**Módulo: Seguridad Informática**

## *ADAPTACIÓN POR CONFINAMIENTO*

Se parte de la base que el alumnado dispone de un PC y conexión a internet para la realización de las tareas y actividades que se le proponga a lo largo del curso, puesto que la Junta de Andalucía garantiza que así sea y el Centro ha estado facilitando recursos para ello.

Dada la naturaleza de las materias relacionadas con el Departamento de Informática y el actual uso constante de la plataforma Moodle del Centro (https://www.iesmarserena.es/moodle) para el desarrollo de las diversas unidades, con la actual semi-presencialidad a partir de 3º ESO y en 1º de SMR se está cubriendo de forma simultánea las adaptaciones para confinamientos puesto que está siendo común que sea habitual que uno o varios alumnos sigan las clases desde casa.

Las programaciones didácticas de este departamento están ideadas para poderse llevar a cabo de manera online en todas las materias y módulos, pudiendo modificar el tipo de ejercicio, práctica o prueba acorde a la no-presencialidad de uno o varios alumnos, o incluso del propio profesorado.

Para el alumnado de 2º de SMR y de 1º de ESO donde el alumnado está en una modalidad presencial, el profesorado igualmente utiliza la plataforma Moodle del Centro y dispone de la facilidad de disponer de actividades sustitutorias y complementarias para escenarios de confinamientos acordes a cada una de las unidades.

Entre otras, es común tanto de forma presencial como semi-presencial y online el uso de herramientas utilizables a distancia desde URL comúnmente utilizadas en otros ciclos de informática como:

- https://www.sololearn.com
- https://www.netacad.com/es
- https://openwebinars.net

A la hora de calificar al alumnado, en el caso de la ESO se establece por norma general la entrega de ejercicios prácticos que son realizables desde casa. En el caso de otras materias y módulos, y de la necesidad en algunos temas o unidades de realizar exámenes, los mismos se podrán realizar de forma online a través de diversas plataformas online, dada la naturaleza de las materias y módulos del Departamento de Informática, más asociadas a las nuevas tecnologías y el uso del PC para su realización.

En caso de confinamiento, al alumnado se le podrá flexibilizar las entregas de trabajos y prácticas, y la realización de los exámenes pertinentes, ambos en lo que a fecha de realización se refiere en casos excepcionales, tales como enfermedad asociada al COVID-19 o a cualquier otra, siguiendo una justificación médica requerida como ya ocurría en cursos pasados.

En cualquier caso, la ponderación de las distintas unidades didácticas no se verá alterada dada la planificación inicial y la posibilidad de seguir las clases de forma online.

## *TEMPORALIZACIÓN*

Según la Orden de 7 de Julio de 2009 al módulo de Seguridad Informática le corresponden para su desarrollo 105 horas repartidas en 5 horas semanales durante dos trimestres (21 semanas aproximadamente).

Los contenidos y la temporalización pueden ser modificados en función de las necesidades del alumnado.

A continuación mostramos la temporalización de los contenidos distribuidos por periodos lectivos (equivalentes a horas).

| U.T | Contenidos | 1ª Ev. | 2ª Ev. | Total |
|---|---|---|---|---|
| 1 | Introducción a la Seguridad Informática | 8 | | 8 |
| 2 | Criptografía | 8 | | 16 |
| 3 | Gestión de dispositivos de almacenamiento | 8 | | 24 |
| 4 | Aplicación de medidas de seguridad pasiva | 20 | | 44 |
| 5 | Software malicioso | 8 | | 52 |
| 6 | Sistemas de identificación | | 14 | 66 |
| 7 | Privacidad de la información | | 17 | 83 |
| 8 | Seguridad en redes | | 17 | 100 |
| | TOTAL | 52 | 48 | 100 |

Las cinco horas restantes hasta completar las 105 horas del módulo estarán reservadas para posibles actividades extraescolares o complementarias.

## *PLAN DE REPETIDORES*

Dado que no hay alumnos que suspendieron curso en el ciclo de grado medio de Sistemas Microinformáticos y Redes, no procede este punto.

## *PLAN DE RECUPERACIÓN DE MATERIAS PENDIENTES DE EVALUACIÓN POSITIVA*

En el ciclo formativo no existen las materias pendientes.

## *RECUPERACIÓN DE OBJETIVOS NO ALCANZADOS*

Existirán distintas actividades teórico/prácticas de recuperación antes de la evaluación trimestral, que englobe una o varias unidades de trabajo que atenderán a la consecución de los objetivos y/o contenidos no superados.

Si una vez realizadas todas las recuperaciones, hubiera algún trimestre suspenso, se realizará un examen final en junio que englobará la teoría y práctica no superada.

