Guía Docente

DATOS DE IDENTIFICACIÓN

Titulación:	Grado en Gestión de la Ciberseguridad
Rama de Conocimiento:	Ciencias Sociales y Jurídicas
Facultad/Escuela:	Derecho, Empresa y Gobierno
Asignatura:	Seguridad en Redes
Tipo:	Obligatoria
Créditos ECTS:	6
Curso:	4
Código:	2264
Periodo docente:	Séptimo semestre
Materia:	Sistemas
Módulo:	Tecnología
Tipo de enseñanza:	Presencial
Idioma:	Castellano
Total de horas de dedicación del alumno:	150

Equipo Docente	Correo Electrónico
Mateo Barrios González	mateo.barrios@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

Esta asignatura se engloba dentro del modulo de Tecnología del Grado en Gestión de la Ciberseguridad cursándose en el primer semestre del cuarto curso.

Hasta hace algunos años la securización de la red empresarial y de los dispositivos que la componen no era una de las prioridades del mundo empresarial, pero eso ha ido cambiando con el paso del tiempo debido a la gran importancia que tiene estar protegido frente a las ciberamenazas (tanto externas como internas). Realizar una buena configuración y securización tanto de los dispositivos de red como de los dispositivos finales es primordial para garantizar la seguridad de la red al completo, evitando el síndrome del eslabón más débil (que siempre es el ser humano).

El estudiante de Seguridad en Redes debe conocer de forma básica como funciona una red, las capas que componen el framework o la pila de protocolos TCP/IP, así como el papel y características principales de cada una de ellas. Debe poseer además un conocimiento básico sobre direccionamiento IP.

En esta asignatura se conocerán los planteamientos generales sobre la seguridad en redes: amenazas y ataques, mecanismos de seguridad, criptosistemas, infraestructuras de seguridad, modelos de confianza, protocolos para provisión de servicios de seguridad, sistemas de autenticación, redes privadas virtuales, cortafuegos, autoridad de certificación, certificados digitales, firma digital y legislación aplicable. Utilizando estándares de los sistemas de gestión de la seguridad.

OBJETIVO

El alumno debe conocer el funcionamiento y la configuración básica que debe realizar en los diferentes dispositivos de red, como podrían ser dispositivos de acceso o dispositivos frontera con una red externa.

Los fines específicos de la asignatura son:

Conocer los dispositivos de securizacion tales como IDS, IPS ,FIREWALL ,SIEM.

Realizar la configuración y securización de los dispositivos a implementar en una red autodefensiva como firewall o IdS.

CONOCIMIENTOS PREVIOS

Haber cursado la asignatura de Fundamentos de Redes de tercer curso.

CONTENIDOS

CONTENIDOS:

Tema 1. Introducción a la seguridad de la red. Normativa legal.
Tema 2. Monitorización y Control de los dispositivos
Tema 3. Control de Acceso y listas de control.
Tema 4. Evolución de los Firewalls. Tipologías de FIREWALL.
Tema 5. Sistema de Prevención de Intrusiones (IPS)

Tema 6. Seguridad de capa de acceso
Tema 7. Criptografía.
Tema 8. Redes Privadas Virtuales (VPNs)
Tema 9. Configuración Firewall.

ACTIVIDADES FORMATIVAS

La asignatura se desarrollará mediante una aplicación eminentemente práctica sobre los fundamentos teóricos de la asignatura.

Para el desarrollo de la presente asignatura, se aplicarán dos metodologías de aprendizaje complementarias entre sí, permitiendo al alumno realizar labores de investigación y reflexión personal, fomentar el trabajo colaborativo y aportar una visión general en el ámbito empresarial y de consumo.

