PROGRAMACIÓN DIDÁCTICA DE MÓDULO

CURSO: 2016 /2017

CICLO FORMATIVO	**Administración de Sistemas Informáticos en Red**	
MODULO	Seguridad y Alta Disponibilidad	
TEMPORALIZACIÓN	**HORAS ANUALES**	**HORAS SEMANALES**
	84 horas	4 horas
PROFESORADO QUE LA IMPARTE	Víctor Miguel Rodríguez Macías (4 horas)	

PROGRAMACIÓN DIDÁCTICA

1.- OBJETIVOS DEL MÓDULO.

La formación del módulo contribuye a alcanzar los objetivos generales del ciclo formativo de Administración de sistemas informáticos en Red, que se relacionan a continuación:

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

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

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

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

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

f) 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.

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

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

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

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

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

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

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

g) 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.

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

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

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

2.- BLOQUES TEMÁTICOS

Bloque temático Nº 1	Nº	Título Unidad didáctica	Horas	Trimestre 1º	2º	3º
Seguridad	1	Principios de seguridad	9	x		
	2	Seguridad física	10	x		
	3	Seguridad lógica	13	x		
	4	Software antimalware	9	x		
	5	Criptografía	10	x	X	
	6	Seguridad en redes corporativas	11		X	
	7	Seguridad perimetral	12		X	

Bloque temático Nº 2	Nº	Título Unidad didáctica	Horas	Trimestre 1º	2º	3º
Alta disponibilidad	8	Configuraciones de alta disponibilidad	6		X	

Bloque temático Nº 3	Nº	Título Unidad didáctica	Horas	Trimestre 1º	2º	3º
Legislación	9	Normativa legal en materia de seguridad en TI	2		X	

Bloque temático Nº 4	Nº	Título Unidad didáctica	Horas	Trimestre 1º	2º	3º
Recuperaciones Finales		Examen recuperación final de marzo	2		X	

3.- AGENDA				
Bloque temático Nº 1	**Nº**	**Título Unidad didáctica**	**Horas**	**Comienzo**
Seguridad	1	Principios de seguridad (explicación)	3	17-sept-15
		Realización prácticas	5	22-sept al 02-oct
		Realización examen test	0,5	20-oct
		Realización examen test recuperación	0,5	3-nov
	2	Seguridad física (explicación)	2	02-oct
		Realización prácticas	7	06-oct al 16-oct
		Realización examen test	0,5	27-oct
		Realización examen test recuperación	0,5	3-nov
	3	Seguridad lógica (explicación)	2	16-oct
		Realización prácticas	10	20-oct al 6-nov
		Realización examen test	0,5	10-nov
		Realización examen test recuperación	0,5	1-dic
	4	Software antimalware(explicación)	2	13-nov
		Realización prácticas	6	12-nov al 20-nov
		Realización examen test	0,5	24-nov
		Realización examen test recuperación	0,5	1-dic
	5	Criptografía (explicación)	2	26-nov
		Realización prácticas	7	26-nov al 10-dic
		Realización examen test	0,5	15-dic
		Realización examen test recuperación	0,5	26-ene
	6	Seguridad en redes corporativas (explicación)	2	19-dic

		Realización prácticas	8	19-dic al 22-ene
		Realización examen test	0,5	19-ene
		Realización examen test recuperación	0,5	26-ene
	7	Seguridad perimetral	3	29-ene
		Realización prácticas	4	28-ene al 5-feb
		Realización examen test	0,5	13-feb
		Realización examen práctico	2	9-feb
		Realización examen test recuperación	0,5	10-mar
		Realización examen práctico recuperación	2	16-feb

Bloque temático Nº 2	**Nº**	**Título Unidad didáctica**	**Horas**	**Comienzo**
Alta disponibilidad	8	Configuraciones de alta disponibilidad (explicación)	2	11-feb
		Realización prácticas	3	18-feb al 3-mar
		Realización examen test	0,5	6-mar
		Realización examen test recuperación	0,5	8-mar

Bloque temático Nº 3	**Nº**	**Título Unidad didáctica**	**Horas**	**Comienzo**
Legislación	9	Normativa legal en materia de seguridad en TI (explicación)	1	4-mar
		Realización prácticas	1	4-8-mar

Recuperaciones Finales Marzo	**Nº**	**Título Unidad didáctica**	**Horas**	**Comienzo**
Recuperaciones Finales		Examen recuperación final de marzo	2	9-mar

Recuperaciones Junio	**Nº**	**Título Unidad didáctica**	**Horas**	**Comienzo**
Recuperaciones Junio		Periodo de recuperación para aquellos alumnos que no hayan recuperado la asignatura.	30	15-mar

Examen de Iptables de Mayo		Primera oportunidad de recuperación del examen práctico de Iptables	2	Semana 10-may
Examen de Iptables de Junio		Última oportunidad de recuperación del examen práctico de Iptables	2	Semana 13-jun
Examen Teóricos de Junio		Última oportunidad de recuperación de los exámenes teóricos (se podría ampliar el número de horas si hubiera necesidad)	2	Semana 13-jun
Entrega de prácticas		Entrega de prácticas tanto para recuperar partes pendientes como para subir nota	2	10-jun

4. METODOLOGÍA.

La organización de clase será en grupos individuales salvo que la actividad planteada en cada momento requiera el trabajo en grupo. Dada la limitación de recursos, puede ser habitual que los alumnos compartan ordenador.

Se empleará una plataforma Moodle para la entrega de actividades.

El desarrollo de cada U.T. incluirá una parte de “clase magistral” que introduzca los conceptos necesarios, una parte de experimentación donde el alumno toma contacto con el tema en cuestión, y finalmente actividades. Este proceso podría repetirse varias veces durante una misma U.T.

Se entregará a los alumnos materiales alternativos al libro base para diversificar las fuentes o apoyar el aprendizaje.

En general la secuenciación de las U.T. será unos días iniciales de explicación teórica del tema, a continuación se pasará a un periodo de realización de prácticas que será de 45 minutos aprox por práctica a realizar (salvo excepciones), una vez terminado el plazo de realización de prácticas se hará un examen test de los conocimientos adquiridos en el tema.

5.- EVALUACIÓN Y RECUPERACIÓN

La evaluación será continua, basada en la observación y calificación de todos los trabajos realizados. Existirán varias pruebas teórico/prácticas que atenderán a la consecución de los objetivos previstos para este módulo.

Se solaparán las actividades de enseñanza con las de evaluación en el momento preciso del aprendizaje, planteando cuestiones en clase, resolviendo ejercicios de las relaciones en la pizarra o pidiendo la entrega de una relación de problemas.

Se hará especial hincapié en el uso de la notación adecuada en cada parte de la asignatura.

Si se detectara **copia de cualquier tipo**, la calificación de dicho elemento calificador sería de 1 (SUSPENSO).

Evaluaciones Parciales.

En las evaluaciones de las unidades se tendrá en cuenta los ejercicios prácticos y las calificaciones de clase, así como la asistencia regular activa a clase de la siguiente manera:

Las personas que falten al 20% del total de horas de clase del módulo, perderán su derecho a evaluación continua. Como excepción, las personas que acrediten un contrato de trabajo que pueda entrar en conflicto con el horario de clase, podrán entregar trabajos teórico/prácticos específicos para las partes de la materia a las que no hayan podido asistir con regularidad.

