

## **PROGRAMACIÓN DIDÁCTICA**

**Departamento:** *Informática y Comunicaciones*

**Curso:** *Curso de especialización en Ciberseguridad en Entornos de las  
Tecnologías de la Información*

**Módulo:** Incidentes de Ciberseguridad

**Profesor/es:** Alejandra San Segundo Hernández

**Año académico:** 2024-2025

## Índice

<b>1.- COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES DEL TÍTULO A LAS QUE CONTRIBUYE EL MÓDULO .....</b>	<b>3</b>
<b>2.- OBJETIVOS.....</b>	<b>3</b>
<b>2.1.- OBJETIVOS GENERALES DEL TÍTULO QUE DESARROLLA EL MÓDULO .....</b>	<b>3</b>
<b>2.2.- OBJETIVOS EXPRESADOS EN RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN .....</b>	<b>4</b>
<b>3.- CONTENIDOS DEL MÓDULO Y DISTRIBUCIÓN TEMPORAL .....</b>	<b>7</b>
<b>3.1 - CONTENIDOS DEL MÓDULO .....</b>	<b>7</b>
<b>3.2 - DISTRIBUCIÓN TEMPORAL .....</b>	<b>9</b>
<b>4.- METODOLOGÍA DIDÁCTICA .....</b>	<b>9</b>
<b>4.1.- ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE .....</b>	<b>9</b>
<b>4.2.- ATENCIÓN A LA DIVERSIDAD .....</b>	<b>11</b>
<b>4.3.- MATERIALES Y RECURSOS DIDÁCTICOS .....</b>	<b>11</b>
<b>4.4.- LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC).....</b>	<b>12</b>
<b>4.5.- ACTIVIDADES INTERDISCIPLINARES.....</b>	<b>12</b>
<b>5.- PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN .....</b>	<b>13</b>
<b>6.- CRITERIOS DE CALIFICACIÓN .....</b>	<b>14</b>
<b>7.- PÉRDIDA DE EVALUACIÓN CONTINUA.....</b>	<b>15</b>
<b>8.- CONTRIBUCIÓN DEL MÓDULO A FOMENTAR LA CULTURA Y EL ESPÍRITU EMPRENDEDOR EN EL ALUMNADO .....</b>	<b>16</b>
<b>9.- COMPETENCIAS Y CONTENIDOS DE CARÁCTER TRANSVERSAL ..</b>	<b>16</b>
<b>10.- PROCEDIMIENTO DE RECLAMACIÓN DE LAS CALIFICACIONES .</b>	<b>17</b>
<b>11.- ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON EL MÓDULO .....</b>	<b>17</b>
<b>12.- MEDIDAS PARA ESTIMULAR EL INTERÉS Y HÁBITO DE LECTURA Y LA CAPACIDAD DE EXPRESARSE CORRECTAMENTE.....</b>	<b>17</b>
<b>13.- CRITERIOS DE EVALUACIÓN DE LA PROGRAMACIÓN.....</b>	<b>18</b>

## **1.- COMPETENCIAS PROFESIONALES, PERSONALES Y SOCIALES DEL TÍTULO A LAS QUE CONTRIBUYE EL MÓDULO**

La formación del módulo contribuye a alcanzar las siguientes competencias del curso de especialización.

- 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.
- 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**

### **2.1.- OBJETIVOS GENERALES DEL TÍTULO QUE DESARROLLA EL MÓDULO**

La formación del módulo contribuye a alcanzar los objetivos generales:

- 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.
- 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.

## ***2.2.- OBJETIVOS EXPRESADOS EN RESULTADOS DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN***

### **1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección.**

Criterios de evaluación:

- a) Se han definido los principios generales de la organización en materia de ciberseguridad, que deben ser conocidos y apoyados por la dirección de la misma.
- b) Se ha establecido una normativa de protección del puesto de trabajo.

- c) Se ha definido un plan de concienciación de ciberseguridad dirigido a los empleados.
- d) Se ha desarrollado el material necesario para llevar a cabo las acciones de concienciación dirigidas a los empleados.
- e) Se ha realizado una auditoría para verificar el cumplimiento del plan de prevención y concienciación de la organización.