A continuación, se procede brevemente a definir cada una de las metodologías utilizadas para el desarrollo de la asignatura:

• Flipped Classroom (Aula Invertida): en esta metodología los elementos tradicionales de la clase se invierten, de tal manera que, el profesor identifica el objetivo de aprendizaje que quiere trabajar, las competencias que van a necesitar poner en juego sus estudiantes, seleccionan los contenidos teóricos de la asignatura que necesitarán para cubrirlos y diseña la actividad.
En este tipo de metodologías, existe una parte de aprendizaje autónomo por parte del estudiante mediante el uso de diversos recursos. También se apoya el aprendizaje colaborativo, creando un espacio común entre profesores y alumnos.

• Aprendizaje basado en proyectos: esta metodología permite a los alumnos adquirir conocimientos y competencias clave a través de la elaboración de proyectos que dan respuesta a problemas de la vida real. En esta metodología, se parte de un problema concreto y real, en lugar del modelo teórico y abstracto tradicional, permitiendo al alumno en el desarrollo de competencias complejas como el pensamiento crítico, la comunicación, la colaboración o la resolución de problemas.

A continuación, se detallan las actividades que se realizaran durante el curso mediante el uso de las metodologías implementadas.

TRABAJO PRESENCIAL

El trabajo presencial se compondrá de diversas tipologías formativas:

* Clases expositivas: Transmisión de conocimientos por el profesor con el fin de activar procesos cognitivos en el estudiante, profundizando en los puntos de mayor interés y dificultad. Siendo muy recomendable que el alumno previamente haya leído los recursos preparados por el profesor y así participar más activamente en clase.

* Clases prácticas: Esta modalidad tiene diversas finalidades y puede seguirse como métodos:
    1. Estudio de casos (adquisición de aprendizajes mediante el análisis de casos reales o simulados).

2. Resolución de ejercicios y problemas (ejercitar, ensayar y poner en práctica los conocimientos previos).

Las clases prácticas se basarán en contenido teórico subido a la plataforma CANVAS (Aula Virtual) previamente por parte del profesorado.

* Exposición de trabajos: Presentación oral del trabajo de investigación elaborado por el alumno en grupos, con el objetivo de favorecer la comprensión y asimilación de los diferentes conceptos previamente adquiridos y el desarrollo de la capacidad argumentativa y crítica del alumno.

* Debates: sobre problemas reales, de manera que el alumno aprenda a discutir razonablemente determinados temas, intercambiando pareceres, aceptando opiniones contrarias, exponiendo razones y argumentaciones, asimilando a la vez los argumentos de la parte contraria, detectando sus puntos fuertes y débiles y desarrollando la capacidad de comunicación y argumentación jurídica.

Tutoría:

a) Personalizada: atención individual del alumno con el objetivo de revisar y debatir los temas presentados en clase y aclarar las dudas que le hayan surgido.

b) Grupal: Supervisión de los estudiantes que trabajan en grupo para el desarrollo de los trabajos planteados

c) Online: mediante los canales habilitados al efecto (foros, correo electrónico, etc.)

Realización de exámenes:

El objetivo es evaluar la adquisición de las competencias planteadas, principalmente de carácter cognitivo, como parte del sistema de evaluación. A la vez que permite evaluar los resultados de aprendizaje obtenidos.

El examen final dispondrá de elementos teóricos y prácticos, que permitirán al evaluador obtener los indicadores que muestren los objetivos y competencias logrados por los alumnos.

TRABAJO AUTÓNOMO

* Trabajo de investigación en grupo: Proyecto llevado a cabo por parte de un grupo de estudiantes sobre un tema específico para cuya elaboración debe tener en cuenta todas las fuentes documentales y prácticas que sean necesarias.

* Trabajo de investigación individual: Proyecto llevado a cabo por parte de un estudiante sobre un tema específico para cuya elaboración debe tener en cuenta todas las fuentes documentales y prácticas que sean necesarias.

* Estudio teórico: Estudio de los contenidos de carácter teórico del programa y preparación de las lecturas recomendadas y recursos audiovisuales puestos a disposición por el profesorado.

