SEGURIDAD INFORMÁTICA

Programación Didáctica

IES Aguadulce

Curso 2013/2014

FORMACIÓN PROFESIONAL DE GRADO MEDIO

2º SISTEMAS MICROINFORMÁTICOS Y REDES

Profesor

Francisco Javier García Rodríguez

INDICE

1. INTRODUCCIÓN

El diseño curricular del módulo profesional de Seguridad Informática, correspondiente al segundo curso del Ciclo Formativo de Grado Medio de Técnico en Sistemas Microinformáticos y Redes viene recogido en la Orden de 7 de Julio de 2009 (BOJA 165 de 25 de agosto), y que a su vez está basado en el Real Decreto 1691/2007.

Este módulo se impartirá en el segundo curso del Ciclo Formativo con una carga lectiva de 5 horas semanales, con un total de horas a lo largo del curso de 105.

2. OBJETIVOS GENERALES DEL CICLO

2.1 OBJETIVOS GENERALES DEL CICLO FORMATIVO

Los objetivos generales de este ciclo formativo, especificados en el BOE nº 15 del 17 de enero de 2008, son los siguientes:

1. Organizar los componentes físicos y lógicos que forman un sistema microinformático, interpretando su documentación técnica, para aplicar los medios y métodos adecuados a su instalación, montaje y mantenimiento.
2. Identificar, ensamblar y conectar componentes y periféricos utilizando las herramientas adecuadas, aplicando procedimientos, normas y protocolos de calidad y seguridad, para montar y configurar ordenadores y periféricos.
3. Reconocer y ejecutar los procedimientos de instalación de sistemas operativos y programas de aplicación, aplicando protocolos de calidad, para instalar y configurar sistemas microinformáticos.
4. Representar la posición de los equipos, líneas de transmisión y demás elementos de una red local, analizando la morfología, condiciones y características del despliegue, para replantear el cableado y la electrónica de la red.
5. Ubicar y fijar equipos, líneas, canalizaciones y demás elementos de una red local cableada, inalámbrica o mixta, aplicando procedimientos de montaje y protocolos de calidad y seguridad, para instalar y configurar redes locales.
6. Interconectar equipos informáticos, dispositivos de red local y de conexión con redes de área extensa, ejecutando los procedimientos para instalar y configurar redes locales.

7. Localizar y reparar averías y disfunciones en los componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
8. Sustituir y ajustar componentes físicos y lógicos para mantener sistemas microinformáticos y redes locales.
9. Interpretar y seleccionar información para elaborar documentación técnica y administrativa.
10. Valorar el coste de los componentes físicos, lógicos y la mano de obra, para elaborar presupuestos.
11. Reconocer características y posibilidades de los componentes físicos y lógicos, para asesorar y asistir a clientes.
12. Detectar y analizar cambios tecnológicos para elegir nuevas alternativas y mantenerse actualizado dentro del sector.
13. Reconocer y valorar incidencias, determinando sus causas y describiendo las acciones correctoras para resolverlas.
14. Analizar y describir procedimientos de calidad, prevención de riesgos laborales y medioambientales, señalando las acciones a realizar en los casos definidos para actuar de acuerdo con las normas estandarizadas.
15. Valorar las actividades de trabajo en un proceso productivo, identificando su aportación al proceso global para conseguir los objetivos de la producción.
16. Identificar y valorar las oportunidades de aprendizaje y empleo, analizando las ofertas y demandas del mercado laboral para gestionar su carrera profesional.
17. Reconocer las oportunidades de negocio, identificando y analizando demandas del mercado para crear y gestionar una pequeña empresa.
18. 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.

2.2 COMPETENCIA GENERAL

La competencia general de este título consiste en instalar, configurar y mantener sistemas microinformáticos, aislados o en red, así como redes locales en pequeños entornos, asegurando su funcionalidad y aplicando los protocolos de calidad, seguridad y respeto al medio ambiente establecidos.

2.3 ENTORNO PROFESIONAL

La actividad se ejerce principalmente en empresas del sector servicios que se dediquen a la comercialización, montaje y reparación de equipos, redes y servicios microinformáticos en general, como parte del soporte informático de la organización, o en entidades de cualquier tamaño y sector productivo que utilicen sistemas microinformáticos y redes de datos para su gestión.

