

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:	Fundamentos de Criptografía		
Tipo:	Optativa	Créditos ECTS:	6
Curso:	3	Código:	2281
Periodo docente:	Sexto semestre		
Materia:	Seguridad de la Información y los Sistemas		
Módulo:	Tecnología		
Tipo de enseñanza:	Presencial		
Idioma:	Castellano		
Total de horas de dedicación del alumno:	150		

Equipo Docente	Correo Electrónico
Eduardo Díaz-Mayordomo Martínez	e.diazmayordomo@ufv.es
Robert Heron Maxwell	robert.maxwell@ufv.es

DESCRIPCIÓN DE LA ASIGNATURA

Esta asignatura se engloba dentro del modulo Optitavas en la Mención en Consultoría de la Seguridad Digital del Grado en Gestión de la Ciberseguridad cursandose en el segundo semestre del tercer curso.

Los contenidos de la asignatura serán: Comprender conceptos básicos de la criptografía: criptosistemas simétricos y asimétricos, esteganografía, criptoanálisis. identificar y conocer los algoritmos de la criptografía clásica de cifrado: monoalfabéticos, polialfabéticos, por sustitución, transposición. Estudio de los algoritmos de criptografía simétrica: DES, RC6, AES. Estudio de los algoritmos de criptografía asimétrica: RSA, Diffie-Hellman,

DSA.

OBJETIVO

Conocer la importancia de implementar mecanismos criptográficos adecuados para proteger la información y las comunicaciones.

Los fines específicos de la asignatura son:

Identificar y conocer los algoritmos de cifrado clásico.

Identificar y conocer los algoritmos de cifrado simétrico.

Identificar y conocer los algoritmos de cifrado asimétrico.

CONOCIMIENTOS PREVIOS

Haber cursado las asignaturas de Matemáticas Aplicadas I y II y Estadística para la Toma de Decisiones.

CONTENIDOS

Tema 1. Introducción a la Criptografía.

Tema 2. Fundamentos matemáticos y criptografía clásica.

Tema 3. Algoritmos de criptografía simétrica.

Tema 4. Algoritmos de criptografía asimétrica.

Tema 5. Criptoanálisis y ataques criptográficos.

ACTIVIDADES FORMATIVAS

La asignatura se desarrollará en torno a 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 realizarán durante el curso mediante el uso de las metodologías implementadas.

TRABAJO PRESENCIAL

Esta modalidad podrá verse alterada, si los escenarios establecidos por las autoridades sanitarias cambian. En este caso, todas las clases presenciales, se realizarán en el mismo horario establecido de manera remota, mediante las herramientas habilitadas por la Universidad.

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.

Las actividades formativas, así como la distribución de los tiempos de trabajo, pueden verse modificadas y adaptadas en función de los distintos escenarios establecidos siguiendo las indicaciones de las autoridades sanitarias.

DISTRIBUCIÓN DE LOS TIEMPOS DE TRABAJO

ACTIVIDAD PRESENCIAL	TRABAJO AUTÓNOMO/ACTIVIDAD NO PRESENCIAL
60 horas	90 horas

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

Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad.

Competencias específicas

Conocer y valorar vulnerabilidades de los sistemas informáticos y de telecomunicaciones de una organización.

Conocer y comprender los principios matemáticos necesarios para una comprensión adecuada de los mecanismos criptográficos de protección de la información relacionados con la aritmética modular, teorías de la información y de la complejidad.

RESULTADOS DE APRENDIZAJE

Conocer e identificar los fundamentos matemáticos criptográficos.

Identificar algoritmos de criptografía simétrica y asimétrica.

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 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 4 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 Y SIGUIENTES

Los estudiantes que acudan a convocatorias extraordinarias deberán presentar los trabajos/ prácticas que al efecto sean propuestos por el profesor con un valor del 70% 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 30% sobre la evaluación total de la asignatura, siendo requisito obligatorio obtener una calificación superior a 4 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%.

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 4 en el examen, entregar los trabajos y/o prácticas propuestos y la participación activa en el aula.

SISTEMA DE EVALUACIÓN ALTERNATIVO

En tanto que las circunstancias pueden verse modificadas y podría ser necesaria la adaptación de la docencia a las recomendaciones que se indiquen por las autoridades públicas de todo orden y especialmente las sanitarias, ya sean a nivel nacional, autonómico o municipal, incluyéndose toda medida que sea necesaria para el cumplimiento de los protocolos de prevención y seguridad así como que pueda instruirse la indicación de una docencia íntegra en remoto/virtual, los porcentajes y SISTEMA DE EVALUACIÓN que engloban la asignatura se mantendrán.

