IES CALDERÓN DE LA BARCA
PINTO
MADRID

CONSEJERÍA DE EDUCACIÓN, JUVENTUD Y DEPORTE
Comunidad de Madrid

Familia Profesional Informática y Comunicaciones

Ciclo Formativo de Grado Medio: Sistemas Microinformáticos y Redes

Módulo: Seguridad Informática
Curso 2021-2022

ANEXO. Hoja informativa para las familias.

Índice

Introducción 3

1. Contenidos 3

2. Metodología Didáctica 5

2.1. Principios rectores. 5

2.2. Estrategias de Enseñanza–Aprendizaje. 6

3. Criterios de Evaluación 7

4. Procedimientos de Evaluación 9

5. Sistema de Recuperación de evaluaciones pendientes 10

6. Criterios de Calificación 10

7. Actividades de Recuperación para alumnos con materias pendientes y profundizaciones y refuerzos para lograr dicha recuperación 11

7.1. Prueba extraordinaria de junio 11

8. Materiales, textos y recursos didácticos 11

9. Adaptación a los distintos escenarios planteados por la Comunidad de Madrid en función de la evolución de la crisis sanitaria por COVID-19 12

Introducción

El Decreto 34/2009, de 2 de abril, establece para la Comunidad de Madrid el currículo del ciclo formativo de grado medio correspondiente al título de Técnico en Sistemas Microinformáticos y Redes, al que pertenece el módulo profesional de Seguridad Informática. Este módulo contribuye a alcanzar la competencia general del título, así como las competencias profesionales, personales y sociales recogidas en el Real Decreto 1691/2007, de 14 de diciembre. El módulo en cuestión constituye la unidad de competencia UC0959_2 (Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos) del Catálogo Nacional de Cualificaciones Profesionales, que se adquieren con el ciclo formativo. De igual forma, en conjunto con otros módulos constituye las unidades de competencia UC0958_2 (Ejecutar procedimientos de administración y mantenimiento en el software base y de aplicación de cliente) y UC0957_2 (Mantener y regular el subsistema físico en sistemas informáticos).

La siguiente programación didáctica recoge las características de los procesos de enseñanza-aprendizaje del módulo.

Título	Técnico en Sistemas Microinformáticos y Redes
Real Decreto del Título	R.D. 1691/2007, de 14 de diciembre (B.O.E. 17/01/2008)
Decreto del Título en la Comunidad de Madrid	D. 34/2009 (B.O.C.M. 20/04/2009)
Familia Profesional	Informática y Comunicaciones
Grado	Grado Medio
Código del Ciclo	IFCM01
Ciclo Formativo	Sistemas Microinformáticos y Redes
Clasificación Internacional Normalizada de la Educación (Referente Europeo)	CINE-3
Código del Módulo	0226
Denominación del Módulo Profesional	Seguridad Informática
Horas Curriculares	85
Curso	2º
Horas Semanales	4

1. Contenidos

UT 1: LA SEGURIDAD INFORMÁTICA

- Visión global de la seguridad informática
- Objetivos de la seguridad informática
- Seguridad física y lógica
- Seguridad activa y pasiva
- Amenazas
- Auditoría de seguridad
- Servicios y mecanismos de seguridad

UT 2: SEGURIDAD FÍSICA PASIVA Y ELÉCTRICA

- Ubicación del CPD
- Centro de respaldo

- SAI/UPS

UT 3: SEGURIDAD EN LOS DISPOSITIVOS DE ALMACENAMIENTO
- Almacenamiento redundante y distribuido: RAID
- Almacenamiento en los medios de almacenamiento online; DAS, NAS, SAN
- Clusters

UT 4: SEGURIDAD PASIVA: BACKUPS
- Backup de datos (copias de seguridad)
- Imagen del sistema

UT 5: CRIPTOGRAFÍA
- Métodos para asegurar la privacidad de la información transmitida. Criptografía clásica.
- Criptografía: Cifrado de clave secreta (simétrica).
- Criptografía: Cifrado de clave pública (asimétrica).
- Criptografía: Criptografía híbrida.
- Criptografía: Funciones de mezcla o resumen (hash).
- Firma electrónica: Certificados digitales.
- Firma electrónica: DNI electrónico.
- Firma electrónica: Distribución de claves. PKI (Public Key Infrastructure).

