PROGRAMACIÓN DIDÁCTICA.		
I.E.S. JULIO VERNE	DEPARTAMENTO DE INFORMÁTICA	
C.F.G.S. ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED		2º CURSO
MÓDULO: SEGURIDAD Y ALTA DISPONIBILIDAD		

CURSO:	2021 – 2022
PROFESOR:	FRANCISCO LUQUE JIMÉNEZ

ÍNDICE

Índice de contenido

1 INTRODUCCIÓN.

El título de formación profesional de **Técnico Superior en Administración de Sistemas Informáticos en Red** tiene una duración de 2000 horas distribuidas en módulos que se desarrollarán durante dos cursos académicos.

La organización de los módulos de dicho título es la siguiente:

l) Formación en centro educativo.
   a) Módulos asociados a la competencia.
   b) Módulos profesionales socioeconómicos.
   c) Módulo profesional integrado.

II) Formación en centro de trabajo.

Atendiendo a esa distribución, el módulo de **Seguridad y Alta Disponibilidad** se enmarca dentro de los de "*formación en centro educativo*" y "*asociado a la competencia*".

La duración del mismo es de **84** horas lectivas impartidas durante el segundo curso de los dos con los que cuenta el ciclo, repartidas en **4** horas semanales (1 sesiones de 2 horas y 2 sesiones de 1 hora). La totalidad de las horas serán impartidas en el aula taller, que incluye una zona de mesas para clases teóricas, además de la equipación informática.

Este módulo será impartido por un profesor responsable de la asignatura.

2 MARCO LEGISTATIVO

El marco legislativo que regula el ciclo formativo viene determinado por el **real decreto 1629/2009**, de 30 de octubre y la **orden de 19 de julio de 2010**

3 REFERENTE CONTEXTUAL

El referente contextual viene determinado por el proyecto educativo del centro

4 OBJETIVOS GENERALES QUE SE DESARROLLAN EN EL CICLO

Recogidos en la programación del departamento

5 OBJETIVOS GENERALES QUE SE DESARROLLAN EN EL MÓDULO

El presente título, según el **real decreto 1629/2009**, de 30 de octubre y la **orden de 19 de julio de 2010** , tiene como **objetivos generales** los siguientes:

Los objetivos generales que se desarrollan en el módulo, son los siguientes:

j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para implementar soluciones de alta disponibilidad.

k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.

l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.

m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.

o) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.

p) Identificar los cambios tecnológicos, organizativos, económicos y laborales en su actividad, analizando sus implicaciones en el ámbito de trabajo, para mantener el espíritu de innovación.

6 COMPETENCIAS QUE SE DESARROLLAN EN EL MÓDULO.

La formación del módulo contribuye a alcanzar las competencias profesionales, personales y sociales de este título que se relacionan a continuación:

e) Optimizar el rendimiento del sistema configurando los dispositivos hardware de acuerdo a los requisitos de funcionamiento.

f) Evaluar el rendimiento de los dispositivos hardware identificando posibilidades de mejoras según las necesidades de funcionamiento.

i) Implementar soluciones de alta disponibilidad, analizando las distintas opciones del mercado, para proteger y recuperar el sistema ante situaciones imprevistas.

j) Supervisar la seguridad física según especificaciones del fabricante y el plan de seguridad para evitar interrupciones en la prestación de servicios del sistema.

k) Asegurar el sistema y los datos según las necesidades de uso y las condiciones de seguridad establecidas para prevenir fallos y ataques externos.

m) Diagnosticar las disfunciones del sistema y adoptar las medidas correctivas para restablecer su funcionalidad.

n) Gestionar y/o realizar el mantenimiento de los recursos de su área (programando y verificando su cumplimiento), en función de las cargas de trabajo y el plan de mantenimiento.

o) Efectuar consultas, dirigiéndose a la persona adecuada y saber respetar la autonomía de los subordinados, informando cuando sea conveniente.

r) Adaptarse a diferentes puestos de trabajo y nuevas situaciones laborales, originadas por cambios tecnológicos y organizativos.

s) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos
dentro del ámbito de su competencia.