Las ocupaciones y puestos de trabajo más relevantes de esta profesión son los siguientes:

- Técnico instalador-reparador de equipos informáticos
- Técnico de soporte informático
- Técnico de redes de datos
- Reparador de periféricos de sistemas microinformáticos
- Comercial de microinformática
- Operador de tele-asistencia
- Operador de sistemas

3. CURRÍCULO DEL MODULO PROFESIONAL

El Currículo del módulo profesional estará constituido por los resultados de aprendizaje y criterios de evaluación que a continuación se citan:

3.1 RESULTADOS DE APRENDIZAJE

1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades.

2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información.

3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático.

4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico.

5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento.

3.2 CRITERIOS DE EVALUACIÓN

Se definen para cada uno de los resultados de aprendizaje.

1. Aplicar medidas de seguridad pasiva en sistemas informáticos, describir características de entornos y relacionarlas con sus necesidades:

- Se ha valorado la importancia de mantener la información segura.
- Se han descrito las diferencias entre seguridad física y lógica.
- Se han definido las características de la ubicación física y las condiciones ambientales de los equipos y servidores.
- Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.
- Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.
- Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.
- Se han indicado las características de una política de seguridad basada en listas de control de acceso.
- Se ha valorado la importancia de establecer una política de contraseñas.
- Se han valorado las ventajas que supone la utilización de sistemas biométricos.

2. Gestionar dispositivos de almacenamiento, describir los procedimientos efectuados y aplicar técnicas para asegurar la integridad de la información:

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

- Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.

3. Aplicar mecanismos de seguridad activa, describir sus características y relacionarlas con las necesidades de uso del sistema informático:

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

4. Asegurar la privacidad de la información transmitida en redes inalámbricas, describir las vulnerabilidades e instalar software específico:

- Se ha identificado la necesidad de inventariar y controlar los servicios de red.
- Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informaticos y robos de información.
- Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
- Se han aplicado medidas para evitar la monitorización de redes cableadas.
- Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.
- Se han descrito y utilizado sistemas de identificación como la firma electrónica o certificado digital, entre otros.
- Se ha instalado y configurado un cortafuegos en un equipo o servidor.

5. Reconocer la legislación y normativa sobre seguridad y protección de datos, y analizar las repercusiones de su incumplimiento:

- Se ha descrito la legislación sobre protección de datos de carácter personal.
- Se ha determinado la necesidad de controlar el acceso a la información personal

almacenada.

- Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.
- Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Se han contrastado las normas sobre gestión de seguridad de la información.

4. CONTENIDOS

A continuación se detallan los contenidos mínimos, establecidos en la legislación vigente, que los alumnos deberán adquirir para poder superar este módulo.

- Aplicación de medidas de seguridad pasiva:
  - Ubicación y protección física de los equipos y servidores.
  - Sistemas de alimentación ininterrumpida.
- Gestión de dispositivos de almacenamiento:
  - Almacenamiento de la información: rendimiento, disponibilidad, accesibilidad.
  - Almacenamiento redundante y distribuido.
  - Almacenamiento remoto y extraíble.
  - Criptografía.
  - Copias de seguridad e imágenes de respaldo.
  - Medios de almacenamiento.
- Aplicación de mecanismos de seguridad activa:
  - Identificación digital. Firma electrónica y certificado digital.
  - Seguridad en los protocolos para comunicaciones inalámbricas.
  - Utilización de cortafuegos en un sistema o servidor.
  - Listas de control de acceso.
  - Política de contraseñas.
  - Recuperación de datos.

  - Software malicioso. Clasificación. Herramientas de protección y desinfección.

- Aseguramiento de la privacidad:
  - Métodos para asegurar la privacidad de la información transmitida.
  - Fraudes informáticos y robos de información.
  - Control de la monitorización en redes cableadas.
  - Seguridad en redes inalámbricas.
  - Sistemas de identificación: firma electrónica, certificados digitales y otros.
  - Cortafuegos en equipos y servidores.
- Cumplimiento de la legislación y de las normas sobre seguridad:
  - Legislación sobre protección de datos.
  - Legislación sobre los servicios de la sociedad de la información y correo electrónico.

4.1 UNIDADES DIDÁCTICAS

Dados los contenidos anteriormente expuestos, se propone un desglose en las siguientes unidades didácticas.

Unidad 1: Conceptos sobre seguridad informática

Unidad 2: Criptografía.

