origen racial, étnico, religioso, de creencias o de discapacidad, o que se realicen contra el alumnado más vulnerable por sus características personales, sociales o educativas.
- El deterioro grave, causado intencionadamente, de las dependencias del centro, de su material o de los objetos y las pertenencias de los demás miembros de la comunidad educativa.
- Las actuaciones y las incitaciones a actuaciones perjudiciales para la salud y la integridad personal de los miembros de la comunidad educativa del centro.
- La realización de grabaciones por cualquier medio electrónico y/o su difusión, así como los comentarios expresados en dichos medios y que supongan acciones de desconsideración, imposición de criterio, amenaza, insulto y falta de respeto, en general, a cualquier miembro de la comunidad educativa.

Además, de lo indicado en líneas anteriores, se tendrá en cuenta las normas del propio departamento a la que pertenece esta programación, los cuales son:

- Respetar la dignidad, integridad, libertad y demás derechos de los profesores, alumnos, así como el resto de la comunidad escolar.
- Asistir a clase con puntualidad.
- Está prohibido instalar, descargar o utilizar programas distintos de los permitidos.

- Está prohibido manipular a sabiendas de forma incorrecta los equipos o programas informáticos.
- Está prohibido intentar deliberadamente burlar la seguridad de la red, especialmente si es con intención de causar daño.
- Está prohibido utilizar Internet sin permiso. No se podrá chatear, ni utilizar el correo, ni descargar música, videos, etc. Sólo podrán utilizar Internet cuando se les autorice, y siempre relacionado con el módulo que se esté impartiendo.
- Si un alumno llega tarde al centro podrá incorporarse a la clase que le corresponda. No obstante, se registrará el correspondiente retraso y se atenderá a lo dispuesto en el RRI para estos casos.
- Cuando algún alumno/a precise ausentarse del Centro, por motivo justificado, o faltar a clase durante uno o más días, el alumno lo comunicará al profesor/tutor con la debida antelación.
- Los alumnos que acumulen más faltas de asistencia que las indicadas en el Reglamento del Régimen Interior perderán el derecho a la evaluación continua.
- No está permitido utilizar en clase el teléfono móvil, auriculares, ni cualquier otro dispositivo sin previa autorización del profesor.
- El aula debe presentar siempre un aspecto cuidado, respetando en todo momento la limpieza, el orden y el material.
- Cada alumno se hará responsable de su puesto de trabajo, comunicando al comienzo de la clase cualquier incidencia que observe en el mismo, sino será a él sobre el que caiga la responsabilidad.
- Los materiales educativos que cualquier profesor de este departamento proporcione a los alumnos, subiéndolos al Aula Virtual o por cualquier otro medio, sólo se podrán utilizar dentro del ámbito educativo y siempre que el alumno previamente pida por escrito la autorización expresa al profesor que se los ha facilitado.

Todos y cada uno de los comportamientos indicados en líneas anteriores, pueden causar la no superación del módulo del que forma parte esta programación.

La nota final de cada evaluación, de 1 a 10 puntos, será la suma de los tres conceptos de calificación ponderados según se ha expuesto anteriormente. Si el alumno no obtuviera un mínimo de 5 puntos, la evaluación se considerará suspensa y el alumno tendrá que recuperar dicha evaluación.

Para aprobar una evaluación, el alumno/a tendrá que conseguir una nota ≥ 5 . La calificación final del módulo al finalizar el curso será la media de la nota de cada RA.

Además, el alumnado no podrá aprobar el módulo si tiene alguna RA con una nota inferior al 5. Se propondrán diferentes actividades y trabajos para recuperar aquellos resultados de aprendizaje que no se completen adecuadamente tanto en la empresa como en el aula.

La nota final del módulo será la media aritmética de las dos evaluaciones siendo obligatorio tener un mínimo de 5 puntos en cada una de ellas. Si no se tuviera el mínimo, el módulo no puede ser superado y el alumno tendrá que realizar la correspondiente recuperación.

El alumnado que perdiera el derecho a la evaluación continua, es decir, que acumule un 15% de faltas injustificadas (aquellas no justificadas por un medio oficial: médico, instituciones públicas, etc.), tendrá que examinarse de todo el módulo al final del tercer trimestre. Asimismo, deberá entregar todas las prácticas realizadas durante el curso, obligatoriamente. Los parámetros para su realización le serán debidamente comunicados al alumno. El examen final contará un 100% de la nota final.

