GRADO

GUÍA DE ESTUDIO DE LA ASIGNATURA SEGURIDAD

2ª PARTE | PLAN DE TRABAJO Y ORIENTACIONES PARA SU DESARROLLO

2014-2015

| Dr. Mª de los Llanos Tobarra Abad — Dr. Roberto Hernández Berlinches

GRADO EN INGENIERÍA INFORMÁTICA

1.- PLAN DE TRABAJO

En el *cronograma semanal* que sigue se ha estimado el esfuerzo del estudiante según el siguiente baremo:

- Aprendizaje de los contenidos teóricos y prácticos: 103 horas. De ellas se invertirán:

  - Lectura y comprensión del material didáctico del libro de texto base: (360 páginas de material didáctico, a razón de unas 5 páginas/hora): 72 horas = 2,88 ECTS.

  - Consulta de enlaces, presentaciones de resúmenes, recopilación y consulta de bibliografía complementaria: 31 horas = 1,24 ECTS.

- Trabajo personal y otras actividades:

  - Contacto virtual a través de la plataforma (participación en foros, consulta de dudas, etc.), a razón de una hora/semana durante 15 semanas: 15 horas = 0,6 ECTS.

  - Repaso de preparación para la Prueba Presencial, durante las dos últimas semanas: 14 horas = 0,56 ECTS.

  - Realización/Repaso de los ejercicios de autoevaluación propuestos por el Equipo Docente: 10 horas = 0,40 ECTS.

  - Realización de Pruebas de Evaluación a Distancia: 6 horas = 0,24 ECTS.

  - Prueba Presencial (Examen): 2 horas = 0.08 ECTS.

Créditos totales: 6 ECTS.

Cronograma Semanal

BLOQUES TEMÁTICOS	LECTURAS Y MATERIALES DE ESTUDIO	Horas	ACTIVIDADES	Horas	Total h.	Semana
MODULO I: Conceptos e implementación de la monitorización de la seguridad en redes						
Unidad 1: Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.	Capítulo 1 (17 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			1
Unidad 2: La seguridad en los elementos físicos existentes en la red.	Capítulo 2 (17 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			2
Unidad 3: La seguridad en los elementos software existentes en una red.	Capítulo 3 (21 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			3
Unidad 4: Métodos de ataque a equipos y redes.	Capítulo 4 (31 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			4
Unidad 5: Defensa básicas ante ataques.	Capítulo 5 (19 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA			5
MODULO II: Prácticas recomendadas en la implantación de procesos de seguridad						
Unidad 6: La política de seguridad como respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.	Capítulo 6 (24 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			6
Unidad 7: Métodos no criptográficos en la implantación de la política de seguridad.	Capítulo 7 (9 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			7
Unidad 8: Redes privadas virtuales.	Capítulo 17 (23 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			8
MODULO III: Sistemas de gestión de la seguridad en redes.						
Unidad 9: Los cortafuegos (firewalls) y sus aplicaciones como elementos básicos de una política de seguridad de redes	Capítulo 8 (20 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			9
Unidad 10: Tecnología de última generación en cortafuegos.	Capítulo 9 (22 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA			10

BLOQUES TEMÁTICOS	LECTURAS Y MATERIALES DE ESTUDIO	Horas	ACTIVIDADES	Horas	Total h.	Semana
Unidad 11: Herramientas de detección de Intrusiones para la monitorización de la seguridad en las comunicaciones.	Capítulo 11 (20 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA			11
MODULO IV: Análisis de Operaciones Intrusivas y herramientas disponibles.						
Unidad 12: Herramientas de análisis de vulnerabilidades para la auditoría de la seguridad en las comunicaciones.	Capítulo 10 (13 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			12
Unidad 13: Diseño seguro de redes. Concepto de alta disponibilidad y diseños redundante	Capítulo 12 (18 páginas) Consulta de material/bibliografía complementaria		Foros Ejercicios autoevaluación			13
Repaso de los Módulos I, II, III y IV			Foros Repaso de las autoevaluaciones Repaso del material del curso	1,0 3,0 8,0	14,0	14
			PRUEBA PRESENCIAL	2,0	2,0	15

2.- ORIENTACIONES PARA EL ESTUDIO DE LOS CONTENIDOS

El contenido de la asignatura se ha divido en *cuatro módulos o unidades temáticas*, por lo que se utilizarán éstas para presentar las orientaciones a seguir en el plan de trabajo. Los módulos son las siguientes:

- MODULO I: Conceptos e implementación de la monitorización de la seguridad en redes.
- MODULO II: Prácticas recomendadas en la implantación de procesos de seguridad.
- MODULO III: Sistemas de gestión de la seguridad en redes.
- MODULO IV: Análisis de Operaciones Intrusivas y herramientas disponibles

2.1 MÓDULO I: Conceptos e Implementación de la Monitorización de la Seguridad en Redes

2.1.1.- Presentación del Módulo I

En este primer módulo introducimos los problemas de la seguridad informática. Debemos tener en cuenta que la seguridad no es un estado que se debe alcanzar, sino un proceso que se adapta al contexto según evoluciona el sistema. Pero para comprender mejor el proceso de la seguridad se presentan los problemas de seguridad que podemos encontrarnos tanto a nivel físico como software. También se dedica atención a la normativa legal vigente que afecta al proceso de seguridad. El proceso de seguridad quedará reflejado en una política de seguridad, que dictamina las principales defensas contra estos posibles ataques. Una vez definida una política de seguridad el siguiente paso es el seguimiento del cumplimiento de esta política. Por último, caracterizaremos el conjunto de intrusiones que se nos pueden presentar.