7 ADAPTACIÓN AL ENTORNO DE LA ECONOMÍA ANDALUZA.

El presente módulo tiene una vigencia máxima en el entorno andaluz. Puede afirmarse esto debido a que el perfil de técnico especialista capacitado para diseñar, instalar, configurar y administrar la seguridad en los sistemas informáticos es muy demandado en la actualidad en Andalucía debido a que el perfil de las empresas es mayoritariamente pequeña y mediana empresa.

8 RESULTADOS DE APRENDIZAJE Y SUS CRITERIOS DE EVALUACIÓN

Resultados de aprendizaje	Criterios de evaluación
1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. i) Se han identificado las fases del análisis forense ante ataques a un sistema.
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema

	operativo. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	a) Se han descrito las características, tipos y funciones de los cortafuegos. b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.

	c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.
5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	a) Se han identificado los tipos de proxy, sus características y funciones principales. b) b) Se ha instalado y configurado un servidor proxy-cache. c) Se han configurado los métodos de autenticación en el proxy. d) Se ha configurado un proxy en modo transparente. e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web. f) Se han solucionado problemas de acceso desde los clientes al proxy. g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor proxy en modo inverso. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. d) Se ha implantado un servidor redundante

	que garantice la continuidad de servicios en casos de caída del servidor principal. e) Se ha implantado un balanceador de carga a la entrada de la red interna. f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	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 el deber 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. g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

9 METODOLOGÍA GENERAL

Recogida en la programación del departamento.

10 CONTENIDOS BÁSICOS DEL MÓDULO

1. **Adopción de pautas y prácticas de tratamiento seguro de la información:**
   1. Fiabilidad, confidencialidad, integridad y disponibilidad.
   2. Elementos vulnerables en el sistema informático. Hardware, software y datos.
   3. Análisis de las principales vulnerabilidades de un sistema informático.
   4. Amenazas. Tipos. Amenazas físicas y lógicas.
   5. Seguridad física y ambiental.
      a) Ubicación y protección física de los equipos y servidores.
      b) Sistemas de alimentación ininterrumpida.
   6. Seguridad lógica.
      a) Criptografía.
      b) Listas de control de acceso.
      c) Establecimiento de políticas de contraseñas.
      d) Políticas de almacenamiento.
      e) Copias de seguridad e imágenes de respaldo.
      f) Medios de almacenamiento.
      g) Análisis forense en sistemas informáticos.
2. **Implantación de mecanismos de seguridad activa:**
   1. Ataques y contramedidas en sistemas personales.
      a) Clasificación de los ataques.
      b) Anatomía de ataques y análisis de software malicioso.
      c) Herramientas preventivas.
      d) Herramientas paliativas.
      e) Actualización de sistemas y aplicaciones.
      f) Seguridad en la conexión con redes públicas.
      g) Pautas y prácticas seguras.
   2. Seguridad en la red corporativa.
      a) Monitorización del tráfico en redes.

   b) Seguridad en los protocolos para comunicaciones inalámbricas.
   c) Riesgos potenciales de los servicios de red.
   d) Intentos de penetración.

3. Implantación de técnicas de acceso remoto. Seguridad perimetral:

1. Elementos básicos de la seguridad perimetral.
2. Perímetros de red. Zonas desmilitarizadas.
3. Arquitectura débil de subred protegida.
4. Arquitectura fuerte de subred protegida.
5. Redes privadas virtuales. VPN. Beneficios y desventajas con respecto a las líneas dedicadas. Técnicas de cifrado. Clave pública y clave privada.
   a) VPN a nivel de red. SSL, IPSec.
   b) VPN a nivel de aplicación. SSH.
6. Servidores de acceso remoto.
   a) Protocolos de autenticación.
   b) Configuración de parámetros de acceso.
   c) Servidores de autenticación.

