ADENDA A LA GUÍA DOCENTE 2019/20 - *ADDENDUM TO THE 2019/20 COURSE DESCRIPTION*

MEDIDAS ESPECIALES PARA LA TRANSICIÓN A LA DOCENCIA NO PRESENCIAL POR COVID19. ADAPTACIONES DE LAS ACTIVIDADES DOCENTES Y DE EVALUACIÓN

SPECIAL MEASURES FOR ADAPTATION OF TEACHING AND EVALUATION ACTIVITIES DUE TO COVID19- TRANSITION TO NON PRESENTIAL TEACHING

Curso Académico: 2019/2020

Asignatura: CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA/CRYPTOGRAPHY AND COMPUTER SECURITY

Código: 15973

Titulación: Grado en Ingeniería Informática; Doble Grado en Ingeniería Informática y Administración de Empresas

Coordinador/a: ANA ISABEL GONZÁLEZ-TABLAS FERRERES

Fecha de Actualización: 23/04/2020

1. HERRAMIENTAS Y PLATAFORMAS UTILIZADAS PARA EL DESARROLLO DE LAS ACTIVIDADES DOCENTES
1. TOOLS AND PLATFORMS USED FOR THE DEVELOPMENT OF THE ACTIVITIES

- En este apartado deben detallarse las plataformas, herramientas y recursos utilizados para la transición al modelo de enseñanza-aprendizaje en modalidad no presencial, y para el conjunto de actividades síncronas y asíncronas realizadas. A modo de ejemplo: Blackboard Collaborate, Aula Global (Moodle), Google Hangouts Meet, …
- También deben indicarse el tipo de metodologías empleadas. A modo de ejemplo: sesiones síncronas, grabaciones de clases, subida de materiales a Aula Global, preparación de ejercicios, utilización de foros, chats, realización de tutorías, exposiciones en aulas virtuales, realización de trabajos …

- Plataformas y herramientas utilizados: BlackBoard Collaborate, Aula Global (Moodle), Google Hangouts Meet, Vimeo, Wooclap.
- Recursos utilizados:
    - Materiales ya disponibles previamente: transparencias, hojas de ejercicios resueltos, libro de problemas de examen resueltos, guiones de prácticas en aula informática.
    - Materiales desarrollados específicamente para la enseñanza-aprendizaje no presencial: tests de teoría (desplegados en Wooclap), grabaciones de video-clases con las transparencias (con BlackBoard Collaborate o Vimeo dependiendo de las preferencias y circunstancias de cada profesor), grabaciones de lecturas interpretadas y soluciones de problemas (con BlackBoard Collaborate o Vimeo). La elaboración de nuevos materiales se ha realizado de forma coordinada por todos los profesores de la asignatura, siendo éstos reutilizados en el resto de grupos.
- Metodología empleada:

  Se ha optado por una metodología mixta combinando (1) materiales grabados (tanto de teoría como de problemas) subidos a Aula Global que los estudiantes pueden trabajar por su cuenta (en horario de grupo reducido y tiempo de trabajo del estudiante) con (2) sesiones síncronas (en horario de grupo magistral) dedicadas a repasar los conceptos más importantes de teoría, resolución de dudas y realización de tests de teoría (incluyendo la revisión pública de los resultados de la clase y cada estudiante individualmente en sus dispositivos). La mayor parte de las sesiones síncronas se graban y luego se ponen a disposición de los estudiantes en Aula Global.

En algunos grupos se instado a los estudiantes a entregar (opcionalmente) la resolución de los problemas propuestos y se ha revisado dicha resolución (en el caso de estar correcta se otorga una insignia de Aula Global).

Todos los profesores están disponibles para realizar tutorías individuales o grupales a través de Google Hangout Meets o BlackBoard Collaborate.

Ya se utilizaban con anterioridad los foros de Aula Global (Foro general, Avisos, Foros creados específicos), pero en esta situación, se están utilizando más intensamente para comunicación con los alumnos.

Las prácticas se mantienen en el mismo formato anterior con la salvedad que se instruye a los estudiantes a instalar el software de prácticas en sus sistemas y la tutorización y resolución de dudas se realiza a través de sesiones online síncronas en horario del grupo reducido (BlackBoard Collaborate principalmente).

Algunas actividades formativas y de evaluación se han sustituido por la realización y entrega de un trabajo grupal diseñado específicamente para esta situación de enseñanza-aprendizaje no presencial.