La Unidad I consta de cinco temas que introducen al estudiante el proceso de la seguridad así. En primer lugar se define la seguridad como un problema que cualquier sistema informático debe abordar. Tras definirlo se resumen las amenazas que un sistema puede recibir tanto a nivel software (aplicaciones y sistemas operativos) como a nivel hardware dentro de las redes, identificando los principales tipos de ataques y caracterizándolos. Tras esta descripción se presentan las primeras herramientas que permiten abordar el proceso de seguridad y que serán tratadas en mayor detalle en los dos próximos módulos

2.1.2- Contextualización en el conjunto de la materia o asignatura

Los objetivos asociados a este módulo son:

- Comprender la trascendencia de introducir (o no) la seguridad como un criterio de diseño en cualquier sistema o aplicación informática.
- Comprender los problemas más habituales actuales que implica la falta de seguridad en sistemas, aplicaciones y redes.
- Clasificar los diferentes ataques desde el punto de vista de peligrosidad, organización y necesidad de recursos.
- Entender, y saber implantar, las defensas básicas en sistemas operativos, aplicaciones y dispositivos básicos de comunicaciones.

Para ello los temas de estudio que forman esta unidad temática son:

- **Unidad 1:** Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.
  - Introducción
  - Las preguntas que deben hacerse para definir el problema
  - Soluciones aparentemente perfectas y soluciones razonables
- **Unidad 2**: La seguridad en los elementos físicos existentes en la red.

    - Introducción
    - Los sistemas de cableado o inalámbricos
    - Repetidores, hubs y conmutadores
    - Encaminadores
    - Los servidores y otras máquinas.
- **Unidad 3:** La seguridad en los elementos software existentes en una red.
    - Introducción
    - Los sistemas operativos de estaciones y servidores
    - Los protocolos y aplicaciones IP
    - Mejoras de seguridad IPv6
    - Criterios de evaluación de seguridad
- **Unidad 4:** Métodos de ataque a equipos y redes.
    - Introducción
    - Taxonomía de los tipos de ataques
    - Ataques orientados a la obtención de información sobre el objetivo
    - Ataques orientados a la obtención no autorizada de información confidencial.
    - Ataques de Denegación de servicios (DoS)
    - Ataques "creativos"
- **Unidad 5:** Defensa básicas ante ataques.
    - Introducción
    - Controles de acceso físico a los sistemas
    - Controles de acceso lógico a los sistemas
    - Otros controles simples de acceso a la información

La **Unidad 1** presenta el concepto de seguridad como un proceso constante y en evolución a lo largo de la vida de un sistema informático. En este tema se detalla las cuestiones que se deben abordar para definir la seguridad como un problema a resolver:

- ¿Qué debe ser protegido?
- ¿Contra quién se quiere proteger?
- ¿Cómo se quiere proteger?
- ¿Cuánto dinero o tiempo se puede emplear en implantar y mantener el sistema de seguridad?

La **Unidad 2** hace un repaso a todos los dispositivos hardware que intervienen en la comunicación de las redes a través de los niveles establecidos por OSI. En cada nivel se presenta el dispositivo, sus características y sus debilidades tanto a nivel de un ataque físico como un ataque al software de control que lo gestiona. También se mencionan las primeras soluciones a estos problemas, como por ejemplo el uso de cables apantallados en el caso de la transmisión de datos por cables de par trenzado.

La **Unidad 3** presta mas atención a los componentes “software” de una red tales como los sistemas operativos, protocolos de comunicaciones (TCP/IP) y servidores. Se presenta los Comon Criteria, siguiendo la norma ISO/IEC 15408 que certifica en cierto grado que los productos software cumplen con condiciones de nuestra futura política de seguridad.

La **Unidad 4** se centra en los ataques y en que las características de los ataques en red, entre ellas destacando su aspecto automático, remoto y su gran propagación de los medios de ataque. Se establece una primera clasificación en la que los ataques pueden ser internos (dentro de una organización) o externos (fuera de la organización). También se pueden clasificar en estructurados, que siguen un esquema de tipo proyecto, o desestructurados. Por último, y en base al objetivo del ataque nos encontramos con:

- Ataques para la obtención de información, como son los de tipo ingeniería social, basados en herramientas informáticas básicas/sofisticadas (nmap por ejemplo) o el uso de analizadores de protocolos (sniffers).

