PROGRAMACIÓN DIDÁCTICA DEL MÓDULO PROFESIONAL

”Seguridad y Alta Disponibilidad”

Código 0378

Curso escolar 2018-19

Xº Curso del Ciclo Formativo de Grado Superior de Administración de Sistemas Informáticos en Red

Profesorado: José Ramón Albendín Ramírez

Índice de contenido

1 Descripción del módulo.

1.1 Identificación del módulo

Identificación	MÓDULO PROFESIONAL	*SEGURIDAD Y ALTA DISPONIBILIDAD*
	CÓDIGO	*0378*
	FAMILIA PROFESIONAL:	*Informática y Comunicaciones*
	TITULO PROF	*Técnico Superior en Administración de Sistemas Informáticos en Red*
	Curso	*2º*
	GRADO	*Superior*
Distribución Horaria	HORARIO Y DURACIÓN:	*4 horas semanales. Total: 84 horas*
Tipología de Módulo	Asociado a Unidad de Competencia	*UC0486_3: Asegurar equipos informáticos.*
	Transversal	*No*

1.2 Marco legal

	Estatal	**Autonómica**
Ordenación	**Ley Orgánica 2/2006**, de 3 de mayo, de Educación modificada por ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa. **Real Decreto 1147/2011**, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.	**Ley 17/2007**, de 10 de diciembre, de Educación de Andalucía. **Decreto 327/2010**, de 13 de julio, por el que se aprueba el Reglamento Orgánico de los Institutos de Educación Secundaria.
Perfil Profesional	**Ley Orgánica 5/2002** de 19 de junio, de las Cualificaciones y de la Formación Profesional que pone en marcha del Sistema Nacional de Cualificaciones y	*(No existe normativa aplicable a nivel autonómico al no tener competencias nuestra Comunidad Autónoma).*

	Formación Profesional. **Real Decreto 1416/2005** de 25 de noviembre, sobre el Catálogo Nacional de Cualificaciones Profesionales. **Real Decreto 295/2004**, de 20 de febrero, y modificada en el Real Decreto 109/2008, de 1 de febrero.	
Título	**Real Decreto *1629/2009, de 30 de octubre*** , por el que se establece el Título de Técnico Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.	ORDEN de 19 de julio de 2010, por la que se desarrolla el currículo correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red (BOJA 27-08-2010). *Desarrolla el Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red, y sustituye en Andalucía al título de Técnico Superior en Administración de Sistemas Informáticos, regulado por el Decreto 131/1995.*
Evaluación	*(No existe normativa aplicable a nivel autonómico al no tener competencias nuestra Comunidad Autónoma).*	**Orden de 29 de septiembre de 2010**, por la que se regula la evaluación, certificación, acreditación y titulación académica del alumnado que cursa enseñanzas de formación profesional inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía.

2 Competencias profesionales, personales y sociales del módulo profesional.

De acuerdo con la Orden de 19 de julio de 2010, la formación del módulo Planificación y

Administración de Redes contribuye a alcanzar las siguientes **competencias profesionales**, personales y sociales del título:

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.

3 Objetivos generales a los que contribuye el Módulo Profesional.

La formación del módulo **contribuye a alcanzar los objetivos generales de este ciclo** formativo que se relacionan a continuación:

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.

4 Resultados de Aprendizaje (RA).

4.1 Relación Objetivos-RA

RELACIÓN ENTRE OBJETIVOS GENERALES Y RESULTADOS DE APRENDIZAJE

	RA 1: Adopta pautas y prácticas de tratamiento seguro ...	RA 2: Implanta mecanismos de seguridad activa, seleccionando y ejecutando contra...	RA 3: Implanta técnicas seguras de acceso remoto a un sistema ….	RA 4: Implanta cortafuegos para asegurar un sistema informático...	RA 5: Implanta servidores proxy, aplicando criterios de configuración ...	RA 6: Implanta soluciones de alta disponibilidad empleando técnicas de virtua...	RA 7: Reconoce la legislación y normativa sobre seguridad y protección de dat...
j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales...	X	X	X	X		X	X
k) Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad...	X	X	X	X		X	X
l) Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas...			X	X	X		X
m) Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad...	X	X	X	X	X	X	X
o) Establecer la planificación de tareas, analizando actividades y cargas de trabajo del sistema para gestionar el mantenimiento.	X	X	X	X	X	X	X

4.2 RA y Criterios de Evaluación.

RA1. 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.