Para superar la evaluación será necesaria y nunca suficiente la realización de las prácticas y actividades exigidas por el profesor. Así como la presentación de los resultados al profesor en tiempo y forma. El profesor indicará para cada actividad el tiempo y la forma en que se realizarán las actividades prácticas. Si estos no se cumplen, el profesor dará por suspenso el ejercicio con una nota entre 0 y 4. En el caso de la **no entrega en la fecha señalada, se ampliará el plazo de a una segunda fecha señalada.** La entrega de más del 10% de los trabajos fuera de la fecha señalada implicará que la nota final se redondeará al entero más cercano hacia abajo y si no supera esta cantidad la nota final se redondeará al entero más cercano hacia arriba. **Si tampoco se entrega en esta segunda fecha, se habilitará un plazo final de entrega de trabajos en fuera de fecha**. Estos trabajos en fuera de fecha se tendrán que entregar antes del 2 de marzo de 2015 y se procederá a su corrección presencial en el periodo de 2 de marzo a 14 de marzo de 2015. A la nota de estos trabajos **se le decrementará un punto en cada uno de ellos por penalización de fuera de fecha.**

Si hay más de dos prácticas que no se entreguen de forma definitiva (que no se vuelvan a corregir más adelante o que no se entreguen) en la fecha inicial se truncará la nota media de ese tema, en caso contrario se redondea a la unidad superior.

Entrega de Trabajos: La entrega de los trabajos prácticos tendrá que realizarse, en general salvo excepciones que se expliquen con antelación al alumnado, de las siguientes condiciones:

1. Los trabajos se harán en formato de pdf con vídeo incrustado mediante el programa de demostraciones Adobe Captative versión de prueba o mediante el programa ScreenExe. El alumno podrá cambiar de programa siempre que tenga prestaciones similares al anterior. El formato de pdf se puede cambiar por otro soporte pero que tenga prestaciones similares al pdf.
2. Los trabajos se corregirán por parte del profesor y en caso de dudas con respecto algún trabajo el alumno expondrá el mismo durante horario de clase al profesor de forma individual. En la exposición se deberá explicar todo el proceso de la práctica y sus partes importantes. Se podrá hacer la exposición con el fichero pdf anteriormente enunciado o mediante demostración en vivo de la práctica. En casos puntuales el profesor podrá pedir que la exposición sea en vivo para valorar los conocimientos adquiridos por el alumno. Para ello se le avisará con anterioridad al alumno para que tenga tiempo de preparación de la demostración.
3. Todos los trabajos se harán sobre máquina virtual o maquina anfitrión y como condición obligatoria es que siempre debe de aparecer un fichero de texto con el nombre del alumno visible en la barra de herramientas para atestiguar que la práctica ha sido realizada por el alumno. En el caso de que no aparezca **se decrementará 1 punto** en el caso de que se pueda averiguar la autoría de la práctica de otra forma y podrá decrementar todo el valor de la práctica si no se puede demostrar de ninguna forma la autoría de la práctica.
4. En aquellos casos en los que haya prácticas con sistemas de red en los que haya que establecer un rango de IP, a cada alumno se le asignará un rango de IP obligatorio que tendrá que utilizar en todas las prácticas. En el caso de no usarse el rango

asignado la práctica **se le descontará un 50% de la nota.**

- En aquellos trabajos / prácticas donde el alumno pueda escoger entre varias posibilidades, con lo que, para la nota final del trabajo, se deberá esperar a la realización por parte de todos los alumnos (salvos aquellos que no hayan entregado en fecha y forma el trabajo/práctica). Una vez corregidos todos los trabajos de los diferentes alumnos, se contará cuantos alumnos han hecho cada una de las posibilidades posibles. Una vez conocida esa cantidad se calculará, por una parte:
    1. La cantidad de trabajos totales / número de posibilidades.
    2. A la cantidad anteriormente se le sumará 1 como margen de desviación.
    3. Después al número de alumnos de cada una de las posibilidades se le resta la cantidad calculada en el paso 2 (así sabremos que desviación se ha producido en esa posibilidad).
    4. Si la cantidad dada en el paso 3 es menor o igual a 0 significa que los alumnos que han realizado estas prácticas están dentro del reparto equitativo de posibilidades por parte del alumnado con lo que el valor de la práctica será el 100% de la nota asignada a la misma.
    5. Si la cantidad dada en el paso 3 es superior significa que ha habido más alumnos de la cuenta (la media +1 tal como se ve en el paso 1 y 2) que han realizado esta práctica. Con lo cual todos ellos sufrirán una merma del valor de la nota alcanzando esta misma un máximo del 50% de la nota. Para el cálculo de esta merma se verá el número de alumnos que han excedido el máximo permitido y por cada alumno que sobrepase se la aplicará un 10% de reducción hasta un máximo de 50% de la nota.
    6. Como ejemplo de lo mismo imaginemos el caso de una práctica con 4 posibilidades que lo realizan una serie de 16 alumnos realizándolo en la siguiente proporción:
        - 1 posibilidad 8 alumnos, 2 posibilidad 4 alumnos, 3 y 4 posibilidad 2 alumnos.
        - PASO1: La media sería 16 alumnos / 4 posibilidades
        - PASO1: Los alumnos se deberían repartir las posibilidades entre ellos a razón de 4 alumnos por cada posibilidad.
        - PASO2: Le sumamos 1 a la media y quedaría en 5. Esto indicaría que los alumnos se podrían desviar en 1 alumno más de la media en ese reparto.
        - PASO3: Calculamos la desviación de cada posibilidad
            - 1º Posibilidad: 8 alumnos - 5 (media+1) = 3.
            - 2º Posibilidad: 4 alumnos - 5 = -1
            - 3º y 4º Posibilidad: 2 alumnos - 5 = -3
        - PASO4: Vemos que la 2º, 3º y 4º Posibilidad están dentro del margen de reparto dado con lo que no se le modifica la nota.
        - PASO5: Vemos que la 1º Posibilidad lo han hecho más alumnos de la cuenta con lo que pasamos a averiguar el porcentaje de reducción de la nota que hay que aplicar, para ello tenemos que multiplicar 3 x 10% y daría que habría que mermarle al conjunto de los alumnos que han realizado esta práctica un 30% de la nota.
- Con el apartado anterior se pretende conseguir
    1. Un clima de cooperación y entendimiento entre los alumnos.
    2. Que los alumnos puedan escoger la práctica que le resulte más atrayente.
- La entrega será en fecha y hora fijada previamente en el servidor Moodle en el lugar habilitado dentro del servidor para ello, adjuntando sólo el fichero resultado del trabajo. Los alumnos dispondrán de varias fechas (salvo para los últimos temas que tendrá de fecha hasta antes de la semana final de evaluaciones) tal como se explicó anteriormente.

Periódicamente se podrán hacer pruebas sorpresa (test de conocimientos) relacionadas a una única U.T. Estas pruebas tendrán un peso del 5% en la nota del trimestre. El valor de la nota

solo se tendrá en cuenta si el resultado es superior a 5.