- Ataques que se aprovechan de la mala administración o configuración de los sistemas, como son el robo de contraseñas, basados en relaciones de confianza de sistemas, basados en aplicaciones de compartición de disco duro, autenticación mal administrada, usando técnicas de suplantación, o la inexistencia de ciertos mecanismos de seguridad.
- Ataques que explotan las vulnerabilidades del software, como son un diseño ineficiente de protocolos, o bien su mala implementación así como el desarrollo de software sin tener en cuenta ciertas medidas de seguridad.
- Ataques de denegación de servicio, basado en las características de los protocolos, malas implementaciones de las aplicaciones, inundación de la red o ataques DoS distribuidos.
- Ataques creativos que combinan varios de los ataques de las categorías anteriores.

La **Unidad 5** describe un conjunto de medidas básicas de seguridad que hay que tener en cuenta para una aproximación básica al problema de la seguridad. Se destaca la necesidad de establecer un perímetro de seguridad que permita un control físico del acceso a los equipos importantes del sistema. Y se han descrito una serie de controles de acceso lógico, tanto locales como remotos, basados en contraseñas, datos biométricos y "Access tokens". Así como se ofrece una lista de recomendaciones para una buena configuración de los sistemas de contraseñas junto con la relevancia de la formación de los usuarios en esta dirección. También se describen los tokens de acceso y su uso en sistemas como AAA o Radius para mantener altos niveles de seguridad incluso gestionando accesos remotos. La última parte del tema se dedica al relevante papel que juegan los sistemas de ficheros de los sistemas operativos en la seguridad que pueden ser mejorados con versiones que incluyen la encriptación y un mayor control de acceso. Junto con las copias de seguridad y otras herramientas de "saneamiento" y gestión eficiente de los ficheros en su almacenamiento.

2.1.3.- Información y orientaciones para el trabajo con los materiales requeridos para el estudio de la unidad

Estos temas corresponden a los **capítulos 1, 2, 3, 4 y 5** del libro de la bibliografía básica: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN de los autores Gabriel Díaz Orueta, Francisco, Mur, Elio Sancristóbal, Manuel Castro Manuel y Juan Peire disponible en la Editorial UNED.

El estudio se llevará a cabo siguiendo la planificación descrita en el aparado del cronograma semanal.

Por otra parte, el Equipo Docente publicará en la plataforma los enlaces de interés para cada tema, así como otro material auxiliar que pueda considerar de interés.
Entre ellos destacar el libro Seguridad en Unix y Redes de Antonio Villalón Huerta, disponible de forma gratuita en: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf, que complementa la visión de los primeros temas con sus capítulos:

- 1. Introducción y conceptos previos
- 2. Seguridad física de los entornos
- 3. Administradores, usuarios y personal
- 5. Programas seguros, inseguros y nocivos
- 8. Autenticación de usuarios

Que amplían y complementan los contenidos del módulo.

2.1.4.- Descripción detallada de cada una de las actividades de aprendizaje a realizar

Una vez terminado el estudio de cada tema, como actividad se deberá realizar una autoevaluación consistente en la resolución de una serie de cuestiones teóricas y/o prácticas. Para ello el Equipo Docente publicará, a través de la plataforma virtual, el enunciado de la autoevaluación y su solución.

Durante la realización de la actividad se podrá recurrir al libro de texto cuantas veces sea necesario. Una vez finalizada ésta el estudiante comparará sus resultados con la solución publicada por el Equipo Docente.

Por otra parte, también se debatirá en los foros sobre aquellos conceptos que los estudiantes quieran reforzar.

2.2. MÓDULO II: Practicas Recomendadas en la Implantación de procesos de Seguridad

2.2.1.- Presentación del Módulo II

Este módulo se centra en los administradores de procesos de seguridad. Se presentan prácticas recomendadas para la estimación, protección, detección y respuesta en un proceso de seguridad. A pesar que a lo largo de los otros módulos veremos recomendaciones, herramientas y técnicas a aplicar, en esta parte se ilustran apoyándose en casos prácticos que mejoran la comprensión de los contenidos teóricos.

El módulo II consta de tres temas bien diferenciados, que describen en que consisten las políticas de seguridad, cuales son los principales métodos no criptográficos posibles y nos encontramos con el primer tema dedicado a un ejemplo práctico como son las redes virtuales privadas (VPN).

2.2.2 - Contextualización en el conjunto de la materia o asignatura

Los objetivos que se desarrollan a lo largo de este módulo son:

- Comprender la necesidad de la puesta en marcha de una política de seguridad informática en cualquier organización.
- Entender la trascendencia para las organizaciones de una correcta implementación de la LOPD (Ley Orgánica de Protección de Datos).
- Aplicar los conceptos más elementales aprendidos, relacionados con la seguridad en redes, sistemas y datos, a una organización concreta.
- Entender la relevancia de la puesta en marcha de un Sistema de Gestión de Seguridad Informática que siga las buenas prácticas recomendadas en los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002.

Los temas de estudio que forman esta unidad temática son:

- **Unidad 6:** La política de seguridad como respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.
  - ¿Qué es una política de seguridad?
  - Aspectos físicos de la política de seguridad
  - Aspectos lógicos de la política de seguridad
  - Aspectos humanos y organizativos de la política de seguridad
  - Aspectos legales de la política de seguridad
- **Unidad 7:** Métodos no criptográficos en la implantación de la política de seguridad.
  - Herramientas que implementen la política de seguridad
  - Otros elementos típicos a tener en cuenta.