UT 6. ATAQUES Y VULNERABILIDADES
- La seguridad en los sistemas. El ataque informático.
- Vulnerabilidades del sistema

UT 7. GESTIÓN ACTIVA DE LA SEGURIDAD: SISTEMA OPERATIVO Y APLICACIONES
- La defensa en profundidad y la seguridad activa
- La caja del ordenador
- La BIOS
- El Boot Manager
- Las particiones y su cifrado
- Identificación y autentificación: password, tarjeas y biometría
- Listas de control de accesos
- Elevación de privilegios
- Cuotas
- Monitorización del sistema

UT 8. SOFTWARE MALICIOSO
- Malware y antivirus
- Clasificación del malware
- Herramientas antimalware
- Congelación

UT 9. SEGURIDAD EN REDES
- Seguridad en redes
- Ataque a una red
- Ataque de denegación de servicio
- Seguridad perimetral y sistemas de detección de intrusos

- Protocolos seguros
- Seguridad en redes inalámbricas

UT 10. IMPLANTACIÓN DE LA SEGURIDAD PERIMETRAL
- Elementos básicos en la seguridad perimetral.
- Seguridad en la red corporativa
- Seguridad y monitorización. Herramientas preventivas y paliativas. Ataques.
- Arquitecturas físicas para la red perimetral.
- El cortafuegos.
- Iptables y Netfilter
- Proxys
- Dispositivos UTM
- Dispositivos adicionales de seguridad en la red.
- Otras técnicas de fortificación.

UT 11. CUMPLICMIENTO DE LA LEGISLACIÓN Y DE LAS NORMAS DE SEGURIDAD
- Legislación sobre protección de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

2. Metodología Didáctica

2.1. Principios rectores.

La base metodológica y didáctica de esta programación es la teoría constructivista del aprendizaje basada en la psicología cognitiva. El docente, en su labor de facilitador fomentará la pedagogía crítica y ayudará a la consecución de un aprendizaje significativo. En esta misma línea, cobra especial importancia el aprender a aprender, y se incidirá en la idea de que es el alumno quien realiza su propio aprendizaje y que debe estar dispuesto a seguir aprendiendo en el futuro, pues la formación no termina nunca. En este sentido se fomentará el uso de distintas fuentes, libros, artículos, vídeos, manuales, etc. y la elaboración de la información en distintos formatos, presentaciones, vídeos, resúmenes, mapas conceptuales, etc.

El objetivo de las actividades de enseñanza – aprendizaje que se desarrollen será el que los alumnos alcancen la competencia profesional. Esto significa que el alumno ha de ser capaz de trasladar lo que realiza en el aula a otras situaciones similares que se presenten en su vida profesional, siempre acorde a una educación en valores.

En la línea de la educación en valores, cobra especial relevancia las habilidades sociales, cada día más importantes en los entornos laborales, siendo una de las competencias profesionales, personales y sociales a alcanzar en este ciclo. Para la consecución de este objetivo, adquiere especial relevancia la interacción entre los alumnos, y será promovida a través de actividades de trabajo por parejas o en grupo.

La síntesis integrada de métodos, técnicas y dinámicas contribuirán a fomentar el aprendizaje de todos los alumnos y alumnas, obteniendo el máximo potencial de cada uno. Se potenciará el desarrollo de las inteligencias múltiples mediante distintos ritmos y estilos de aprendizaje. Deben arbitrarse métodos que favorezcan la integración de los alumnos con problemas de aprendizaje y con necesidades educativas especiales. De igual

forma, se atenderá a los alumnos que destaquen por su interés por el conocimiento, persiguiendo el desarrollo de las capacidades potenciales de cada uno, y se los agrupará según sus intereses a veces, o buscando la complementariedad en otros casos.