Unidad 3: Seguridad pasiva. Equipos.

Unidad 4: Seguridad pasiva. Almacenamiento.

Unidad 5: Seguridad activa. Sistema Operativo y Aplicaciones.

Unidad 6: Seguridad activa. Acceso a Redes.

Unidad 7: Seguridad activa. Control de redes.

Unidad 8: Ataques y contramedidas.

A continuación se detallan para cada unidad didáctica los contenidos que se impartirán en cada una de ellas.

Unidad 1: Conceptos sobre seguridad informática

Contenidos Conceptuales

- Visión global de la seguridad informática. Conceptos.
- Planificación de la seguridad:
  - Activos.
  - Amenazas.
  - Identificación y tipos de amenazas.
  - Riesgos.
  - Vulnerabilidades.
  - Impactos.
- Servicios y mecanismos de seguridad:
  - Confidencialidad.
  - Integridad.
  - Identificación/Autenticación.
  - No repudio.
  - Control de accesos.
  - Auditoría.
  - Disponibilidad.
  - Alarmas.
- Seguridad física vs. seguridad lógica.
  - Modelo de seguridad.
  - Política de seguridad.
- Legislación sobre protección de datos:
  - Ley Orgánica de Protección de Datos de Carácter Poersonal (LOPD).
  - Reglamento de Medidas de Seguridad (RMS).
  - Ley de Datos de Carácter Personal en la Comunidad de Madrid.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico:
  - Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI-CE).
  - Ley sobre normas reguladoras de firma electrónica.
  - Ley sobre el DNI electrónico.

Contenidos procedimentales

- Conocer las diferencias entre seguridad física y lógica.
- Conocer la necesidad de proteger físicamente los sistemas informáticos.
- Saber cómo establecer las características de una política de seguridad basada en listas de control de acceso.
- Valorar la importancia de establecer una política de contraseñas.
- Valorar las ventajas que supone la utilización de sistemas biométricos.
- Conoce la legislación sobre protección de datos de carácter personal.
- Conoce las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.
- Conocer la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.
- Conocer las normas sobre gestión de seguridad de la información.

Contenidos actitudinales

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a posibles amenazas, tanto físicas como lógicas.
- Valorar la necesidad de utilizar todas las medidas de seguridad necesarias para proteger la información.
- Mostrar interés en la adquisición de conocimientos.
- Darse cuenta de lo importante que es saber proteger correctamente los equipos de las posibles amenazas, tanto físicas como lógicas.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 2: Criptografía

Contenidos conceptuales

- Métodos para asegurar la privacidad de la información transmitida.
- Criptoanálisis y criptografía.
- Criptografía clásica.
- Criptografía moderna:
  - Cifrado de clave secreta (simétrica): funcionamiento, algoritmos, aplicaciones.
  - Cifrado de clave pública (asimétrica): funcionamiento, algoritmos, aplicaciones.
  - Funciones de mezcla o resumen (hash): características, aplicaciones, algoritmos

hash.

- Sistemas de identificación: firma electrónica, certificados digitales y otros:
  - Firma electrónica: propiedades, utilidad.
  - Certificados digitales: autoridades de certificación.
  - Distribución de claves. PKI (Public Key Infrastructure): componentes, estructura, procedimiento, aplicaciones que requieren PKI.
  - Tarjetas inteligentes.

Contenidos procedimentales

- Cifrar textos mediante diversos algoritmos.
- Generar parejas de claves para el cifrado asimétrico.
- Exportar e importar certificados.
- Intercambiar claves o certificados.
- Revocar un certificado.
- Instalar una entidad emisora de certificados.
- Realizar peticiones de certificados a una entidad emisora.
- Retirar certificados.
- Firmar mensajes.
- Obtener certificados digitales.
- Enviar correos electrónicos haciendo uso del certificado digital.

Contenidos actitudinales

- Apreciar la necesidad de cifrar la información para mantener la confidencialidad.
- Valorar la importancia del uso de los certificados y firmas digitales.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 3: Seguridad pasiva. Equipos.

Contenidos conceptuales

Ubicación del CPD.

- Protección.
- Aislamiento.
- Ventilación.
- Control de acceso.

- Centro de Respaldo.