- **Unidad 8**: Redes privadas virtuales.
    - Caracterización de las redes privadas virtuales
    - Ventajas e inconvenientes de las redes virtuales privadas
    - Arquitecturas de redes privadas virtuales
    - Diseño y planificación de redes privadas virtuales
    - Problemas de rendimiento, mantenimiento y seguridad.

La **Unidad 6** establece cuales son las características esenciales que debe tener cualquier política de seguridad con respecto al propósito que se busca con ello. Así mismo analiza toda una serie de principios de diseño que deben ser cumplidos pro cualquier política de seguridad. Además se resalta la importancia de tener una serie de normas específicas y más fáciles de actualizar de forma individual. También se han enumerado cuales son las normas típicas de cualquier política. Esta unidad también profundiza en la necesidad de recordar que la seguridad es un proceso, cuyo eje principal es la política de seguridad. Como proceso debe superar una serie de fases: puesta en marcha, monitorización, análisis de vulnerabilidades y nueva implantación de la siguiente versión de la política. Por último, se analizado elementos de influencia como son los aspectos de control de acceso físico, acceso lógico, humanos y organizativos así como la legislación vigente que se debe tener en cuenta en España para que nuestra política de seguridad cumpla con la norma vigente.

La **Unidad 7** realiza una enumeración de dispositivos y herramientas no criptográficas utilizadas para hacer cumplir la política de seguridad junto con el diseño seguro de redes. Este concepto de seguridad difiere del visto hasta ahora haciendo mención a conceptos como fiabilidad y alta disponibilidad del sistema. Para ello se describen las técnicas de tolerancia a fallos como los discos redundantes (RAID), las copias de seguridad, planes de recuperación tras un fallo y la tolerancia a fallos de los servidores más significativos.

La **Unidad 8** se concentra en las características, funcionalidades y problemas en torno a las redes privadas virtuales. Una red privada virtual como un enlace seguro a través de una red pública insegura. Las redes VPN suelen tener una serie de características deseables: integridad, autenticación, privacidad, control de acceso, calidad de servicio, etc. Casi todas ellas utilizan métodos criptográficos que aunque quedan fuera de los contenidos del curso se introducen brevemente. Entre las ventajas que presentan este tipo de redes destaca la flexibilidad y escalabilidad de esta solución, la rebaja en costes que suponen y la mayor seguridad que se puede obtener con una implantación y una configuración correcta. Por otra parte, entre los inconvenientes analizados, destacar que suelen conllevar una perdida de la calidad de los servicios. Se analizan los componentes que pertenecen a una VPN como son las pasarelas y los distintos tipos de clientes que interaccionan con la red (móviles, ordenadores, tabletas…). Por último se resumen los principales problemas que suelen acompañar a la implantación de una red privada virtual como es el rendimiento, la seguridad y su mantenimiento. Destacar que las redes privadas virtuales es un tipo de red en crecimiento en el mercado actual.

2.2.3.- Información y orientaciones para el trabajo con los materiales requeridos para el estudio de al unidad

Estos temas corresponden a los **capítulos 6, 7 y 17** del libro de la bibliografía básica: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN de los autores Gabriel Díaz Orueta, Francisco, Mur, Elio Sancristóbal, Manuel Castro Manuel y Juan Peire disponible en la Editorial UNED.

El estudio se llevará a cabo siguiendo la planificación descrita en el aparado del cronograma semanal.

Por otra parte, el Equipo Docente publicará en la plataforma los enlaces de interés para cada tema, así como otro material auxiliar que pueda considerar de interés.

Entre ellos destacar el libro Seguridad en Unix y Redes de Antonio Villalón Huerta, disponible de forma gratuita en: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf, que complementa la visión de los primeros temas con sus capítulos:

- 7. Copias de seguridad
- 22. Gestión de la seguridad
- Apéndice A. Seguridad básica para administradores.

Que amplían y complementan los contenidos del módulo.

.

Así mismo dentro de este módulo los alumnos dispondrán del PDF del libro LA PROTECCIÓN DE DATOS PERSONALES, SOLUCIONES EN ENTORNOS MICROSOFT, VERSIÓN 2.0 cuyos autores Alonso J.M. y otros, para abordar los aspectos legales de la seguridad. La primera parte (legal) del texto de Alonso y otros complementa con mucho detalle el apartado del libro básico sobre la LOPD (Ley Orgánica de Protección de Datos). Aunque no será objeto de evaluación, su segunda parte (técnica) es una muy buena presentación de cómo usar una tecnología concreta para implementar correctamente la LOPD.

2.2.4.- Descripción detallada de cada una de las actividades de aprendizaje a realizar

Una vez terminado el estudio de cada tema, como actividad se deberá realizar una autoevaluación consistente en la resolución de una serie de cuestiones teóricas y/o prácticas. Para ello el Equipo Docente publicará, a través de la plataforma virtual, el enunciado de la autoevaluación y su solución.