6.1.4. Evaluación extraordinaria

En el caso de que algún alumno/a suspenda el módulo en la convocatoria ordinaria, producida en fechas propuestas por el docente, dispondrá de la convocatoria extraordinaria, la cual consistirá en una prueba que incluirá TODOS los contenidos del módulo. Esta convocatoria será comunicada en el tablón de anuncios, la cual es propuesta por parte del departamento y por el docente del módulo que ha impartido este.

6.1.5. Instrumentos de evaluación

Los instrumentos de evaluación que se aplican en el módulo de esta programación son los siguiente:

- Pruebas objetivas escritas (exámenes) con cuestiones tipo test y preguntas cortas sobre ejercicios y contenidos teóricos de cada unidad.
- Resolución de los ejercicios y prácticas de cada unidad didáctica.

7. RECUPERACIÓN

Los alumnos que suspendan alguna evaluación tendrán derecho a realizar una recuperación por cada evaluación suspensa. El conjunto de notas formado por cada evaluación y sus correspondientes recuperaciones será considerado como la evaluación final ordinaria, y la nota obtenida se trasladará a la convocatoria ordinaria.

Las pruebas de recuperación de cada evaluación se realizarán sobre aquellas evaluaciones que el alumno no haya superado durante el curso y en base a los mínimos exigibles de esta programación.

Aquellos alumnos cuyas faltas de asistencia no justificadas superen el 15% de las horas totales del módulo y sea imposible aplicarles la evaluación continua, perderán el derecho a las recuperaciones por cada evaluación, debiendo presentarse a la evaluación final extraordinaria. Para poder acceder a esta prueba, será obligatorio entregar todas las prácticas en fecha y forma, según lo descrito en el apartado de Criterios de Calificación.

Si algún alumno no ha superado el módulo en la convocatoria ordinaria, tendrá derecho a una evaluación final extraordinaria en junio donde se examinarán con todo el contenido de la asignatura.

En la evaluación final extraordinaria se aplicarán los mismos RA y calificación que en la evaluación final ordinaria.

8. ATENCIÓN A LA DIVERSIDAD

Como consecuencia de la heterogeneidad de las aulas y de la naturaleza individual del proceso de enseñanza-aprendizaje se hace necesario establecer una serie de pautas por parte del docente. Aparte del apoyo del personal especializado cuando se requiera, que ofrezcan al alumno la posibilidad de alcanzar los objetivos marcados para el módulo a un ritmo acorde a sus aptitudes.

Podemos distinguir como alumnos con necesidad específica de apoyo educativo a los siguientes:

Alumnos con necesidades educativas especiales:

- Alumnos con trastornos graves de conducta:
 - Se insistirá básicamente en reforzar los contenidos mínimos mediante actividades de refuerzo pedagógico como, por ejemplo:
 - Modificar la ubicación en clase.
 - Repetición individualizada de algunas explicaciones.

- Propuesta de actividades complementarias que sirvan de apoyo.
 - Potenciar la participación en clase.
 - Propuesta de interrogantes para potenciar la curiosidad y con ello el aprendizaje.
-
- Alumnos con discapacidad física:
 - Se debería estudiar el tipo de dispositivos (periféricos) que precisan y hacer la pertinente consulta y solicitud a las autoridades o asociaciones dedicadas a tal fin.
-
- Alumnos con altas capacidades intelectuales:
 - Se procurará sustituir las actividades que cubran los conocimientos ya adquiridos por otras que requieran un planteamiento más laborioso y que permita desarrollar su capacidad de investigación y razonamiento (actividades de proacción).
-
- Alumnos con integración tardía al sistema educativo español:
 - Alumnos con graves carencias lingüísticas:
 - Se puede suministrar el programa, en la medida que sea posible, en su idioma. Si no es viable y la comunicación es prácticamente nula se podría optar por derivarlo a un aula de inmersión lingüística para adquirir los conceptos mínimos idiomáticos.
-
- Alumnos con carencia de base:
 - Si el alumno carece de cierta base en otras asignaturas que le impiden avanzar en el módulo se proporcionarán programas autodidactas que faciliten un aprendizaje de base para continuar sus estudios y se reforzarán los contenidos mínimos de la misma forma que para alumnos con necesidades educativas especiales.

9. RECLAMACIONES

En el caso de que un alumno no esté de acuerdo con su calificación se seguirá el procedimiento establecido en la ORDEN EDU/1575/2024, de 23 de diciembre, por la que se regula el proceso de evaluación del alumnado que curse enseñanzas de grados D y E del sistema de formación profesional en la Comunidad de Castilla y León y en concreto en los Artículos 18, 19 y 20 (Consejería de Educación de Castilla y León, 2024a).