## **2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de detección y alertas de seguridad.**

Criterios de evaluación:

- a) Se ha clasificado y definido la taxonomía de incidentes de ciberseguridad que pueden afectar a la organización.
- b) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes.
- c) Se han establecido controles y mecanismos de detección e identificación de incidentes de seguridad física.
- d) Se han establecido controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a través de la investigación en fuentes abiertas (OSINT: Open Source Intelligence).
- e) Se ha realizado una clasificación, valoración, documentación y seguimiento de los incidentes detectados dentro de la organización.

## **3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar.**

Criterios de evaluación:

- a) Se han recopilado y almacenado de forma segura evidencias de incidentes de ciberseguridad que afectan a la organización.
- b) Se ha realizado un análisis de evidencias.
- c) Se ha realizado la investigación de incidentes de ciberseguridad.
- d) Se ha intercambiado información de incidentes, con proveedores y/o organismos competentes que podrían hacer aportaciones al respecto.
- e) Se han iniciado las primeras medidas de contención de los incidentes para limitar los posibles daños causados.

#### **4. Implementa medidas de ciberseguridad en redes y sistemas respondiendo a los incidentes detectados y aplicando las técnicas de protección adecuadas.**

Criterios de evaluación:

- a) Se han desarrollado procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes de ciberseguridad más habituales.
- b) Se han preparado respuestas ciberresilientes ante incidentes que permitan seguir prestando los servicios de la organización y fortaleciendo las capacidades de identificación, detección, prevención, contención, recuperación y cooperación con terceros.
- c) Se ha establecido un flujo de toma de decisiones y escalado de incidentes interno y/o externo adecuados.
- d) Se han llevado a cabo las tareas de restablecimiento de los servicios afectados por un incidente hasta confirmar la vuelta a la normalidad.
- e) Se han documentado las acciones realizadas y las conclusiones que permitan mantener un registro de “lecciones aprendidas”.
- f) Se ha realizado un seguimiento adecuado del incidente para evitar que una situación similar se vuelva a repetir.

## **5. Detecta y documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos.**

Criterios de evaluación:

- a) Se ha desarrollado un procedimiento de actuación detallado para la notificación de incidentes de ciberseguridad en los tiempos adecuados.
- b) Se ha notificado el incidente de manera adecuada al personal interno de la organización responsable de la toma de decisiones.
- c) Se ha notificado el incidente de manera adecuada a las autoridades competentes en el ámbito de la gestión de incidentes de ciberseguridad en caso de ser necesario.
- d) Se ha notificado formalmente el incidente a los afectados, personal interno, clientes, proveedores, etc., en caso de ser necesario.
- e) Se ha notificado el incidente a los medios de comunicación en caso de ser necesario.

### **3.- CONTENIDOS DEL MÓDULO Y DISTRIBUCIÓN TEMPORAL**

El módulo de Incidentes de Ciberseguridad (abreviando IC) se imparte en curso de especialización de Ciberseguridad en Entornos de Tecnologías de la Información. Dispone de una carga lectiva de 80 horas que se distribuyen a razón de 4 horas semanales durante aproximadamente 20 semanas.

#### **3.1 - CONTENIDOS DEL MÓDULO**

Los contenidos se dividen en tres bloques:

#### **Bloque I: Conceptos generales en materia de Incidentes de Ciberseguridad**

Se compone de las siguientes unidades:

##### **UNIDAD 1: Qué es un incidente de ciberseguridad**

- Definiciones
- Normativa de referencia
- Taxonomía de los incidentes

## **Bloque II: Estructuras y organismos de actuación de respuesta ante Incidentes de Ciberseguridad**

Se compone de las siguientes unidades:

### UNIDAD 2: Capacidad de respuesta ante incidentes

- Equipo de respuesta ante incidentes (ERI)
- SOC, CSIRT, CERT
- Equipo humano
- Otros actores involucrados
- Unidad de ciberinteligencia

### UNIDAD 3: Organización en materia de ciberseguridad

- Responsabilidades y roles dentro de la organización
- Esquema conceptual de la Seguridad de la información y la Protección de datos
- Directiva NIS

## **Bloque III: Gestión del ciclo de vida de Incidentes de Ciberseguridad**

Se compone de las siguientes unidades:

### UNIDAD 4: Ciclo de vida de la gestión de un incidente

- Estándares de referencia
- Fases del ciclo de vida de la gestión de un incidente

