Guía Docente: Auditoría y seguridad avanzada de sistemas y redes de comunicaciones

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Mención en Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Primer Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se precisa

DATOS DEL PROFESORADO			
Profesor Responsable	Diego Ramírez Jiménez	**Correo electrónico**	diego.ramirez@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Mi Linkedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	En la asignatura abordaremos el proceso que se sigue para la realización de una auditoría de seguridad informática, y para ello, centraremos buena parte de su contenido en el estudio de los distintos tipos de debilidades de los sistemas informáticos, así como cuáles son las técnicas de análisis y evaluación de estas vulnerabilidades. También veremos las principales herramientas para analizar las redes. Por último, abordaremos las características y el papel desempeñado por los cortafuegos de red, en la Auditoría de la Seguridad Informática. La profesión de la auditoría de sistemas informáticas está muy demandada, ya que cada vez las empresas son más dependientes de los mismos, y nadie está exento de recibir posibles ataques. Es por ello, muy importante detectar las posibles debilidades y vulnerabilidades, función desempeñada por el analista de sistemas con una preparación adecuada. Esta materia se engloba dentro de la Mención de Criptología y Seguridad de la Información.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CMC09: Capacidad para plantear, desarrollar y dirigir el proceso de auditoría de un sistema en red, de forma manual y a través del uso de herramientas automáticas, generando un informe que resume los resultados. • CMC06: Capacidad para concebir, desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales. • CU15: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • CU16: Saber transmitir un informe técnico de la especialidad.
Resultados de aprendizaje de la asignatura	• Realiza una correcta auditoría de caja negra de un sistema en red, detectando, identificando y explotando sus principales vulnerabilidades. • Conoce y utiliza correctamente los distintos enfoques de una auditoría de red, eligiendo el más adecuado en cada caso y generando un informe final de resultados. • Conoce los aspectos relacionados con la seguridad de los sistemas SCADA e infraestructuras críticas. • Concibe, desarrolla y despliega proyectos globales y políticas de seguridad corporativas, teniendo en cuenta criterios organizacionales, económicos y aspectos legales.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	El objetivo de esta asignatura es formar al alumno en el área de las auditorias de red y sistemas. Para ello, se estudiarán detalladamente todas los fases de un proceso de auditoría, incluyendo sus diferentes tipos y la definición del alcance, las fases y metodologías, las herramientas más comunes y casos prácticos donde puedan aplicarse los conocimientos adquiridos.
Contenidos	**Unidad Didáctica 1. Criterios generales sobre auditoría informática** 1. Código deontológico de la función de auditoría 1.1. Normas profesionales y código de ética 1.2. Principios Deontológicos Aplicables a los Auditores 2. Relación de los distintos tipos de auditoría en el marco de los sistemas de información 3. Criterios a seguir para la composición del equipo auditor 3.1. Aspectos a considerar en la composición del equipo auditor 3.2. Funciones generales del equipo auditor 3.3. Conocimientos y destrezas del equipo auditor 4. Tipos de pruebas a realizar en el marco de la auditoría 5. Herramientas y software de auditoría 6. Requerimientos que deben cumplir los hallazgos de auditoría 6.1. Requisitos de un hallazgo de auditoría 6.2. Elementos de un hallazgo de auditoría 6.3. Comunicación de los hallazgos de auditoría 7. Categorización de hallazgos **Unidad Didáctica 2. Análisis de riesgos de los sistemas de información (I)** 1. Términos relacionados con la seguridad informática 2. Introducción al análisis de riesgos 2.1 Análisis de riesgos 2.2 Reducción del Riesgo: Mecanismos de Seguridad (Controles) 3. Principales elementos del análisis de riesgos y sus modelos de relaciones 4. Metodologías de análisis de riesgos 5. Identificación de los activos involucrados en el análisis de riesgos y su valoración 5.1 El inventario de activos

5.2 Valoración de los activos

6. Identificación de las amenazas que pueden afectar a los activos identificados previamente

6.1 Naturaleza de las amenazas

6.2 Amenazas Físicas

6.3 Amenazas Lógicas

7. Análisis e identificación de vulnerabilidades

7.1 Pensando como el enemigo

7.2 Pruebas de Penetración

7.3 Evaluación de vulnerabilidad

7.4 Herramientas de evaluación de vulnerabilidades

Unidad Didáctica 3. Análisis de riesgos de los sistemas de información (II)

1. Optimización del proceso de auditoría y contraste de vulnerabilidades

2. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

2.1. Funciones de salvaguarda en sistemas de información.

3. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

4. Determinación de la probabilidad e impacto de materialización de los escenarios

5. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

5.1. ¿Cómo valorar la probabilidad de una amenaza?

