Introducción

La normativa de referencia a tener en cuenta para la elaboración de la programación didáctica del módulo de **Seguridad y Alta Disponibilidad** (***SAD***) es la siguiente:

- El Real Decreto 1147/2011, de 29 de Julio**,** por el que se establece la ordenación general de la formación profesional del sistema educativo.
- El Real Decreto 1629/2009, de 30 de octubre, establece el título de **Técnico Superior en Administracion de Sistemas Informáticos en Red**, y fija sus enseñanzas mínimas.
- La 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** (***ASIR***) en Andalucía.
- Resto de disposiciones de aplicación para evaluación, organización de enseñanzas a distancia, etc.

Este módulo profesional contiene parte de la formación necesaria para desempeñar la función de Administración de Sistemas Informáticas en Red, que incluye aspectos como:

- Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha soluciones de alta disponibilidad.
- Identificar condiciones de equipos e instalaciones, interpretando planes de seguridad y especificaciones de fabricante, para supervisar la seguridad física.
- Aplicar técnicas de protección contra amenazas externas, tipificándolas y evaluándolas para asegurar el sistema.
- Aplicar técnicas de protección contra pérdidas de información, analizando planes de seguridad y necesidades de uso para asegurar los datos.
- Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios
- Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.
- La elaboración e interpretación de documentación técnica.

El módulo profesional, debido a lo extenso de sus contenidos y a la enorme importancia que tiene en la adquisición de competencias del ciclo formativo, se desglosa en 5 **unidades de trabajo**.

Al tratarse de una **enseñanza en modalidad semipresencial** en la que una parte importante se desarrolla online se le ha dado mucha importancia a la información obtenida a través de Internet, por lo que se ofrece un listado de direcciones en donde se podrán ampliar los conocimientos adquiridos, aclarar dudas, etc.

Cada una de las unidades de trabajo presenta los objetivos, criterios de evaluación y algunas orientaciones sobre cómo trabajar la unidad y sobre los recursos para el desarrollo de las actividades.

En la **modalidad de enseñanza presencial**, a este módulo profesional le corresponden 84 horas de clase **(1 horas semanales y 2 horas telemáticas durante 32 semanas)**. En esta modalidad semipresencial no es posible indicar una dedicación horaria para cada módulo, ya que esto depende del alumno, entre otros condicionantes, pero puede ser interesante considerar este número de horas como una referencia relativa y utilizarlo para baremar y comparar el tiempo necesario para superar cada módulo. Debe tenerse en cuenta que los alumnos en la modalidad presencial, además de esas 5 horas semanales de clase, deben dedicar también tiempo en casa para estudiar y hacer tareas, por lo que el tiempo requerido es sin duda mayor.

1. Competencias, objetivos y resultados de aprendizaje

1.1. Competencias profesionales, personales y sociales

- Relación de **Competencias profesionales**, personales y sociales, respetando la letra con la que se relaciona en la Orden que regula el ciclo formativo de ASIR en Andalucía:

  - 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) Resolver problemas y tomar decisiones individuales, siguiendo las normas y procedimientos establecidos, definidos dentro del ámbito de su competencia.
  - s) Gestionar su carrera profesional, analizando las oportunidades de empleo, autoempleo y de aprendizaje.

1.2. Objetivos generales

- La formación del **módulo profesional SAD**, contribuye a alcanzar los siguientes **Objetivos generales**, respetando la letra con la que se relaciona en la Orden que regula el ciclo formativo de **ASIR** en Andalucía:

- j) Seleccionar sistemas de protección y recuperación, analizando sus características funcionales, para poner en marcha 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) Asignar los accesos y recursos del sistema, aplicando las especificaciones de la explotación, para administrar usuarios
- p) Aplicar técnicas de monitorización interpretando los resultados y relacionándolos con las medidas correctoras para diagnosticar y corregir las disfunciones.

1.3. Resultados de aprendizaje

Finalmente, pasamos a desglosar los **Resultados de Aprendizaje** (abreviado **RA**) a los que contribuye este módulo profesional de ***SAD***, según la Orden que regula este ciclo formativo.

- RA1. Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo.
- RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.
- RA3. Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad.
- RA4. Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna.
- RA5. Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio.
- RA6. Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba.
- RA7. Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia.