Durante la realización de la actividad se podrá recurrir al libro de texto cuantas veces sea necesario. Una vez finalizada ésta el estudiante comparará sus resultados con la solución publicada por el Equipo Docente.

Por otra parte, también se debatirá en los foros sobre aquellos conceptos que los estudiantes quieran reforzar.

2.3. MÓDULO III: Sistemas de Gestión de la Seguridad en Redes

2.3.1.- Presentación del Módulo III

Dentro de este módulo se presentan los principales métodos utilizados para la implantación de diversas normas de seguridad.
Por una parte, se analizar las técnicas de cortafuegos, desde las más sencillas, como los filtros de paquetes las más sofisticadas basadas en filtros dinámicos de conexión. Todos ellos se exponen en la primera parte del módulo incluyendo ejemplos ilustrativos.
La segunda parte del módulo se concentra en los sistemas de detección de intrusos (IDS), que suelen implementar prácticamente todas las técnicas de monitorización reseñadas en el primer módulo del temario. Por lo tanto, debemos conocer qué requisitos deben satisfacer, las diferencias ente los IDS basados en máquinas y los basados en redes, así como las diferencias tecnológicas entre los que basan su trabajo en la detección de anomalías, de usos indebidos o de firmas de ataque.

2.3.2 - Contextualización en el conjunto de la materia o asignatura

Los objetivos que se desarrollan a lo largo de este módulo son:

- Comprender qué son los cortafuegos y herramientas de scanning de seguridad, cómo se usan y qué papel juegan en una política de seguridad.
- Conocer herramientas de software libre para el análisis del tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.
- Comprender qué son los sistemas de detección de intrusiones (IDS) y qué papel juegan en una política de seguridad.
- Conocer herramientas de software libre para el análisis del tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.
- Describir las mejores herramientas para la puesta en marcha de una política de seguridad.

Los temas de estudio que forman esta unidad temática son:

- *Parte 1: Protección de la red Cortafuegos*
  - **Unidad 9:** Los cortafuegos (firewalls) y sus aplicaciones como elementos básicos de una política de seguridad de redes
    - Los filtros de paquetes
    - Los gateways de aplicación o servidores proxy
    - ¿Qué se puede mejorar?
  - **Unidad 10:** Tecnología de última generación en cortafuegos.
    - Caso práctico: el modelo Cisco PIX Firewall
    - Caso práctico: el modelo Checkpoint Firewall-1
    - La confusión reinante
- *Parte 2: Sistemas de detección de intrusos (IDS)*
  - **Unidad 11:** Herramientas de detección de Intrusiones para la monitorización de la seguridad en las comunicaciones.
    - Introducción
    - Caso práctico: los sistemas Cisco Secure IDS
    - Caso práctico: los sistemas Red Secure de ISS
    - ¿Qué son los Honey Pots?

La **Unidad 9** presenta a los cortafuegos como herramienta fundamental para prevenir los ataques externos a un sistema. En la unidad también se resalta que un cortafuegos no puede resolver cualquier problema interno surgido en la red a proteger, no puede hacer nada contra ataques realizados mediante tráfico que no puede analizar. A lo largo de la unidad, además de recorrer las ventajas e inconvenientes que presentan, se ofrece una clasificación de los tipos de cortafuegos más significativos: filtros de paquetes, servidores proxy y híbridos. También se detalla el concepto de red DMZ, una red entre el cortafuegos y la red interna, donde poder colocar equipos que, por un lado interese tener cerca de la red externa y, por otro lado, no tener en la propia red interna. Para ello se ha comentado las posibles topologías junto con los distintos tipos de cortafuegos descritos en la unidad.

La **Unidad 10** extiende los conceptos de la unidad anterior a las técnicas de cortafuegos más novedosas: el uso de la inspección completa y dinámica de paquetes, conocida también como “stateful inspection”; o bien a la combinación de los cortafuegos con características de seguridad no propias de un cortafuegos. Para ilustrar estas tendencias se describen dos cortafuegos actuales como es PIX de Cisco Systems y Firewall-1 de Checkpoint.

La **Unidad 11** se realiza un análisis de las características y funcionamiento generales de las herramientas conocidas como sistemas de detección de intrusiones, utilizadas dentro de la denominada fase de monitorización del desarrollo del proceso de seguridad de una organización. Desde la definición y los usos de los IDS, se realiza una caracterización de los distintos tipos de IDS del mercado, catalogándolos por la

tecnología de captura de mensajes de ataque (de anomalías o de firmas) y por ubicación de los IDS en la topología de la red (ubicados en sistemas o basados en la red). En particular, se estudia el caso de los IDS basados en firmas y de red de Cisco Systems llamados CSID y los entornos Real Secure de ISS, que gestionan varios sistemas IDS desde la misma consola. Además se analizaran los honey pots como una nueva herramienta de obtención de información sobre los hábitos y herramientas de trabajo de los posibles atacantes. Por último, se repasan los posibles inconvenientes como los falsos positivos y el impacto que puede tener en el sistema.