- Platforms and tools: BlackBoard Collaborate, Aula Global (Moodle), Google Hangouts Meet, Vimeo, Wooclap.
- Resources:
    - Materials already available: slides, exercises and problems with solutions, final exam problem collection book, lab assignment instructions.
    - Materials specifically developed for non presential teaching and learning modality: theory tests (using Wooclap), video recordings of lectures using previously existing slides (BlackBoard Collaborate or Vimeo), video recordings of problem's statement interpretation and solving (BlackBoard Collaborate or Vimeo). Elaboration of new materials has been distributed among all the teachers involved in the subject, being reused in the groups.
- Methodology:

We have adopted a mixed methodology combining (1) recorded materials (for both theory and problem solving) uploaded to Aula Global and that students can work on by their own (in small group hours and student work time) and (2) synchronous sessions (during big group hours) dedicated to reviewing the most important concepts of theory, doubts resolution and answering tests with Wooclap (including the public review of class results and each student individually in their devices). Most synchronous sessions are recorded and then made available to students through Aula Global.

In some groups, students were suggested to submit (optionally) the resolution of the proposed problems and submissions have been revised (if correct, an Aula Global badge is awarded).

All teachers are available for individual or group tutoring through Google Hangout Meets or BlackBoard Collaborate.

The Aula Global forums (General Forum, Notices, Specific Forums) were previously used, but in this situation, they are being used more intensively for communication with students.

Laboratory assignments are kept in the same previous format with the exception that students are instructed to install the needed software in their systems and the student guidance and doubt resolution is carried out through online synchronous sessions in small group hours (BlackBoard Collaborate mainly).

Some teaching and assessment activities have been replaced by a new group assignment specifically designed for the non presential teaching-learning modality.

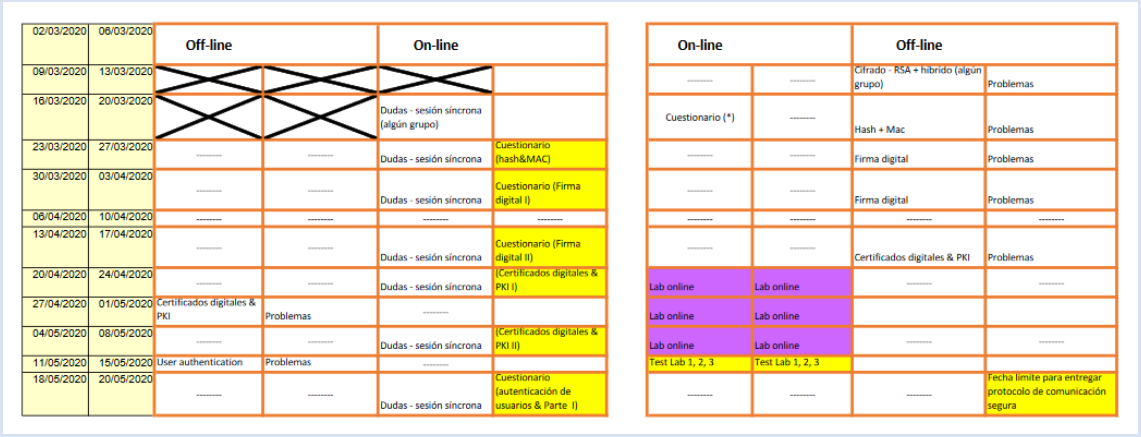
2. ADAPTACIÓN DE LAS ACTIVIDADES Y DE LA PROGRAMACIÓN TEMPORAL DE LAS MISMAS

2. ADAPTATION OF TEACHING ACTIVITIES AND TIME SCHEDULE

- En este apartado deben detallarse los contenidos formativos desarrollados en la asignatura, con indicación de la eliminación o adaptación que haya podido producirse, y/o de la reorganización temporal en la impartición de estos que haya podido producirse

IMPORTANTE: En asignaturas con experimentalidad, deben detallarse las actividades realizadas para dar cobertura al aprendizaje de tipo práctico realizadas en sustitución de los laboratorios, de manera que se pueda garantizar la adquisición de las competencias de los estudiantes

Los contenidos formativos de la asignatura son los mismos, pero su programación temporal ha sido adaptada según la imagen siguiente y de acuerdo a la metodología descrita en la sección 1. El orden de impartición no ha variado significativamente, teniendo en cuenta que este curso se había desplazado la realización de las prácticas al final del curso.