- SAI/UPS.
  - Tipos.
  - Monitorización.
  - Triggers
  - Mantenimiento

Contenidos procedimentales

- Determinar los problemas que pueden surgir por no escoger correctamente la ubicación de un CPD.
- Valorar los problemas que pueden surgir por no considerar la seguridad necesaria en los centros de procesamiento de datos.
- Determinar la necesidad de los planes de recuperación en caso de desastre.
- Conocer las ventajas del uso de equipos SAI y seleccionarlos correctamente para satisfacer las necesidades concretas del sistema.
- Valorar la necesidad de utilizar sistemas de almacenamiento redundante o distribuido para proteger los datos de los equipos.
- Determinar qué tipo de sistema de almacenamiento redundante o distribuido es más adecuado para nuestros equipos.

Contenidos actitudinales

- Apreciar la importancia de mantener los equipos informáticos y la información protegidos frente a amenazas físicas.
- Valorar la necesidad de utilizar todas las medidas necesarias para proteger nuestros sistemas.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 4: Seguridad pasiva. Almacenamiento.

Contenidos conceptuales

Estrategias de almacenamiento.

- Rendimiento y redundancia. RAID en Windows y Linux.
- Almacenamiento en red. NAS y SAN. Clústers.
- Almacenamiento en la nube y P2P.

- Backup de datos.

- Tipos de dispositivos locales y remotos. Robosts de cintas.
- Tipos de copias.
- Copia y recuperación en Windows y Linux.

- Imagen del sistema.
  - Creación y recuperación. LiveCD.
  - Congelación.
  - Registro de Windows y puntos de restauración.
  - Herramientas de chequeo de discos.

Contenidos procedimentales

- Ser capaz de analizar la documentación técnica relativa a la política de almacenamiento.
- Reconocer los distintos factores inherentes al almacenamiento de la información (rendimiento, disponibilidad y accesibilidad, entre otros).
- Conocer los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.
- Conocer las tecnologías de almacenamiento redundante y distribuido.
- Conocer las estrategias para la realización de copias de seguridad.
- Reconocer la importancia de la frecuencia y el esquema de rotación.
- Ser capaz de realizar copias de seguridad con distintas estrategias.
- Conocer las características de los medios de almacenamiento remotos y extraíbles.
- Ser capaz de utilizar medios de almacenamiento remotos y extraíbles.
- Ser capaz de crear y restaurar imágenes de respaldo de sistemas en funcionamiento.

Contenidos actitudinales

- Valorar la necesidad de realizar copias de respaldo para recuperar la información en caso de perderla.
- Apreciar la importancia que tiene la realización de imágenes de sistema.
- Valorar la necesidad de conocer software específico para recuperar información borrada.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

Unidad 5: Seguridad activa. Sistema Operativo y Aplicaciones

Contenidos conceptuales

- Estrategias de seguridad
  - La caja del ordenador.
  - La BIOS del ordenador.
  - El Boot Manager.
  - Cifrado de Particiones.
- Autenticación en el Sistema Operativo.
  - Usuario/Password.
  - Tarjetas
  - Biometría.
  - Elevación de priviligegios.
- Cuotas.
- Actualizaciones y parches.
- Antivirus.
- Monitorización.
- Aplicaciones Web.
- Cloud Computing

Contenidos procedimentales

- Proteger el arranque del sistema frente a intrusos.
- Cifrar particiones para que no sean accesibles a personal ajeno.
- Crear cuotas de disco.
- Definir políticas de contraseñas.
- Crear contraseñas seguras.
- Definir listas de control de acceso.
- Monitorizar el sistema.
- Hacer ARP spoofing y DNS spoofing.
- Comprometer una sesión telnet.
- Configurar un análisis con antivirus.
- Detectar las amenazas del sistema.

Contenidos actitudinales

- Apreciar la necesidad de proteger al sistema frente a los atacantes.
- Valorar la importancia de definir cuotas de disco.
- Valorar la importancia de monitorizar el sistema.
- Valorar la repercusión del uso de antivirus para evitar la entrada de troyanos, gusanos y virus.
- Mostrar interés en la adquisición de los conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 6: Seguridad activa. Acceso a redes.

Contenidos conceptuales

- Redes cableadas.
  - VLAN.
  - Autenticación en el puerto. MAC y 802.1X.
- Redes inalámbricas.
  - Asociación y transmisión.
  - Cifrado. WEP, WAP, WAP2.
  - WPA empresarial: RADIUS.
- VPN.
- Servicios de Red. Nmap y Netstat.