2.3.3.- Información y orientaciones para el trabajo con los materiales requeridos para el estudio de al unidad

Estos temas corresponden a los **capítulos 8,9 y 11** del libro de la bibliografía básica: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN de los autores Gabriel Díaz Orueta, Francisco, Mur, Elio Sancristóbal, Manuel Castro Manuel y Juan Peire disponible en la Editorial UNED.

El estudio se llevará a cabo siguiendo la planificación descrita en el aparado del cronograma semanal.

Por otra parte, el Equipo Docente publicará en la plataforma los enlaces de interés para cada tema, así como otro material auxiliar que pueda considerar de interés.
Entre ellos destacar el libro Seguridad en Unix y Redes de Antonio Villalón Huerta, disponible de forma gratuita en: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf, que complementa la visión de los primeros temas con sus capítulos:

- 15. Cortafuegos: Conceptos Teóricos
- 16. Cortafuegos: Casos de Estudio
- 18. Sistemas de Detección de Intrusos

Que amplían y complementan los contenidos del módulo.

2.3.4.- Descripción detallada de cada una de las actividades de aprendizaje a realizar

Una vez terminado el estudio de cada tema, como actividad se deberá realizar una autoevaluación consistente en la resolución de una serie de cuestiones teóricas y/o prácticas. Para ello el Equipo Docente publicará, a través de la plataforma virtual, el enunciado de la autoevaluación y su solución.

Durante la realización de la actividad se podrá recurrir al libro de texto cuantas veces sea necesario. Una vez finalizada ésta el estudiante comparará sus resultados con la solución publicada por el Equipo Docente.

Por otra parte, también se debatirá en los foros sobre aquellos conceptos que los estudiantes quieran reforzar.

2.4. MÓDULO IV: Análisis de Operaciones Intrusivas y Herramientas Disponibles

2.4.1.- Presentación del Módulo IV

La monitorización de redes se basa en la captura y análisis de esta información para poder detectar y bloquear posibles intrusiones. Por ello es importante dedicar un espacio a presentar las herramientas disponibles en la actualidad así como la información que nos ofrecen y su interpretación. De esta forma nuestra política de seguridad tendrá mayores posibilidades de éxito.

2.4.2 - Contextualización en el conjunto de la materia o asignatura

Los objetivos que se desarrollan a lo largo de este módulo son:

- Comprender que son los analizadores de vulnerabilidades y cómo se usan.
- Conocer herramientas de software libre para el análisis del tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.

Describir las mejores herramientas para la puesta en marcha de una política de seguridad.

Los temas de estudio que forman esta unidad temática son:

- **Unidad 12**: Herramientas de análisis de vulnerabilidades para la auditoría de la seguridad en las comunicaciones.
  - Introducción
  - Caso práctico: el modelo Cisco Secure Scanner
  - Caso práctico: los programas de Internet Security Systems.
- **Unidad 13:** Diseño seguro de redes. Concepto de alta disponibilidad y diseños redundante
  - Introducción
  - Diseño de soluciones de alta disponibilidad
  - Los problemas de infraestructura y soluciones
  - Los problemas en el nivel 2 de OSI y soluciones
  - Los problemas en el nivel 3 de OSI y soluciones
  - Consideraciones para el resto de los niveles OSI
  - Consideraciones para el almacenamiento en red: SAN (Storage Area Networks)
  - Consideraciones para los dispositivos de seguridad

La **Unidad 12** realiza un análisis de las herramientas de búsqueda de vulnerabilidades en sistemas y dispositivos de una red, que es una parte fundamental en el proceso de implantación de un proceso de seguridad correcto, señalando cuáles deben ser las condiciones mínimas de uso, configuración y mantenimiento de estas herramientas para poder cumplir con su misión con éxito. En concreto, nos enfocaremos en la capacidad de prevención que nos permiten estas herramientas, de forma que podamos anticiparnos a posibles problemas. Dentro del capítulo se analizan dos aplicaciones como casos de estudio: Cisco Secure Scanner y Internet Scanner.

La **Unidad 13** se centra en los conceptos de alta disponibilidad, ya comentados con anterioridad en la Unidad 7, en este caso para redes analizando los posibles problemas y sus soluciones actuales. Así que partiendo de la arquitectura por niveles del modelo OSI, se analiza nivel a nivel, que problemas plantea la alta disponibilidad y que soluciones existen actualmente. También se realiza un recordatorio como se debe gestionar mediante políticas el tráfico de una red, para dar prioridades a cada tipo de tráfico según sus necesidades, de forma que no solo la red sino los servicios necesarios para su correcto funcionamiento permanezcan disponibles. Asimismo se analizan los problemas y soluciones asociados a los subsistemas de almacenamiento altamente disponibles, SAN y RAID, resaltando la necesidad actual de su completa disponibilidad para muchas organizaciones. Por último, se comentaran las topologías típicas para obtener alta disponibilidad también para los cortafuegos, como punto clave del control de la política de seguridad de una organización.

