



**INFORME DE SEGUIMIENTO Y PLAN DE MEJORAS DE LA
TITULACIÓN**

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

CURSO 2020/2021

Resultados de las asignaturas del plan de estudios curso 2020/2021

Asignatura	Matriculados	% estudiantes 1ª matrícula	Tasa de rendimiento	% aptos	% suspensos	% no presentados	Tasa de éxito	% aprobados 1ª matrícula
ANÁLISIS DE MALWARE	44	100	70,45	100	0	29,545	100	70,46
ANÁLISIS FORENSE	58	94,83	81,03	97,917	2,08	17,241	97,92	83,64
AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD	49	93,88	83,67	100	0	16,327	100	84,78
CIBERILÍCITOS	44	97,73	81,82	97,297	2,7	15,909	97,3	81,4
CONSULTORÍA Y AUDITORÍA	18	94,44	77,78	100	0	22,222	100	82,35
CRIPTOGRAFÍA APLICADA	48	97,92	77,08	100	0	22,917	100	76,6
ÉTICA Y LEGISLACIÓN	14	85,71	92,86	100	0	7,143	100	91,67
GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	30	100	66,67	95,238	4,76	30	95,24	66,67
HACKING ÉTICO	46	100	84,78	100	0	15,217	100	84,78
INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD	24	95,83	83,33	100	0	16,667	100	82,61

Asignatura	Matriculados	% estudiantes 1ª matrícula	Tasa de rendimiento	% aptos	% suspensos	% no presentados	Tasa de éxito	% aprobados 1ª matrícula
MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO	3	100	66,67	100	0	33,333	100	66,67
PROGRAMACIÓN Y ESTRUCTURAS DE DATOS AVANZADAS								
REDES DE COMPUTADORES								
SEGURIDAD								
SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS	47	97,87	74,47	94,595	5,41	21,277	94,59	73,91
SISTEMAS DISTRIBUIDOS	3	66,67	100	100	0	0	100	100
SISTEMAS OPERATIVOS	3	100	100	100	0	0	100	100
TEORÍA DE LA INFORMACIÓN Y CRYPTOGRAFÍA BÁSICA								
TRABAJO DE FIN DE MÁSTER EN CIBERSEGURIDAD	19	100	73,68	100	0	26,316	100	73,68

Resultados de las asignaturas del plan de estudios curso 2019/2020

Asignatura	Matriculados	% estudiantes 1ª matrícula	Tasa de rendimiento	% aptos	% suspensos	% no presentados	Tasa de éxito	% aprobados 1ª matrícula
ANÁLISIS DE MALWARE	21	100	76,19	100	0	23,81	100	76,19
ANÁLISIS FORENSE	23	100	69,57	100	0	30,435	100	69,57
AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD	21	100	47,62	100	0	52,381	100	47,62
CIBERILÍCITOS	13	100	76,92	100	0	23,077	100	76,92
CONSULTORÍA Y AUDITORÍA	9	88,89	88,89	100	0	11,111	100	87,5
CRIPTOGRAFÍA APLICADA	16	100	68,75	91,667	8,33	25	91,67	68,75
ÉTICA Y LEGISLACIÓN	13	100	61,54	100	0	38,462	100	61,54
GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	11	100	81,82	100	0	18,182	100	81,82
HACKING ÉTICO	22	100	81,82	100	0	18,182	100	81,82
INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD	9	100	77,78	100	0	22,222	100	77,78
MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO	3	100	66,67	100	0	33,333	100	66,67

Asignatura	Matriculados	% estudiantes 1ª matrícula	Tasa de rendimiento	% aptos	% suspensos	% no presentados	Tasa de éxito	% aprobados 1ª matrícula
PROGRAMACIÓN Y ESTRUCTURAS DE DATOS AVANZADAS								
REDES DE COMPUTADORES								
SEGURIDAD								
SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS	30	100	70	100	0	30	100	70
SISTEMAS DISTRIBUIDOS	4	100	25	100	0	75	100	25
SISTEMAS OPERATIVOS	4	75	75	100	0	25	100	100
TEORÍA DE LA INFORMACIÓN Y CRİPTOGRAFÍA BÁSICA								
TRABAJO DE FIN DE MÁSTER EN CIBERSEGURIDAD	3	100	100	100	0	0	100	100

Valoración de las asignaturas (estudiantes/tutores) curso 2020/2021

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
ANÁLISIS DE MALWARE	85,47	11		