Examen Teórico: En determinados temas se realizará un examen teórico tipo test mediante la plataforma Moodle. Para el cálculo de la nota se tendrá se contará el número de preguntas acertadas y se le restará el porcentaje de probabilidad de las preguntas erróneas (por ej. Si una pregunta errónea tiene 3 opciones el porcentaje de probabilidad es 1/3, esta cantidad es la que se le descontará a la nota por cada pregunta errónea).

Nota Final del Tema: La nota final de la evaluación del tema en la parte práctica será la media aritmética ponderada (en el caso de que alguna de las pruebas sea de contenido superior al resto) de las pruebas prácticas, supeditada siempre esta puntuación a las circunstancias anteriormente explicitadas.

La nota final de la evaluación del tema será la media aritmética ponderada (la ponderación de los temas se verá más adelante) de la prueba teórica, de la prueba práctica, y de los otros aspectos evaluables (falta de asistencia, trabajo en clase, etc). Para poder realizar el cálculo de esa media el alumno deberá superar cada parte (práctica y teoría) con más de un 4, en caso de no superar esa parte deberá recuperar sólo la parte con menos de un 4 (o la práctica, o la teoría, o ambos dependiendo de que parte tenga menos de un 4)

Nota Final

Para los alumnos que hayan perdido el derecho de evaluación continua (por faltar a más del 20% de las horas de la evaluación- Art. 58.8 del ROF) sólo se tendrá en cuenta solo la nota obtenida en la prueba teórico-práctica final. Si tuviera algún examen aprobado con anterioridad la nota de ese examen pasará a ser 0. Además, tendrá que entregar todas las prácticas realizadas durante el curso, habilitándole para ello una zona en la plataforma Moodle para su entrega.

Sólo se podrá considerar a un alumno como aprobado si en todas las partes con pruebas prácticas/escritas ha sacado más de un 40% de la nota individual por partes y en las demás partes ha sacado al menos el 50% de nota individual por partes y la nota media global de todas las partes supera o iguala el 50% (ver medidas de recuperación para mayor aclaración)

Para los alumnos que no alcancen una calificación requerida en todos o algunos de los contenidos programados, existirá una prueba complementaria, y según la materia concreta, podrán existir relaciones de ejercicios o supuestos que ayuden a la adquisición de los conocimientos pendientes.

NOTA: Las personas que acrediten la adquisición de las competencias correspondientes a cualquiera de los trimestres, podrán ser evaluados mediante la entrega de un trabajo teórico/práctico que cubra los contenidos a evaluar.

Periodo de Marzo a Junio

Durante el periodo de Marzo a Junio, los alumnos que hayan superado la asignatura, podrán subir sus notas mediante la entrega de trabajos, tanto aquellos trabajos que le falten o en los que se desee subir la nota de algún trabajo previamente entregado.

Aquellos ejercicios que hayan sufrido un decremento de -1 por haberlos entregado en fuera de fecha se le quitará esta penalización.

Para aquellos alumnos que no hayan superado la asignatura, dispondrán de 2 horas semanales de clase, para la realización o corrección de aquellas prácticas que deseen para subir la nota de la parte práctica. Además dispondrán de dos exámenes prácticos del tema 7 (ver apartado de Agenda) y un examen teórico de cada tema (ver apartado de Agenda)

4.1.- VALORACIÓN DE LOS CONTENIDOS

EVALUACIÓN DE CONTENIDOS	PORCENTAJE	
Pruebas teóricas	20,00%	Dependiendo de la U.T.
Ejercicios Prácticos y/o Pruebas prácticas	80,00%	
En caso de que en alguna de las evaluaciones no se hubieran realizado tareas evaluables en alguno de estos apartados (p.e. no se hubieran mandado trabajos) el porcentaje correspondiente se incrementaría por parte iguales en la prueba prácticas y en las teóricas En caso de que en alguna de los módulos no haya una prueba escrita esta pasará a la prueba práctica y viceversa. En el caso de que no haya ni pruebas prácticas ni escritas ese porcentaje pasará al de trabajo.		

4.2.- MEDIDAS DE RECUPERACIÓN

4.2.a.- Para pruebas finales: (Medidas a tomar entre las evaluaciones parciales y la evaluación final)

Si un alumno no supera la 2ª evaluación parcial, deberá presentarse a la 3ª evaluación final. No superar la 2ª evaluación parcial significa que el alumno no ha superado alguna de las evaluaciones parciales (incluyendo sus respectivas recuperaciones: ver apartado 4).

Se conservará la nota de las evaluaciones de las unidades.

En el periodo entre la evaluación ordinaria y la extraordinaria se ofrecerán clases de apoyo donde se repasará **bajo demanda** del alumno el temario del curso, realizando actividades, leyendo textos, impartiendo clases, y cualquier otra cuestión necesaria. El horario será como mínimo del 50% del horario lectivo regular.

NOTA: Los alumnos que hayan superado la 2ª evaluación parcial, podrá presentarse a la evaluación final para subir nota (mediante realización de las prácticas que le falten o tenga que corregir o mediante la realización de los exámenes teórico/práctico de alguna unidad), pudiendo (o no) asistir a clases de apoyo.

NOTA: Si se detectara **copia de cualquier tipo**, la calificación de dicho elemento calificador sería de 1 (SUSPENSO).

Para mayor aclaración ver el **apartado de Evaluación y recuperación el subapartado de Periodo de Marzo a Junio**

4.3.- 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 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.

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) 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.

4.4.- PROCEDIMIENTOS DE EVALUACIÓN

La evaluación será continua e individualizada, y la observación sistemática será un instrumento de evaluación habitual. Dada la complejidad de la evaluación, se utilizarán distintas técnicas para realizarla, ya que evaluar los aspectos cuantitativos y cualitativos de rendimiento con una sola forma resultaría siempre insuficiente. Los procedimientos de análisis irán desde los más estructurados (tests) a los menos estructurados («notas u observaciones de clase»). La interpretación de los datos y los análisis debe ser holista (totalista), debe considerarse en su conjunto; la percepción ha de ser de los aspectos cualitativos y fundamentales.

1) La **observación sistemática**:
   a) de las actitudes personales del alumno,
   b) de su forma de organizar el trabajo,
   c) de las estrategias que utiliza,
   d) de cómo resuelve las dificultades que se encuentra, etc.
2) La **revisión y análisis de los trabajos/prácticas** de los alumnos. Esto nos permite comprobar los materiales que han ido "produciendo" los alumnos/as a lo largo del desarrollo de la unidad. Se debe revisar los ejercicios mandados a casa, se revisarán y corregirán los trabajos individuales o en equipo, así como sus exposiciones orales en las puestas en común, sus actuaciones, la resolución de ejercicios en la pizarra; etc.
3) La **entrevista con el alumno**, es un instrumento de gran utilidad, ya podemos aprovechar el momento para la resolución de dudas puntuales o para "investigar" el caudal de aprovechamiento del alumno y la intensidad de su ritmo de aprendizaje.
4) Realizar una **prueba específica** de evaluación de aquellas unidades en las que se haya observado que el alumnado no ha trabajado lo suficiente para intentar adquirir los conocimientos deseados.