2.4.3.- Información y orientaciones para el trabajo con los materiales requeridos para el estudio de al unidad

Estos temas corresponden a los **capítulos 10 y 12** del libro de la bibliografía básica: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN de los autores Gabriel Díaz Orueta, Francisco, Mur, Elio Sancristóbal, Manuel Castro Manuel y Juan Peire disponible en la Editorial UNED.

El estudio se llevará a cabo siguiendo la planificación descrita en el aparado del cronograma semanal.

Por otra parte, el Equipo Docente publicará en la plataforma los enlaces de interés para cada tema, así como otro material auxiliar que pueda considerar de interés.
Entre ellos destacar el libro Seguridad en Unix y Redes de Antonio Villalón Huerta, disponible de forma gratuita en: http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf, que complementa la visión de los primeros temas con sus capítulos:

- 6. Auditoria del sistema
- 13. El sistema de red
- 14. Algunos servicios y protocolos
- 21. Algunas herramientas de seguridad

Que amplían y complementan los contenidos del módulo.

2.4.4.- Descripción detallada de cada una de las actividades de aprendizaje a realizar

Una vez terminado el estudio de cada tema, como actividad se deberá realizar una autoevaluación consistente en la resolución de una serie de cuestiones teóricas y/o prácticas. Para ello el Equipo Docente publicará, a través de la plataforma virtual, el enunciado de la autoevaluación y su solución.

Durante la realización de la actividad se podrá recurrir al libro de texto cuantas veces sea necesario. Una vez finalizada ésta el estudiante comparará sus resultados con la solución publicada por el Equipo Docente.

Por otra parte, también se debatirá en los foros sobre aquellos conceptos que los estudiantes quieran reforzar.

3.- ORIENTACIONES PARA LA REALIZACIÓN DEL PLAN DE ACTIVIDADES

La metodología seguida para el aprendizaje de esta asignatura es la propia de una universidad de educación a distancia que se caracteriza por el empleo conjunto de medios y recursos virtuales. Los materiales docentes específicos, las comunidades virtuales de aprendizaje, la asistencia presencial a los estudiantes a través de profesores tutores en los diferentes centros asociados y el uso de los diversos mecanismos de comunicación (teléfono, correo electrónico,…) son los medios con los que cuenta la UNED para la enseñanza a distancia y son utilizados en esta asignatura.

3.1.- Evaluación del aprendizaje

Los conocimientos, destrezas y habilidades, adquiridos durante el curso, se evaluarán mediante una **prueba presencial** y en la realización de **varias pruebas de evaluación a distancia**.

La **calificación máxima** que se puede obtener en la asignatura será de **10 puntos**. Para calcular la nota final de la asignatura se sumarán las notas obtenidas en la prueba presencial y en las pruebas de evaluación a distancia con los siguientes pesos:

- **Prueba presencial: 70%** (supondrá, por tanto, un máximo de 8 puntos en la nota final de la asignatura).

- **Pruebas de evaluación de distancia: 30%** (supondrá, por tanto, un máximo de 2 puntos en la nota final de la asignatura).

Para aprobar la asignatura se exigirá una puntuación mínima de 3.5 puntos (sobre 7) en la prueba presencial y 1.5 punto (sobre 3) en las pruebas de evaluación a distancia. Con el fin de obtener la calificación de *matrícula de honor*, el estudiante deberá haber realizado todas las pruebas, obligatorias y voluntarias, con la máxima de calificación de 10.

La **prueba presencial** consistirá en un **examen teórico/práctico** a realizar en un **tiempo máximo de 2 horas**. Como se ha indicado, la **nota máxima** que se puede alcanzar en esta prueba es de **7 puntos** y **para superarla** se deberá obtener una **puntuación mínima** de **3.5 puntos**. Durante la realización de la prueba no se podrá utilizar ningún tipo de material. La **prueba presencial** se realizará en el Centro Asociado que corresponda a cada estudiante, en las fechas y horarios establecidos por la UNED.

Con respecto a la **pruebas de evaluación a distancia**, no será necesario que el estudiante acuda al Centro Asociado para realizar las mismas, ya que éstas podrán realizarse en su totalidad a través del curso virtual. Estas actividades serán corregidas por un profesor Tutor. Durante el curso **se realizarán tres pruebas**, siendo la **nota máxima** que se puede obtener de **3 puntos**. Cada prueba consistirá en varias preguntas de test y/o ejercicios de respuesta única. Para cada pregunta de la prueba se propondrán 3 ó 4 respuestas de las que sólo una será correcta. **No restarán las respuestas incorrectas o no contestadas**. Las **pruebas de evaluación a distancia se realizarán en la plataforma virtual** en las fechas y horarios que se indiquen en dicha plataforma, y se dispondrá de un tiempo límite para contestar y enviar la prueba, pasado ese tiempo la puntuación será de 0 puntos. Sólo se dispondrá de un intento para realizar cada una de las pruebas.