### UNIDAD 5: Etapa de Planificación

- Procedimientos de respuesta ante incidentes (POS). *Playbooks*.
- Intercambio de información
- Monitorización de eventos
- Simulacros (*Role-Play*) y ciberejercicios
- Prevención y concienciación en ciberseguridad

### UNIDAD 6: Detección del incidente y valoración

- Registro de incidentes de ciberseguridad
- Casos de uso



- Creación de reglas de correlación
- *Threat hunting*
- Notificación de incidentes
- Valoración y toma de decisiones

#### UNIDAD 7: Respuesta al incidente

- Contención del incidente
- Erradicación del incidente
- Recuperación
- Recopilación y análisis de evidencias
- Recursos materiales
- Estrategia de comunicación

#### UNIDAD 8: Lecciones aprendidas

- Informes de incidentes de ciberseguridad

### *3.2 - DISTRIBUCIÓN TEMPORAL*

#### **Primera evaluación**

- UT1: Qué es un incidente de ciberseguridad
- UT2: Capacidad de respuesta ante incidentes
- UT3: Organización en materia de ciberseguridad
- UT4: Ciclo de vida de la gestión de un incidente

#### **Segunda evaluación**

- UT5: Etapa de Planificación
- UT6: Detección del incidente y valoración
- UT7: Respuesta al incidente
- UT8: Lecciones aprendidas

### *4.- METODOLOGÍA DIDÁCTICA*

#### *4.1.- ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE*

Este módulo profesional contiene la formación necesaria para introducir al alumno en el ecosistema de la ciberseguridad, haciendo hincapié en los conceptos generales de la materia, los tipos de organización que conviven en este entorno y la gestión del ciclo de vida de los incidentes, tanto en la planificación como en la gestión de la crisis.

- Se impartirán los conceptos generales en materia de Incidentes de Ciberseguridad que serán transversales en todos los módulos del presente curso.
- Se darán a conocer las distintas estructuras de organización que coexisten en este ámbito para dar respuesta ante incidentes de ciberseguridad.
- Se explicarán las fases del ciclo de vida de los incidentes de ciberseguridad, manifestando las prácticas a llevar a cabo en las mismas: métodos y herramientas para la preparación, documentación y gestión para resolver una situación de crisis.

La metodología didáctica para seguir en el proceso de enseñanza-aprendizaje del módulo será la siguiente:

### **Exposición teórica**

En primer lugar, habrá una exposición, de cada unidad temática, que se estructurará de la siguiente forma:

- Introducción al tema y breve descripción de los contenidos a tratar.
- Explicación de contenidos.
- Exposición de dudas y sugerencias por parte de los alumnos.

### **Realización de actividades**

Se realizarán actividades en las que se abarcarán los conceptos teóricos, estos ejercicios se realizarán sobre papel.

La corrección de estos ejercicios se realizará mediante una puesta en común o bien mediante la exposición individual del trabajo realizado

La realización de actividades prácticas tendrá de manera habitual un componente de investigación personal por parte del alumno. También se utilizarán distintas técnicas, herramientas o métodos impartidos en clase para la realización de las prácticas.

Será importante inculcar en el alumno la capacidad para, dado un objetivo, encontrar por su cuenta, y en base a sus conocimientos, los métodos y herramientas necesarios para conseguir llevarlo a cabo.

### **Desarrollo actitudinal en el aula**

Aquellos alumnos que lleguen tarde a clase, sin motivo justificado y/o en reiteradas ocasiones **se computarán cómo retraso de asistencia** aplicándose lo dispuesto en el **Reglamento de Régimen Interior** del Centro.

El profesor mantendrá un sitio web de la asignatura donde estarán disponibles:

- Los recursos tanto teóricos como prácticos referentes al módulo.
- Un diario con todo lo acontecido en cada clase y con las tareas que los alumnos deben realizar.
- Una red social para el intercambio de mensajes entre profesor y alumnos.

Este medio será también el utilizado por los alumnos para entregar la resolución de los ejercicios y comprobar la evolución continua de sus calificaciones.

#### *4.2.- ATENCIÓN A LA DIVERSIDAD*

Para atender a los alumnos con necesidades educativas especiales se trabajará estrechamente con el Departamento de Orientación del Instituto siguiendo sus recomendaciones y aplicación siempre que sea posible.