Las líneas de actuación en el proceso de enseñanza-aprendizaje que permitirán alcanzar los objetivos anteriores estarán relacionadas con:

- El conocimiento de las prácticas y pautas adecuadas, relativas a la seguridad física y lógica en un sistema informático.
- El conocimiento y análisis de técnicas y herramientas de seguridad activa, que actúen como medidas preventivas y/o paliativas ante ataques al sistema.
- El análisis y aplicación de técnicas y herramientas de seguridad activa.
- El análisis y aplicación de técnicas seguras de acceso remoto a un sistema.
- El análisis de herramientas y técnicas de protección perimetral para un sistema.
- La instalación, configuración y prueba de cortafuegos y servidores proxy como herramientas básicas de protección perimetral.
- El análisis de los servicios de alta disponibilidad más comunes, que garanticen la continuidad de servicios y aseguren la disponibilidad de datos.
- El conocimiento y análisis de la legislación vigente en el ámbito del tratamiento digital de la información.

2. Unidades de Trabajo

El módulo profesional lo componen un total de 5 Unidades de Trabajo:

- U.T.1: Aspectos básicos de Seguridad
- U.T.2: Seguridad perimetral y acceso remoto
- U.T.3: Cortafuegos y proxys
- U.T.4: Implementación de alta disponibilidad.
- U.T.5: Legislación y normas de seguridad.

UT01: Aspectos básicos de seguridad

RA	Contenidos propuestos	Contenidos según normativa
1	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: 4.1. Amenazas físicas. 4.2. Amenazas lógicas. 5. Ejemplos de amenazas. 6. Estadísticas. 7. Seguridad física y ambiental: 7.1. Ubicación y protección física de los equipos y servidores. 7.2. Sistemas de alimentación ininterrumpida. 8. Seguridad lógica: 8.1. Criptografía. 8.2. Listas de control de acceso. 9. Establecimiento de políticas de contraseñas. 10. Utilización de sistemas biométricos de identificación. 11. Políticas de almacenamiento. 12. Copias de seguridad e imágenes de respaldo. 13. Medios de almacenamiento. 14. Recuperación de datos. 15. Realización de auditorías de seguridad. 16. Análisis forense en sistemas informáticos: 16.1. Objetivo del análisis forense. 16.2. Recogida y análisis de evidencias. 16.3. Herramientas del análisis.	Adopción de pautas de seguridad informática: − 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. • Amenazas 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:

RA	Contenidos propuestos	Contenidos según normativa

1 y 2	1. Ataques y contramedidas en sistemas personales: 1.1. Clasificación de los ataques. 1.2. Anatomía de ataques y análisis de software malicioso. 1.3. Herramientas preventivas. Instalación y configuración. 1.4. Herramientas paliativas. Instalación y configuración. 1.5. Actualización de sistemas y aplicaciones. 2. Seguridad en la conexión con redes públicas: 2.1. Identificación digital. 2.2. Firma electrónica y certificado digital. 2.3. Publicidad y correo no deseado. 2.4. Otros. 3. Elaboración de un manual de seguridad y planes de contingencia. 3.1. Pautas y prácticas seguras. 4. Seguridad en la red corporativa: 4.1. Monitorización del tráfico en redes: aplicaciones para la captura y análisis del tráfico, aplicaciones para la monitorización de redes y equipos. 4.2. Seguridad en los protocolos para comunicaciones inalámbricas. 4.3. Riesgos potenciales de los servicios de red. 4.4. Intentos de penetración: 4.4.1. Craqueado de contraseñas, forzado de recursos, puertas traseras. Sistemas de detección de intrusiones.	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. Instalación y configuración. • Herramientas paliativas. Instalación y configuración. • 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

UT02: Seguridad Perimetral y acceso remoto

RA	Contenidos propuestos	Contenidos según normativa
1,2 y 3	1.Elementos básicos de la seguridad perimetral: 1.1 «Router» frontera. 1.2 Cortafuegos. 1.3 Redes privadas virtuales. 1.4 Perímetros de red. Zonas desmilitarizadas. 1.5 Arquitectura débil de subred protegida. 1.6 Arquitectura fuerte de subred protegida. 2. Políticas de defensa en profundidad: 2.1Defensa perimetral. 2.2 Defensa interna. 2.3Factor Humano. 3. Redes privadas virtuales. VPN. 3.1 Beneficios y desventajas con respecto a las líneas dedicadas. Técnicas de cifrado. 3.2 Clave pública y clave privada: 3.3 VPN a nivel de enlace. 3.4 VPN a nivel de red. SSL, IPSec. 3.5 VPN a nivel de aplicación. SSH. 3.6 Intérprete de comandos SSH. 3.7 Gestión de archivos SSH. 4 Servidores de acceso remoto: 4.1 Protocolos de autenticación. 4.2 Configuración de parámetros de acceso. 4.3 Servidores de autenticación.	Implantación de técnicas de 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.