4.5.- CRITERIOS DE CALIFICACIÓN

A rasgos generales, se evaluará la parte teórica mediante una **prueba teórica escrita realizada en el servidor Web Moodle** y la parte práctica mediante ejercicios prácticos, salvo los casos concretos de alguna unidad didáctica que requiera una **prueba práctica** de evaluación para demostrar los conocimientos prácticos, en el caso de que no se haya demostrado mediante los ejercicios prácticos a realizar por los alumnos sus conocimientos prácticos.

Se calificará también la ortografía, descontando 0’1 por cada falta de ortografía con un máximo del 15% de la nota.

Si se detecta copia (en trabajo o en exámenes) la calificación será de 1.

5.- MATERIALES Y RECURSOS DIDÁCTICOS.

18 Pcs anticuados.

Copias de prueba de Windows XP, Windows 7 y Windows server 2008.

Imágenes de Ubuntu Desktop y Ubuntu Server.

Servidor Web Moodle

PacketTracer

VirtualBox OSE

Vmware Workstation

Cañón

Bibliografía:

Seguridad y Alta Disponibilidad. RA-MA. Jesús Costas Santos.

Hacking Linux Exposed. 3rd edition

Hacking Windows Exposed.

UNIX and Linux System Administration Handbook (4th edition)

Pro Data Backup and Recovery

Practical UNIX and Internet Security

Hacking Exposed. Malware and rootkits

Hacking Exposed. Network Security Secrets and Solutions

Hacking. The next generation.

Foundations of security.

IT Security Interviews Exposed.

6. PREVENCIÓN RIESGOS LABORALES

Manipular adecuadamente los equipos, evitando caidas de los ordenadores, cortes o descargas eléctricas.

Adoptar la postura correcta al sentarse delante del ordenador.

Conocer la toxicidad de algunos de los materiales con los que se trabaja, y utilizarlos adecuadamente.

7.- SECUENCIACIÓN UNIDADES DIDÁCTICAS.

Nota a tener en cuenta		Debido a que la seguridad informática es un concepto que va cambiando rápidamente (los programas que a inicio de curso son válidos, puede que a mediados de curso se queden obsoletos), se pueden producir cambios en los contenidos y las actividades posibles programadas. Si sucede algún cambio el profesor adaptará los cambios en los contenidos o actividades y los explicará durante la explicación del tema. Si estos cambios son detectados una vez terminada la explicación del tema, durante la realización de las actividades o después, estos cambios se programarán para el siguiente año.
Núm.	**1**	**Título** Principios de seguridad
Objetivos Didácticos		• Analizar la problemática general de la seguridad informática. • Conocer los principios sobre los que se sustenta. • Conocer el significado de alta disponibilidad. • Identificar las principales vulnerabilidades, ataques y medidas de seguridad a adoptar sobre los sistemas. • Diferenciar la seguridad física y lógica, y la pasiva de la activa
Contenidos		1.1. INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA 1.2. FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD Práctica 1.1: Confidencialidad Práctica 1.2: Integridad Práctica 1.3: Disponibilidad 1.2.1. Alta disponibilidad 1.3. ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS 1.4. 1.4.AMENAZAS 1.4.1. Amenazas provocadas por personas 1.4.2. Amenazas físicas y lógicas 1.4.3. Técnicas de ataque 1.1.1.1. En PCs 1.1.1.2. En Android 1.2. PROTECCIÓN 1.2.1. Auditoría de seguridad de sistemas de información 1.2.2. Medidas de seguridad 1.3. REFERENCIAS WEB
Actividades Posibles		• Actividad 1 • Práctica de FootPrinting y FingerPrinting • Práctica de busqueda de vulnerabilidades • Práctica Metasploit 1 • Práctica Metasploit 2 • Práctica SET • Actividad sobre FING • Actividad sobre Android • Ejercicios propuestos 1-13 • Ficheros de Prácticas 1,2,3

Actividades A entregar (80% de la nota final de la unidad)	• Práctica de FootPrinting y FingerPrinting (1,75 ptos) • Práctica de busqueda de vulnerabilidades (1 pto) • Práctica Metasploit 1 (1 pto) • Práctica Metasploit 2 (1 pto) • Práctica SET (1 pto) • Ficheros de Prácticas 1 (1 pto) • Ficheros de Prácticas 2 (1’25 ptos) • Ficheros de Prácticas 3 (1 pto) • A libre elección: realiza el ejercicio 11 o 12 (1 pto)
Criterios de Evaluación	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 analizado supuestos y situaciones en las que se hace necesario implementar soluciones de alta disponibilidad.

Núm.	**2**	**Título**	Seguridad física
Objetivos Didácticos			• Profundizar en aspectos de seguridad pasiva, como son las copias de seguridad y medidas específicas de seguridad física y ambiental. • Valorar la importancia de realizar periódicamente copias de seguridad de la información sensible de nuestros sistemas. • Analizar los distintos aspectos que influyen en la ubicación física de los sistemas. • Valorar la importancia para la empresa de un centro de procesamiento de datos (CPD) y analizar qué medidas específicas requiere analizar los distintos dispositivos hardware que permiten mejorar la seguridad física como sistemas de alimentación ininterrumpida (SAI), sistemas de refrigeración, armarios de seguridad, circuitos cerrados de televisión, etc. • Investigar sobre nuevos métodos de seguridad física y de control de acceso a los sistemas mediante biometría.

Contenidos	2.1. PRINCIPIOS DE LA SEGURIDAD PASIVA 2.2. COPIAS DE SEGURIDAD 2.2.1. Modelos de almacén de datos 2.2.2. Recomendación sobre el tipo de copia a efectuar 2.2.2.1.1. Práctica 2.1: Copias de seguridad con herramientas del sistema 2.2.2.1.2. Práctica 2.2: Copias de seguridad con aplicaciones específicas 2.2.3. Recuperación de datos 2.2.3.1.1. Práctica 2.3: Recuperación de datos 2.3. SEGURIDAD FÍSICA Y AMBIENTAL 2.3.1. Centros de procesado de datos (CPD) 2.3.2. Ubicación y acondicionamiento físico 2.3.3. Control de acceso físico 2.3.4. Sistemas biométricos 2.3.5. Circuito cerrado de televisión (CCTV) 2.4. 2.4.SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI) 2.4.1. Tipos de SAI 2.4.2. Potencia necesaria 2.4.2.1.1. Práctica 2.4: Monitorización de SAI 2.4.2.1.2. Práctica 2.5: Cálculo energético de SAI 2.5. REFERENCIAS WEB
Actividades Posibles	• Prácticas 2.1 sobre copias de seguridad de sistema en Windows • Prácticas 2.2 sobre copias de seguridad de sistema en Linux • Prácticas 2.3 sobre aplicaciones de copias de seguridad • Prácticas 2.4 sobre aplicaciones de recuperación de datos. • Prácticas 2.5 sobre cálculo de SAI o ejercicio propuesto 18 • Prácticas 2.6 sobre copias de seguridad en android nativas • Prácticas 2.7 sobre copias de seguridad en android no nativas • Ejercicios propuestos 1-51
Actividades A entregar (80% de la nota final de la unidad)	• Prácticas 2.1 sobre copias de seguridad de sistema en Windows (1 pto) • Prácticas 2.2 sobre copias de seguridad de sistema en Linux (1,7 ptos) • Prácticas 2.3 sobre aplicaciones de copias de seguridad (1,7 ptos) • Prácticas 2.4 sobre aplicaciones de recuperación de datos. (1,7 ptos) • Prácticas 2.5 sobre cálculo de SAI o ejercicio propuesto 18 (1,2 ptos) • Prácticas 2.6 sobre copias de seguridad en android nativas (0,95 ptos) • Prácticas 2.7 sobre copias de seguridad en android no nativas (1,3 ptos) • Ejercicio propuesto 33 (0,45 ptos) • Ejercicio propuesto 20 (Opcional vale 1 pto extra)