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
ANÁLISIS FORENSE	84,76	13		
AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD	63,69	6		
CIBERILÍCITOS	72,72	7		
CONSULTORÍA Y AUDITORÍA	81,39	3		
CRIPTOGRAFÍA APLICADA	76,60	5		
ÉTICA Y LEGISLACIÓN	37,59	2		
GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	30,70	6		
HACKING ÉTICO	68,05	9		
INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD	82,50	3		
MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO				
PROGRAMACIÓN Y ESTRUCTURAS DE DATOS AVANZADAS			86,08	16
REDES DE COMPUTADORES			70,76	10

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
SEGURIDAD				
SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS	69,85	9		
SISTEMAS DISTRIBUIDOS			92,50	1
SISTEMAS OPERATIVOS			84,40	13
TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA			85,33	1
TRABAJO DE FIN DE MÁSTER EN CIBERSEGURIDAD	77,14	12		

Valoración de las asignaturas (estudiantes/tutores) curso 2019/2020

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
ANÁLISIS DE MALWARE	84,72	13		
ANÁLISIS FORENSE	86,73	2		
AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD	82,67	3		

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
CIBERILÍCITOS	77,80	3		
CONSULTORÍA Y AUDITORÍA	78,11	4		
CRIPTOGRAFÍA APLICADA				
ÉTICA Y LEGISLACIÓN	49,66	3		
GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD	46,15	3		
HACKING ÉTICO	87,60	2		
INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD	52,02	2		
MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO	99,09	1		
PROGRAMACIÓN Y ESTRUCTURAS DE DATOS AVANZADAS				
REDES DE COMPUTADORES				
SEGURIDAD				
SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS	68,17	10		

asignatura	val. estudiantes	resp. estudiantes	val. tutores	resp. tutores
SISTEMAS DISTRIBUIDOS				
SISTEMAS OPERATIVOS	80,91	1		
TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA				
TRABAJO DE FIN DE MÁSTER EN CIBERSEGURIDAD	89,09	3		

Cuadro de indicadores de la titulación

Indicador	Valor anterior	Valor actual
Tasa de rendimiento	71,22	▲ 78,68
Tasa de evaluación	71,71	▲ 79,74
Tasa de éxito	99,32	▼ 98,66
Ratio estudiantes por PDI	1,33	▲ 3,35
Calificación media	8,13	▲ 8,24
Tasa de abandono	25	▼ 21,88

Indicador	Valor anterior	Valor actual
Tasa de graduación	41,67	▼ 18,75
Número de egresados	3	▲ 14
Nota media egresados	8,33	▲ 8,51
Duración media conclusión título	1	▲ 1,90
Tasa de eficiencia de egresados	100	▶ 100
Estudiantes nuevo ingreso (matrícula conformada)	36	▲ 64
Satisfacción global estudiantes con el título	75,29	▼ 72,93
Satisfacción estudiantes con el PDI	79,90	▼ 79,42
Satisfacción estudiantes con los recursos materiales	70	▼ 69,34
Satisfacción egresados	65,67	▲ 68,81
Satisfacción PDI	76,92	▲ 83,75

Preguntas/requisitos

1.- Puntos fuertes de la titulación

- Las asignaturas están coordinadas de una manera adecuada. Los equipos docentes mantienen una interacción fluida. La coordinación del máster realizó reuniones telemáticas con los equipos docentes para realizar el seguimiento del curso y analizar la posibilidad de realizar modificaciones, concluyéndose en general que lo más adecuado era no realizar cambios significativos.
- Los contenidos del máster y su propio carácter e intencionalidad son eminentemente prácticos. Se trabajan situaciones reales y se entrena para afrontarlas, de aplicación en el ámbito profesional.
- La tasa de evaluación, de rendimiento y de éxito son satisfactorios. La tasa de rendimiento ha aumentado del 71,22 al 78,68 y la de evaluación del 71,71 al 79,74. La tasa de éxito ha disminuido levemente del 99,32 al 98,66. La tasa de egresados es de 14, con porcentajes de notables y sobresalientes alrededor del 40% en ambos casos. La satisfacción global de los estudiantes con el título es alrededor del 70%, del 80% con el PDI y del 70% con los materiales.
- El punto fuerte más destacable es la calidad de nuestros estudiantes, en general. Aunque el primer año en el primer cuatrimestre suelen tener más dificultades en adaptarse a la metodología se puede percibir rápidamente que son estudiantes maduros y generalmente profesionales en ejercicio por lo que sus resultados suelen ser buenos aunque en tiempo suelen dilatarse normalmente por razones profesionales. Así mismo, han demostrado una gran motivación e interés.