Los artículos indicados anteriormente indican lo siguiente:

“Artículo 18. Aclaraciones.

- 1. Cuando exista desacuerdo sobre las decisiones de la correspondiente sesión de evaluación, el alumnado y, en caso de minoría de edad, sus progenitores o representantes legales, podrán solicitar aclaraciones acerca de las calificaciones, así como de la decisión de promoción o titulación.*
- 2. La solicitud de aclaraciones se realizará el primer día hábil posterior a la comunicación de los resultados o, en su caso, de la decisión de promoción o titulación. El centro deberá informar a los padres, madres o personas que ejerzan la tutela legal del alumnado de este derecho.*

Artículo 19. Procedimiento de reclamación en el centro.

- 1. El alumnado y, en caso de minoría de edad, sus progenitores o representantes legales, podrán reclamar, por escrito, ante la dirección del centro, las calificaciones o decisiones de promoción o titulación, en el plazo de dos días hábiles contados a partir del siguiente a aquel en que se produjo la entrega por escrito de la información de la evaluación final o en su caso de la comunicación de la decisión de promoción o titulación. La reclamación debe contener las alegaciones que justifiquen la disconformidad con la calificación o decisión adoptada. Una vez presentada en el centro, la reclamación será tramitada a través de quien ejerza la jefatura de estudios.*
- 2. La Jefatura de estudios del centro trasladará la reclamación, en el mismo día en que se presente, al departamento didáctico que corresponda y lo comunicará a la persona que ejerce la tutoría, como responsable de la coordinación de la sesión de evaluación final.*

3. Cuando la reclamación tenga por objeto la modificación de las calificaciones, el departamento que corresponda analizará la solicitud de revisión y elaborará un informe de respuesta motivado, que contendrá:
- a) La descripción de los hechos y actuaciones previas.
 - b) El análisis de la consecución de los resultados de aprendizaje, que se realizará teniendo en cuenta los criterios de evaluación, según lo establecido en la programación didáctica correspondiente.
 - c) El análisis de la adecuación de los procedimientos e instrumentos de evaluación utilizados, conforme a lo señalado en la programación didáctica.
 - d) El análisis de la corrección en la aplicación de los criterios de calificación respecto a lo establecido en la programación didáctica.
 - e) La decisión adoptada respecto a la solicitud de revisión y las alegaciones presentadas.
 - f) Cualquier otra cuestión que pueda considerarse de interés.
4. El informe de cada departamento didáctico se presentará ante la jefatura de estudios, en el siguiente día hábil de la recepción de la reclamación. La persona titular de la jefatura de estudios del centro deberá cerciorarse de que el informe se ajusta a la presente orden y demás normativa vigente, requiriendo al correspondiente departamento las modificaciones del mismo que sean necesarias.
5. En el caso de reclamación de calificaciones, la jefatura de estudios remitirá el informe o informes a la persona a cargo de la dirección del centro; si hay modificaciones en la calificación, la persona titular de la jefatura de estudios procederá a reunir al equipo docente, en sesión excepcional, en el segundo día hábil posterior a la recepción de la reclamación para modificar el acta de evaluación. Si como consecuencia de la modificación de la calificación el alumno o alumna está en condiciones de promocionar o titular, el equipo docente valorará esta circunstancia.
6. Cuando la reclamación tenga por objeto la revisión de las decisiones sobre promoción o titulación, en el segundo día hábil, después de la recepción de la solicitud, se reunirá el equipo docente, en sesión excepcional, para analizar la reclamación y adoptar el acuerdo de modificación o ratificación de la decisión de promoción o titulación, de acuerdo con lo establecido en esta Orden. La persona que ejerza la tutoría del grupo recogerá en el acta de la sesión excepcional los acuerdos adoptados y lo comunicará a la dirección del centro.

7. *Los centros deben prever, en el calendario de final de curso, los días en que deben celebrarse las sesiones de evaluación excepcionales de los equipos docentes para el cumplimiento de lo establecido en el apartado anterior.*
8. *La persona a cargo de la dirección del centro comunicará por escrito y de forma fehaciente, con constancia de la fecha de recepción, al alumno o alumna y si procede, a sus progenitores o representantes legales, la decisión razonada de modificación o ratificación, en el plazo de dos días hábiles contados a partir de su adopción. En dicha comunicación se informará, además, que, contra la decisión adoptada, sus progenitores o representantes legales, y si procede, el alumno o alumna, podrán solicitar que se eleve la reclamación, a través de la dirección del centro, ante la persona titular de la dirección provincial de educación correspondiente, en el plazo de dos días hábiles, contados a partir de la fecha de recepción de la respuesta a la reclamación. En todo caso, la comunicación pondrá fin al procedimiento de reclamación en el centro.*
9. *En los centros privados, serán los órganos determinados en sus respectivos Reglamentos de Régimen Interior, los que tramiten las revisiones académicas siguiendo el mismo procedimiento y plazos.*

Artículo 20. Procedimiento de reclamación ante la dirección provincial de educación.