RA2. 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.

RA3. 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 interna.
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.
RA4. 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.
RA5. 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) 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.

RA6. 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.

RA7. 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.

5 Bloques de contenidos básicos.

Adopción de pautas y prácticas de tratamiento seguro de la información.

Implantación de mecanismos de seguridad activa.

Implantación de técnicas de acceso remoto. Seguridad perimetral.

Instalación y configuración de cortafuegos.

Instalación y configuración de servidores proxy.

Implantación de soluciones de alta disponibilidad.

Reconocimiento de la legislación y normativa sobre seguridad y protección de datos.

6 Unidades didácticas.

Unidad 1. 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.

Unidad 2. Legislación y normativa.

- Legislación sobre protección de datos. Figuras legales en el tratamiento y mantenimiento de los ficheros de datos.
- Legislación sobre los servicios de la sociedad de la información y correo electrónico.

Unidad 3. 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.

Unidad 4. Acceso remoto. Seguridad perimetral

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

Unidad 5. 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.

Unidad 6. 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.

Unidad 7. Alta disponibilidad.

- Definición y objetivos.
- Análisis de configuraciones de alta disponibilidad.
  - Funcionamiento ininterrumpido.
  - Integridad de datos y recuperación de servicio.
  - Servidores redundantes.
  - Sistemas de clusters.
  - Balanceadores de carga.
- Instalación y configuración de soluciones de alta disponibilidad.
- Virtualización de sistemas.
- Posibilidades de la virtualización de sistemas.
- Herramientas para la virtualización.
- Configuración y utilización de máquinas virtuales.
- Alta disponibilidad y virtualización.
- Simulación de servicios con virtualización.

7 Tablas de relación entre Objetivos, Unidades didácticas y los RA.

7.1 Relación entre las U.D. y los R.A. y su temporalización.

Unidades didácticas	RA1	RA2	RA3	RA4	RA5	RA6	RA7	Carga horaria
1. Trat. seguro información	*							12 h (14 %)
2. Legislación y normativa							*	8 h (9 %)
3. Seguridad activa		*						12 h (14 %)
4. Acceso remoto. Seg. Per.			*					14 h (16 %)
5. Cortafuegos				*				16 h (19 %)
6. Servidores proxy					*			8 h (9 %)
7. Sol. Alta disponibilidad						*		14 h (16 %)

7.2 Relación y ponderación entre los R.A. y los Criterios de Evaluación

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.	15%	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos.	10%	EXT,TRI,TRG
		b) Se han descrito las diferencias entre seguridad física y lógica.	10%	EXT,TRI,TRG
		c) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen.	10%	EXT,TRI,TRG
		d) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos.	10%	EXT,TRI,TRG
		e) Se han adoptado políticas de contraseñas.	10%	EXP,EXT,TRI,TRG
		f) Se han valorado las ventajas que supone la utilización de sistemas biométricos.	10%	EXT,TRI,TRG
		g) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información.	20%	EXP,TRI,TRG
		h) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas.	10%	EXT,TRI,TRG
		i) Se han identificado las fases del análisis forense ante ataques a un sistema.	10%	EXT,TRI,TRG
		Criterios de Evaluación	%	Instrumentos

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.	10%	a) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático.	10%	EXT,TRI
		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.	10%	EXP,TRI
		c) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.	10%	EXT,TRI
		d) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.	10%	EXT,TRI
		e) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.	15%	EXP,TRI
		f) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.	15%	EXP,TRI
		g) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas.	10%	EXT,TRI