UT03: Cortafuegos y Proxy

RA	Contenidos propuestos	Contenidos según normativa
1,2 y 4	1. Utilización de cortafuegos. 2. Filtrado de paquetes de datos. 3. Tipos de cortafuegos. 3.1. Características. 3.2. Funciones principales. 4. Instalación de cortafuegos. 4.1. Ubicación. 5. Reglas de filtrado de cortafuegos. 6. Pruebas de funcionamiento. 6.1. Sondeo. 7. Registros de sucesos de un cortafuegos. 8. Cortafuegos integrados en los sistemas operativos. Cortafuegos libres y propietarios. 10. Distribuciones libres para implementar cortafuegos en máquinas dedicadas. 11. Cortafuegos hardware.	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 un cortafuegos.

RA	Contenidos propuestos	Contenidos según normativa
	1. Tipos de «proxy». 1.1. Características 1.2. Funciones. 2. Instalación de servidores «proxy». 3. Instalación y configuración de clientes «proxy».	Instalación y configuración de servidores «proxy»: − Tipos de «proxy». Características y funciones. − Instalación de servidores «proxy». − Instalación y configuración de clientes «proxy».

1 y 5	4. Configuración del almacenamiento en la caché de un «proxy». 5. Configuración de filtros. 6. Métodos de autenticación en un «proxy». 7. «Proxys» inversos. 8. «Proxys» encadenados. 9. Pruebas de funcionamiento. 9.1. Herramientas gráficas.	− Configuración del almacenamiento en la caché de un «proxy». − Configuración de filtros. − Métodos de autenticación en un «proxy».

UT05: Implantación de soluciones de alta disponibilidad

RA	Contenidos propuestos	Contenidos según normativa
1 y 6	1. Definición y objetivos. 2. Análisis de configuraciones de alta disponibilidad: 2.1. Funcionamiento ininterrumpido. 2.2. Integridad de datos y recuperación de servicio. 2.3. Servidores redundantes. 2.4. Sistemas de «clusters». 2.5. Balanceadores de carga. 2.6. Instalación y configuración de soluciones de alta disponibilidad. 2.7. Virtualización de sistemas. 2.8. Posibilidades de la virtualización de sistemas. 3. Herramientas para la virtualización: 3.1. Entornos personales. 3.2. Entornos empresariales. 4. Configuración y utilización de máquinas virtuales. 4.1. Alta disponibilidad y virtualización. 4.2. Simulación de servicios con virtualización. 4.3. Servicios reales con virtualización. 4.4. Análisis de la actividad del sistema virtualizado. 5. Pruebas de carga. 5.1. Cargas sintéticas. 6. Modelos predictivos y análisis de tendencias.	Implantación de soluciones de 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.

UT06: Legislación y normas de seguridad

RA	Contenidos propuestos	Contenidos según normativa
7	1. Legislación sobre protección de datos. 2. Legislación sobre los servicios de la sociedad de la información y correo electrónico. 3. Normas ISO sobre gestión de seguridad de la información. 4. Organismos de gestión de incidencias.	Legislación y normas sobre seguridad: − Legislación sobre protección de datos. − Legislación sobre los servicios de la sociedad de la información y correo electrónico. Orientaciones

3. Metodología y materiales didácticos

El alumnado, a través de los contenidos que se le ofrecen a lo largo del curso, irá adquiriendo los conceptos básicos para introducirse en el módulo profesional. Las actividades de autoevaluación y las tareas afianzarán y concretarán su aprendizaje funcional.

Se suscitará el debate y la puesta en común de ideas, mediante la participación activa del alumnado a través del foro, respetando la pluralidad de opinión.

Se propiciará que el alumnado sea sujeto activo de su propio aprendizaje, intentando igualmente fomentar el trabajo y la participación.

Se contemplan los siguientes materiales didácticos:

- Unidades de trabajo expuestas en pantalla.
- Casos prácticos.
- Cuestionarios.
- Tareas.
- Material complementario.