Criterios de Evaluación	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 valorado las ventajas que supone la utilización de sistemas biométricos. d) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles

Núm.	**3**	**Título**	Seguridad lógica
Objetivos Didácticos			• Profundizar en aspectos de seguridad lógica. • Valorar la importancia del uso de contraseñas seguras. • Restringir el acceso autorizado en el arranque, sistemas operativos, ficheros, carpetas y aplicaciones. • Analizar las ventajas de disponer el sistema y aplicaciones actualizadas. • Garantizar el acceso restringido de los usuarios a datos y aplicaciones, mediante políticas de seguridad.
Contenidos			3.1. PRINCIPIOS DE LA SEGURIDAD LÓGICA 3.2. CONTROL DE ACCESO LÓGICO 3.2.1. Política de contraseñas 3.2.1.1.1. Práctica 3.1: Configuración de contraseñas seguras 3.2.1.1.2. Práctica 3.2: Peligros de distribuciones Live! 3.2.2. Control de acceso en la BIOS y gestor de arranque 3.2.2.1.1. Práctica 3.3: Configurando contraseña en la BIOS 3.2.2.1.2. Práctica 3.4: Contraseña en el gestor de arranque 3.2.3. Control de acceso en el sistema operativo 3.2.3.1.1. Práctica 3.5: Recuperación de contraseñas 3.2.3.1.2. Práctica 3.6: Modificación de contraseñas 3.3. POLÍTICA DE USUARIOS Y GRUPOS 3.3.1.1.1. Práctica 3.7: Control de acceso a datos y aplicaciones 3.4. REFERENCIAS WEB

Actividades Posibles	• Actividad Comprobación de passwords • Actividad Generación de passwords. • Actividad Passwords de bancos online • Actividad Cifrado de contraseñas • Actividad tipos de encriptacion y esquemas de codificación • Actividad Ataque password guessing por SMB • Actividad Ataque password guessing por WMI • Actividad Ataque password guessing a SSH • Actividad Directivas de auditoría Windows • Actividad Políticas de Contraseñas Windows • Actividad Bloqueo de cuentas Windows • Actividad Ataque a cuenta de administrador en sistemas Windows • Actividad Resumen de defensas Windows contra ataques online • Actividad Configuración de pam_cracklib para Linux • Actividad Periodo validez contraseñas Linux. • Actividad Bloqueo de cuentas Linux • Actividad John the Ripper contra SAM Windows 7 • Actividad Modificar Contraseñas Usuario • Actividad StickyKeys Windows • Actividad mkpasswd Linux • Actividad SYSKEY con Ophcrack • Actividad Keepass • Actividad Permisos usuario Linux • Actividad POSIX ACL • PRÁCTICA 3.1: CONFIGURACIÓN DE CONTRASEÑAS SEGURAS • PRÁCTICA 3.2: PELIGROS DE DISTRIBUCIONES LIVE • PRÁCTICA 3.3: CONFIGURANDO CONTRASEÑA EN LA BIOS • PRÁCTICA 3.4: CONTRASEÑA EN EL GESTOR DE ARRANQUE • PRÁCTICA 3.5: RECUPERACIÓN DE CONTRASEÑAS • PRÁCTICA 3.6: MODIFICACIÓN DE CONTRASEÑAS • PRÁCTICA 3.7: CONTROL DE ACCESO A DATOS Y APLICACIONES • Ejercicios propuestos 1-9

Actividades A entregar (80% de la nota final de la unidad)	• PRÁCTICA 3.1: CONFIGURACIÓN DE CONTRASEÑAS SEGURAS (0,7 ptos)
	• PRÁCTICA 3.3: CONFIGURANDO CONTRASEÑA EN LA BIOS (0,7 ptos)
	• PRÁCTICA 3.4: CONTRASEÑA EN EL GESTOR DE ARRANQUE (0,725 ptos)
	• PRÁCTICA 3.5: RECUPERACIÓN DE CONTRASEÑAS (1,2 ptos)
	• PRÁCTICA 3.6: MODIFICACIÓN DE CONTRASEÑAS (1,2 ptos)
	• PRÁCTICA 3.7: CONTROL DE ACCESO A DATOS Y APLICACIONES (1 ptos)
	• Actividad Cifrado de contraseñas (0,25 ptos)
	• Opción1: Escoger una de las siguientes: (1 ptos)
	  • Actividad Ataque password guessing por SMB
	  • Actividad Ataque password guessing por WMI
	  • Actividad Ataque password guessing a SSH
	• Actividad Ataque a cuenta de administrador en sistemas Windows (0,725 ptos)
	• Tarea1: Hacer las 3 actividades siguientes: (1 pto)
	  • Actividad Configuración de pam_cracklib para Linux
	  • Actividad Periodo validez contraseñas Linux.
	  • Actividad Bloqueo de cuentas Linux
	• Actividad John the Ripper contra SAM Windows 7 (0,75 ptos)
	• Actividad SYSKEY con Ophcrack (0,5 ptos)
	• Actividad Keepass (0,25 ptos)

Criterios de Evaluación	a) Se han adoptado políticas de contraseñas. b) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. c) Se ha verificado el origen y la autenticidad de las aplicaciones Instaladas en un equipo, así como el estado de actualización del sistema operativo. d) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.

Núm.	**4**	**Título**	Software antimalware
Objetivos Didácticos			• Comprender qué es el software malicioso (malware) y sus posibles fuentes. • Crear conciencia de análisis de riesgo y toma de precauciones en las operaciones informáticas. • Identificar las nuevas posibilidades y riesgos que poseen Internet y las redes sociales. • Analizar las distintas herramientas de seguridad software antimalware existentes.