Por lo que respecta a la EVALUACIÓN CONTINUA, se modifica los medios de entrega de las actividades formativas que se presentarán y resolverán a través de las herramientas/ recursos creados al efecto en el aula virtual.

Por lo que respecta al EXAMEN FINAL, tanto en convocatoria ordinaria como en convocatoria extraordinaria, y ante un escenario sanitario que impida la presencialidad en el aula para su desarrollo, se realizará a través del aula virtual de la asignatura en la que se abrirá una sesión en BLACKBOARD u otra herramienta puesta a disposición por la Universidad específica de CONVOCATORIA DE EXAMEN. El profesor estará presente en la sesión durante todo el tiempo en el que se desarrolle el examen (sesión síncrona) y que consistirá en una prueba teórico-práctica. De producirse cualquier incidencia técnica que dificulte y/o imposibilite el desarrollo del examen para alguno/a y/o todos/as los alumnos, el examen se desarrollará ORALMENTE al día siguiente de la fecha en la que quede convocado el examen final y a través de sesión en BLACKBOARD u otra herramienta puesta a disposición por la Universidad abierta al efecto, siguiéndose el orden que al efecto indique el profesor. Todas las sesiones que se desarrollen a través de Canvas (Aula Virtual), examen incluido, serán grabadas, indicándose esta circunstancia a los alumnos/as y para constatar la evidencia del desarrollo de las sesiones, quedando absolutamente prohibida la reproducción, difusión y/o descarga de las mismas salvo que conste el consentimiento expreso del profesor.

De desarrollarse el examen (tanto en convocatoria ordinaria como extraordinaria) a través de Canvas (Aula Virtual), todos los alumnos/as deberán tener conectada tanto la cámara como el audio, debiendo el profesor identificar a cada alumno/a a través de su documento nacional de identidad, pasaporte o documento público análogo en el que conste fotografía del mismo/a, y le pedirá consentimiento expreso para la grabación de la sesión de examen a los fines de evidenciar su presencia en el aula, constatándose que se respeta la privacidad y

los derechos de imagen del alumno/a. Durante el desarrollo del examen el profesor podrá solicitar en cualquier momento que el/los alumnos/as estén visibles y por tanto la cámara web del alumno/ a se mantendrá activa durante todo el tiempo que dure el examen y desde el momento en que se incorporen en el aula a la hora indicada. Durante el desarrollo del examen el profesor podrá en cualquier momento solicitar a cualquier alumno/a que comparta pantalla con el profesor.

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.

Cualquier fraude o plagio (*) por parte del alumno en una actividad evaluable será sancionado e implicará un 0 en la calificación de esa parte de la asignatura, anulando la convocatoria en curso. Este comportamiento, además, será comunicado a la Dirección de la Carrera que a su vez comunicará a la Dirección General, siguiendo el Protocolo establecido por 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 y con autorización del director del título, estén dispensados de asistir a clase. El alumno deberá acogerse a una de las dos opciones y solicitar la correspondiente autorización en el plazo de cinco días naturales desde el comienzo del cuatrimestre.

2. De conformidad con cuanto prevé el art. 14 de la Normativa de Evaluación de la Universidad Francisco de Vitoria, los estudiantes, en cualquier prueba de evaluación, están obligados a observar las reglas elementales sobre autenticidad del ejercicio y privacidad de este. Cuando un alumno disponga o se valga de medios ilegítimos en la celebración de una prueba de evaluación, incurra en plagio, o se atribuya indebidamente la autoría de trabajos académicos requeridos para la evaluación, será puntuado con la calificación numérica de cero, anulándose cualquier derecho que las presentes normas le reconozcan, pudiendo, asimismo, ser objeto de sanción previa apertura de expediente disciplinario. El profesor debe advertir a los alumnos de las consecuencias académicas y disciplinarias que puede acarrear cualquier acto que contravenga las reglas mencionadas, especialmente antes de la realización de las pruebas de evaluación. Es obligación del profesor poner los medios para evitar el fraude entre los alumnos. El profesor que detecte cualquier tipo de fraude deberá ponerlo en conocimiento del director de la titulación quien actuará según el procedimiento establecido al efecto en la Normativa de Convivencia.

BIBLIOGRAFÍA Y OTROS RECURSOS

Básica

Caballero Gil, P. (2002). Introducción a la criptografía. Madrid: Editorial Ra-Ma.

Fuster Sabater, A. (2004). Técnicas criptográficas de protección de datos. Madrid: Editorial Ra-Ma.

Complementaria

MUÑOZ, Alfonso (2020) Criptografía ofensiva. Atacando y defendiendo organizaciones.