* Estudio práctico: Estudio de los contenidos de carácter práctico del programa y resolución de casos prácticos.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL

60 horas	90 horas
Introducción a la seguridad de la red. Normativa legal. 4h Monitorización y Control de los dispositivos 6h Control de Acceso y listas de control. 8h Evolución de los Firewalls. Tipologías de FIREWALL. 6h Sistema de Prevención de Intrusiones (IPS) 6h Seguridad de capa de acceso. 6h Criptografía. 8h Redes Privadas Virtuales (VPNs). 8h Configuración Firewall. 8h	Introducción a la seguridad de la red. 6h Monitorización y Control de los dispositivos. 9h Control de Acceso y listas de control. 12h Evolución de los Firewalls. 9h Sistema de Prevención de Intrusiones (IPS). 9h Seguridad de capa de acceso. 9h Criptografía. 12h Redes Privadas Virtuales (VPNs). 12h Configuración Firewall. 12h

COMPETENCIAS

Competencias básicas

Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio

Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio

Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética

Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado

Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

Competencias generales

Conocer las materias básicas y tecnologías, que le capaciten para el aprendizaje y desarrollo de nuevos métodos, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

Competencias específicas

Identificar, conocer y comprender los marcos regulatorios, organizaciones de referencia, estándares y recomendaciones existentes en el ámbito de las redes digitales y de la ciberseguridad.

Conocer y comprender los fundamentos básicos de las configuraciones, arquitectura, protocolos y sistemas de seguridad utilizados en la transmisión de datos.

Conocer y comprender la estructura, organización, funcionamiento, administración e interconexión de los diferentes dispositivos de seguridad de red y su configuración para la resolución de problemas propios en el ámbito de la seguridad.

RESULTADOS DE APRENDIZAJE

Comprender el funcionamiento de los dispositivos de securización tales como IDS, Siem, firewall y las funciones que realizan.

Configurar y administrar diferentes dispositivos para asegurar la fortificación de la red según normativa.

Analizar, revisar e implementar la configuración de seguridad de los dispositivos de red.

SISTEMA DE EVALUACIÓN DEL APRENDIZAJE

Se aplicará la modalidad de evaluación continua que se hará efectiva a través del seguimiento de los resultados de cada alumno en las distintas actividades propuestas durante el desarrollo de la asignatura. El sistema de evaluación contempla los siguientes apartados: CONVOCATORIA ORDINARIA 1. Evaluación Continua (60%) aplicándose Flipped Classroom y aprendizaje basado en proyectos. Asistencia activa y participación en las actividades presenciales en el aula y virtualmente mediante Canvas (Aula Virtual): 10% Trabajo grupal: 20% Pruebas prácticas: 30% 2. Examen Final (40%): Consistirá en la realización de una prueba con contenido teórico y práctico. Prueba escrita u oral, de desarrollo, de respuesta corta o tipo test: 40% Todos los trabajos/casos prácticos que se propongan, se entregarán al profesor en formato electrónico en las fechas establecidas y se resolverán a través de tutorías presenciales/online o a través de aula virtual. Para la aplicación de la totalidad de los porcentajes con los que se califica globalmente la asignatura, es requisito obligatorio que el alumno obtenga una calificación superior a **5** en el examen, entregar los trabajos y/o prácticas propuestos y la participación activa en el aula. La asistencia a las clases teóricas y prácticas es obligatoria. No aplicable a alumnos en segunda y siguientes matrículas o en situaciones especiales. CONVOCATORIA EXTRAORDINARIA Los estudiantes que acudan a convocatorias extraordinarias deberán presentar los trabajos/ prácticas que al efecto sean propuestos por el profesor con un valor del 60% sobre la evaluación total de la asignatura. En todo caso, el examen será por escrito sobre la materia teórica y práctica impartida con un valor del 40% sobre la evaluación total de la asignatura, siendo requisito obligatorio obtener una calificación superior a **5** en el examen, así como la entrega de los trabajos y/o prácticas propuestos, así como la participación activa en el aula para la aplicación de la totalidad de los porcentajes con los que se califica globalmente la asignatura. 1. Evaluación Continua (60%) aplicándose Flipped Classroom y aprendizaje basado en proyectos. Asistencia activa y participación en las actividades presenciales en el aula: 10% Trabajo grupal: 20% Pruebas prácticas: 30% 2. Examen Final (40%): Consistirá en la realización de una prueba con contenido teórico y práctico. Prueba escrita u oral, de desarrollo, de respuesta corta o tipo test: 40%. SISTEMA ALTERNATIVO CONVOCATORIA PARA ALUMNOS SEGUNDAS o SIGUIENTES MÁTRICULAS Y SITUACIONES ESPECIALES. ORDINARIA Y EXTRAORDINARIA. Aquellos/as estudiantes que se encuentren en SEGUNDA O SIGUIENTES MATRÍCULAS, o bien por una circunstancia justificada y/o se les haya reconocido DISPENSA ACADÉMICA y/o se encuentren cursando ERASMUS y no puedan hacer un seguimiento regular de la asignatura, el sistema de evaluación previsto será: 1. Evaluación Continua (50%) aplicándose Flipped Classroom y aprendizaje basado en proyectos. Trabajo grupal: 20% Pruebas prácticas: 30% 2. Examen Final (50%): Consistirá en la realización de una prueba con contenido teórico y práctico. Prueba escrita u oral, de desarrollo, de respuesta corta o tipo test: 50% Todos los trabajos/casos prácticos que se propongan, se entregarán al profesor en formato electrónico en las fechas establecidas y se resolverán a través de tutorías presenciales o a través de aula virtual. Para la aplicación de la totalidad de los porcentajes con los que se califica globalmente la asignatura, es requisito