Contenidos	4.1. SOFTWARE MALICIOSO 4.2. CLASIFICACIÓN DEL MALWARE 4.2.1. Métodos de infección 4.2.1.1.1. Práctica 4.1: Keylogger 4.3. PROTECCIÓN Y DESINFECCIÓN 4.3.1. Clasificación del software antimalware 4.3.1.1.1. Práctica 4.2: Antimalware 4.3.1.1.2. Práctica 4.3: Antimalware GNU/Linux 4.3.1.1.3. Práctica 4.4: Análisis antimalware Live! 4.3.2. La mejor herramienta antimalware 4.3.2.1.1. Práctica 4.5: Análisis antimalware a fondo 4.4. REFERENCIAS WEB
Actividades Posibles	• Actividad 1: métodos de infección • Actividad 2: verify • Actividad 3: Process Explorer svchost • Actividad 4: Process Explorer cadena de texto • Actividad 5: Process Explorer dlls • Actividad 6: Process Explorer drivers • Actividad 7: Process Explorer whois • Actividad 8: Process Explorer autoruns • Actividad 9: process monitor • Actividad 10a: Keyloggers • Actividad 10b: Keyloggers • Actividad 11: Spy-Net • Creación de un Troyano. • Descargar de moodle el fichero posibilidad1.rar y seguir los pasos del video. • Descargar de moodle el fichero posibilidad2.rar y seguir los pasos del video. • Actividad 12: Creación de un Troyano • Actividad 13: Creación de un Virus • Actividad 14: CrackMe2 • Actividad 15: Antirookit • Actividad 16: Antimalware • Actividad 17: Antispyware • Actividad 18: Cortafuegos software • Actividad 19: Herramientas • PRÁCTICA 4.2: ANÁLISIS ANTIMALWARE A FONDO • PRÁCTICA 4.3: CLAMAV • PRÁCTICA 4.4: ANÁLISIS ANTIMALWARE LIVE • PRÁCTICA 4.5: REALIZACIÓN DE UN VIRUS Y UN TROYANO MEDIANTE BATCH • Ejercicios propuestos 1-12

Actividades A entregar (80% de la nota final de la unidad)	• Tarea 1 (1,25 ptos): • Actividad 2: verify • Actividad 3: Process Explorer svchost • Actividad 4: Process Explorer cadena de texto • Actividad 5: Process Explorer dlls • Actividad 6: Process Explorer drivers • Actividad 7: Process Explorer whois • Actividad 8: Process Explorer autoruns • Actividad 9: process monitor • Opcional (1 pto): • Actividad 10a: Keyloggers • Actividad 10b: Keyloggers • Actividad 11: Spy-Net (1,5 ptos) • Opcional: Creación de un Troyano. Escoger una de las 3 posibilidades (1,25 ptos) • Descargar de moodle el fichero posibilidad1.rar y seguir los pasos del video. • Descargar de moodle el fichero posibilidad2.rar y seguir los pasos del video. • Actividad 12: Creación de un Troyano • Actividad 13: Creación de un Virus (1,25 pto) • PRÁCTICA 4.2: ANÁLISIS ANTIMALWARE A FONDO (1,5 ptos) • PRÁCTICA 4.3: CLAMAV (1 pto) • PRÁCTICA 4.4: ANÁLISIS ANTIMALWARE LIVE (0,5 ptos) • PRÁCTICA 4.5: REALIZACIÓN DE UN VIRUS Y UN TROYANO MEDIANTE BATCH (0,75 ptos) •
Criterios de Evaluación	a) Se han clasificado las principales vulnerabilidades de un sistema informático, según su tipología y origen. b) Se han clasificado los principales tipos de amenazas lógicas contra un sistema informático. c) Se ha verificado el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo. d) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. e) Se han analizado diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados. f) Se han implantado aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso. g) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.

Núm.	**5**	**Título**	Criptografía
Objetivos Didácticos			• Profundizar en aspectos de criptografía asociada a la confidencialidad de la información y de las comunicaciones. • Garantizar la confidencialidad de la información. • Garantizar la privacidad de las comunicaciones.

	• Diferenciar ventajas e inconvenientes de la criptografía simétrica y asimétrica. • Analizar nuevos procesos de identificación digital seguros mediante firma digital, certificado digital y DNI electrónico.
Contenidos	5.1. PRINCIPIOS DE CRIPTOGRAFÍA 5.2. TIPOS DE ALGORITMOS DE CIFRADO 5.2.1.1.1. Práctica 5.1: Scripts de cifrado 5.2.2. Criptografía simétrica 5.2.2.1.1. Práctica 5.2: Cifrado simétrico 5.2.2.1.2. Práctica 5.3: Cifrado de datos y particiones 5.2.3. Criptografía de clave asimétrica 5.2.3.1.1. Práctica 5.4: Funciones resumen (hash) 5.2.4. Criptografía híbrida 5.2.4.1.1. Práctica 5.5: Cifrado asimétrico 5.2.5. Firma digital 5.2.5.1.1. Práctica 5.6: Firma digital de un documento 5.3. CERTIFICADOS DIGITALES 5.3.1.1.1. Práctica 5.7: Utilidades de certificados 5.3.2. Terceras partes de confianza 5.3.3. Documento Nacional de Identidad electrónico (DNIe) 5.4. REFERENCIAS WEB
Actividades Posibles	• PRACTICA 5.1: SCRIPTS DE CIFRADO CESAR • PRACTICA 5.2: PROGRAMAS ANDROID CIFRADO • PRÁCTICA 5.3: CIFRADO SIMETRICO • PRÁCTICA 5.4: CIFRADO DE DATOS Y PARTICIONES TRUECRYPT • PRÁCTICA 5.4b: CIFRADO DE DATOS EN ANDROID • PRÁCTICA 5.6: CIFRADO ASIMÉTRICO • PRÁCTICA 5.7: FIRMA DIGITAL DE UN DOCUMENTO • PRÁCTICA 5.8: UTILIDADES DE CERTIFICADOS • Actividades 1 a 5 • Ejercicios Propuestos 1-9
Actividades A entregar (80% de la nota final de la unidad)	• PRACTICA 5.1: SCRIPTS DE CIFRADO CESAR (1pto) • PRACTICA 5.2: PROGRAMAS ANDROID CIFRADO (1,25 ptos) • PRÁCTICA 5.3: CIFRADO SIMETRICO (1,25 ptos) • PRÁCTICA 5.4: CIFRADO DE DATOS Y PARTICIONES TRUECRYPT (1,25 ptos) • PRÁCTICA 5.4b: CIFRADO DE DATOS EN ANDROID (1,25 ptos) • PRÁCTICA 5.5: seguridad_funciones_resumen_hash (0,75 ptos) • PRÁCTICA 5.6: CIFRADO ASIMÉTRICO (1,5 ptos) • PRÁCTICA 5.7: FIRMA DIGITAL DE UN DOCUMENTO (1,25 ptos) • PRÁCTICA 5.8: UTILIDADES DE CERTIFICADOS (0,5 ptos)
Criterios de Evaluación	a) Se ha valorado la importancia de asegurar la privacidad, coherencia y disponibilidad de la información en los sistemas informáticos. b) Se han aplicado técnicas criptográficas en el almacenamiento y transmisión de la información. c) Se han utilizado técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.