1. *En el supuesto de que tras la comunicación de quien ejerza la dirección del centro persista el desacuerdo sobre los resultados de calificación final, o sobre la decisión de promoción o titulación adoptada, el alumno o alumna o, en caso de que fuese menor de edad, los padres, madres o personas que ejerzan la tutela legal del alumnado podrán solicitar que su reclamación sea elevada al titular de la dirección provincial de educación.*
2. *La solicitud deberá formularse mediante escrito dirigido a quien ejerza la dirección del centro, pudiéndose incorporar nuevas alegaciones.*
3. *El plazo será de dos días hábiles desde la notificación de la resolución de quien ejerza la dirección del centro. El centro deberá informar al alumno o alumna o, en caso de que fuese menor de edad, a los padres, madres o personas que ejerzan la tutela legal del alumnado de este derecho, así como del plazo en el que puede formularse dicha solicitud.*
4. *Quien ejerza la dirección del centro remitirá el expediente de la reclamación al titular de la dirección provincial de educación, en el plazo no superior a dos días hábiles desde que se formuló la solicitud, incluyendo al menos el escrito de reclamación, los informes emitidos, la*

respuesta dada por el centro, las programaciones didácticas, los instrumentos de evaluación, además de la documentación que sea procedente.

- 5. La persona titular de la dirección provincial, previo informe del área de inspección educativa dispondrá, desde el momento en que reciba el expediente del centro, de diez días hábiles para adoptar la resolución pertinente, que será motivada en todo caso, y que se comunicará inmediatamente a la dirección del centro docente para su aplicación y traslado a la persona que haya realizado la reclamación.*
- 6. Si tras el proceso de reclamación procediera la modificación de alguna calificación final o de la decisión de promoción o titulación adoptada para el alumno o alumna, la secretaria del centro insertará en las actas de evaluación y, en su caso, en el expediente académico la oportuna diligencia que será visada por la dirección del centro educativo.*
- 7. Contra la resolución de la dirección provincial de educación, el alumno o alumna o sus responsables legales podrán interponer recurso de alzada ante la correspondiente Delegación Territorial de la Junta de Castilla y León, en los términos previstos en la normativa sobre procedimiento administrativo común.”*

10. RECURSOS MATERIALES

En el presente curso se cuenta con los siguientes materiales de trabajo:

- Aula específica de informática.
- Dieciséis ordenadores personales con sistema operativo Windows 10 que se encuentran en dominio con la Junta de Castilla y León.
- Kit de videoconferencia.
- Encerado blanco y rotuladores.
- Pizarra digital.
- Una línea digital ADSL con salida a Internet.
- Mobiliario de aula.
- Medios audiovisuales.
- Equipamiento informático en red.

- Aplicaciones informáticas de uso general y específico del ciclo formativo.

11. BIBLIOGRAFÍA

Consejería de Educación de Castilla y León. (2024a). ORDEN EDU/1575/2024, de 23 de diciembre, por la que se regula el proceso de evaluación del alumnado que curse enseñanzas de grados D y E del sistema de formación profesional en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 3, pp. 22-24). <https://bocyl.jcyl.es/boletines/2025/01/07/pdf/BOCYL-D-07012025-1.pdf>

Consejería de Educación de Castilla y León. (2024b). DECRETO 24/2024, de 21 de noviembre, por el que se establece el currículo de los ciclos formativos de grado superior, correspondiente a la oferta de grado D y nivel 3 del Sistema de Formación Profesional, conducentes a la obtención del título de Técnico Superior, en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 229, pp. 22-45).

Consejería de Educación de Castilla y León. (2024c). ORDEN EDU/1287/2024, de 26 de noviembre, por la que se concretan los aspectos específicos del currículo del Ciclo Formativo de Grado Superior en Administración de Sistemas Informáticos en Red en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 234, pp. 116-122).