4. **Instalación y configuración de cortafuegos:**

1. Utilización de cortafuegos.
2. Filtrado de paquetes de datos.
3. Tipos de cortafuegos. Características. Funciones principales.
4. Instalación de cortafuegos. Ubicación.
5. Reglas de filtrado de cortafuegos.
6. Pruebas de funcionamiento. Sondeo.
7. Registros de sucesos de cortafuegos.

5. Instalación y configuración de servidores proxy:

1. Tipos de proxy. Características y funciones.
2. Instalación de servidores proxy.
3. Instalación y configuración de clientes proxy.
4. Configuración del almacenamiento en la caché de un proxy.
5. Configuración de filtros.
6. Métodos de autenticación en un proxy

6. **Implantación de soluciones de alta disponibilidad:**

1. Definición y objetivos.
2. Análisis de configuraciones de alta disponibilidad.
   a) Funcionamiento ininterrumpido.

   b) Integridad de datos y recuperación de servicio.
   c) Servidores redundantes.
   d) Sistemas de clusters.
   e) Balanceadores de carga.
3. Instalación y configuración de soluciones de alta disponibilidad.
4. Virtualización de sistemas.
5. Posibilidades de la virtualización de sistemas.
6. Herramientas para la virtualización.
7. Configuración y utilización de máquinas virtuales.
8. Alta disponibilidad y virtualización.
9. Simulación de servicios con virtualización.

7. Legislación y normas de seguridad.
   1. Legislación sobre protección de datos.

11 CONTENIDOS.

Las unidades didácticas en las que se distribuye la asignatura son las siguientes:

1. Seguridad en los Sistemas Informáticos.
2. Seguridad activa
3. Técnicas de acceso remoto. Seguridad Perimetral.
4. Cortafuegos.
5. Proxy.
6. Alta Disponibilidad.
7. Legislación y normas de seguridad.

Tanto la temporización como la división en unidades didácticas, ha sido realizado atendiendo a distintos factores, como son la experiencia obtenida de años anteriores, la carga teórica y práctica de las distintas unidades así como las capacidades profesionales que se desarrollan en cada una de las unidades.

12 TEMPORIZACIÓN

UNIDAD	Nº SESIONES
1. Seguridad en los Sistemas Informáticos	12
2. Implantación de mecanismos de seguridad activa	14
3. Técnicas de acceso remoto. Seguridad Perimetral	8
4. Cortafuegos	14
5. Proxy	14
6. Alta Disponibilidad	16
7. Legislación y normas sobre seguridad	6
TOTAL	**84**

Total: 84 horas

La materia se impartirá durante las dos primeras evaluaciones, siendo la tercera una evaluación de repaso para el alumnado que no haya conseguido aprobar en la segunda evaluación. Aproximadamente, el reparto de unidades didácticas en evaluaciones será así:

- Primera Evaluación: Unidades 1 a 3.
- Segunda Evaluación: Unidades 4 a la 7.
- Tercera Evaluación: Repaso de las unidades 1 a la 7.

13 TABLA DE UNIDAD CON RESULTADO APRENDIZAJE

UNIDAD	RESULTADOS APRENDIZAJE	CRITERIOS DE EVALUACIÓN

1. Seguridad en los Sistemas Informáticos	1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han descrito las diferencias entre seguridad física y lógica. c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos. e) Se han adoptado políticas de contraseñas. f) Se han valorado las ventajas que supone la utilización de sistemas biométricos. g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. i) Se han identificado las fases del análisis forense ante ataques a un sistema.

2. Seguridad Activa	2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. b) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas. g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. h) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. i) Se han descrito los tipos y características de los sistemas de detección de intrusiones.