5.2. ¿Cómo valorar la magnitud del daño?

6. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

7. Relación de las distintas alternativas de gestión de riesgos

8. Guía para la elaboración del plan de gestión de riesgos

9. Exposición de la metodologías para el análisis de riesgos

9.1. ENS y el análisis de riesgos

Unidad Didáctica 4. Uso de herramientas de análisis de vulnerabilidades en la auditoría de sistemas

1. Herramientas del sistema operativo

2. Herramientas de análisis de red, puertos y servicios

	3. Herramientas de análisis de vulnerabilidades tipo Nessus **Unidad Didáctica 5. Uso de herramientas de análisis de red para la auditoría de sistemas** 1 Analizadores de protocolos de red 2 Analizadores de páginas web 3 Ejecución de ataques en redes **Unidad Didáctica 6. Uso de cortafuegos en la auditoría de Sistemas Informáticos.** 1 Principios generales sobre cortafuegos 2 Componentes de un cortafuegos de red 2.1 Filtrado de paquetes 2.2 El proxy de aplicación 2.3 Monitorización y Detección de Actividad sospechosa 3 Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad 4 Arquitecturas de cortafuegos de red 5 Otras arquitecturas de cortafuegos de red 5.1. Gestión unificada de amenazas: UTM appliance

METODOLOGÍA	
Actividades formativas	En cada una de las 6 Unidades didácticas, el alumnado deberá llevar a cabo actividades que le conduzcan a la asimilación de los conceptos y a su puesta en práctica. Entre otros, se propondrán las siguientes actividades: • **Estudio de Caso real de aplicación práctica:** Se plantearán estudios de caso real en varias unidades didácticas sobre algún tema de la unidad. Se trata de ejercicios introductorios sobre el que se deberá investigar en la web para resolverlos y donde el alumno deberá utilizar los recursos necesarios aplicando los conceptos y aspectos desarrollados en las unidades didácticas. Han de servir además como motivación y conducción del pensamiento reflexivo personal. • **Contenidos teóricos:** Texto Canónico donde se explican los nuevos conceptos de cada unidad didáctica, apoyado por el uso de material gráfico y enlaces a información multimedia que ayuden a la mejor comprensión de dichos conceptos. Además, en cada unidad didáctica se incluyen actividades autoevaluables (no computables para la calificación final) para ayudar al alumnado en el proceso de asimilación de contenidos de cada una de las diferentes unidades didácticas. Así mismo, se plantearán cuestionarios de autoevaluación que sí computarán para la nota final; en ellos, los alumnos y alumnas valorarán la comprensión de los contenidos de las unidades didácticas a través de un cuestionario final en cada una de ellas • **Foros de Debate:** Los alumnos debatirán para aportar ideas sobre temas de la asignatura, relacionados con aspectos de la vida cotidiana. • **Trabajo Colaborativo:** Se planteará un ejercicio práctico relacionado con los contenidos de la asignatura, y que deberá resolverse siguiendo alguna técnica de trabajo colaborativo grupal.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a