obligatorio que el alumno obtenga una calificación superior a **5** en el examen, entregar los trabajos y/o prácticas propuestos y la participación activa en el aula. MATRICULA DE HONOR Es facultad exclusiva del profesor de esta asignatura como reconocimiento de la excelencia, conceder o no está distinción, conforme a los criterios de la normativa académica y siempre que el estudiante haya demostrado una especial proactividad, dominio de la materia, capacidad de interrelación con el resto de las disciplinas del Grado, capacidad de investigación autónoma, etc. PLAGIO En la presente asignatura y para todas las actividades formativas que se desarrollan en la misma, incluido el Examen, se activa la herramienta TURNITIN aplicándose, de advertirse similitudes, la normativa de Evaluación de la Universidad Francisco de Vitoria. Se remite al alumno a la lectura de la Normativa de Convivencia de la universidad, poniendo en especial atención a las infracciones que se derivan por plagio (*) y/o copia en exámenes que serán consideradas como Infracción Grave conforme al artículo 7 de dicha Normativa. (*) Se considera "plagio" cualquier tipo de copia de cuestiones o ejercicios de examen, memorias de trabajos, prácticas, etc., ya sea de manera total o parcial, de trabajos ajenos al alumno con el engaño de hacer creer al profesor que son propios. IMPORTANTE 1. De conformidad con cuanto prevé el art. 8.4 de la Normativa de Evaluación de la Universidad Francisco de Vitoria, los alumnos que matriculen una asignatura por segunda o sucesivas veces podrán optar entre acogerse al sistema ordinario previsto en la Guía Docente –en cuyo caso deberán cumplir con todos los requisitos que se prevean en cada caso, incluida la asistencia a clase– o acogerse al sistema alternativo previsto para aquellos alumnos que, por causa justificada ó con autorización del director del título, estén dispensados de asistir a clase. El alumno deberá acogerse a una de las dos opciones indicándose al profesorado de la asignatura.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Ernesto Ariganello. Redes Cisco :guía de estudio para la certificación CCNA Security / Paracuellos de Jarama, Madrid :Ra-Ma,2014.

Gabriel Díaz Orueta [y otros 3]. Procesos y herramientas para la seguridad de redes / Madrid :UNED - Universidad Nacional de Educación a Distancia,[2014]

Luis Herrero Pérez. Hacking ético de redes y comunicaciones :curso práctico / Madrid :RA-MA Editorial,2022.