Se iniciará a los estudiantes en el conocimiento con los principios básicos del método científico. Se fomentará el desarrollo de la observación y la intuición, la formulación y verificación de hipótesis y el uso del razonamiento intuitivo y deductivo. Se promoverá un pensamiento crítico, autónomo y responsable. También se fomentará el desarrollo del espíritu emprendedor, la iniciativa personal y la capacidad para aprender a aprender, planificar, tomar decisiones y asumir responsabilidades. En la misma línea, en la puesta en práctica de los conocimientos teóricos aplicados, de cara a su inserción laboral, se emulará el mundo del trabajo, exigiendo que las entregas de actividades sean realizadas en tiempo y forma.

2.2. Estrategias de Enseñanza–Aprendizaje.

Este módulo contiene la formación necesaria para desempeñar la función de implantación de medidas de seguridad en sistemas informáticos, y como tal, las líneas de actuación en el proceso de enseñanza-aprendizaje versarán sobre:

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

Para la consecución de estas líneas de actuación, el equipo docente planteará una evaluación para el aprendizaje. Todas las unidades de trabajo, así como todas las actividades a realizar por los alumnos, irán orientadas al aprendizaje del alumno, y serán sistemáticamente evaluadas con el fin de que el alumno comprenda cómo están siendo sus procesos de aprendizaje. Esta evaluación, que en principio será dirigida por el docente, irá encaminada a que el alumno adquiera las capacidades de aprender a aprender, desde el punto de vista crítico con su propio aprendizaje. La evaluación, también se nutrirá de las aportaciones que el resto de los compañeros puedan hacer sobre el aprendizaje y el grado de consecución de los objetivos marcados en cada tarea. Puesto que la orientación del alumno está también dirigida hacia la calificación, se fomentará que las actividades que se realicen formen parte de la calificación final del alumno, si bien, no todas ellas contribuirán en su calificación.

Respecto a las actividades a realizar, tratarán de ser eminentemente prácticas, si bien, suelen partir de fundamentaciones teóricas. Todos los contenidos, siempre serán apoyados, previamente o a posteriori, por el profesor. Se seguirá la filosofía “Learning by doing”, donde los alumnos aprenderán haciendo proyectos, ejercicios, y/o simulando entornos reales de trabajo.

Las actividades estarán fundamentadas desde un punto de vista didáctico partiendo de la aplicación de metodologías activas, siendo gran parte de ellas basadas en el aprendizaje cooperativo. Entre las posibles actividades a realizar, el profesor tratará de utilizar las más adecuadas al contexto del aula, intentando respetar los tiempos asignados a cada unidad de trabajo, con el único fin de que los alumnos adquieran un aprendizaje significativo, y consigan la competencia del módulo en particular y las del ciclo formativo en general. El sistema metodológico consistirá en la utilización de métodos y técnicas didácticas

pertinentes para el logro de los objetivos educativos que se pretenden conseguir. Este sistema metodológico se fundamente en tres pilares básicos:

- Exposición – orientación del docente, que tratará de minimizar la narración de los contenidos objeto de aprendizaje y se centrará más en la ayuda para la búsqueda de la información por parte del alumno.
- El trabajo personal del alumno, su auto-aprendizaje y el estudio individual o autónomo.
- El trabajo en grupo, en equipo, el estudio socializado o el trabajo cooperativo.

Dentro de las estrategias individuales, y sin pretender ser exhaustivos, se utilizará el estudio dirigido, la enseñanza personalizada y el estudio o trabajo autónomo. Las estrategias centradas en el trabajo en equipo (por parejas o pequeños grupos) podrán ser el estudio de casos, Phillips 66, role-playing, puzle, aprendizaje basado en proyectos o aprendizaje basado en problemas. A nivel de todo el grupo, también se realizarán actividades y dinámicas basadas en técnicas, que además de la expositiva, pueden ser el brainstorming, el simposio o el foro. En línea con la aplicación de modelos y metodologías de aprendizaje activas, y en la medida de lo posible, a lo ya indicado, se intentará aplicar gamificación, y si es posible, clases invertidas.

La mayoría de las actividades serán realizadas o apoyadas mediante el uso de las TICs. El trabajo con el ordenador será constante por parte de los alumnos, pues es lo más parecido al mercado laboral al que se incorporarán. A la hora de planificar las actividades, se tendrá en cuenta el horario establecido para el grupo de manera que, las sesiones más complicadas -normalmente las últimas horas-, tengan un carácter más dinámico (exposiciones, vídeos,...).