través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o

	no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	• Coopers & Lybrand (Instituto de Auditores Internos de España) (1996). Control interno, auditoría y seguridad Informática. Ed. Recoletos. Descripción de los sistemas de Gestión de Riesgo dentro de la Auditoría y Seguridad Informática. • Gomez Vieites, A. (2011). Auditoría de Seguridad Informática. Certificado de Profesionalidad (MF0487_3). Ed. RA-MA Este libro analiza la problemática de la auditoría de la seguridad informática y, para ello, centra buena parte de su contenido en el estudio de los distintos tipos de debilidades de los sistemas informáticos, así como cuáles son las técnicas de análisis y evaluación de estas vulnerabilidades. Merecen una especial atención los virus informáticos y otros códigos dañinos, ya que en la actualidad constituyen una de las principales amenazas para la seguridad de los sistemas informáticos. Por otra parte, el libro también analiza los principales aspectos relacionados con los delitos informáticos y con la normativa para así garantizar la protección de los datos personales y la privacidad de los ciudadanos. Por último, el libro aborda las características y el papel desempeñado por los cortafuegos de red en la Auditoría de la Seguridad Informática.
Bibliografía complementaria	• Lazaro, J. and Blanco, E., 2008. *Auditoría y sistemas informáticos*. Editorial Félix Varela. • Naranjo, A., 2009. *Conceptos de la auditoria de sistemas*. El Cid Editor. • Bell, T., Peecher, M., Solomon, I. and Marrs, F., 2007. *Auditoría basada en riesgos: perspectiva estratégica de sistemas*. Ecoe Ediciones. • Sánchez-Toledo, A., 2021. *Guía para la auditoría de los sistemas de gestión de la seguridad y salud en el trabajo. España: AENOR - Asociación Española de Normalización y Certificación*. AENOR Ediciones. • CCN-CERT, 2017. *Guía de Seguridad de las TIC CCN-STIC 802, ENS*. [ebook] CCN-CERT. Available at: <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html> [Accessed 3 May 2021].

- 2012. *versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro I - Método*. [ebook] Available at: <https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf> [Accessed 3 May 2021].
- Mayora, E., 2021. *Metodología de Gestión de Riesgo NIST 800-30*. [ebook] Available at: <https://prezi.com/p8moufe0ikyl/metodologia-de-gestion-deriesgo-nist-800-30/> [Accessed 3 May 2021].
- Es.wikipedia.org. 2021. *ISO/IEC 27000-series - Wikipedia, la enciclopedia libre*. [online] Available at: <https://es.wikipedia.org/wiki/ISO/IEC_27000-series> [Accessed 3 May 2021].
- Rodriguez, F., 2006. *AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN: UN RETO PARA LOS PROFESIONALES TIC*. [ebook] Sevilla. Available at: <https://administracionelectronica.gob.es/pae_Home/dam/jcr:e24c6a42-52ef-4963-ace6-256ad9a817d6/auditoria_informatica.pdf> [Accessed 3 May 2021].
- CCN-CERT, 2021. *Soluciones*. [online] Ccn-cert.cni.es. Available at: <https://www.ccn-cert.cni.es/soluciones-seguridad.html> [Accessed 3 May 2021].

Otros recursos

- Erb, M., 2021. *9. Clasificación de Riesgo*. [online] Gestión de Riesgo en la Seguridad Informática. Available at: <http://protejete.wordpress.com/gdr_principal/clasificacion_riesgo/> [Accessed 3 May 2021].
- Joint Task Force Transformation Initiative, 2021. *Guide for Conducting Risk Assessments*. [online] csrc.nist.gov. Available at: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final> [Accessed 3 May 2021].
- iso27001security.com. 2013. *Information technology — Security techniques — Information security management systems — Requirements (second edition)*. [online] Available at: <https://www.iso27001security.com/html/27001.html> [Accessed 3 May 2021].
- Administracionelectronica.gob.es. 2012. *PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. [online] Available at: <http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vr3Oy_LhDDe> [Accessed 3 May 2021].
- Wireshark.org. 2021. *Wireshark User's Guide*. [online] Available at: <https://www.wireshark.org/docs/wsug_html_chunked/> [Accessed 3 May 2021].
- Rediris.es. 2002. *RedIRIS - Cortafuegos: Conceptos teóricos*. [online] Available at: <http://www.rediris.es/cert/doc/unixsec/node23.html> [Accessed 3 May 2021].
- 2021. *Decálogo ciberseguridad empresas: una guía de aproximación para el empresario*. 1st ed. [ebook] León: Incibe. Available at: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf> [Accessed 3 May 2021].
- 2021. *Decálogo ciberseguridad empresas: una guía de aproximación para el empresario*. 1st ed. [ebook] León: Incibe. Available at: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf> [Accessed 3 May 2021].
- Artículos relacionados con vulnerabilidades. 2021. *Blog*. [online] Available at: <https://www.incibe.es/protege-tu-empresa/blog/filtro/vulnerabilidades> [Accessed 3 May 2021].
- Ccn-cert.cni.es. 2021. *Boletines de Vulnerabilidades*. [online] Available at: <https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html> [Accessed 3 May 2021].