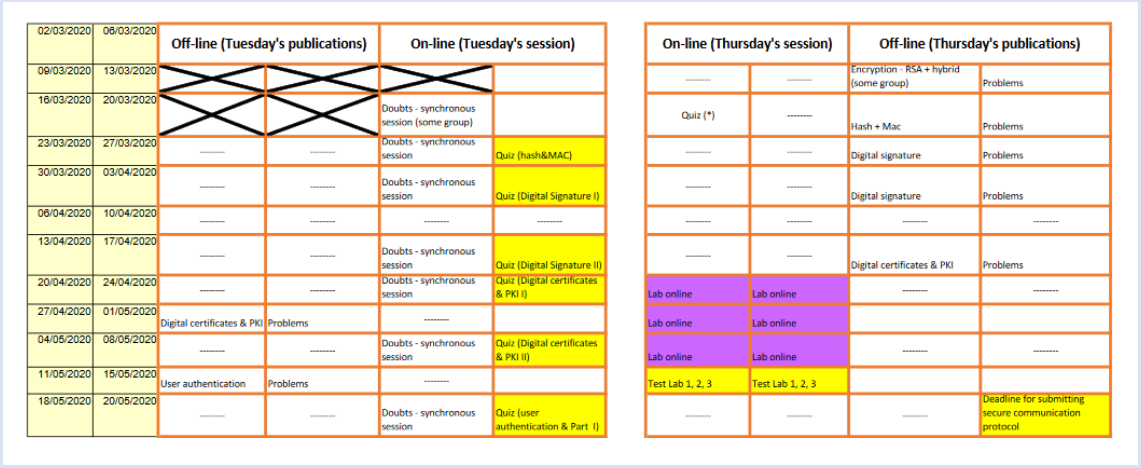
		Off-line		On-line	
02/03/2020	06/03/2020				
09/03/2020	13/03/2020				
16/03/2020	20/03/2020			Dudas - sesión síncrona (algún grupo)	
23/03/2020	27/03/2020	----------	----------	Dudas - sesión síncrona	Cuestionario (hash&MAC)
30/03/2020	03/04/2020	----------	----------	Dudas - sesión síncrona	Cuestionario (Firma digital I)
06/04/2020	10/04/2020	----------	----------	----------	----------
13/04/2020	17/04/2020	----------	----------	Dudas - sesión síncrona	Cuestionario (Firma digital II)
20/04/2020	24/04/2020	----------	----------	Dudas - sesión síncrona	(Certificados digitales & PKI I)
27/04/2020	01/05/2020	Certificados digitales & PKI	Problemas	----------	
04/05/2020	08/05/2020	----------	----------	Dudas - sesión síncrona	(Certificados digitales & PKI II)
11/05/2020	15/05/2020	User authentication	Problemas	----------	
18/05/2020	20/05/2020	----------	----------	Dudas - sesión síncrona	Cuestionario (autenticación de usuarios & Parte I)

On-line		Off-line	
----------	----------	Cifrado - RSA + híbrido (algún grupo)	Problemas
Cuestionario (*)	----------	Hash + Mac	Problemas
----------	----------	Firma digital	Problemas
----------	----------	Firma digital	Problemas
----------	----------	----------	----------
----------	----------	Certificados digitales & PKI	Problemas
Lab online	Lab online	----------	----------
Lab online	Lab online		
Lab online	Lab online	----------	----------
Test Lab 1, 2, 3	Test Lab 1, 2, 3		
----------	----------	----------	Fecha límite para entregar protocolo de comunicación segura

La experimentalidad se cubre en las 4 sesiones de prácticas (en la última de ellas, además, se realizará el test que evalúa dichas prácticas) así como por la realización de múltiples problemas todas las semanas.

La adaptación de actividades más significativa es la inclusión de una actividad nueva en la que los estudiantes deben acabar de diseñar un esquema de comunicación segura entre dos interlocutores y utilizarlo para que se intercambien mensajes.

Course contents are the same, but the scheduling has been adapted according to the following image and according to the methodology described in section 1. The order has not changed significantly considering that this course lab sessions had been placed at the end of the course.



		Off-line (Tuesday's publications)		On-line (Tuesday's session)	
02/03/2020	06/03/2020				
09/03/2020	13/03/2020				
16/03/2020	20/03/2020			Doubts - synchronous session (some group)	
23/03/2020	27/03/2020	----------	----------	Doubts - synchronous session	Quiz (hash&MAC)
30/03/2020	03/04/2020	----------	----------	Doubts - synchronous session	Quiz (Digital Signature I)
06/04/2020	10/04/2020	----------	----------	----------	----------
13/04/2020	17/04/2020	----------	----------	Doubts - synchronous session	Quiz (Digital Signature II)
20/04/2020	24/04/2020	----------	----------	Doubts - synchronous session	Quiz (Digital certificates & PKI I)
27/04/2020	01/05/2020	Digital certificates & PKI	Problems	----------	
04/05/2020	08/05/2020	----------	----------	Doubts - synchronous session	Quiz (Digital certificates & PKI II)
11/05/2020	15/05/2020	User authentication	Problems	----------	
18/05/2020	20/05/2020	----------	----------	Doubts - synchronous session	Quiz (user authentication & Part I)