3. Técnicas de Acceso Remoto Seguro.	3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
4. Seguridad Perimetral	4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	a) Se han descrito las características, tipos y funciones de los cortafuegos. b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico. c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. h) Se ha elaborado documentación relativa a la instalación,

		configuración y uso de cortafuegos.
	5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	a) Se han identificado los tipos de proxy, sus características y funciones principales. b) b) Se ha instalado y configurado un servidor proxy-cache. c) Se han configurado los métodos de autenticación en el proxy. d) Se ha configurado un proxy en modo transparente. e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web. f) Se han solucionado problemas de acceso desde los clientes al proxy. g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas. h) Se ha configurado un servidor proxy en modo inverso. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.
5. Alta Disponibilidad	6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad. b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema. c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad. d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal. e) Se ha implantado un balanceador de carga a la entrada de la red interna. f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos. g) Se ha evaluado la utilidad de los sistemas de clusters para

		aumentar la fiabilidad y productividad del sistema. h) Se han analizado soluciones de futuro para un sistema con demanda creciente. i) Se han esquematizado y documentado soluciones para diferentes supuestos con necesidades de alta disponibilidad.
6.- Legislación y normas sobre seguridad.	7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	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 el deber 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. g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.

14 ESPECIFICACIÓN DE LAS UNIDADES DIDÁCTICAS

UNIDAD DIDÁCTICA 1. Seguridad en los Sistemas Informáticos

Descripción: Pretende dotar al alumnado de las competencias profesionales "Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo ", e "Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema."

Criterios de evaluación: 1.a, …, 1.g.	**Nº sesiones**: 6
Contenidos	**Metodología**
Adopción de pautas y prácticas de tratamiento seguro de la información: Fiabilidad, confidencialidad, integridad y disponibilidad. Elementos vulnerables en el sistema informático. Hardware, software y datos. Análisis de las principales vulnerabilidades de un sistema informático. Amenazas. Tipos. Amenazas físicas y lógicas. Seguridad física y ambiental. Ubicación y protección física de los equipos y servidores. Sistemas de alimentación ininterrumpida. Seguridad lógica. Criptografía. Listas de control de acceso. Establecimiento de políticas de contraseñas. Políticas de almacenamiento. Copias de seguridad e imágenes de respaldo. Medios de almacenamiento. Análisis forense en sistemas informáticos.	• Exposiciones teóricas. • Búsquedas en Internet de información técnica relativa al tema. • El alumnado realizará guías tipo how-to. • Debates en clase sobre el tema. • Ejercicios y supuestos prácticos. • Prácticas de Criptografía.
Observaciones:	

<table>
<tr><th colspan="2">UNIDAD DIDÁCTICA 2: Seguridad Activa</th></tr>
<tr><td colspan="2">Descripción: Pretende dotar al alumnado de la competencia profesional “Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.”</td></tr>
<tr><td>Criterios de evaluación: 2.a, ..., 2.g.</td><td>Nº sesiones: 8</td></tr>
<tr><th>Contenidos</th><th>Metodología</th></tr>
<tr><td>Implantación de mecanismos de seguridad activa:
Ataques y contramedidas en sistemas personales.
• Clasificación de los ataques.
• Anatomía de ataques y análisis de software malicioso.
• Herramientas preventivas.
• Herramientas paliativas.
• Actualización de sistemas y aplicaciones.
• Seguridad en la conexión con redes públicas.
• Pautas y prácticas seguras.
Seguridad en la red corporativa.
• Monitorización del tráfico en redes.
• Seguridad en los protocolos para comunicaciones inalámbricas.
• Riesgos potenciales de los servicios de red.
• Intentos de penetración.</td><td>• Exposiciones teóricas.
• Búsquedas en Internet de información técnica relativa al tema.
• El alumnado realizará guías tipo how-to.
• Debates en clase sobre el tema.
• Ejercicios y supuestos prácticos.
• Prácticas de sniffing.
• Prácticas de ataques.
• Prácticas de defensa.</td></tr>
<tr><td colspan="2">Observaciones:</td></tr>
</table>

UNIDAD DIDÁCTICA 3: Seguridad Perimetral

Descripción: Pretende dotar al alumnado de las competencias profesionales "Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna" y "Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio."