En los primeros días de clase se informará a los alumnos sobre:

- La programación didáctica del módulo. En este sentido se facilitará al alumno copia simplificada de la programación, remarcando los puntos fundamentales de la misma.
- El carácter no obligatorio pero presencial de este tipo de enseñanzas, y de lo que ello implica. Esto se recordará las veces que sea necesario a lo largo del curso.

3. Criterios de Evaluación

Los objetivos expresados en términos de resultados de aprendizaje y los criterios de evaluación, según el Decreto 34/2009, son los definidos en el Real Decreto 1691/2007. Cada resultado de aprendizaje va acompañado de sus criterios de evaluación de la siguiente forma:

1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.

Criterios de evaluación:

a) Se ha valorado la importancia de mantener la información segura.
b) Se han descrito las diferencias entre seguridad física y lógica.
c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.
d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.

e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.
h) Se ha valorado la importancia de establecer una política de contraseñas.
i) Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.

Criterios de evaluación:

a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento.
b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).
c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.
e) Se han seleccionado estrategias para la realización de copias de seguridad.
f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.
g) Se han realizado copias de seguridad con distintas estrategias.
h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.
i) Se han utilizado medios de almacenamiento remotos y extraíbles.
j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.

Criterios de evaluación:

a) Se han seguido planes de contingencia para actuar ante fallos de seguridad.
b) Se han clasificado los principales tipos de software malicioso.
c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.
d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.
e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.
f) Se han aplicado técnicas de recuperación de datos.

4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

Criterios de evaluación:

a) Se ha identificado la necesidad de inventariar y controlar los servicios de red.

b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.
c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
d) Se han aplicado medidas para evitar la monitorización de redes cableadas.
e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.
g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.
h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.

Criterios de evaluación:

a) Se ha descrito la legislación sobre protección de datos de carácter personal.
b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.
c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.
e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
f) Se han contrastado las normas sobre gestión de seguridad de la información.

4. Procedimientos de Evaluación

Se realizarán dos evaluaciones de carácter trimestral y la recuperación de la primera evaluación. La evaluación continua valorará la adquisición de las competencias profesionales, personales y sociales, así como de la consecución de los objetivos y el alcance de los resultados de aprendizaje, durante el transcurso del curso en base a los siguientes datos y observaciones:

- Resultados de los controles individuales, ya sean escritos o en el ordenador.
- Entrega de trabajos propuestos por el profesor en el plazo fijado.
- Resolución de casos prácticos en clase, ya sea de forma individual o en grupo.
- Asistencia a clase en caso de que sea presencial
- Buen comportamiento (según el Plan de Convivencia)
- Progreso en el proceso de aprendizaje.

Quedarán excluidos de las evaluaciones trimestrales aquellos alumnos que hayan perdido el derecho a la evaluación continua, aunque el/la alumno/a tendrá que realizar una prueba escrita en la evaluación ordinaria, además de entregar y aprobar las actividades que determine el profesor. Como en el Plan de Convivencia no se indica el número máximo de faltas fijado para la pérdida del derecho a evaluación continua, el departamento ha fijado este número en el 50% de las sesiones en un trimestre.

5. Sistema de Recuperación de evaluaciones pendientes

El primer trimestre podrá ser recuperado en el siguiente trimestre, mediante una prueba que será el total de la calificación de ese trimestre a recuperar. El criterio de redondeo es el mismo que para la calificación ordinaria

6. Criterios de Calificación

La calificación trimestral de los alumnos dependerá de los siguientes criterios:

- Controles escritos teórico-prácticos (examen): Aportarán el 70% de la calificación.
- Ejercicios, tareas y prácticas obligatorias (prácticas): Aportarán un 30% de la calificación. Si una práctica se presenta después del plazo de presentación, será calificada como 0. Todas las tareas serán evaluables, pero no todas serán calificables (no todas aportarán nota).