Para aquellos alumnos que presenten discapacidades físicas, las soluciones en este caso pueden pasar por:

- Posición del alumno adelantada en clase.
- Monitores de grandes dimensiones y teclados adaptados.
- Uso de auriculares y amplificadores de sonido.
- Posibilidad de aumentar los tiempos de entrega de ciertas actividades.

En cualquier caso, dadas las circunstancias particulares del alumno con necesidades, podrán tomarse medidas específicas para permitir el correcto desarrollo de las actividades de enseñanza-aprendizaje planteadas

#### *4.3.- MATERIALES Y RECURSOS DIDÁCTICOS*

Se considera necesario un aula laboratorio para poder realizar las prácticas de instalación y configuración de redes dotada de:

- Conexión a Internet de banda ancha.

- Ordenadores

**Otros materiales que se requieren son:**

- Pizarra blanca para la exposición de conceptos teóricos.
- Manuales técnicos
- Libros de consulta del departamento.
- Equipos informáticos y servidores.
- Apuntes proporcionados por el profesor.

***4.4.- LA UTILIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC)***

El nivel de certificación TIC que posee el centro le confiere una serie de capacidades en lo referente a la aplicación de las tecnologías de la información y comunicación, de metodologías activas, y una serie de recursos materiales y humanos que hacen efectiva la integración de las TIC en todos los niveles de concreción curricular.

Debido a la propia naturaleza de las enseñanzas de los Ciclos Formativos de Informática, esta integración es directa, puesto que estas enseñanzas emplean las TIC en absolutamente todas las materias/módulos, siendo medio y fin del proceso didáctico.

***4.5.- ACTIVIDADES INTERDISCIPLINARES***

El módulo de Incidentes de Ciberseguridad requiere de conocimientos tanto teóricos como prácticos en todos los ámbitos de la informática (desde la programación a los sistemas operativos, pasando por las redes o el funcionamiento de los dispositivos hardware), así como de otras disciplinas como son: todo lo referente a normativas y estándares, la documentación y la redacción de informes técnicos, la investigación acerca de cuestiones técnicas, incluyendo la búsqueda de información, la criba y el filtrado de fuentes de información, el resumen y la síntesis, etc.

El módulo de Incidentes de Ciberseguridad también introduce los conceptos generales de ciberseguridad que se contemplarán en el resto de módulos del ciclo.

## 5.- *PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN*

Los instrumentos empleados para realizar la evaluación son:

- La observación directa del alumno en el aula.
- El análisis de las actividades realizadas por el alumno tanto en clase como fuera de ella.
- La realización y análisis de pruebas individuales.

Las faltas de asistencias justificadas o no justificadas del alumno no darán derecho a la repetición o recuperación de las actividades programadas para esa jornada.

### Actividades/prácticas

Las actividades podrán ser guiadas o no guiadas y deberán entregarse de forma individual en la fecha indicada. La realización de las actividades es obligatoria, y por tanto serán necesarias para poder superar y aprobar el módulo. Toda práctica entregada fuera de la fecha límite deberá entregarse dentro de un plazo razonable pudiendo obtener así una nota máxima de 5 sobre 10. Para completar las actividades, los alumnos deberán exponer en ciertas ocasiones los resultados de sus trabajos oralmente ante la clase o ante el profesor.

Para la calificación de las actividades se tendrá en cuenta:

- El grado de autoría de la misma.
- La corrección y completitud del trabajo.
- La buena presentación.
- La asimilación de los contenidos y procedimientos trabajados.
- El interés y esfuerzo demostrados por el alumno, así como el tiempo empleado en su ejecución.

La evaluación de estas actividades se realizará tanto por observación directa como a través de los documentos escritos o en formato electrónico aportados por el alumno. El profesor puede requerir al alumno de ciertas explicaciones acerca de las actividades realizadas.

### Pruebas individuales

Las pruebas individuales podrán ser de 4 tipos:

- Escritas (en papel o en ordenador)
- Orales.

- Proyecto integrador.

Las pruebas escritas podrán tener 2 partes: una teórica y una práctica. La primera podrá ser de tipo test, de preguntas cortas o de preguntas a desarrollar, y podrá cerrar el acceso a la parte práctica (será necesario obtener como mínimo un 5). La parte práctica también requerirá de un 5 como mínimo para ser considerada superada.