## *CRITERIOS DE EVALUACIÓN*

La evaluación irá encaminada a determinar la medida en que el alumno o alumna consiga llegar a los objetivos establecidos, teniendo en cuenta para ello, los criterios de evaluación, además del tramo recorrido por éstos desde el estado inicial hasta el finalmente alcanzado.

| Valoración de los aprendizajes específicos del módulo | Ponderación |
|---|---|
| Actividades y/o prácticas y/o tareas de refuerzo y/o consolidación | 40 % |
| Pruebas objetivas escritas y/o prácticas. | 60 % |

Las actividades, las prácticas y las pruebas se valorarán de 0 a 10.

Las actividades y las prácticas podrán ser realizadas de forma individual o en grupo, dependiendo del tipo de actividad, su entrega es obligatoria. En el caso de obtener una calificación negativa en alguna de ellas o de no haberla entregada, se entregarán antes de la evaluación. La valoración de las actividades fuera de plazo será el 50%.

Existirán distintas pruebas teórico-prácticas a lo largo de cada trimestre, que englobe una o varias unidades de trabajo que atenderán a la consecución de los objetivos programados en el módulo y cuyo peso en la nota de cada evaluación irá relacionado con el número de sesiones/horas utilizadas. En el caso de no superar alguna de ellas, antes de la evaluación trimestral se realizará una recuperación de los contenidos no superados.

Para considerar una prueba, actividad o práctica aprobada el alumnado ha de obtener en ella una nota de 5 sobre 10.

**Evaluación final**:

Si una vez realizadas todas las recuperaciones, hubiera algún bloque suspenso, se realizará un examen final en mayo/junio que englobará la teoría y práctica no superada. La fecha del examen será determinada por Jefatura de Estudios.

La nota del módulo de Formación en Centros de Trabajo será: Apto/No Apto.

| **Primera evaluación final** | |
|---|---|
| 1er curso | Media aritmética de las calificaciones obtenidas en la primera, segunda y tercera evaluación |
| 2º curso | Media aritmética de las calificaciones obtenidas en la primera y segunda evaluación |
| **Segunda evaluación final** | |
| 1er curso | Todos aquellos alumnos y alumnas que no consigan superar el módulo en la **primera evaluación final de mayo**, tendrán la oportunidad de hacerlo en el mes de **junio**. |
| 2º curso | Todos aquellos alumnos y alumnas que no consigan superar el módulo en la **primera evaluación final de marzo**, tendrán la oportunidad de hacerlo en el mes de **junio**. |
| En dichas pruebas **la calificación de 5 supondrá el aprobado** en el módulo. | |

## *ADAPTACIONES*

En el presente curso académico 2020-2021, informados por el Departamento de Orientación o mediante la aplicación de medidas preventivas para la detección de necesidades atendiendo a los distintos ritmos de aprendizajes:

- Evaluación inicial.
- Análisis de los trabajos realizados.
- Actividades iniciales sobre meta-aprendizaje: expiración de métodos de trabajo de las unidades de trabajo, destrezas básicas para estudiarlas y procedimientos de control sobre el propio aprendizaje.
- Medidas ordinarias: Actividades de refuerzo y complementarias. Se diseñarán actividades que irán encaminadas a facilitar que el alumnado con dificultades puedan encontrar la forma de enfrentarse a las tareas.
- Para alumnos con problemas de asistencia se les animará a que sigan estudiando y siguiendo el curso lectivo desde el aula virtual. Se prestará especial atención a la optimización de la comunicación profesor-alumno utilizando cauces previamente establecidos (correo interno, mensajes instantáneos, videoconferencia, etc).
- En aquellos casos en que se detecte que algún alumno o alumna presenta dificultades de tipo cognitivo o procedimental se le podrán proponer actividades o recursos específicos encaminados a subsanar tales dificultades.