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.	15%	a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	5%	EXT,TRI
		b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	5%	EXT,TRI
		c) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización.	10%	EXT,TRI
		d) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles.	20%	EXP,TRG,TRI
		e) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas.	20%	EXP,TRG,TRI
		f) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela.	20%	EXP,TRG,TRI
		g) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.	20%	EXP,TRG,TRI
		Criterios de Evaluación	%	Instrumentos
		a) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna.	5%	EXT,TRI
		b) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral.	5%	EXT,TRI

Resultados de aprendizaje	%	Criterios de Evaluación	%	Intrumentos
4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.	20%	a) Se han descrito las características, tipos y funciones de los cortafuegos.	10%	EXT, TRI
		b) Se han clasificado los niveles en los que se realiza el filtrado de tráfico.	10%	EXT, TRI
		c) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red.	10%	EXT, TRI
		d) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado.	15%	EXP, EXT,TRI
		e) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente.	15%	EXP,TRI
		f) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware.	15%	EXP,TRI
		g) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos.	15%	EXP,TRI
		h) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos.	10%	TRI
		Criterios de Evaluación	%	Intrumentos

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
5. Implanta servidores proxy, aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.	10%	a) Se han identificado los tipos de proxy, sus características y funciones principales.	5%	EXT,TRI
		b) Se ha instalado y configurado un servidor proxy-cache.	5%	EXP,TRI
		c) Se han configurado los métodos de autenticación en el proxy.	15%	EXP,TRI
		d) Se ha configurado un proxy en modo transparente.	10%	EXP,TRI
		e) Se ha utilizado el servidor proxy para establecer restricciones de acceso web.	15%	EXP,TRI
		f) Se han solucionado problemas de acceso desde los clientes al proxy.	15%	EXP,TRI
		g) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas.	15%	EXP,TRI
		h) Se ha configurado un servidor proxy en modo inverso.	15%	EXP,TRI
		i) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.	5%	TRI

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.	15%	a) Se han analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.	5%	EXT,TRI
		b) Se han identificado soluciones hardware para asegurar la continuidad en el funcionamiento de un sistema.	5%	EXT,TRI
		c) Se han evaluado las posibilidades de la virtualización de sistemas para implementar soluciones de alta disponibilidad.	5%	EXT,TRI
		d) Se ha implantado un servidor redundante que garantice la continuidad de servicios en casos de caída del servidor principal.	20%	EXP,TRI
		e) Se ha implantado un balanceador de carga a la entrada de la red interna.	20%	EXP,TRI
		f) Se han implantado sistemas de almacenamiento redundante sobre servidores y dispositivos específicos.	20%	EXP,TRI
		g) Se ha evaluado la utilidad de los sistemas de clusters para aumentar la fiabilidad y productividad del sistema.	10%	EXT,TRI
		h) Se han analizado soluciones de futuro para un sistema con demanda creciente.	10%	EXT,TRI

Resultados de aprendizaje	%	Criterios de Evaluación	%	Instrumentos
7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.	10%	a) Se ha descrito la legislación sobre protección de datos de carácter personal.	15%	EXT,TRI
		b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.	15%	EXT,TRI
		c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.	10%	EXT,TRI
		d) Se ha contrastado el deber de poner a disposición de las personas los datos personales que les conciernen.	15%	EXT,TRI
		e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.	15%	EXT,TRI
		f) Se han contrastado las normas sobre gestión de seguridad de la información.	15%	EXT,TRI
		g) Se ha comprendido la necesidad de conocer y respetar la normativa legal aplicable.	15%	EXT,TRI

8 Contenidos Transversales.

Muchos de los problemas que padece nuestra sociedad tienen que ver con la falta de educación en valores, de ahí la necesidad de incluir en los currículos de nuestro sistema educativo los llamados temas transversales. Los contenidos de carácter trasversal estarán presentes de forma continuada en el día a día del módulo. Los contenidos clave son:

- Educación moral y cívica, donde se desarrollarán criterios de actuación que favorezcan intercambios responsables y comportamientos de respeto, honestidad, tolerancia y flexibilidad con los compañeros, paro lo cual, colocaremos al alumnado en situaciones que le supongan un conflicto o dilema, en las que tenga que reflexionar, valorar, argumentar, decidir y/o actuar sobre este tema.
- Educación para la paz, donde se desarrollarán habilidades para el trabajo en grupo, escuchando y respetando las opiniones de los demás y se trabajará con los mismos estándares que en toda la comunidad internacional están implantados. Se realizarán prácticas en grupo, organizando el trabajo para una armoniosa colaboración entre sus componentes.
- Educación para la salud, respetando las normas de seguridad e higiene referidas a la manipulación de herramientas, equipos e instalaciones, efectuando las prácticas con rigor, de forma que el resultado cumpla con la normativa y no tenga efectos nocivos para la salud o integridad física de las personas y así conseguir que el alumnado reflexione sobre la necesidad de establecer unas normas de seguridad e higiene personales y del producto, que las conozca y las ponga en práctica en el desarrollo de las actividades formativas, así como tomen conciencia de las posibles consecuencias de no cumplirlas.
- Educación ambiental, para que el alumnado desarrolle criterios de uso racional de los recursos existentes, tomando conciencia de su escasez o agotamiento, conociendo las alternativas disponibles (reutilización, reciclaje...) y las repercusiones ecológicas. Concienciaremos al alumnado de la necesidad de efectuar una correcta disposición de los residuos para facilitar su posterior reciclaje.
- Educación para la igualdad de oportunidades entre ambos sexos, tomando una actitud abierta a nuevas formas organizativas basadas en el respeto, la cooperación y el bien común, prescindiendo de los estereotipos de género vigentes en la sociedad, profundizando en la condición humana, en su dimensión emocional, social, cultural y fisiológica, estableciendo condiciones de igualdad en el trabajo en equipo. Además

debe desarrollarse un uso del lenguaje no sexista y mantener una actitud crítica frente a expresiones sexistas a nivel oral y escrito. El artículo 14 de la Constitución inspira y debe inspirar todas las actividades de enseñanza “Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social”.

- Nuevas tecnologías, donde los alumnos y alumnas valoren e incorporen las nuevas tecnologías, familiarizándose con los instrumentos que ofrece la tecnología para crear, recoger, almacenar, organizar, procesar, presentar y comunicar la información. Utilizando las nuevas tecnologías en la consulta de información técnica, en los informes, memorias y exposiciones orales y escritas.

9 Orientaciones pedagógicas y líneas de actuación en el proceso de enseñanza-aprendizaje

Este módulo profesional contiene la formación necesaria para seleccionar y utilizar técnicas y herramientas específicas de seguridad informática en el ámbito de la administración de sistemas. Además, servirá para conocer arquitecturas de alta disponibilidad y utilizar herramientas de virtualización en la implantación de servicios de alta disponibilidad. Las funciones de la administración segura de sistemas incluyen aspectos como:

- El conocimiento y correcta manipulación de todos los elementos que forman el componente físico y lógico de los equipos.
- La adopción de prácticas seguras de acuerdo al plan de seguridad física del sistema.
- La adopción de prácticas seguras de acuerdo al plan de seguridad lógica del sistema.
- El conocimiento y uso de técnicas seguras de acceso remoto a un sistema, tanto en modo usuario como en modo administrativo.
- La selección y aplicación de técnicas y herramientas de seguridad activa que actúen como medidas preventivas y/o paliativas ante ataques a al sistema.
- La instalación y configuración de herramientas de protección perimetral, cortafuegos y servidores proxy.
- La instalación y configuración de servicios de alta disponibilidad que garanticen la continuidad de servicios y la disponibilidad de datos.
- El conocimiento y aplicación de la legislación vigente en el ámbito del tratamiento digital de la información.
-

10 Metodología.

10.1 Del proceso de enseñanza

Los principios de actuación metodológica serán:

- **Aprendizaje activo, funcional y autónomo:** facilitar al alumnado la construcción de sus propios aprendizajes, la comprobación y el interés de la utilidad de lo aprendido y la funcionalidad de los aprendizajes.
- **Constructivismo y aprendizaje significativo**: el alumnado elabora el conocimiento haciéndolo suyo para poder construir los nuevos conocimientos, favoreciendo asía el pensamiento crítico al producir conocimientos más duraderos y significativos.
- **Cooperativismo**: el aprendizaje cooperativo se basa en la construcción participativa del conocimiento. Dentro del proceso de aprendizaje cooperativo se destaca la participación activa y la interacción tanto de alumnado como de profesorado.
- **Individualización**: se tendrá en cuenta los intereses y motivaciones personales para motivar más al alumnado. Además se hará un seguimiento continuo de cada alumno/a.
- **Creatividad**: se pretende formar a personas amantes de los riesgos y listas para afrontar los obstáculos y problemas que se les presentarán en el mundo labora.
- **Conectivismo**: mediante el uso de las TIC, formarán redes y comunidades para lograr un aprendizaje permanente.

En cada una de las unidades se profundizará en la adquisición de competencias profesionales pero siempre bajo una visión global de los procesos que se van a realizar. Todas las unidades de trabajo estarán relacionadas entre sí, de tal manera que los conocimientos adquiridos serán aplicados en las siguientes y en diversas situaciones a lo largo del curso.

El desarrollo del módulo comprende aspectos tanto teóricos como prácticos. En todo caso:

- Al alumno se le introducirá en la materia planteándole problemas y dudas y desarrollando aspectos teóricos necesarios para su identificación y posterior resolución (teórica y práctica).
- El alumno investigará y analizará mediante la consulta de revistas, libros especializados, instrucciones de dispositivos, artículos de periódicos, ficheros de ayudas y sitios Web. Profundizará de forma autónoma para la resolución de problemas.
- Identificará casos prácticos que evaluará, documentará y resolverá. debe gozar el alumno, el profesorado supervisará en todo momento su evolución, solicitará trabajos y ejercicios y procurará una metodología racional y crítica.

10.2 Del tiempo, espacio y agrupamientos.

Su fin es adecuar las diversas actividades al tempo disponible, entendiendo siempre esta adecuación como flexible a las necesidades y características del momento.

El orden en el que llevamos a cabo la temporalización es:
1º) Asignar un periodo realista de tiempo a cada Unidad Didáctica.
2º) Secuenciar sus contenidos y el tiempo para cada actividad.
3º) Prever posibles horas dedicadas a actividades extraescolares.

Los agrupamientos serán diferentes y flexibles en función de los objetivos y los contenidos. Se harán equipos de trabajo con el fin de usar estrategias de indagación que posteriormente requeriran de exposiciones verbales, gráficas o documentales.

10.3 Materiales y recursos didácticos

Toda la documentación necesaria para el estudio por parte de los alumnos estará en el portal de teleformación:

http://moodle.iesgrancapitan.org

11 Medidas de atención a la diversidad.

La metodología de trabajo incluye distintas actividades individuales y trabajos en equipo que facilitan la adaptabilidad del ritmo de aprendizaje, con distintos ritmos de trabajo que facilitan tanto el refuerzo como la ampliación de contenidos.

Esto es así para paliar los desfases detectados y propiciar un mejor nivel de adquisición de conocimientos.

Durante el periodo comprendido entre la última evaluación parcial y la evaluación final, se realizarán actividades de refuerzo o de mejora de las competencias, que permitan al alumnado matriculado en la modalidad presencial la superación del módulo profesional pendiente de evaluación positiva o, en su caso, mejorar la calificación obtenida en el mismo.

Para el alumnado que haya obtenido evaluación positiva, las actividades de mejora de las competencias profundizarán en contenidos del módulo, desarrollados preferentemente como proyectos propuestos por el profesorado que lo imparte.

Por otra parte, y para el alumnado cuya evaluación no haya resultado positiva, se planificarán actividades de refuerzo, desarrolladas a modo de ejercicios, prácticas y pruebas escritas.