On-line (Thursday's session)		Off-line (Thursday's publications)	
----------	----------	Encryption - RSA + hybrid (some group)	Problems
Quiz (*)	----------	Hash + Mac	Problems
----------	----------	Digital signature	Problems
----------	----------	Digital signature	Problems
----------	----------	----------	----------
----------	----------	Digital certificates & PKI	Problems
Lab online	Lab online	----------	----------
Lab online	Lab online		
Lab online	Lab online	----------	----------
Test Lab 1, 2, 3	Test Lab 1, 2, 3		
----------	----------	----------	Deadline for submitting secure communication protocol

Experimentality is covered by the 4 lab sessions (last one also allocates the lab test) as well as by carrying out multiple problems every week.

The most significant activity adaptation is the inclusion of a new activity in which students are requested to design a secure communication scheme between two parties and use it to exchange messages.

3. SISTEMA DE EVALUACIÓN
3. ASSESSMENT SYSTEM

- En este apartado debe describirse el proceso de evaluación continua empleado para la evaluación de la asignatura (conjunto de elementos considerados para la misma)
- También debe indicarse el tipo de evaluación final empleado, en su caso (entrega trabajo, ensayo o proyecto, examen tipo test, prueba oral, etc.)

La evaluación de la convocatoria ordinaria será completamente online y se compone de las siguientes actividades de evaluación:

- Tests de teoría. Estos tests se pueden realizar en modalidad síncrona (Wooclap en las sesiones síncronas programadas) o asíncrona (tests Wooclap a tu ritmo los días siguientes a la sesión síncrona). Estos tests en total, en el caso de contestarlos todos de forma síncrona, cuentan hasta 1 punto. En el caso de realizarlos todos asíncronamente, cuentan como máximo 0,6 puntos.

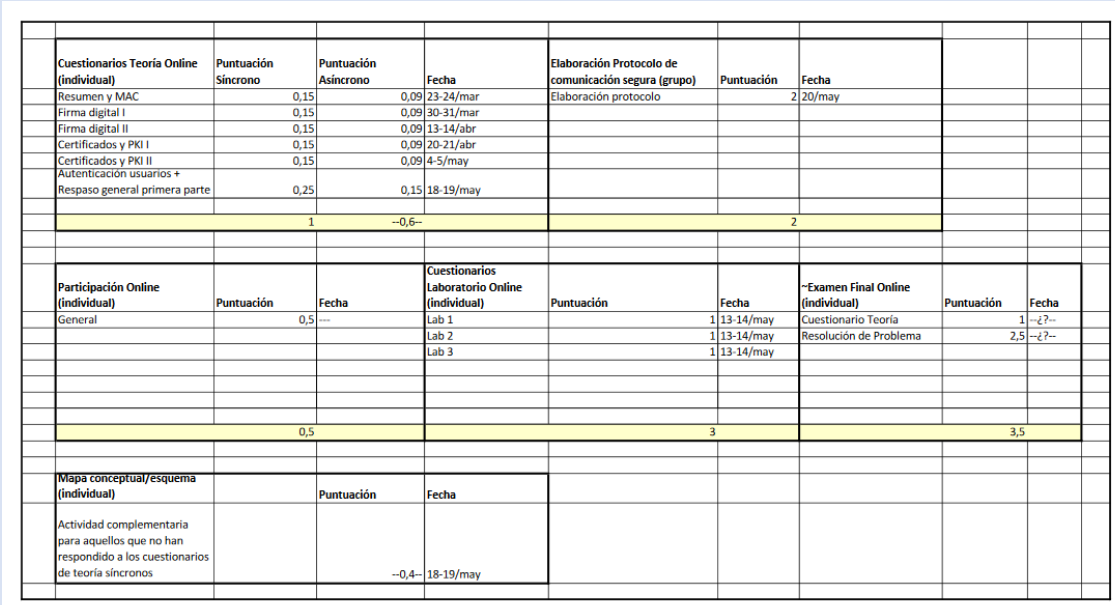
- Participación activa en las actividades online. Este aspecto valorará la participación en las actividades online (foro, asistencia sesiones síncronas, entrega de problemas…) hasta un máximo de 0,5 puntos.