Para aprobar un trimestre, será necesario obtener una puntuación mayor o igual a 5. La nota mínima de cada prueba debe ser al menos de 3,5 puntos para poder hacer media con el resto de las notas. Las calificaciones trimestrales se redondearán, excepto en el caso de que, al redondear, se alcanzase la calificación de 5.
La nota global del curso en la convocatoria ordinaria será la media ponderada de las calificaciones trimestrales, teniendo en cuenta los siguientes casos:

- Aquellos alumnos que no hayan perdido el derecho a la evaluación continua recibirán su calificación proveniente de la media ponderada de las calificaciones trimestrales siempre y cuando dichas notas no sean inferiores a 5. En el caso en que tenga una calificación trimestral por debajo de 5 y la media sea superior a dicha calificación, dicha calificación se rebajará al 4.
- Aquellos alumnos que no hayan perdido el derecho a la evaluación continua y su calificación ordinaria no supere el 5, deberán realizar una prueba de recuperación de los contenidos de los trimestres suspensos, siempre que al menos uno de ellos esté aprobado. Además, deberán presentar y aprobar todas las prácticas solicitadas del trimestre a recuperar. La calificación del trimestre será la calificación del examen. La calificación ordinaria se recalculará de nuevo con las notas resultantes de las pruebas de recuperación en los mismos términos que en el caso anterior.
- Aquellos alumnos que no hayan perdido el derecho a la evaluación continua y no se encuentren en la situación anterior, o bien, decidan por propia voluntad así hacerlo, se podrán presentar a una prueba final para demostrar el dominio de los contenidos de todo el módulo. En este caso la calificación de convocatoria ordinaria proviene del resultado de la prueba final.
- Aquellos alumnos que hayan perdido el derecho a la evaluación continua por acumulación de faltas deberán superar una prueba final diseñada para demostrar el dominio de los contenidos del módulo. Los alumnos deberán entregar y aprobar las actividades que determine el profesor que imparte el módulo para poder presentarse a esa prueba. En este caso la calificación de convocatoria ordinaria proviene del resultado de la prueba final.

Si por circunstancias extraordinarias y a juicio del profesor tras la correspondiente justificación, algún alumno no pudiera realizar una prueba, bien en evaluación continua

o bien en evaluación ordinaria o extraordinaria, el profesor podrá reajustar estos criterios con el fin de no perjudicar al alumno.

7. Actividades de Recuperación para alumnos con materias pendientes y profundizaciones y refuerzos para lograr dicha recuperación

7.1. Prueba extraordinaria de junio

Cuando el alumno no haya superado la materia, en evaluación ordinaria, se le propondrán, para el periodo comprendido entre la evaluación ordinaria y la evaluación extraordinaria, actividades de apoyo, refuerzo y tutorización de aquellos resultados de aprendizaje no conseguidos, para la realización de las pruebas extraordinarias de evaluación. En esta prueba se evaluará el módulo completo y tendrá la misma estructura que la ordinaria.

8. Materiales, textos y recursos didácticos

- Un ordenador para cada alumno.
- Pizarra.
- Pizarra interactiva conectada al PC del profesor, pero de uso autónomo también.
- Aula virtual alojada en la página web del instituto y accesible por los alumnos, tanto desde el centro educativo como desde casa.
- Índices de contenidos elaborados por el profesor como eje estructural en la exposición de las unidades de trabajo y como guía ante la posible pérdida de ubicación de los alumnos/as dentro de las unidades de trabajo.
- Resúmenes elaborados por el profesor o los mismos alumnos/as.
- Múltiples ejercicios y problemas que fomenten la comprensión de los conceptos soporte y faciliten el aprendizaje y consolidación de los procedimientos. Los problemas y tareas en su grado de complejidad más alto acercarán al alumno/a a la realidad.

TEXTOS

Los textos recomendados como bibliografía de apoyo son:

Título: Seguridad Informática
Autor: Ignacio Triviño Mosquera.
Editorial: Síntesis

Y los textos para profundizar:

Título: Seguridad y alta disponibilidad
Autor: Alfredo Abad Domingo
Editorial: Garceta

9. Adaptación a los distintos escenarios planteados por la Comunidad de Madrid en función de la evolución de la crisis sanitaria por COVID-19

Todos los apartados indicados en esta programación están diseñados para adaptarse a los escenarios planteados por la Comunidad y por tanto, no sufrirán ninguna variación, salvo que en algunos de ellos se utilicen más las TIC que en otros.