Para la parte presencial del módulo profesional se fijarán los siguientes tipos de sesiones presenciales:

- Sesiones de presentación de contenidos;
- Sesiones prácticas (p.ej. resolución de ejercicios, prácticas en los ordenadores, etc.);
- Sesiones de repaso y dudas;
- Sesiones de evaluación.

4. Criterios y procedimiento de evaluación

Tal y como establece el **Decreto 359/2011 de 7 de diciembre** que regulan las modalidades semipresencial y a distancia de las enseñanzas de Formación Profesional Inicial que forma parte del sistema educativo en la Comunidad Autónoma de Andalucía, las enseñanzas ofertadas en la modalidad semipresencial se impartirán mediante la combinación de sesiones lectivas colectivas presenciales, de obligada asistencia para el alumnado, y sesiones de docencia telemática. Así mismo, los criterios de evaluación recogidos en las programaciones didácticas de las enseñanzas impartidas en las modalidades semipresencial y a distancia, recogerán de forma cuantificada o porcentual el peso en la evaluación de cada una de las actividades que intervienen en el proceso de aprendizaje y, en el caso de enseñanzas impartidas en la modalidad semipresencial, se valorarán de forma proporcional, además, las actividades realizadas por el alumnado en las sesiones presenciales.

El proceso de evaluación se llevará a cabo a lo largo de todo el periodo que comprende el curso, siendo el resultado la media ponderada de la suma de una serie de componentes.

Estos componentes son los siguientes:

Componente a evaluar	Porcentaje para este módulo profesional
Actividades realizadas de forma presencial	20 %
Exámenes presenciales	40 %
Tareas en el aula virtual.	25 %
Cuestionarios en el aula virtual	5 %
Participación en las herramientas de comunicación	10 %

Los diferentes apartados que intervienen en la evaluación se puntuarán siempre de **0 a 10 puntos**. Se considerará superado el módulo profesional, cuando la media ponderada comentada anteriormente sea **mayor o igual a 5, siempre y cuando la calificación media ponderada de las distintas pruebas presenciales haya sido superior o igual a 5.**

En el caso que el alumnado tenga más del 20% de faltas de asistencia en las sesiones lectivas presenciales, perderá el derecho a la evaluación continua.

El alumnado que haya perdido el derecho a la evaluación continua podrá presentarse a la convocatoria final de Junio, siempre que haya entregado todas las tareas y actividades que se han realizado durante el curso.

4.1. Actividades presenciales

El alumnado, a lo largo del curso, irá realizando en las sesiones presenciales una serie de actividades prácticas. El profesorado evaluará la actitud y la destreza de los alumnos en el desarrollo de estas actividades. El profesor enviará a los alumnos tareas y/o custrionarios referidos a dichas actividades presenciales.

En el apartado 5.1. Sesiones presenciales puede ver un listado de todas las actividades presenciales a realizar en el curso así como su planificación.

4.2. Exámenes presenciales

El decreto 359/2011 establece en su artículo 9.2 que *la realización de pruebas de evaluación, requerirán la identificación personal fehaciente del alumnado que las realice y se corresponden con el enfoque práctico empleado, como elemento validador de las actividades presenciales o virtuales desarrolladas a lo largo del curso.*

En virtud de lo anterior, en los exámenes presenciales prevalece el enfoque práctico y debe tener en cuenta que la prueba presencial está basada en los resultados de aprendizaje del módulo profesional.

Se prevé la realización de cinco pruebas presenciales de carácter eliminatorio. Dos en el primer y en el segundo trimestre, y una última en el tercer trimestre. Además, se realizará el examen final presencial en junio. La planificación de las pruebas es la siguiente:

Prueba Presencial Escrita	Contenido del examen
1ª evaluación	Unidades 1 y 2
2ª evaluación	Unidades 3
3ª evaluación	Unidades 4 y 5

Las fechas previstas para la realización de las pruebas presenciales (exámenes) son:

Prueba Presencial	Fechas previstas 1er examen	Fechas previstas 2º examen
1ª evaluación	noviembre de 2016	diciembre de 2016
2ª evaluación	febrero de 2017	marzo de 2017
3ª evaluación	mayo de 2017	----
FINAL (JUNIO)	junio de 2017	

Nota: Las fechas de la tabla anterior son orientativas. Las fechas y horas definitivas de los exámenes se comunicarán al alumnado con suficiente antelación a lo largo del curso.