Criterios de evaluación: 4.a, ..., 4.h, 5.a, ..., 5.i	**Nº sesiones**: 16
Contenidos	**Metodología**
Instalación y configuración de cortafuegos: • Utilización de cortafuegos. • Filtrado de paquetes de datos. • Tipos de cortafuegos. Características. Funciones principales. • Instalación de cortafuegos. Ubicación. • Reglas de filtrado de cortafuegos. • Pruebas de funcionamiento. Sondeo. • Registros de sucesos de cortafuegos. **Instalación y configuración de servidores proxy:** • Tipos de proxy. Características y funciones. • Instalación de servidores proxy. • Instalación y configuración de clientes proxy. • Configuración del almacenamiento en la caché de un proxy. • Configuración de filtros. • Métodos de autenticación en un proxy	• Exposiciones teóricas. • Búsquedas en Internet de información técnica relativa al tema. • El alumnado realizará guías tipo how-to. • Debates en clase sobre el tema. • Boletín de Ejercicios prácticos de iptables. • Prácticas de iptables. • Prácticas de Proxy.
Observaciones:	

<table>
<tr><th colspan="2">UNIDAD DIDÁCTICA 4: Técnicas de Acceso Remoto Seguro</th></tr>
<tr><td colspan="2">Descripción: Pretende dotar al alumnado de la competencia profesional “Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.”</td></tr>
<tr><td>Criterios de evaluación: 3.a, ..., 3.g</td><td>Nº sesiones: 4</td></tr>
<tr><th>Contenidos</th><th>Metodología</th></tr>
<tr><td>Implantación de técnicas de acceso remoto. Seguridad perimetral:
1. Elementos básicos de la seguridad perimetral.
2. Perímetros de red. Zonas desmilitarizadas.
3. Arquitectura débil de subred protegida.
4. Arquitectura fuerte de subred protegida.
5. Redes privadas virtuales. VPN. Beneficios y desventajas con respecto a las líneas dedicadas. Técnicas de cifrado. Clave pública y clave privada.
6. VPN a nivel de red. SSL, IPSec.
7. VPN a nivel de aplicación. SSH.
8. Servidores de acceso remoto.
9. Protocolos de autenticación.
10. Configuración de parámetros de acceso.
11. Servidores de autenticación.</td><td>• Exposiciones teóricas.
• Búsquedas en Internet de información técnica relativa al tema.
• El alumnado realizará guías tipo how-to.
• Debates en clase sobre el tema.
• Ejercicios y supuestos prácticos.
• Prácticas de instalación y administración de un servidor ssh en Linux.
• Prácticas de instalación y administración de un servidor de acceso remoto en Windows Server.</td></tr>
<tr><td colspan="2">Observaciones:</td></tr>
</table>

UNIDAD DIDÁCTICA 5: Alta Disponibilidad	
Descripción: Pretende dotar al alumnado de la competencia profesional "Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba."	
Criterios de evaluación:6.a, ..., 6.i	**Nº sesiones**: 8
Contenidos	**Metodología**

Implantación de soluciones de alta disponibilidad:
1. Definición y objetivos.
2. Análisis de configuraciones de alta disponibilidad.
  1. Funcionamiento ininterrumpido.
  2. Integridad de datos y recuperación de servicio.
  3. Servidores redundantes.
  4. Sistemas de clusters.
  5. Balanceadores de carga.
3. Instalación y configuración de soluciones de alta disponibilidad.
  1. Virtualización de sistemas.
  2. Posibilidades de la virtualización de sistemas.
  3. Herramientas para la virtualización.
  4. Configuración y utilización de máquinas virtuales.
  5. Alta disponibilidad y virtualización.
  6. Simulación de servicios con virtualización.
	• Exposiciones teóricas.
	• Búsquedas en Internet de información técnica relativa al tema.
	• El alumnado realizará guías tipo how-to.
	• Debates en clase sobre el tema.
	• Ejercicios y supuestos prácticos.
	• Prácticas de virtualización.