Contenidos procedimentales

- Conocer la necesidad de inventariar y controlar los servicios de red.
- Ser capaz de aplicar medidas para evitar la monitorización de redes cableadas.
- Conocer y valora las propiedades de seguridad de los protocolos usados en redes inalámbricas.
- Conocer los sistemas de identificación como la firma electrónica y el certificado digital, entre otros.

Contenidos actitudinales

- Valorar la importancia de proteger nuestros sistemas cuando se utilizan redes no seguras, ya sean cableadas o inalámbricas.
- Mostrar iniciativa para proteger la red domestica.

- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 7: Seguridad Activa. Control de redes.

Contenidos conceptuales

- Métodos para asegurar la privacidad de la información transmitida.
- Introducción a protocolos seguros.
- Control de la monitorización en redes.
- Seguridad de red (accesos en red y seguridad perimetral):
  - Amenazas y ataques.
  - Intrusiones externas vs. intrusiones internas.
  - Seguridad en los accesos de red: arranque de servicios, puertos.
- Cortafuegos en equipos y servidores:
  - Concepto y funciones principales.
  - Tipos de cortafuegos: clasificación por tecnología, clasificación por ubicación.
  - Filtrado de paquetes.
  - Arquitecturas de cortafuegos.
  - Instalación de cortafuegos.
  - Utilización de cortafuegos en un sistema o servidor.
  - Reglas de filtrado.
  - Logs y registros de actividad.
- Proxys:
  - Proxy. Características y funcionamiento.
  - Filtrado de paquetes.
  - Proxy-caché.
  - Proxy transparente.
  - Configuración de clientes proxy.
- Servidores proxy en sistemas operativos libres y propietarios:
  - Instalación.
  - Arranque y parada.
  - Ficheros y parámetros de configuración.
  - Filtrar accesos y tráfico.

- Gestión de la caché.
- Métodos de autenticación en un proxy.
- Monitorización y logs.
- Herramientas para generar informes sobre logs de servidores proxy.

• Servidores antispam.

Contenidos procedimentales

• Conocer la necesidad de inventariar y controlar los servicios de red.
• Conocer la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.
• Ser capaz de aplicar medidas para evitar la monitorización de redes cableadas.
• Ser capaz de instalar y configurar un cortafuegos en un equipo o servidor.

Contenidos actitudinales

- Valorar la importancia de proteger nuestros equipos de accesos desde el exterior y el interior de nuestra red.
- Utilizar la lógica para establecer las reglas de filtrado más adecuadas en cada situación.
- Mostrar iniciativa para proteger la red doméstica.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos aprendidos.

Unidad 8: Ataque y contramedidas.

Contenidos conceptuales

• Ataques TCP/IP. MITM
• Contramedidas.
• Ataques wifi. Aircrack-ng.
• Contramedidas.
• Ataques web. WebGoat.
• Contramedidas.
• Ataques proxy. Ultrasurf.
• Contramedidas.

Contenidos procedimentales

- Ser capaz de aplicar mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.
- Saber asegurar la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software específico.

Contenidos actitudinales

- Organizar y analizar el trabajo, antes de realizarlo y durante su desarrollo.
- Tener una actitud crítica pero respetuosa con los compañeros, lo que favorece unas mejores relaciones laborales en un futuro puesto de trabajo.
- Resolver problemas y tomar decisiones siguiendo las normas y procedimientos establecidos.
- Participar de forma activa en la vida económica, social y cultural con una actitud crítica y responsable.
- Reconocer los derechos y deberes.
- Mostrar interés en la adquisición de conocimientos.
- Utilizar el vocabulario correcto para referirse a los nuevos conceptos y procedimientos aprendidos.