2.- Puntos débiles de la titulación

- El proceso de preinscripción es ineficiente. La Comisión del Máster aprueba las titulaciones que dan acceso con sus complementos formativos, en su caso, y no hay más que aplicarlas. Sin embargo, se reciben constantes solicitudes de evaluación de currículos con titulaciones que no están aprobadas por la Comisión, lo que lleva una carga administrativa innecesaria.
- La Coordinación y los equipos docentes han recibido un gran número de consultas de ciudadanos previa preinscripción solicitando información sobre el Máster en diferentes ámbitos, desde los económicos hasta detalles sobre asignaturas, en muchas ocasiones derivados por unidades de administración de la UNED. Entendemos que la información institucional publicada en la web cumple con los requisitos y que se debería redirigir a ella a los ciudadanos interesados, no al equipo docente.
- Dada la demanda y la exigencia de admisión de un buen número de solicitantes y teniendo en cuenta que no hay ninguna unidad de la universidad que informe a los estudiantes, los equipos docentes y los docentes encargados de la gestión han tenido una presión innecesaria en ámbitos que no les competen.
- Los docentes han tenido que responder un elevado número de consultas administrativas y burocráticas lo que parece indicar que la información facilitada en la web institucional es insuficiente.
- La capacidad para la adquisición de equipos para la preparación de prácticas por parte de los equipos docentes ha sido inexistente. La forma de contratación de la universidad ha impedido una vez más que se mejoren las prácticas.
- La dotación económica que la universidad asigna al máster para su desarrollo ha sido ínfima, menos de lo que paga un estudiante. Con este presupuesto, los equipos asignados han de ser financiados por otros centros de gasto. Así mismo, las actividades de valor añadido como por ejemplo conferencias han sido muy limitadas.

3.- Propuestas de mejora de la titulación para los dos próximos cursos académicos

- Dentro de las competencias de los profesores del Máster y de la Comisión del mismo, para el próximo curso se dedicará un esfuerzo especial en dotar a los estudiantes de contenidos adicionales formativos y motivadores sin aumentar la carga docente. En este contexto se planificarán conferencias y encuentros en la medida en que el presupuesto lo permita.
- En cuanto a los demás aspectos descritos en los puntos débiles, se seguirán haciendo constar en la Comisión del Máster y se seguirán manifestando en los órganos colegiados de la universidad, desde la Junta de Escuela hasta el Consejo de Gobierno.
- Por último, atendiendo al elevado número de consultas administrativas y burocráticas que han tenido que ser atendidas por los equipos docentes, y que algunos cambios en la página oficial parecen complicados (como por ejemplo que quede clara la diferencia entre las asignaturas del Máster y los complementos formativos) el próximo curso se valorará la necesidad de crear un web propia que recoja la información requerida por los estudiantes.

4.- Seguimiento y revisión de las acciones de mejora propuestas en cursos anteriores

- La Coordinación del Máster analizó numerosos planes de estudio y fueron sometidos a la consideración de la Comisión del Máster para establecer las titulaciones de ingreso en la próxima convocatoria. Así mismo, se decidió realizar de nuevo estas revisiones en los meses de octubre y noviembre con el fin de actualizarlas en la Comisión del Máster a celebrar en diciembre.
- La coordinación ha celebrado reuniones independientes con los equipos docentes de las asignaturas con el fin de realizar el seguimiento y valorar los cambios necesarios. Como conclusión se estableció mantener estables los contenidos y en algunas asignaturas proponer algunos ejercicios más para que los estudiantes tengan confianza a la hora de realizar el examen presencial.
- Se ha comunicado a los órganos competentes las necesidades derivadas de los problemas administrativos y burocráticos, con pocos resultados hasta el momento.