## *TABLA CON CONTENIDOS - CRITERIOS DE EVALUACIÓN - PONDERACIÓN - INSTRUMENTOS DE EVALUACIÓN*

| UNIDAD DE TRABAJO | OBJETIVOS | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN | INSTRUMENTOS DE EVALUACIÓN | PESO |
|---|---|---|---|---|---|
| UT 1: Introducción a la Seguridad Informática | • Saber los motivos de la seguridad informática y valorar la importancia de mantener un sistema seguro.<br>• Conocer y saber diferenciar los tipos de seguridad existentes.<br>• Saber cuáles son los objetivos de la seguridad.<br>• Conocer y distinguir los tipos de amenazas.<br>• Conocer la necesidad de proteger físicamente los sistemas informáticos y controlar sus condiciones ambientales.<br>• Conocer las leyes y normas relativas a la seguridad informática. | 1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.<br><br>5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento. | • Conoce la importancia de proteger los equipos de un sistema informático.<br>• Conoce la importancia de mantener la información de un sistema informático segura.<br>• Identifica los elementos de seguridad física y seguridad lógica en un sistema informático.<br>• Identifica los elementos de seguridad activa y seguridad pasiva en un sistema informático.<br>• Conoce los objetivos de la seguridad informática y los relaciona con las amenazas.<br>• Conoce y sabe aplicar la legislación vigente referente a la seguridad informática. | Actividades propuestas: 40 %<br>• Casos prácticos para identificar los diferentes elementos y objetivos de la seguridad informática.<br>• Trabajo de investigación sobre la legislación vigente referente a la seguridad informática.<br>Prueba objetiva: 60% | 8% |
| UT 2: Criptografía | • Conocer las razones que hacen necesaria la criptografía para afianzar la seguridad informática.<br>• Conocer la evolución histórica de la criptografía y los tipos de criptografía a través de la historia.<br>• Conocer los tipos de cifrado actuales.<br>• Conocer las principales funciones y algoritmos de la criptografía moderna. | 2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información. | • Conoce las razones que hacen necesaria la criptografía para afianzar la seguridad informática.<br>• Conoce la evolución histórica de la criptografía.<br>• Conoce diferentes tipos de cifrado actuales.<br>• Conoce las principales aplicaciones de la criptografía moderna y sus algoritmos y funciones. | Actividades propuestas: 40 %<br>• Casos prácticos para reconocer las necesidades y las aplicaciones reales de la criptografía en la seguridad informática<br>Prueba objetiva: 60% | 8% |

| UNIDAD DE TRABAJO | OBJETIVOS | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN | INSTRUMENTOS DE EVALUACIÓN | PESO |
|---|---|---|---|---|---|
| UT 3:<br>Gestión de dispositivos de almacenamiento | • Conocer la importancia del almacenamiento de la información.<br>• Conocer los diferentes factores a tener en cuenta a la hora de elegir el tipo almacenamiento.<br>• Conocer los diferentes tipos de almacenamiento.<br>• Saber trabajar con discos dinámicos.<br>• Conocer el concepto de volumen y el concepto de imágenes de respaldo.<br>• Saber administrar las cuotas de disco.<br>• Conocer la importancia de las copias de seguridad.<br>• Saber realizar copias de seguridad e imágenes de respaldo. | 2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información. | • Conoce la importancia del almacenamiento de la información, las copias de seguridad y los distintos tipos de almacenamiento.<br>• Identifica el sistema de almacenamiento idóneo dependiendo de los factores ambientales, económicos,...<br>• Conoce el concepto de volumen, y sabe diferenciar entre volumen dinámico y volumen básico.<br>• Conoce las tecnologías de almacenamiento redundante y distribuido.<br>• Identifica y aplica el tipo de almacenamiento, redundante o distribuido, según las necesidades del caso.<br>• Conoce los distintos tipos de copias de seguridad, la importancia de las mismas y las sabe realizar.<br>• Sabe realizar imágenes de respaldo. | Actividades propuestas: 40 %<br>• Casos prácticos para reconocer los riesgos a los que se enfrenta la información y las medidas más adecuadas de protección.<br>• Configurar imágenes de respaldo, copias de seguridad, discos redundantes y distribuidos, volúmenes dinámicos y básicos en diferentes sistemas operativos.<br>Prueba objetiva: 60% | 20% |