- Tests de laboratorio. Estos tests tendrán el formato de un cuestionario en Aula Global, con preguntas sobre todos los laboratorios. Contarán como máximo 3 puntos (para el total de laboratorios). El test tendrá lugar en la última sesión de laboratorio, en el horario del grupo pequeño.

- Elaboración de un protocolo/esquema de comunicación segura. Esta actividad es nueva en la asignatura. Contará como máximo 2 puntos y se realizarás en grupos de 4 estudiantes pertenecientes al mismo grupo magistral.

- Examen final en fecha por determinar. Se realizará a través de Aula Global y constará de un test de teoría y la resolución de un problema online (a través de Aula Global). Valor máximo de 3,5 puntos. Se exigirá la obtención de unos resultados mínimos para poder aprobar la asignatura.

La programación de las actividades de evaluación mencionadas se detalla en la siguiente imagen:



Cuestionarios Teoría Online (individual)	Puntuación Síncrono	Puntuación Asíncrono	Fecha	Elaboración Protocolo de comunicación segura (grupo)	Puntuación	Fecha
Resumen y MAC	0,15	0,09	23-24/mar	Elaboración protocolo	2	20/may
Firma digital I	0,15	0,09	30-31/mar			
Firma digital II	0,15	0,09	13-14/abr			
Certificados y PKI I	0,15	0,09	20-21/abr			
Certificados y PKI II	0,15	0,09	4-5/may			
Autenticación usuarios + Respaso general primera parte	0,25	0,15	18-19/may			
	1	--0,6--			2	

Participación Online (individual)	Puntuación	Fecha	Cuestionarios Laboratorio Online (individual)	Puntuación	Fecha	~Examen Final Online (individual)	Puntuación	Fecha
General	0,5	---	Lab 1	1	13-14/may	Cuestionario Teoría	1	--¿?--
			Lab 2	1	13-14/may	Resolución de Problema	2,5	--¿?--
			Lab 3	1	13-14/may			
	0,5			3			3,5	

Mapa conceptual/esquema (individual)		Puntuación	Fecha
Actividad complementaria para aquellos que no han respondido a los cuestionarios de teoría síncronos		--0,4--	18-19/may

% EVALUACIÓN CONTINUA	% EVALUACIÓN FINAL
65%	*35%*

All ordinary sitting assessment activities will be online. They are the following ones:

- Theory tests. Done in synchronous or asynchronous mode through Wooclap web app. In the first case they will have a maximum weight of 1 mark; in the second case, 0,6 marks.

- Active participation in online activities. This aspect will have a maximum weight of 0,5 marks (forum participation, attendance to online sessions, …).

- Lab tests. These tests will take the form of a questionnaire in Aula Global, including questions about all the labs. They'll have a maximum weight of 3 marks (as a whole). Lab test will take place in the last lab session (small group time slot).

- Design and specification of a secure communication protocol/scheme. This is a new activity in the course. It will have a maximum weight of 2 marks and it will be done in groups of 4 students enrolled in the same big group.

- Final exam, date to be determined. It will be done through Aula Global and will consist of an online theory test and solving a problem. A minimum performance will be required to pass the course.

Assessment activities are scheduled as next image shows:

Online Theory Tests (individual)	**Marks - Synchronous**	**Marks - Asynchronous**	**Date**	**Protocol Elaboration (group)**	**Marks**	**Date**
Hash & MAC	0,15	0,09	23-24/mar	Protocol elaboration	2	20/may
Digital Signature I	0,15	0,09	30-31/mar			
Digital Signature II	0,15	0,09	13-14/apr			
Certificates & PKI I	0,15	0,09	20-21/apr			
Certificates & PKI II	0,15	0,09	4-5/may			
User authentication + Review of first part	0,25	0,15	18-19/may			
	1	--0,6--			2	

Online Participation (individual)	**Marks**	**Date**	**Online Lab Tests (individual)**	**Marks**	**Date**	**~Online Final Exam (individual)**	**Marks**	**Date**
General	0,5	---	Lab 1	1	13-14/may	Theory Test	1	--¿?--
			Lab 2	1	13-14/may	Problem Solving	2,5	--¿?--
			Lab 3	1	13-14/may			
	0,5			3			3,5	

Mind map/schema (individual)		**Marks**	**Date**
Supplementary activity for those that have not answered synchronous theory tests		--0,4--	18-19/may

% CONTINUOUS ASSESSMENT	% FINAL ASSESSMENT
65%	*35%*