Núm.	6	Título	Seguridad en redes corporativas
Objetivos Didácticos			• Valorar los nuevos peligros derivados de la conexión a redes. • Adoptar medidas de seguridad en redes corporativas o privadas tanto cableadas como inalámbricas. • Analizar las principales vulnerabilidades de las redes inalámbricas. • Comprender la importancia de los puertos de comunicaciones y las amenazas existentes en protocolos poco seguros. • Conocer y emplear protocolos y aplicaciones seguras en comunicaciones.
Contenidos			6.1. AMENAZAS Y ATAQUES 6.1.1.1.1. Práctica 6.1: Sniffing – MitM – ARP Spoofing – Pharming 6.1.2. Amenazas externas e internas 6.2. SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS) 6.2.1.1.1. Práctica 6.2: IDS – Snort 6.3. RIESGOS POTENCIALES EN LOS SERVICIOS DE RED 6.3.1.1.1. Práctica 6.3: Análisis de puertos 6.4. COMUNICACIONES SEGURAS 6.4.1.1.1. Práctica 6.4: SSH 6.5. Práctica 6.5: TLS/SSL. Protocolos seguros 6.5.1. V PN 6.5.1.1.1. Práctica 6.6: Conexión remota con VPN 6.6. REDES INALÁMBRICAS 6.6.1. Sistemas de seguridad en WLAN 6.6.1.1.1. Práctica 6.7: WEP 6.6.1.1.2. Práctica 6.8: WPA 6.6.1.1.3. Práctica 6.9: Servidor de autenticación Radius 6.6.2. Recomendaciones de seguridad en WLAN 6.6.2.1.1. Práctica 6.10: Configuración AP seguro 6.7. REFERENCIAS WEB
Actividades Posibles			• PRACTICA 6.1: Sniffing - MitM - ARP Spoofing - Pharming • PRACTICA 6.2: IDS-SNORT • PRACTICA 6.3: ANÁLISIS DE PUERTOS • PRACTICA 6.4: SSH • PRACTICA 6.5: TLS/SSL. PROTOCOLOS SEGUROS • PRACTICA 6.6: CONEXIÓN REMOTA CON VPN • PRACTICA 6.7: WEP • PRACTICA 6.8: WPA • PRACTICA 6.9: SERVIDOR DE AUTENTICACIÓN RADIUS • PRACTICA 6.10: CONFIGURACIÓN AP SEGURO • PRACTICA 6.11: Configuración Red Wifi con Autenticación contra Servidor NPS • Ejercicios propuesto 1-34

Actividades A entregar (80% de la nota final de la unidad)	• PRACTICA 6.1: Sniffing - MitM - ARP Spoofing – Pharming (0,9 puntos) • PRACTICA 6.2: IDS-SNORT(0,9 puntos) • PRACTICA 6.4: SSH(0,9 puntos) • PRACTICA 6.5: TLS/SSL. PROTOCOLOS SEGUROS(0,9 puntos) • PRACTICA 6.6: CONEXIÓN REMOTA CON VPN(0,9 puntos) • PRACTICA 6.9: SERVIDOR DE AUTENTICACIÓN RADIUS(0,9 puntos) • PRACTICA 6.11: Configuración Red Wifi con Autenticacion contra Servidor NPS (0,9 puntos) • Ejercicio propuesto 21 (0,9 puntos) • Ejercicio propuesto 23 (1 puntos) • Ejercicio propuesto 25 (0,9 puntos) • Ejercicio a escoger: Escoger entre los ejercicios propuestos 30, 31 y 32 y atacar a la red de andared y la wifi de la clase (o otras que se tenga en la casa del alumno con WEP y otra con WPA) (0,9 puntos)
Criterios de Evaluación	a) Se han identificado la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles. b) Se han evaluado las medidas de seguridad de los protocolos usados en redes inalámbricas. c) Se ha reconocido la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema. d) Se han descrito los tipos y características de los sistemas de detección de intrusiones. e) Se han descrito escenarios típicos de sistemas con conexión a redes públicas en los que se precisa fortificar la red interna. f) Se han clasificado las zonas de riesgo de un sistema, según criterios de seguridad perimetral. g) Se han identificado los protocolos seguros de comunicación y sus ámbitos de utilización. h) Se han configurado redes privadas virtuales mediante protocolos seguros a distintos niveles. i) Se ha implantado un servidor como pasarela de acceso a la red interna desde ubicaciones remotas. j) Se han identificado y configurado los posibles métodos de autenticación en el acceso de usuarios remotos a través de la pasarela. k) Se ha instalado, configurado e integrado en la pasarela un servidor remoto de autenticación.
Núm. **7**	**Título** Seguridad perimetral
Objetivos Didácticos	• Valorar los peligros externos a las redes corporativas y conocer las medidas de seguridad perimetrales para hacerles frente. • Comprender la importancia de los puertos de comunicaciones y su filtrado mediante cortafuegos o firewall. • Aprender el significado de las listas de control de acceso (ACL) en routers y cortafuegos. • Comprender la importancia y aprender a configurar servidores y clientes proxy.

Contenidos	7.1. CORTAFUEGOS 7.1.1.1.1. Práctica 7.1: Configuración de cortafuegos 7.1.1.1.2. Práctica 7.2: Archivos log 7.1.2. Tipos de cortafuegos 7.1.2.1.1. Práctica 7.3: Configuración Router-Firewall 7.1.2.1.2. Práctica 7.4: Configuración de cortafuegos con entorno gráfico 7.1.3. DMZ 7.2. PROXY 7.2.1. Tipos, características y funciones principales 7.2.1.1.1. Práctica 7.5: Configuración de Proxy. Gestión de caché, log, clientes y filtros web 7.3. REFERENCIAS WEB
Actividades Posibles	• PRACTICA 7.1: CONFIGURACIÓN DE CORTAFUEGOS • PRACTICA 7.2: ARCHIVOS LOGS • PRACTICA 7.3: CONFIGURACION ROUTER-FIREWALL • PRACTICA 7.4: CONFIGURACIÓN DE CORTAFUEGOS CON ENTORNO GRÁFICO Kerio 1 • PRACTICA 7.4B : CONFIGURACIÓN DE CORTAFUEGOS CON ENTORNO GRÁFICO Kerio 2 • PRACTICA 7.5: CONFIGURACIÓN DE PROXY. GESTIÓN DE CACHÉ, LOG, CLIENTES Y FILTROS WEB. • PRÁCTICA 7.6: DMZ • PRÁCTICA 7.7: IPTABLES • Actividad 1 • Actividad 2 • Ejercicios propuesto 1-9
Actividades A entregar (40% de la nota final de la unidad)	• PRACTICA 7.1: CONFIGURACIÓN DE CORTAFUEGOS (1 pto) • PRACTICA 7.2: ARCHIVOS LOGS (1 pto) • PRACTICA 7.3: CONFIGURACION ROUTER-FIREWALL (1 pto) • PRACTICA 7.4B : CONFIGURACIÓN DE CORTAFUEGOS CON ENTORNO GRÁFICO Kerio 2 (1 pto) • PRACTICA 7.5: CONFIGURACIÓN DE PROXY. GESTIÓN DE CACHÉ, LOG, CLIENTES Y FILTROS WEB. (1 pto) • PRÁCTICA 7.6: DMZ (1,25 ptos) • PRÁCTICA 7.7: IPTABLES (1,25 ptos) • Actividad 1 (1,25 ptos) • Ejercicio propuesto 9 (1,25 ptos)