5. TEMPORIZACIÓN

La duración total del módulo es de 105 horas, a impartir en dos trimestres, y con una carga semanal de 5 horas. La finalización del periodo lectivo está prevista para el día 15 de marzo de 2013. La temporización estiamada en cada uno de los trimestres es la siguiente:

1º Trimestre: Unidades 1 a 4 (14 semanas)

2º Trimestre: Unidades 5 a 8 (10 semanas)

A continuación se desglosa, para cada una de las unidades didácticas, la duración estimada:

Unidad 1: Conceptos sobre seguridad informática. (10 horas)

Unidad 2: Criptografía. (15 horas)

Unidad 3: Seguridad pasiva. Equipos. (15 horas)

Unidad 4: Seguridad pasiva. Almacenamiento. (15 horas)

Unidad 5: Seguridad activa. Sistema Operativo y Aplicaciones. (15 horas)

Unidad 6: Seguridad activa. Acceso a Redes. (15 horas)

Unidad 7: Seguridad activa. Control de redes. (10 horas)

Unidad 8: Ataques y contramedidas. (10 horas)

6. MATERIALES DIDÁCTICOS Y RECURSOS

El equipamiento informático con el que se cuenta para este módulo es el siguiente:

- Un aula con 8 ordenadores.
- Ordenador del profesor.
- Una impresora.
- Un proyector multimedia.
- Red con acceso a Internet.

Así, al ser el número de alumnos y alumnas superior al número de ordenadores, el trabajo se organiza de forma que cada ordenador es ocupado por dos alumnos/as, salvo que las circunstacias puntuales de la clase permitan que cada alumno/a tenga su propio ordenador. Igualmente, cada alumno, si lo desesa, podrá hacer uso de su ordenador portátil personal.

Se utilizará también el proyector multimedia para que el alumnado pueda ver directamente en una pantalla grande las instrucciones que hay que realizar con el ordenador para llevar a cabo una tarea determinada.

El departamento de informática dispone de un plataforma moodle como apoyo a la docencia. En ella, se colgarán los apuntes y materiales necesarios para el desarrollo de la clase, así como los alumnos subirán tareas y ejercicios propuestos. La dirección de la plataforma moodle es la siguiente:

http://192.168.20.20/moodle

En cuanto al material didáctico empleado para el diseño de las actividades a realizar en el aula y de esta programación, se ha partido del primer libro que se anexa en la bibliografía, así como de material recopilado en Internet.

7. METODOLOGÍA

La metodología a seguir deberá ser flexible y dinámica, adaptada en todo momento a objetivos y contenidos, y orientada de manera constante por un proceso de evaluación formativa. Dicha metodología deberá adecuarse en todo momento al tipo de alumnado que se nos presente.

A priori no se descarta ninguno de los recursos metodológicos comúnmente admitidos: charla, ejercicio práctico, debate, conferencia, medios audiovisuales, formulación de problemas, exposición, orientación, trabajos individuales y de grupo, investigación en el medio, visitas técnicas, etc..

En términos generales cabe establecer el siguiente esquema:

- En las cuestiones de contextualización y fundamentos se recurrirá a la exposición, trabajo individual y de grupo, investigación y debate.
- En las más auténticamente procedimentales, la exposición (inicialmente necesaria) se reducirá al mínimo, dando paso de manera inmediata a los ejemplos, ejercicios prácticos, resolución de problemas, realización de trabajos y crítica de los mismos, práctica en ordenador con las herramientas de desarrollo, etc.
- En las de profundización la exposición tomará un papel más relevante, pero sin descuidar en ningún caso los aspectos de aplicación.

De una u otra forma, la metodología tenderá a conseguir progresivamente hábitos de autonomía y autosuficiencia en el alumnado, a través de la resolución de las dificultades que paulatinamente vayan surgiendo, dando especial relevancia a la iniciativa, la lógica, el método, la acumulación de experiencia y la capacidad de reacción; en suma, el desarrollo de habilidades, destrezas y criterios propios que producirán un gradual aumento de la independencia del alumnado respecto del profesor.

La organización del espacio físico tenderá a optimizarlo y adecuarlo a los fines perseguidos; sería deseable distribuirlo en dos áreas, una con estructura de aula convencional y otra orientada al trabajo en ordenador, pero si ello no resulta factible necesariamente se

configurará como un área única polivalente.

Se utilizará un portal web en el que se compartirá infomación con el alumnado. Este portal web también se utilizará para la comunicación profesor-alumno y para el envío de tareas y trabajos. Toda la información aquí presente formará parte de los contenidos del módulo, y por tanto, se podrán preguntar en exámenes.

Se fomentará la lectura realizando lecturas sobre unidades o artículos relacionados con los temas que se traten en cada momento.

Por último, a modo de síntesis y sin perjuicio del necesario rigor conceptual, se tendrá siempre presente la consideración de que lo importante es desarrollar las capacidades para abordar realizaciones prácticas similares a aquellas que se va a tener que afrontar en la vida profesional, una vez concluida la etapa formativa.