Observaciones:	

UNIDAD DIDÁCTICA 6: Normativa sobre seguridad	
Descripción: Pretende dar al alumnado una visión general sobre la normativa que afecta a la seguridad.	
Criterios de evaluación:7.a, ..., 7.g	**Nº sesiones**: 8
Contenidos	**Metodología**
Reconocimiento de la legislación y normativa sobre seguridad y protección de datos: 1. Legislación sobre protección de datos. Figuras legales en el tratamiento y mantenimiento de los ficheros de datos. 2. Legislación sobre los servicios de la sociedad de la información y correo electrónico.	• Exposiciones teóricas. • Búsquedas en Internet de información técnica relativa al tema. • El alumnado realizará guías tipo how-to. • Debates en clase sobre el tema. • Ejercicios y supuestos prácticos.
Observaciones:	

15 CONTENIDOS ACTITUDINALES

Recogidos en la programación del departamento.

16 PROCESO DE EVALUACIÓN – CALIFICACIÓN. Relación de instrumentos de evaluación con las unidades, criterios de evaluación e indicadores

Cada unidad didáctica debe ser superada por separado y teniendo en cuenta que los contenidos de dichas unidades son independientes, la superación de una unidad didáctica no puede implicar la superación de otras.

La separación de unidades didácticas por evaluaciones será la siguiente:

Unidad Didáctica	Evaluación
1,2,3	1ª
4,5,6,7	2ª
Todas (recuperación)	3ª

Para aprobar la asignatura debe aprobarse cada una de las unidades didácticas completas por separado, esto es, el/la alumn@ debe aprobar las unidades 1, 2, 3, 4,5,6 y 7 por separado.

Unidad Didáctica 1									
Criterios de Evaluación	1								
Indicadores	1.a	1.b	1.c	1.d	1.e	1.f	1.g	1.h	1.i
Práctica					x		x		
Examen	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen1									

Unidad Didáctica 2									
Criterios de Evaluación	1								
Indicadores	2.a	2.b	2.c	2.d	2.e	2.f	2.g	2.h	2.i
Práctica					x		x		
Examen	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen1									

Unidad Didáctica 2									
Criterios de Evaluación	1								
Indicadores	2.a	2.b	2.c	2.d	2.e	2.f	2.g	2.h	2.i
Práctica					x		x		
Examen	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen1									

Unidad Didáctica 3							
Criterios de Evaluación	3						
Indicadores	3.a	3.b	3.c	3.d	3.e	3.f	3.g
Práctica				x	x	x	x
Examen	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen							

Unidad Didáctica 4								
Criterios de Evaluación	4							
Indicadores	4.a	4.b	4.c	4.d	4.e	4.f	4.g	4.h
Práctica1				x	x	x		x
Examen1	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen								

Unidad Didáctica 5									
Criterios de Evaluación	5								
Indicadores	5.a	5.b	5.c	5.d	5.e	5.f	5.g	5.h	5.i
Práctica		x	x	x	x	x	x	x	x
Examen	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen									

Unidad Didáctica 6									
Criterios de Evaluación	6								
Indicadores	6.a	6.b	6.c	6.d	6.e	6.f	6.g	6.h	6.i
Práctica				x	x	x	x	x	x
Examen	x	x	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: 0,3*Práctica + 0,7*Examen									

Unidad Didáctica 7							
Criterios de Evaluación	7						
Indicadores	7.a	7.b	7.c	7.d	7.e	7.f	7.g
Test	x	x	x	x	x	x	x
Criterios de Calificación: • Cada prueba se calificará entre 0 y 10. • La calificación del módulo será igual a: Test							