Las pruebas orales se realizarán cuando el profesor lo considere oportuno, y tendrán una duración variable en función de la materia (entre 15" y 30") y se podrá preguntar al alumno cualquier contenido teórico o práctico del módulo.

Los proyectos integradores servirán para la evaluación de un caso práctico en el que se evaluarán contenidos vistos en el módulo, y en ocasiones, contenidos y técnicas nuevas que el alumno deberá estudiar por su cuenta. En ocasiones este proyecto podrá servir de nexo entre varios módulos del curso de especialización, de modo que se permita al alumno experimentar de manera integral los contenidos vistos a lo largo de todo el curso de especialización.

## 6.- CRITERIOS DE CALIFICACIÓN

Para poder superar la asignatura en primera convocatoria ordinaria es necesario:

- Que al finalizar el curso la media global de las actividades sea igual o superior a 5 puntos sobre 10.
- Que en todas y cada una de las pruebas individuales la calificación obtenida sea de al menos 5 puntos sobre 10.
- Que la media final del curso sea al menos de 5 puntos sobre 10.

La calificación o media de cada evaluación y del final del curso vendrá dada en función de los siguientes criterios con una ponderación tal y como se indica a continuación:

- Pruebas individuales: 70%.
- Prácticas, trabajos y ejercicios propuestos: 30%.

En caso de no haberse realizado en cualquiera de las evaluaciones ningún trabajo, práctica o ejercicio, ese 30% de ponderación, pasará a contabilizarse en el primer apartado de *Pruebas individuales*, **pasando éste a ponderar un 100%**. Del mismo modo, en caso de no realizarse ninguna prueba individual en una

evaluación, la totalidad de la nota vendrá dada por las calificaciones obtenidas en las prácticas, trabajos y ejercicios propuestos.

La utilización de medios **no autorizados** en las pruebas individuales (apuntes, chuletas, medios de comunicación, ayuda de otro compañero, etc.) **supondrá una calificación de 0 puntos** en la prueba para los alumnos implicados.

Tanto las actividades como las pruebas individuales tendrán pesos que computarán de forma distinta para obtener las medias de ambos apartados en función del caso concreto.

## IA Y PLAGIO

- El engaño al profesor (copiar en un examen o intentarlo, utilizar cualquier medio NO indicado por el profesor sin permiso, etc.), hará que el alumno suspenda esa prueba con un cero. En el concepto de copia, se incluye el uso de tecnologías basadas en autogeneración de código, como pueden ser aplicaciones basadas en IA. Algunos ejemplos serían ChatGPT o Copilot.
- Todas las pruebas escritas, orales, individuales o en grupo que hayan sido copiadas en parte o en su totalidad, serán calificadas con cero puntos.
- En caso de Sospecha de plagio:
  - Se podrá solicitar al alumnado, sin previo aviso, la defensa de cualquiera de los instrumentos de evaluación que haya presentado o esté realizando para demostrar su autoría y comprensión.
  - La calificación final de cualquier instrumento evaluable estará sospechas de plagio, pendiente de una defensa oral por parte del alumno cuando el profesor lo considere necesario. La defensa se realizará en presencia de al menos tres miembros del equipo docente, siendo uno el profesor implicado. Si el equipo docente, presente en la defensa, determina por mayoría simple que el instrumento evaluable no es de su autoría total o parcial, tendrá un 1 en la evaluación afectada en caso de ser trimestral, o un 0 si es de recuperación final.

## 7.- PÉRDIDA DE EVALUACIÓN CONTINUA

### Criterios pérdida de evaluación continua

Para que el alumno pueda acogerse a la evaluación continua es necesario que las faltas de asistencia no superen el 10% para el caso de faltas injustificadas. El departamento tratará de forma individual aquellos casos de carácter excepcional, siempre y cuando se aleguen razones “de peso” y se acompañen de los debidos documentos que justifiquen esta medida.

La pérdida de evaluación continua será comunicada por el profesor titular del módulo al tutor del grupo y también al alumno implicado.

### **Procedimiento de evaluación alternativo a la evaluación continua**

Aquellos alumnos que pierdan el derecho a la evaluación continua deberán realizar:

- Una prueba individual planteada por el profesor en la sesión de evaluación final (ya sea en primera o en segunda convocatoria).
- Opcionalmente y según criterio del profesor, un proyecto que abarque todos los contenidos del módulo y que será asignado por el profesor de manera individual a cada alumno 15 días antes de la prueba individual comentada en el punto anterior. El alumno deberá defender este proyecto el mismo día que realice la prueba individual.