8. EVALUACIÓN

8.1 CRITERIOS, ESTRATEGIAS Y PROCEDIMIENTOS DE EVALUACIÓN

La evaluación, en sus diversas vertientes, constituye un análisis de los factores y elementos que intervienen en el proceso educativo, valorando su adecuación y eficacia. En función del momento en que se realice, se puede distinguir:

a) Evaluación inicial. Se realiza antes de comenzar el proceso de enseñanza-aprendizaje y su finalidad será obtener un diagnóstico previo sobre ideas y conocimientos previos del alumno, su nivel inicial y posibles dificultades de aprendizaje.
b) Evaluación formativa. Esta evaluación será continua, realizándose un seguimiento constante de los progresos del alumnado, teniendo en cuenta sus capacidades, el interés manifestado, el esfuerzo realizado y los criterios de evaluación que marca la legislación.
c) Evaluación sumativa. Tiene por objeto medir el resultado al finalizar el proceso de enseñana-aprendizaje.

Los resultados de aprendizaje expresan en forma de resultados, que deben ser alcanzados por los alumnos, los aspectos básicos de la competencia profesional y del nivel de formación que acredita el título. Caracterizan y establecen la validez del título en todo el territorio del Estado, y determinan la cualificación mínima del mismo que debe ser alcanzada por todas las administraciones educativas, a fin de conseguir la preparación profesional básica y su necesario grado de homogeneidad. Cabría pues plantearse su adaptación al entorno circundante, con objeto de reflejar su realidad y mejorar las expectativas de los alumnos. La evaluación será continua, realizándose un seguimiento constante de los progresos del alumnado. Además se tendrán en cuenta sus capacidades, el interés manifestado, el esfuerzo realizado y los criterios de evaluación que marca la legislación.

Los criterios de evaluación establecidos, que se traducirán en actividades concretas, son los establecidos por la legislación vigente.

8.2 INSTRUMENTOS DE EVALUACIÓN

Los instrumentos de evaluación del alumnado serán la observación sistemática, la observación directa, exposición y la realización de trabajos. El seguimiento individual del alumno o alumna se llevará a cabo a través del trabajo diario de clase, la realización de ejercicios individuales, las preguntas individualizadas y la realización de supuestos prácticos. El seguimiento del alumno o alumna como miembro de un grupo se hará con el trabajo diario, ejercicios del grupo, preguntas y supuestos.

Se recurrirá básicamente al trabajo práctico con y sin herramientas de desarrollo (tanto individual como por parejas, con o sin la posterior defensa), resolución de problemas y ejercicios sobre aspectos parciales. Se realizarán pruebas escritas a fin de valorar el grado de adquisición de los contenidos por parte del alumnado. Además, el alumnado contará con una libreta o similar donde recogerán la teoría y problemas expuestos en clase, y esta podrá será revisada puntualmente por el profesor y las puntuaciones obtenidas formarían parte de la nota final.

Se valorará la iniciativa, originalidad y participación del alumnado, la exactitud y precisión en el desarrollo de los ejercicios y prácticas realizadas. Todos los trabajos tienen

nota, y ésta contará en la nota correspondiente a cada trimestre.

8.3. SUPERACIÓN DEL MÓDULO

Para conseguir la promoción de este módulo se tendrán en cuenta los criterios de evaluación antes mencionados, que se traducirán en actividades específicas, con su correspondiente componente práctico, sobre todo, las relacionadas con los supuestos prácticos.

Por tanto, el alumno o alumna, para poder superar el modulo deberá haber hecho los supuestos prácticos planteados por el profesor y haber participado y trabajado en clase, superando las pruebas específicas que en cada momento se establezcan. La nota final de promoción del alumnado estará en base a los siguientes porcentajes aplicados en cada trimestre:

Exámenes	60%
Trabajos realizados	30%
Participación y asistencia	10%

Se deberá obtener un mínimo de 5 en la media de los exámenes, así como en el examen final del trimestre, para poder realizar la media final de la evaluación. Para el cálculo de la nota final del trimestre, se usará la ponderación arriba expresada.

La obtención de la nota final del módulo vendrá dada por la media aritmética de la calificación obtenida por el alumnado en cada trimestre. Si un alumno no llega al 5 en alguno de los trimestres se realizará, al finalizar el segundo trimestre, un examen de recuperación para que aquel alumno o alumna que no haya superado alguna de las dos evaluaciones. En este examen, cada alumno o alumna se presentará sólo a la evaluación que no haya superado.