Consejería de Educación de Castilla y León. (2024d). ORDEN EDU/1575/2024, de 23 de diciembre, por la que se regula el proceso de evaluación del alumnado que curse enseñanzas de grados D y E del sistema de formación profesional en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 3). <https://bocyl.jcyl.es/boletines/2025/01/07/pdf/BOCYL-D-07012025-1.pdf>

Consejería de Educación de Castilla y León. (2025a). ORDEN EDU/411/2025, de 15 de abril, por la que se concreta la optatividad en las enseñanzas de grado D, niveles 2 y 3 del Sistema de Formación Profesional y se establece el procedimiento de oferta y autorización de complementos de formación de los grados D y E, niveles 2 y 3 del Sistema de Formación Profesional, en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 79, pp. 303-309). <https://bocyl.jcyl.es/boletines/2025/04/28/pdf/BOCYL-D-28042025-3.pdf>

Consejería de Educación de Castilla y León. (2025b). ORDEN EDU/173/2025, de 20 de febrero, por la que se desarrolla la formación en empresa u organismo equiparado, para las ofertas de formación profesional de los grados D y E del Sistema de Formación Profesional en la Comunidad de Castilla y León. En *Boletín Oficial de Castilla y León* (Vol. 42). <https://www.educa.jcyl.es/pt/resumenbocyl/orden-edu-173-2025-20-febrero-desarrolla-formacion-empresa>

Consejo escolar. (2025). REGLAMENTO DE RÉGIMEN INTERIOR. En *IES María Moliner Segovia* (pp. 24-25).

Costas Santos, J. (2011). *Seguridad y Alta Disponibilidad (Grado Superior)* (1.^a ed.). Grupo Editorial RA-MA. https://www.ra-ma.es/libro/seguridad-y-alta-disponibilidad-grado-superior_48299/

España. (2008). 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 sus enseñanzas mínimas. En *Boletín Oficial del Estado [BOE-A-2008-819]*, de 17 de enero de 2008 (Vol. 15, pp. 3445-3470). <https://www.boe.es/boe/dias/2008/01/17/pdfs/A03445-03470.pdf>

España. (2009). 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. En *Boletín Oficial del Estado [BOE-A-2009-18355]*, de 18 de noviembre de 2009 (Vol. 278, pp. 97846-97914). <https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18355>

España. (2022). Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional. En *Boletín Oficial del Estado [BOE-A-2022-5139]*, de 1 de abril de 2022 (Vol. 78, pp. 43546-43625). <https://www.boe.es/buscar/act.php?id=BOE-A-2022-5139>

España. (2023a). Real Decreto 658/2024, de 9 de julio, por el que se modifican el Real Decreto 132/2010, de 12 de febrero, por el que se establecen los requisitos mínimos de los centros que impartan las enseñanzas del segundo ciclo de la educación infantil, la educación primaria y la educación secundaria, y el Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional. En *Boletín Oficial del Estado [BOE-A-2024-14079]*, de 10 de julio de 2023 (Vol. 166, pp. 86582-86582). <https://www.boe.es/boe/dias/2024/07/10/pdfs/BOE-A-2024-14079.pdf>

España. (2023b). Real Decreto 659/2023, de 18 de julio, por el que se desarrolla la ordenación del Sistema de Formación Profesional. En *Boletín Oficial del Estado [BOE-A-2023-16889]*, de 22 de julio de 2023 (Vol. 174, pp. 106265-106464). <https://www.boe.es/boe/dias/2023/07/22/pdfs/BOE-A-2023-16889.pdf>



España. (2024). Real Decreto 500/2024, de 21 de mayo, por el que se modifican determinados reales decretos por los que se establecen títulos de Formación Profesional de grado superior y se fijan sus enseñanzas mínimas. En *Boletín Oficial del Estado [BOE-A-2024-10685]*, de 28 de mayo de 2024 (Vol. 129, pp. 61160-61409). <https://www.boe.es>

Gómez López, J., Villar Fernández, E. E., & Alcayde García, A. (2011). Seguridad en Sistemas Operativos Windows y GNU/Linux (2ª Edición Actualizada). En *Grupo Editorial RA-MA* (2.ª ed., Vol. 1). Grupo Editorial Ra-Ma. https://www.ra-ma.es/libro/seguridad-en-sistemas-operativos-windows-y-gnu-linux-2a-edicion-actualizada_48384/

POSTIGO PALACIOS, A. (2020). Seguridad informática Edición 2020. En : *Paraninfo.es : Libros :* ISBN 9788428344555. Paraninfo. <https://www.paraninfo.es/catalogo/9788428344555/seguridad-informatica--edicion-2020->

Roa Buendia, J. F. (2013). *Seguridad informática* (2.ª ed.). MacGrawHill. <https://www.mheducation.es/seguridad-informatica-9788448183967-spain>