Anexo. Aportaciones de los equipos docentes

ANÁLISIS DE MALWARE

Puntos fuertes

- Existe una coordinación del equipo docente involucrado en la asignatura y otros equipos docentes de asignaturas relacionadas con esta asignatura. La distribución de las actividades y trabajos de evaluación entre el equipo docente facilita el seguimiento y corrección de las pruebas. Estas actividades están coordinadas dentro del plan de trabajo de la asignatura.
- La distribución modular de la asignatura permite especializar la atención al estudiante en los objetivos específicos asociados a cada módulo. La asignatura contiene además recursos multimedia elaborados por los docentes: presentaciones, vídeo-clases, etc.
- Las tasas de evaluación y rendimiento han sido de un 70,45% y la de éxito un 100%. Para el examen "presencial" se ha utilizado la plataforma AvEx, debido a la pandemia de COVID-19. La calificación media ha sido de 9.06.
- La valoración global del cuestionario de satisfacción por parte de los estudiantes en el curso 2020-21 ha sido de 85,47 sobre 100, ligeramente superior al curso anterior, y una significación estadística muy alta. Resultado por encima de la media de la Titulación, Escuela y Universidad. Un total de 11 cuestionarios han sido respondidos.

Puntos débiles

- No existen demasiadas interacciones con los estudiantes utilizando las herramientas del curso virtual. Se intentarán proponer temas de discusión adicionales, así como informar a los estudiantes de eventos de tipo científico/técnico (ya se hace a nivel de Máster/Escuela).
- La precisión de los cuestionarios de satisfacción rellenados por parte de los estudiantes es mejorable.

Propuestas de mejora

- Se intentará animar aún más si cabe a los estudiantes a que respondan la encuesta sobre la evaluación de la asignatura para llevar a obtener unos datos más significativos. La cantidad de encuestas respondidas en el curso académico 2020-21 con respecto al anterior ha sido algo menor.
- Actualización de las actividades prácticas, ya que es una temática en continua evolución.

Seguimiento y revisión de las acciones de mejora

- Se han mejorado las actividades prácticas para la evaluación de la asignatura, siempre respetando las competencias y resultados de aprendizaje aprobados por ANECA en la memoria de verificación de la Titulación. Por otra parte, se ha intentado animar a los estudiantes en diversas ocasiones a que respondan la encuesta sobre la evaluación de la asignatura incrementando la cantidad de encuestas de satisfacción llevadas a cabo por parte de los estudiantes.

ANÁLISIS FORENSE

Puntos fuertes

- La distribución modular de la asignatura permite especializar la atención al estudiante en los objetivos específicos asociados a cada módulo. La asignatura contiene recursos multimedia: presentaciones, vídeo-clases, etc., y se van incrementando/actualizando. Se han creado además ejercicios que permiten la evaluación continua de la asignatura.

- Existe una coordinación del equipo docente involucrado en la asignatura y en otras pertenecientes a la materia a la que pertenece la asignatura.
- El número de estudiantes matriculados durante el curso 2020-2021 ha sido de 58. Las tasas de evaluación, éxito y rendimiento en el curso 2019-2020 han sido bastante buenas y similares a las del curso anterior:
 - Tasa de evaluación de la asignatura: 82.76%.
 - Tasa de éxito de la asignatura: 97.92%.
 - Tasa de rendimiento de la asignatura: 81.03%.
- La calificación media de la asignatura en el curso 2020-2021 ha sido de 8.24. En este sentido, cerca de un 20% de los estudiantes han tenido como calificación final un Aprobado (19.10%), algo más de un tercio la calificación de Notable (36.24%), y una minoría han sido de Sobresaliente (38.81%), siendo el 1.38% restante suspensos.
- La calificación global de la evaluación por parte de los estudiantes en el curso 2020-2021 ha sido de 84,76 (12 cuestionarios respondidos), por encima de los de la Titulación. Sin embargo, no es estadísticamente representativa.

Puntos débiles

- La parte teórica de la asignatura sigue siendo demasiado compleja. Sería interesante incluir más actividades prácticas que permitan fomentar el interés del alumnado. Así como facilitar más recursos que ayuden a su comprensión.
- En el plan de trabajo se observa que algunos contenidos necesitan su actualización, en su mayoría debido a los cambios tecnológicos acontecidos en la ciberseguridad.