| UNIDAD DE TRABAJO | OBJETIVOS | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN | INSTRUMENTOS DE EVALUACIÓN | PESO |
|---|---|---|---|---|---|
| UT 4: Aplicación de medidas de seguridad pasiva | • Conocer las diferencias entre seguridad activa y pasiva.<br>• Conocer los elementos físicos de la seguridad pasiva.<br>• Conocer las mejores características para la ubicación física de los equipos informáticos.<br>• Conocer la necesidad y características de los sistemas de alimentación ininterrumpida.<br>• Conocer la importancia de otros elementos importantes para evitar perder el sistema informático y su información en caso de cualquier contingencia | 1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades. | • Diferencia los elementos de seguridad activa y seguridad pasiva en un sistema informático.<br>• Identifica los elementos de la seguridad física pasiva.<br>• Selecciona ubicaciones idóneas para los equipos informáticos, así como determina sus condiciones ambientales.<br>• Sabe seleccionar los puntos de aplicación de los sistemas de alimentación ininterrumpida y las características de éstos. | Actividades propuestas: 40 %<br>• Casos prácticos para reconocer los diferentes elementos de la seguridad activa y pasiva y física.<br>• Casos prácticos para diseñar entornos seguros para la instalación de equipos informáticos.<br>• Casos prácticos para reconocer los riesgos físicos a los que se enfrentan los equipos.<br>Prueba objetiva: 60% | 8% |
| UT 5: Software malicioso | • Saber qué es el software malintencionado.<br>• Conocer y saber diferenciar los distintos tipos de software malintencionado y sus efectos sobre el sistema informático.<br>• Conocer las medidas de protección y distinguir unas de otras.<br>• Saber utilizar las herramientas de protección y desinfección del sistema informático. | 3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático. | • Conoce qué es y sabe diferenciar los distintos tipos de software malintencionado y sus efectos sobre el sistema informático.<br>• Conoce las medidas de protección y las asocia a los distintos tipos de software malintencionado.<br>• Sabe utilizar las herramientas de protección y desinfección del sistema informático y las relaciona a los distintos tipos de software malintencionado.<br>• Configura correctamente distintas herramientas de protección del sistema. | Actividades propuestas: 40 %<br>• Casos prácticos para aplicar medidas de protección contra software malicioso.<br>• Casos prácticos de desinfección y configuración de herramientas de protección contra software malicioso.<br>Prueba objetiva: 60% | 9% |

| UNIDAD DE TRABAJO | OBJETIVOS | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN | INSTRUMENTOS DE EVALUACIÓN | PESO |
|---|---|---|---|---|---|
| UT 6:<br>Sistemas de identificación | • Conocer los diferentes sistemas de control de acceso al sistema informático.<br>• Conocer los distintos sistemas de identificación digital.<br>• Saber configurar y utilizar los elementos de identificación digital. | 1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades. | • Identifica los diferentes sistemas de control de acceso al sistema informático.<br>• Conoce los distintos sistemas de identificación digital.<br>• Sabe configurar y utilizar la firma electrónica y el certificado digital. | Actividades propuestas: 40 %<br>• Casos prácticos para identificar la necesidad de uso de los sistemas de identificación.<br>• Casos prácticos que requieran de uso de la firma electrónica y el certificado digital.<br>Prueba objetiva: 60% | 14% |
| UT 7:<br>Privacidad de la información | • Conocer los diferentes métodos para asegurar la privacidad de la información.<br>• Conocer los principales fraudes y robos de la información.<br>• Conocer la importancia de una buena política de contraseñas.<br>• Saber aplicar la política de contraseñas.<br>• Conocer la importancia de los registros del sistema.<br>• Saber obtener información de los registros del sistema. | 4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico. | • Conoce los diferentes protocolos relacionados con la transmisión de información de forma segura.<br>• Sabe configura la seguridad de diferentes tipos de navegadores.<br>• Conoce los diferentes métodos para asegurar la privacidad de la información y sabe establecer conexiones seguras<br>• Conoce los principales fraudes informáticos y robos de la información.<br>• Conoce la importancia de una buena política de contraseñas y sabe aplicarlas.<br>• Conoce la importancia de los registros del sistema y sabe tratar la información recogida en ellos. | Actividades propuestas: 40 %<br>• Casos prácticos para conocer los principales problemas de privacidad de la información y aplicar las medidas necesarias para solventarlos.<br>Prueba objetiva: 60% | 17% |

| UNIDAD DE TRABAJO | OBJETIVOS | RESULTADOS DE APRENDIZAJE | CRITERIOS DE EVALUACIÓN | INSTRUMENTOS DE EVALUACIÓN | PESO |
|---|---|---|---|---|---|
| UT 8:<br>Seguridad en redes | • Comprender la necesidad de la seguridad especial en las redes inalámbricas.<br>• Saber monitorizar el tráfico dentro de una red.<br>• Saber utilizar las listas de control de acceso para proteger nuestro sistema.<br>• Conocer la utilidad y saber configurar los cortafuegos.<br>• Conocer qué son los proxys y los diferentes tipos. | 4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico. | • Comprende la especial atención a la seguridad en las redes inalámbricas.<br>• Conoce los diferentes tipos de redes inalámbricas y las medidas de seguridad a aplicar a cada una.<br>• Sabe monitorizar el tráfico de una red.<br>• Sabe configurar y utilizar las listas de control de acceso en diferentes sistemas operativos.<br>• Conoce la utilidad y sabe configurar cortafuegos.<br>• Conoce que es un proxy y sus diferentes tipos.<br>• Sabe configurar un proxy dependiendo del uso al que está destinado. | Actividades propuestas: 40 %<br>• Casos prácticos para reconocer las vulnerabilidades de seguridad en redes y aplicar las medidas de seguridad adecuadas en cada caso.<br>Prueba objetiva: 60% | 17% |