IMPORTANTE:

- Las pruebas tienen carácter eliminatorio.
- La nota final de pruebas presenciales será, aproximadamente, la media ponderada de los exámenes de las tres evaluaciones.
- En caso de que la media ponderada de los distintos componentes de la evaluación (citados en el apartado 4.) no sea superior a 5 se realizará la prueba final.
- Para superar el módulo profesional es indispensable que la nota media ponderada de todos los componentes de los tres trimestres sea superior o igual a 5, o se supere la prueba final.

4.3. Tareas en el aula virtual

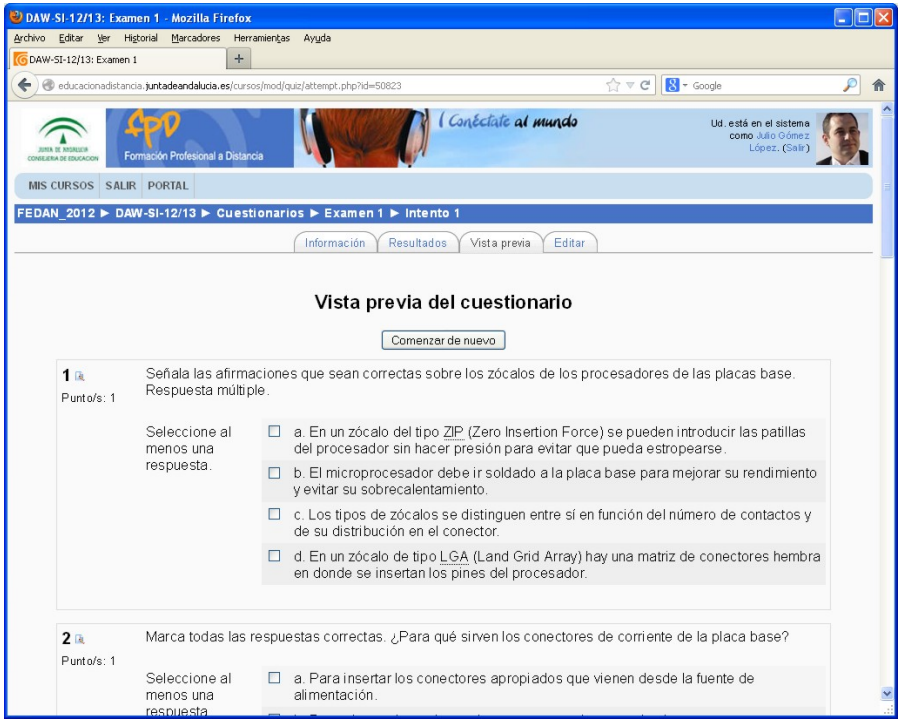
El alumnado **podrá entregar hasta un máximo de 2 veces la solución de una misma tarea**, siempre que la primera entrega tenga una nota inferior a 5 y superior a 1 sobre 10.

El segundo intento tendrá un plazo máximo de entrega de 7 días naturales después de que el profesor/a haya calificado como suspensa la tarea. Este segundo intento deberá ajustarse siempre a la fecha obligatoria de entrega indicada en la tabla de temporalización de cada unidad y/o bloque.

Es recomendable que el envío de las tareas se realice de forma escalonada y progresiva, evitando enviar un conjunto grande de tareas. En los supuestos casos que la entrega de tareas se realice sobre la fecha límite de la misma, no se garantiza respetar la posibilidad del segundo reenvío, ya que podría darse el caso en que el docente no cuente con tiempo suficiente para responder al envío masivo de tareas.

4.4. Cuestionarios en el aula virtual

El alumnado deberá realizar los cuestionarios on-line asociados a cada unidad que el profesor proponga, **pudiendo realizar un máximo de tres intentos de cada uno, y conservándose la mayor nota de todos los intentos que haya realizado.**



Captura de pantalla de la plataforma de FPaD

4.5. Participación en foros y herramientas de comunicación

Para valorar la participación del alumnado en el foro, éste criterio se dejará a la opinión del profesor o profesora que imparte el módulo profesional. De cualquier forma, y con carácter general, se valorará las aportaciones que se hagan en el foro y que sean de utilidad para el resto de alumnos/as (tanto respuestas correctas como preguntas “interesantes”), se valorará la participación colaborativa.