Propuestas de mejora

- Se van a incluir/actualizar vídeo clases adicionales acompañándolos de documento de texto para facilitar su estudio y otros recursos multimedia, y se tiene la intención de proporcionar documentación adicional. Todo ello, con el fin de que los estudiantes vean esta asignatura, de por sí es bastante teórica, de una manera más práctica.
- Se intentará animar aún más si cabe a los estudiantes a que respondan la encuesta sobre la evaluación de la asignatura para llevar a obtener unos datos significativos
- Se va a continuar con la inclusión de nuevas actividades prácticas sobre la seguridad de redes, e incrementar la utilización de laboratorios virtuales para dicho propósito. De esta manera, el estudiante adquirirá una formación práctica en el campo del análisis forense.

Seguimiento y revisión de las acciones de mejora

- Se han incrementado los recursos multimedia existente con video-clases, se van a añadir más documentos textuales para ayudar al estudio, incrementar los ejemplos y los ejercicios para facilitar la comprensión de la asignatura. Se ha seguido trabajando con laboratorios virtuales para la realización de prácticas significativas, así como el uso de gamificación en el aprendizaje. Y se reforzaron los mensajes para animar a los estudiantes a la participación en

AUDITORÍA Y MONITORIZACIÓN DE LA SEGURIDAD

Puntos fuertes

- Tasa de evaluación de 83,67, muy por encima de la titulación (64,12).
- La asignatura tiene un componente práctico muy importante. Especialmente destacable en la segunda práctica con el despliegue de un SIEM completo a seleccionar por el estudiante.
- Se fomenta la discusión en los foros para la resolución de los problemas. Esto fomenta una actitud colaborativa y de trabajo en grupo entre los alumnos. Y hace que los alumnos no se sientan tan solos.

■ Valoración muy positiva de la nota media de los estudiantes de la asignatura: 8,60. Esta nota se sitúa por encima de la nota media de los aptos de las asignaturas del curso y nivel de la asignatura: 8,19

■ Material gratuito, compuesto por: libros de teoría, apuntes y videos elaborados por equipo docente.

Puntos débiles

- El número de cuestionarios es bajo (6) respecto del total de matriculados (49)
- La satisfacción de los estudiantes con la asignatura es baja (63,69), específicamente respecto de la de la titulación (76,70)
- La apuesta por material gratuito puede conllevar una cierta desestructuración de los materiales y un trabajo adicional por parte de los alumnos que tienen que manejar varias fuentes de información (libros, apuntes, documentación de las herramientas, material de internet, etc.).

Propuestas de mejora

- Fomentar el desarrollo de los cuestionarios de evaluación por parte de los estudiantes.
- Seguir con la mejora en la organización del material para evitar los desajustes en la asignación de horas adicionales por parte de los estudiantes.

Seguimiento y revisión de las acciones de mejora

- Se ha conseguido una mejora estructural de los contenidos, pero sigue habiendo alguna cuestión mejorable. Se ha mejorado significativamente en los tiempos de corrección de las actividades prácticas.

CIBERILÍCITOS

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

CONSULTORÍA Y AUDITORÍA

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

CRIPTOGRAFÍA APLICADA

Puntos fuertes

- Los ejercicios y problemas propuestos ayudan a los estudiantes a centrar la asignatura y su corrección por parte de equipo docente les permite avanzar.
- La asignatura está bien organizada. Los estudiantes conocen desde el principio el nivel de exigencia y los trabajos a desarrollar.
- La coordinación del equipo docente es excelente

Puntos débiles

- Convendría disponer un tutor para que los plazos de corrección de los ejercicios y problemas propuestos se redujera
- Los estudiantes no participan en el foro. Prefieren correo electrónico al equipo docente.

Propuestas de mejora

- Intentar disponer de un tutor
- Realizar algunas conferencias que sirvan de motivación

Seguimiento y revisión de las acciones de mejora

- El seguimiento se realiza constantemente.

ÉTICA Y LEGISLACIÓN

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Puntos fuertes

- Asignatura con buena parte de carga práctica
- Hay abundante material de consulta
- Se desarrollan también aspectos normativos, no solamente técnicos

Puntos débiles

- NO hay todavía un texto base, debido en parte a lo cambiante de la materia
- No se dispone de un simulador de SOC para operar sobre incidentes o adquirir competencias en el triage y en las contramedidas

Propuestas de mejora

- Disponer de un simulador de SOC mediante oferta de TFM
- Actualizar el material disponible con videoclases

Seguimiento y revisión de las acciones de mejora

- Se revisará el material para detectar -si hubiere- actualizaciones necesarias, en especial con lo relacionado con la normativa del CCN en notificación de incidentes.