La calificación del módulo vendrá dada por la media aritmética de ambos apartados en una escala de 1 a 10. Se considerará que el alumno ha superado el módulo en caso de que obtenga una nota igual o superior al 5 en ambos apartados.

### **8.- *CONTRIBUCIÓN DEL MÓDULO A FOMENTAR LA CULTURA Y EL ESPÍRITU EMPRENDEDOR EN EL ALUMNADO***

Durante la impartición del módulo se buscará fomentar el espíritu emprendedor del alumno a través de las diferentes actividades que se llevarán a cabo; para ello, se tratará de fomentar su autonomía en la resolución de las diferentes prácticas que se propongan, y se propondrán debates que permitan intercambiar opiniones entre los alumnos.

Al mismo tiempo, se tratará de abrir al alumno, dentro de lo posible, al mundo profesional de la ciberseguridad, dando a conocer recursos y fuentes de información pública, de modo que pueda aprender y actualizar conocimientos sobre incidentes de ciberseguridad de una forma autodidacta.

### **9.- *COMPETENCIAS Y CONTENIDOS DE CARÁCTER TRANSVERSAL***

En este apartado se desarrollarán los elementos transversales que se llevarán a cabo durante el curso escolar, de forma complementaria al resto de contenidos propios del módulo profesional. Se van a destacar los siguientes:

#### **Ética**

- Debido al carácter especial del módulo se tendrá muy en cuenta la reflexión personal acerca de las acciones que llevamos a cabo, no sólo



desde el punto de vista legal de nuestros actos, sino también desde una perspectiva ética y de la reflexión de los principios morales que nos permiten o nos impiden utilizar nuestros conocimientos.

### **Igualdad**

- Para la creación de grupos de trabajo solo se tendrán en cuenta criterios académicos, en ningún momento se diferenciarán personas por su género, diversidad, etc.

### **Valores sociales**

- El ambiente de trabajo deberá responder a normas básicas de respeto entre personas. La opinión de cada integrante de la clase deberá ser escuchada, respetada y valorada. El trabajo en equipo es clave en el desarrollo profesional propuesto en esta programación didáctica y se realizará con un velo de respeto interpersonal.

## ***10.- PROCEDIMIENTO DE RECLAMACIÓN DE LAS CALIFICACIONES***

Las reclamaciones de las calificaciones trimestrales se ajustarán a lo establecido en la *Programación Didáctica del Departamento*

## ***11.- ACTIVIDADES COMPLEMENTARIAS Y EXTRAESCOLARES RELACIONADAS CON EL MÓDULO***

No se programa ninguna actividad complementaria o extraescolar fuera de las recogidas en la *Programación Didáctica de Departamento*.

## ***12.- MEDIDAS PARA ESTIMULAR EL INTERÉS Y HÁBITO DE LECTURA Y LA CAPACIDAD DE EXPRESARSE CORRECTAMENTE***

### **Interés y hábito de lectura**

- El profesor recomendará la lectura de artículos de periódicos, revistas o documentos en Internet sobre asuntos de interés. Posteriormente, se comentarán en grupo.
- A lo largo del curso el profesor recomendará libros relacionados con los temas a tratar.

### **Capacidad de expresarse correctamente**

- El profesor corregirá las expresiones incorrectas que los alumnos utilicen en el aula.

- En las pruebas escritas el profesor señalará a los alumnos las faltas de ortografía, de significado o de sintaxis cometidas.

### **13.- CRITERIOS DE EVALUACIÓN DE LA PROGRAMACIÓN**

Para la realización de una perfecta evaluación del proceso de enseñanza-aprendizaje es imprescindible evaluar la propia programación, para lo cual se tendrán en cuenta los siguientes aspectos:

- Grado de cumplimiento en la impartición de los contenidos.
- Porcentaje (real) de los alumnos que superan el módulo.
- Evaluación subjetiva, por parte del profesor, de los materiales y recursos didácticos.
- Evaluación subjetiva, por parte del alumnado, de los materiales, apuntes, actividades de enseñanza-aprendizaje o métodos y herramientas de evaluación.

En Ávila, a 11 de octubre de 2024

*Fdo. Alejandra San Segundo Hernández*