Captura de pantalla de la plataforma de FPaD

5. Secuenciación de Unidades de Trabajo y temporalización

Las fechas aproximadas previstas de presentación de cada Unidad de Trabajo son las siguientes:

Unidad	Fecha de inicio	Fecha de finalización	Fecha tope obligatoria de entrega de tareas
BLOQUE 1ª Evaluación.			
UT1: Aspectos básicos de Seguridad	19/09/2016	07/11/2016	19/12/2016
UT2: Seguridad Perimetral y Acceso Remoto	07/11/2016	19/12/2016	
BLOQUE 2ª Evaluación:			
UT3: Cortafuegos y Proxy	09/01/2017	06/03/2017	06/03/2017
BLOQUE 3ª Evaluación			
UT4: Implementación de alta disponibilidad.	06/03/2017	08/05/2017	22/05/2017
UT5: Legislación y normas de seguridad	08/05/2017	29/05/2017	

- La **fecha tope obligatoria de entrega** indica el último día que se recogerán las tareas indicadas (incluido el segundo envío en caso de que fuera necesario).
- Se recomienda al alumnado la entrega progresiva de tareas conforme se vayan finalizando las unidades didácticas, garantizándose así la posibilidad de un segundo reenvío.
- No se aceptará ningún envío de tareas fuera de esos plazos, salvo circunstancias excepcionales, que valorará el profesor o profesora previa acreditación documental de las mismas

5.1. Sesiones presenciales

El artículo 3.2. establece que l*as sesiones de docencia presencial tendrán como objetivo facilitar al alumnado las ayudas pertinentes en la realización de tareas, resolver dudas respecto a los aspectos esenciales del currículo, orientar hacia el uso de las herramientas de comunicación empleadas por esta modalidad de enseñanza, afianzar las interacciones cooperativas entre el alumnado, promover la adquisición de los conocimientos, competencias básicas o profesionales que correspondan y, en su caso, reforzar la práctica de las destrezas orales.* Por lo tanto, se establece tres tipos de sesiones presenciales:

- Las **sesiones de acogida del alumnado** se realizan en la primera semana del curso para explicar al alumnado los aspectos generales del ciclo, características de la enseñanza semipresencial, el uso del Aula Virtual, las características más importantes de cada módulo, etc.
- El objetivo de las **sesiones presenciales** es la exposición de los contenidos de una unidad, resolución de dudas, realización de prácticas en el Centro, etc.
- Al final de cada trimestre se fijarán **sesiones de recuperación** para que el alumnado pueda recuperar las actividades presenciales que no haya podido realizar.

Tal y como establece el horario del grupo, las clases de este módulo profesional se realizan los Lunes.

1ª evaluación

Fechas	Unidad	Descripción
15/09/16	-	Sesión de acogida del alumnado Cuestionario inicial del alumnado
19/09/16 - 07/11/16	UT01	Presentación de la unidad - Ejercicios y dudas.Examen
07/11/16 - 19/12/16	UT02	Presentación de la unidad - Ejercicios, dudas. Examen

2ª evaluación

Fecha	Unidad	Descripción
09/01/17 - 06/03/17	UT03	Presentación de la unidad - Ejercicios y dudas. Examen.

3ª evaluación

Fecha	Unidad	Descripción
06/03/17 - 08/05/17	UT04	Presentación de la unidad - Ejercicios y dudas. 1º Examen
08/05/17 - 29/05/17	UT05	Presentación de la unidad - Ejercicios y dudas. 2º Examen.

6. Bibliografía

Recomendación

Libros

- Jesús costas santos., Seguridad y Alta Disponibilidad. Editorial Rama
- Alfredo abad domingo, Seguridad y Alta Disponibilidad. Editorial Garceta.
- Seguridad Informática 2ºedicion, Ethical Hacking. Editorial Eni
- Kevin Mitnick. El arte de la intrusion como ser un hacker. Editorial Alfaomega
- Merce Molist. Hackstory.es (Historia del hacking en España) (www.hackstory.es)..

Páginas web

- *http://www.elotroladodelmal.com/*
- *http://www.inteco.es/*
- *http://www.penetration-testing.com/*
- http://www.hispasec.com/

7. Recursos necesarios

Debes conocer

En los materiales suministrados por el profesor se incluirán enlaces a las distintas páginas de las que debemos descargar el software necesario para realizar las tareas, las prácticas en las sesiones presenciales y los exámenes presenciales.