Cada una de las pruebas a realizar por el estudiante a distancia se encargará de evaluar lo siguiente:

- En la primera prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad I. Esta prueba vale un 20% de la calificación dedicada a las pruebas de evaluación a distancia.
- En la segunda prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad II, en concreto, a la parte dedicada a Cortafuegos. Esta prueba vale un 40% de la calificación dedicada a las pruebas de evaluación a distancia.
- En la tercera prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad II, en concreto, a la parte dedicada a Sistemas de Detección de Intrusos. Esta prueba vale un 40 % de la calificación dedicada a las pruebas de evaluación a distancia.

De esta manera la calificación final se calcula usando la siguiente fórmula:

Nota final = 0,7x [nota prueba presencial] + 0,3x (0,2 x [nota de la primera prueba de evaluación] + 0,4 x [nota de la primera segunda de evaluación] + 0,4 x [nota de la tercera prueba de evaluación])

Para aquellos alumnos cuya nota final del curso esté entre 4,5 y 5 puntos, se les ofrecerá la posibilidad de realizar de forma optativa una prueba teórico-práctica de evaluación a distancia. La realización de este ejercicio optativo servirá para subir la nota en 0,5 puntos. Esta práctica optativa solamente se corregirá en el cuatrimestre en el que se imparte la asignatura.

El estudiante debe tener en cuenta que **sólo se corregirán las pruebas de evaluación a distancia durante el cuatrimestre en el que se imparte la asignatura**. Por tanto, para poder presentarse en la convocatoria extraordinaria de septiembre, es necesario que el estudiante haya entregado las pruebas de evaluación que son condición necesaria para aprobar durante el plazo establecido en el cuatrimestre. En estos casos se mantendrá la nota obtenida en las mismas para la convocatoria de septiembre**.**

Por otra parte, en esta asignatura se plantea a los estudiantes un **proceso de autoevaluación**, basado en la realización de pruebas de test en el curso virtual. Estos ejercicios no serán evaluables, pero servirán para que el estudiante pueda medir su nivel de conocimientos. Cada ejercicio consistirá en una serie de cuestiones teóricas y/o prácticas que el estudiante deberá resolver. Periódicamente el equipo docente publicará, a través de la plataforma virtual, la solución a las cuestiones planteadas. El objetivo de estos ejercicios es permitir al estudiante autoevaluarse para hacer un seguimiento de su propio proceso de aprendizaje.

3.2.- Resumen de actividades

En la siguiente tabla se encuentra un resumen de las actividades a realizar tanto del tipo **autoevaluación** como del tipo **pruebas de evaluación a distancia**, indicando en dicha tabla cuando se deben realizar. En cualquier caso el Equipo Docente publicitará en los foros la fecha concreta de realización de cada una de las **pruebas de evaluación a distancia**.

Además, a lo largo del curso el Equipo Docente propondrá en los foros algunos temas de debate relacionados con la materia de estudio con el fin de promover las discusiones y participaciones de los estudiantes.

BLOQUES TEMÁTICOS	ACTIVIDADES	Semana
MODULO I: Conceptos e implementación de la monitorización de la seguridad en redes		
Unidad 1: Descripción del problema de la seguridad en las comunicaciones y en la información. Tipos de ataques.	Foros Ejercicios autoevaluación	1
Unidad 2: La seguridad en los elementos físicos existentes en la red.	Foros Ejercicios autoevaluación	2
Unidad 3: La seguridad en los elementos software existentes en una red.	Foros Ejercicios autoevaluación	3
Unidad 4: Métodos de ataque a equipos y redes.	Foros Ejercicios autoevaluación	4
Unidad 5: Defensa básicas ante ataques.	Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA	5
MODULO II: Prácticas recomendadas en la implantación de procesos de seguridad		
Unidad 6: La política de seguridad como respuesta razonable a los problemas de seguridad en las comunicaciones y en la información.	Foros Ejercicios autoevaluación	6

BLOQUES TEMÁTICOS	ACTIVIDADES	Semana
Unidad 7: Métodos no criptográficos en la implantación de la política de seguridad.	Foros Ejercicios autoevaluación	7
Unidad 8: Redes privadas virtuales.	Foros Ejercicios autoevaluación	8
MODULO III: Sistemas de gestión de la seguridad en redes.		
Unidad 9: Los cortafuegos (firewalls) y sus aplicaciones como elementos básicos de una política de seguridad de redes	Foros Ejercicios autoevaluación	9
Unidad 10: Tecnología de última generación en cortafuegos.	Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA	10
Unidad 11: Herramientas de detección de Intrusiones para la monitorización de la seguridad en las comunicaciones.	Foros Ejercicios autoevaluación PRUEBA DE EVALUACIÓN A DISTANCIA	11
MODULO IV: Análisis de Operaciones Intrusivas y herramientas disponibles.		
Unidad 12: Herramientas de análisis de vulnerabilidades para la auditoría de la seguridad en las comunicaciones.	Foros Ejercicios autoevaluación	12
Unidad 13: Diseño seguro de redes. Concepto de alta disponibilidad y diseños redundante	Foros Ejercicios autoevaluación	13
Repaso de los Módulos I, II, III y IV	Foros Repaso de las autoevaluaciones Repaso del material del curso	14
	PRUEBA PRESENCIAL	15