12 Evaluación.

12.1 Instrumentos de Evaluación.

Cada criterio de evaluación de cada resultado de aprendizaje tiene asociados unos instrumentos de evaluación enumerados por prioridad:

- EXT: Pruebas teóricas
- EXP: Pruebas prácticas
- TRI: Trabajo individual
- TRG: Trabajo en grupo.
- RUB: Rúbricas para evaluar las diferentes pruebas prácticas y trabajos.

Los instrumentos de evaluación se concretarán para cada unidad de trabajo en la programación de aula y serán decisión de cada docente.

Todas las calificaciones se recogerán en el cuaderno del profesor, donde aparecerán reflejadas todas las variables a evaluar y su correspondiente calificación.

12.2 Requisitos para una calificación positiva

En el apartado 1 del Art. 16 de la Orden de 29 de septiembre de 2010, indica que "*la evaluación conllevará una calificación que reflejará los resultados obtenidos por el alumno o alumna en su proceso de enseñanza-aprendizaje. La calificación de los módulos profesionales de formación en el centro educativo y del módulo profesional de proyecto se expresará en valores numéricos de 1 a 10, sin decimales. Se considerarán positivas las iguales o superiores a 5 y negativas las restantes*".

Para superar el módulo, el alumnado debe haber alcanzado todos los resultados de aprendizaje establecidos en la Orden que regula la titulación en la que se encuentra enmarcado el presente módulo, es decir, deberá superar cada uno de ellos de manera individual con una nota igual o superior a 5 sobre 10.

13 Actividades de refuerzo

Se contemplarán en la programación de aula dentro del desarrollo de cada una de las unidades, serán de carácter individual y estarán enfocadas a ayudar al alumnado a conseguir los resultados de aprendizaje en nivel suficiente como para poder obtener una calificación positiva del módulo.

14 Actividades de mejora de resultados y ampliación

Para aquellos alumnos con mayor capacidad o mayor interés, la atención a la diversidad se concretará en:

- Oferta de una adecuada diversificación y ampliación de los aspectos del saber y del saber hacer.

- Diseño por parte de los alumnos implicados diferentes actividades de ampliación, estimulando así la formación de personas autónomas.

Tanto las actividades de refuerzo/recuperación como las de ampliación, están planificadas para ser realizadas entre la sesión de evaluación previa a la realización del módulo profesional de formación en centros de trabajo y la sesión de evaluación final, según se indica en el apartado 4.c del artículo 2 de la Orden de 29 de septiembre de 2010: "*La determinación y planificación de las actividades de refuerzo o mejora de las competencias, que permitan al alumnado matriculado en la modalidad presencial la superación de los módulos profesionales pendientes de evaluación positiva o, en su caso, mejorar la calificación obtenida en los mismos. Dichas actividades se realizarán en primer curso durante el periodo comprendido entre la última evaluación parcial y la evaluación final y, en segundo curso durante el periodo comprendido entre la sesión de evaluación previa a la realización del módulo profesional de formación en centros de trabajo y la sesión de evaluación final.*"

15 Pérdida de evaluación continua

Tal y como se indica en el ROF del centro, la asistencia regular a las clases es un requisito imprescindible para la evaluación y calificación continuas. En esta línea, la expresión "asistencia regular" y sus efectos sobre la evaluación continua se pueden especificar en los siguientes términos:

- El derecho a la evaluación continua, lo pierde cualquier alumno que haya tenido faltas de asistencia, justificadas y no justificadas, **en la medida que establece el Reglamento Organización y Funcionamiento del Centro**.
- Aquellos alumnos que pierdan el derecho a la evaluación continua, tendrán derecho a un sistema de evaluación especial que consistirá en un conjunto de pruebas y trabajos individuales, asociados a cada Criterio de Evaluación.

16 Procedimiento para el seguimiento de la programación.

La programación será revisada a final de curso y se establecerán los cambios acordados, si procede, por el equipo docente.