HACKING ÉTICO

Puntos fuertes

- Curso virtual estructurado e indicando plazos
- El material no requiere la compra de ningún libro

Puntos débiles

- Conseguir más participación en el foro.

Propuestas de mejora

- Conseguir más participación en el foro a través de temas de debate

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

INTRODUCCIÓN AL APRENDIZAJE AUTOMÁTICO PARA CIBERSEGURIDAD

Puntos fuertes

- Los resultados de valoración global en las encuestas son bastante más altos que la media de la titulación en general.
- En las encuestas se refleja que la asignatura es del máximo interés para los estudiantes.
- Las actividades evaluables a distancia muy guiadas ayudan a afianzar los conocimientos expuestos en el libro base.

Puntos débiles

- Todavía se detecta algún estudiante que ha elegido esta asignatura optativa con conocimientos de programación bajos.

Propuestas de mejora

- Se intentará mejorar la preparación de scripts y datos para las actividades.
- Se revisarán los materiales para ver si es posible añadir otros materiales adicionales sin aumentar demasiado la carga de trabajo para el estudiante.

Seguimiento y revisión de las acciones de mejora

- Se revisó la guía de curso para hacer más énfasis en la necesidad de conocimientos de programación previos para realizar la asignatura.

MARCO JURÍDICO DE LA DEFENSA NACIONAL EN EL CIBERESPACIO

Puntos fuertes

- Los materiales de estudio están completamente actualizados y se distribuyen directamente a los alumnos a través de la plataforma virtual.
- La asignatura cuenta con prueba de evaluación continua, además del examen de la asignatura. Todo el sistema de evaluación se basa en la resolución de casos prácticos en formato test.
- Ofrece una visión concreta y, a la vez, pormenorizada, de las cuestiones que atañen a la defensa del ciberespacio nacional, por lo que integra cuestiones relativas a la prevención y al control de las ciberamenazas desde una perspectiva militar y académica.
- Contamos con un profesor colaborador externo con experiencia directa en la materia.
- Se trata de una asignatura completamente original por su contenido y objeto de estudio.

Puntos débiles

- Algunos de los materiales pueden ser de difícil comprensión si los estudiantes no tienen cierta base académica.
- Algunos materiales requieren que los estudiantes tengan nociones básicas de inglés.
- La participación de los estudiantes en los Foros es escasa, probablemente debido a que se trata de una asignatura optativa con un número de alumnos limitado.

Propuestas de mejora

- Se recomienda, en el futuro, la confección de un manual recomendado para el estudio de la asignatura.
- Aún es pronto para la evaluación del rendimiento de la asignatura. Por el momento, en los cursos académicos ya realizados, la valoración de la asignatura es positiva. La constante renovación legislativa en un área sometida a muchos cambios puede dificultar el mantenimiento de la actualización de los materiales de estudio. Es preciso atender a las innovaciones en materia de prevención de la defensa del ciberespacio nacional.

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

PROGRAMACIÓN Y ESTRUCTURAS DE DATOS AVANZADAS

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

REDES DE COMPUTADORES

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

SEGURIDAD

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

SEGURIDAD EN INFRAESTRUCTURAS CRÍTICAS

Puntos fuertes

- Gran interés debido a la actualidad constante e implicaciones del día a día de los contenidos
- Gran implicación en debates y en las comunicaciones entre alumnos y con equipo docente
- Buena preparación anterior en general, grupos bastante homogéneos

Puntos débiles

- Dificultad de encontrar simuladores sencillos adecuados a los contenidos
- Dificultad en un grupo de entender la indeterminación de las soluciones para este tipo de contextos

Propuestas de mejora

- Encontrar simuladores sencillos que ayuden a crear prácticas didácticas
- Abrir debates sobre lo que los alumnos consideran que necesitarían conocer previamente a la asignatura

Seguimiento y revisión de las acciones de mejora

- El curso pasado no fue posible solucionar los problemas detectados

SISTEMAS DISTRIBUIDOS

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

SISTEMAS OPERATIVOS

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA

Puntos fuertes

Sin aportaciones

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones

TRABAJO DE FIN DE MÁSTER EN CIBERSEGURIDAD

Puntos fuertes

■ No tiene sentido este cuestionario. Son TFMs..

Puntos débiles

Sin aportaciones

Propuestas de mejora

Sin aportaciones

Seguimiento y revisión de las acciones de mejora

Sin aportaciones