Criterios de calificación generales

- Cada unidad didáctica coincide con un módulo de contenidos.
- Un módulo estará aprobado o superado si su nota es igual a superior a cinco (5).
- Los módulos aprobados se guardan hasta el final del curso.
- La entrega de trabajos y prácticas fuera de fecha implica que se evaluará negativamente a razón de -0,5 ptos por semana de retraso o fracción.
- Todos los trabajos tendrán que entregarse antes de las distintas pruebas de recuperación para poder presentarse a las mismas.
- **La nota de la 1ª Evaluación** será:
  - Si se han superado los módulos 1,2 y 3 la nota de la 1ª Evaluación será la media aritmética de las notas de dichos módulos.
  - Si NO se ha superado alguno de los módulos, la nota de la 1ª Evaluación será la media aritmética de las notas de dichos módulos, siempre que ésta sea igual o inferior a cuatro (4). En otro caso, la nota de la 1ª Evaluación será igual a cuatro (4).
- **La nota de la 2ª Evaluación** será:
  - Si se han superado los módulos 4, 5,6 y 7 la nota de la 2ª Evaluación será la media aritmética de las notas de dichos módulos.
  - Si NO se ha superado alguno de los módulos módulos, la nota de la 2ª Evaluación será la media aritmética de las notas de dichos módulos, siempre que ésta sea igual o inferior a cuatro (4). En otro caso, la nota de la 2ª Evaluación será igual a cuatro (4).
- **La nota final del curso** vendrá determinada por la nota de todos los módulos:
  - Si se han superado TODOS los módulos, la nota final será la media aritmética de las notas de los módulos.
  - Si NO se ha superado alguno de los módulos, la nota final será la media aritmética de las notas de los módulos, siempre que ésta sea igual o inferior a cuatro (4). En otro caso, la nota final será igual a cuatro (4).

- **Ocasiones para aprobar cada módulo:**
  - 1ª Oportunidad: Cuando se termine de impartir cada módulo y se hayan ejecutado todas sus pruebas, se le dará al alumnado la nota que ha obtenido en el mismo.
  - 1ª Evaluación: Al final de la 1ª evaluación se harán las pruebas necesarias para que el alumnado pueda recuperar los módulos 1, 2 y 3.
  - 2ª Evaluación: Al final de la 2ª evaluación se harán las pruebas necesarias para que el alumnado pueda recuperar los módulos 1, 2, 3, 4,5,6 y 7.
  - 3ª Evaluación: Al final de la 3ª evaluación se harán las pruebas necesarias para que el alumnado pueda recuperar los módulos 1, 2, 3, 4, 5, 6 y 7.
- El alumnado que tenga módulos aprobados podrán optar a presentarse a subir nota exclusivamente al final de la 2ª y de la 3ª evaluación. En cualquier caso se les guardarán las notas aprobadas y no podrán bajar nota.

17 ADAPTACIONES CURRICULARES.

Recogidas en la programación del departamento.

18 RECURSOS DIDÁCTICOS.

En el caso de este módulo los recursos los dividimos en dos tipos: Humanos y Materiales.

a) **Recursos Humanos:** El módulo cuenta con un profesor titular.
b) **Recursos Materiales:** Se pueden inventariar los siguientes:
    - *Un aula taller,* donde se ubican todas las clases del grupo tanto prácticas como teóricas
    - Un proyector de video/SVGA.
    - Cuatro servidores de virtualización para prácticas (Intel i5, 16 Gb RAM, 1Tb SSD).
    - Un ordenador por cada alumno/a (Intel i3, 6 u 8 Gb de RAM, 500 Gb de disco duro, tarjeta de red Gigabit Ethernet y tarjeta de red Wifi 802.11n).
    - Una impresora láser.
    - Una LAN cableada GigabitEth que integra todos los ordenadores de los talleres del Departamento de Informática.
    - Una red Wifi de soporte conectada a la red del Centro.
    - Licencias Microsoft ilimitadas de todos los sistemas operativos, herramientas de desarrollo y de servicios de Internet (Plan DreamSpark para instituciones de enseñanza TIC).
    - *Linux* de libre distribución.
    - Plataforma Moodle *aula.iesjulioverne.es* de apoyo.
    - Servidor Proxmox del Departamento para prácticas y exámenes.
    - Acceso a Internet por red propia del Departamento de Informática de 600/600Mbps.
    - Acceso a Internet alternativo por red del Centro de 1,2 Gbps.

19 BIBLIOGRAFÍA RECOMENDADA.

Toda la bibliografía recomendada consiste en documentos y webs técnicas, de acceso libre y gratuito. Su uso varía mucho con el tiempo, estando siempre referenciadas en la plataforma Moodle de esta asignatura.

20 ANEXO I. SUSPENSIÓN DE CLASES PRESENCIALES POR CONFINAMIENTO

Recogido en la programación del departamento.