Dentro del apartado de trabajos realizados, también se tendrá en cuenta las tareas diarias realizadas por el alumnado, ejercicios de clase, además de los trabajos y proyectos entregados.

Tal y como se establece en el proyecto educativo, se perderá el derecho de evaluación continua cuando se acumulen más del 20% de horas de faltas de asistencia (justificadas o

injustificadas), de la duración total del módulo. En nuestro caso, si un alumno o alumna falta más de 21 horas perderá este derecho y deberá presentarse al examen ordinario, debiendo realizar el examen de los contenidos impartidos en todo el módulo. En este caso, la calificación final del módulo vendrá establecida por la ponderación establecida en el proyecto educativo.

Para fomentar los hábitos de lectura en el alumnado, se realizarán lecturas de los contenidos de las unidades durante las clases, con el objetivo de adquirir hábitos de lectura en el alumnado. Se realizarán trabajos escritos en los que se verá la capacidad expresiva del alumnado, así como se tendrán en cuenta las faltas de ortografía del alumano tanto en las actividades diarias de clase como en los exámenes. Si se detectan faltas graves de ortografía, se requerirá al alumnado que vuelva a escribir de manera correcta las palabras mal escritras. Estas faltas de ortografía podrán llevar una puntuación negativa en las actividades y exámenes del alumnado, desapareciendo estas puntuaciones negativas en el momento en que se muestre que ha escrito correctamente las palabras mal expresadas.

Las faltas muy graves de convivencia, como acciones de falta de respeto a los compañeros o al profesor, o el mal uso intencionado de los recursos informáticos, podrán ser sancionados con la pérdida del derecho a la evaluación continua, independientemente de las medidas disciplinarias que adopte el centro. Se entiende que tales actitudes imposibilitan alcanzar los resultados de aprendizaje del módulo e impiden la posterior transición al mercado laboral.

8.4 EVALUCIÓN ORDINARIA

A finales del mes de junio se realizará la convocatoria ordinaria para aquellos alumnos que no hayan superado el módulo en las evaluaciones parciales que se hayan establecido (primer y segundo trimestre),así como para el alumnado que haya perdido la evaluación continua. Esta convocatoria versará sobre todos los contenidos desarrollados durante el curso, y consistirá en una serie de preguntas teóricas y el desarrollo de varios supuestos prácticos, pudiendo ser mediante prueba escrita o con ordenador (o ambos simultáneamente). La calificación aquí obtenida vendrá ponderada con lo establecido a tal efecto en el proyecto educativo del centro.

9. ATENCIÓN AL ALUMNADO CON CARACTERÍSTICAS EDUCATIVAS ESPECÍFICAS

Se debe regular la atención a los alumnos y alumnas con necesidades educativas específicas. Por este motivo en este módulo se tendrán en cuenta, en caso de necesidad, la utilización del material adecuado para los alumnos y alumnas con deficiencias auditivas, visuales o motoras.

- Para los alumnos o alumnas con deficiencias auditivas el profesor de apoyo que conoce el lenguaje de signos ayudará en las explicaciones y todo el material se le dará por escrito.
- Para los alumnos o alumnas con deficiencia visual se adaptarán el hardware y el software a sus necesidades.
- Los alumnos o alumnas con deficiencia motora estarán ubicados en las mesas y sillas que pertinentemente se soliciten a tal efecto.

10. CONEXIÓN CON LOS TEMAS TRANSVERSALES

Durante el desarrollo de este módulo profesional se intentará fomentar en los alumnos y alumnas actitudes relacionadas con:

- La educación para la igualdad entre los sexos, mediante trabajos con grupos mixtos.
- La educación para el cuidado del medio ambiente, mediante reciclado de papel y tóner.
- La educación moral y cívica, mediante una actitud de respeto en clase.
- La educación para la salud, mediante ergonomía y hábitos posturales.

11. BIBLIOGRAFÍA DE AULA Y DEPARTAMENTO

- *Seguridad Informática*: ed. McGraw-Hill. José Fabián Roa Buendía.
- *Seguridad Informática*: Ed. Ra-Ma. Costas, Jesús.
- Material aportado por el profesor.