Criterios de Evaluación	a) Se ha reconocido la necesidad de establecer un plan integral de protección perimetral, especialmente en sistemas conectados a redes públicas. b) Se han descrito las características, tipos y funciones de los cortafuegos. c) Se han clasificado los niveles en los que se realiza el filtrado de tráfico. d) Se ha planificado la instalación de cortafuegos para limitar los accesos a determinadas zonas de la red. e) Se han configurado filtros en un cortafuegos a partir de un listado de reglas de filtrado. f) Se han revisado los registros de sucesos de cortafuegos, para verificar que las reglas se aplican correctamente. g) Se han probado distintas opciones para implementar cortafuegos, tanto software como hardware. h) Se han diagnosticado problemas de conectividad en los clientes provocados por los cortafuegos. i) Se ha elaborado documentación relativa a la instalación, configuración y uso de cortafuegos. j) Se han identificado los tipos de proxy, sus características y funciones principales. k) Se ha instalado y configurado un servidor proxy-caché. l) Se han configurado los métodos de autenticación en el proxy. m) Se ha configurado un proxy en modo transparente. n) Se ha utilizado el servidor proxy para establecer restricciones de acceso web. o) Se han solucionado problemas de acceso desde los clientes al proxy. p) Se han realizado pruebas de funcionamiento del proxy, monitorizando su actividad con herramientas gráficas. q) Se ha configurado un servidor proxy en modo inverso. r) Se ha elaborado documentación relativa a la instalación, configuración y uso de servidores proxy.

Núm.	**8**	**Título**	Configuraciones de alta disponibilidad
Objetivos Didácticos			• Analizar las distintas configuraciones de alta disponibilidad. • Valorar la importancia de realizar un buen análisis de riesgos potenciales en sistemas críticos y adoptar medidas para paliar sus posibles consecuencias. • Aprender las diferencias, ventajas e inconvenientes entre los sistemas de almacenamiento redundante (RAID) y conocer sus opciones de configuración y prueba. • Conocer las opciones de configuración y administración de balanceo de carga entre distintas conexiones de red. • Realizar configuraciones de alta disponibilidad de servidores mediante virtualización de sistemas operativos.

Contenidos	8.1. SOLUCIONES DE ALTA DISPONIBILIDAD 8.2. RAID 8.2.1.1.1. Práctica 8.1: Configuración de Raid mediante software 8.3. BALANCEO DE CARGA 8.3.1.1.1. Práctica 8.2: Balanceo de carga 8.4. VIRTUALIZACIÓN 8.4.1. Virtualización de servidores 8.4.1.1.1. Práctica 8.3: Creación de máquinas virtuales 8.4.1.1.2. Práctica 8.4: Configuración de red de máquinas virtuales 8.4.1.1.3. Práctica 8.5: Servidor NAS virtual 8.5. REFERENCIAS WEB
Actividades Posibles	• PRACTICA 8.1: CONFIGURACIÓN DE RAID MEDIANTE SOFTWARE. • PRACTICA 8.2: BALANCEO DE CARGA. • PRACTICA 8.3: CREACIÓN MAQUINAS VIRTUALES • PRACTICA 8.4: CONFIGURACIÓN DE RED DE MÁQUINAS VIRTUALES • PRACTICA 8.5: SERVIDOR NAS VIRTUAL • Ejercicios propuestos 1-10
Actividades A entregar (80% de la nota final de la unidad)	• PRACTICA 8.1: CONFIGURACIÓN DE RAID MEDIANTE SOFTWARE. (2,25 puntos) • PRACTICA 8.2: CONFIGURACIÓN DE RAID MEDIANTE SOFTWARE. (2,25 puntos) • PRACTICA 8.3: CREACIÓN MAQUINAS VIRTUALES(2,25 puntos) • PRACTICA 8.4: CONFIGURACIÓN DE RED DE MÁQUINAS VIRTUALES(1 punto) • PRACTICA 8.5: SERVIDOR NAS VIRTUAL(2,25 puntos)
Criterios de Evaluación	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.

Núm.	9	Título	Normativa legal en materia de seguridad en TI
Objetivos Didácticos			• Conocer la normativa española en materia de seguridad informática. • Analizar la normativa y aplicaciones de la LOPD, en materia de seguridad de los datos de carácter personal. • Analizar la normativa y aplicaciones de la LSSICE, en materia de comercio electrónico y actividades empresariales vía Internet. • Valorar la importancia de la normativa como reguladora de derechos y obligaciones a ciudadanos y empresas.
Contenidos			9.1. LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD) 9.1.1. Ámbito de aplicación de la LOPD 9.1.2. Agencia Española de Protección de Datos 9.1.3. Tratamiento de los datos Práctica 9.1: Formulario LOPD 9.1.4. Niveles de seguridad Práctica 49: Normas de la organización 9.2. LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSICE) 9.2.1. Entornos Web Práctica 9.2: LSSICE Web 9.2.2. Comunicaciones comerciales Práctica 9.3: LOPD y LSSICE en el correo electrónico 9.3. REFERENCIAS WEB
Actividades Posibles			• PRACTICA 9.1 FORMULARIO LOPD • PRACTICA 9.2 NORMAS DE LA ORGANIZACION • PRACTICA 9.3 LSSICE WEB • PRACTICA 9.4 LOPD LSSICE EN EMAIL.pdf • Ejercicios propuestos 1-7
Actividades A entregar (100% de la nota final de la unidad)			• PRACTICA 9.1 FORMULARIO LOPD (2,5 puntos) • PRACTICA 9.2 NORMAS DE LA ORGANIZACION (2,5 puntos) • Ejercicio propuesto 5 (2,5 puntos) • PRACTICA 9.4 LOPD LSSICE EN EMAIL (2,5 puntos)
Criterios de Evaluación			a) Se ha descrito la legislación sobre protección de datos de carácter personal. b) Se ha determinado la necesidad de controlar el acceso a la Información personal almacenada. c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. d) Se ha contrastado 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.

Nota sobre las actividades: Las actividades expuestas en esta programación podrán variar a lo largo del curso debido al cambio que se produce en esta asignatura diariamente (cada día aparecen alrededor de más de 10000 malware nuevos en el mundo y aparecen herramientas para detectar y eliminar esos malware). Las actividades definitivas se le informará al alumno antes del periodo de comienzo de las prácticas de esas actividades.

8. ATENCIÓN DEL ALUMNADO CON NECESIDADES EDUCATIVAS ESPECIALES

Entendemos por atención a la diversidad toda aquella actuación educativa que este dirigida a dar respuesta a las diferentes capacidades, ritmos y estilos de aprendizaje, motivaciones e intereses, situaciones sociales, étnicas, de inmigración y de salud del alumnado.

El proceso de atención al alumnado con necesidades educativas especiales se basará en el marco legislativo vigente al respecto. Alguna de esa normativa que podemos destacar es:

- R.D. 777/1998, Disposición adicional undécima: «Las Administraciones educativas competentes podrán establecer las medidas organizativas y de adaptación curricular para que los alumnos con necesidades educativas especiales puedan alcanzar los objetivos y finalidades de las enseñanzas reguladas en el presente Real Decreto».

- R.D. 147/2002, Articulo 23: «El alumnado con discapacidad que curse las enseñanzas de bachillerato y formación profesional podrá realizarlas con las adaptaciones de acceso al currículo que sean necesarias».