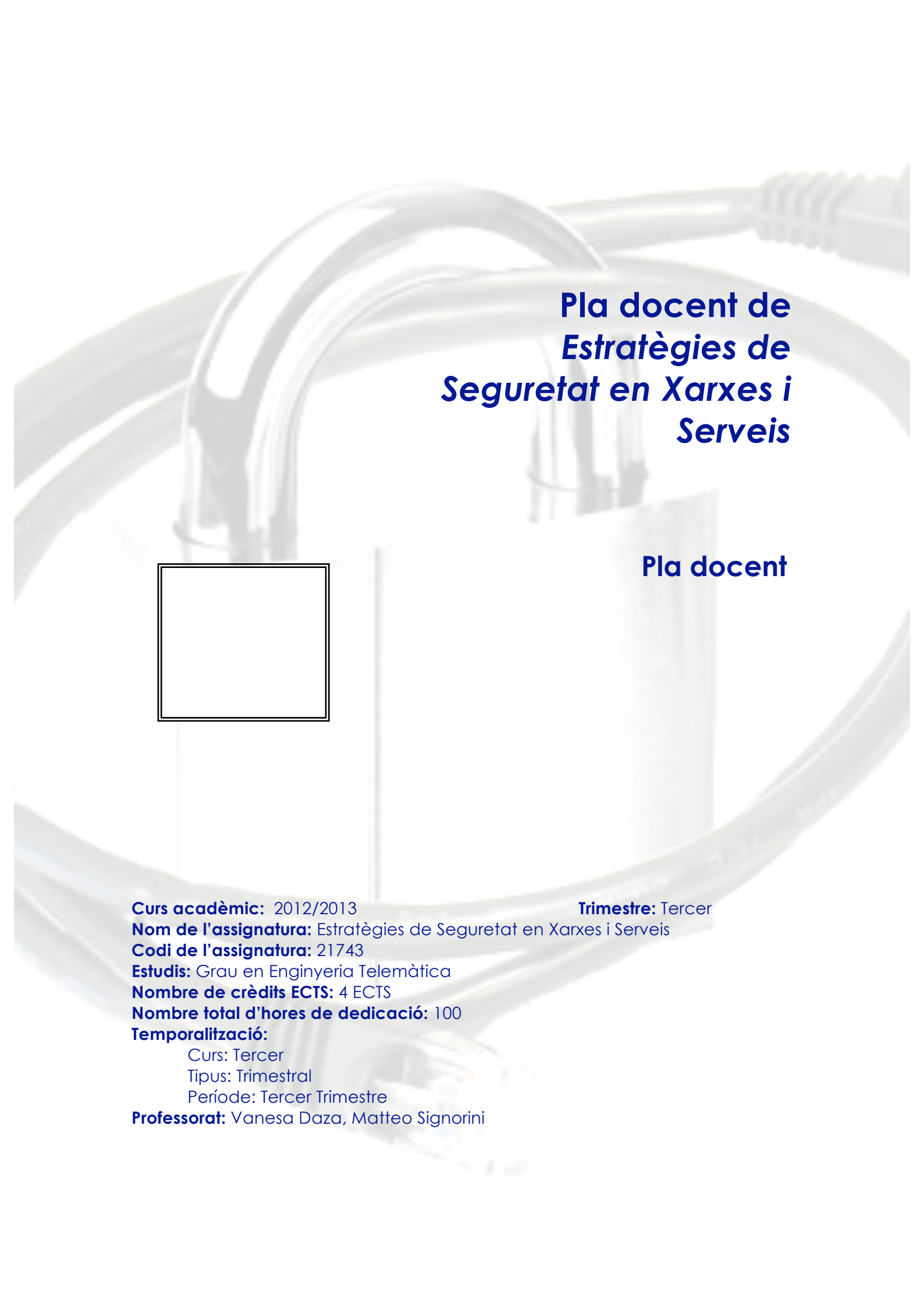
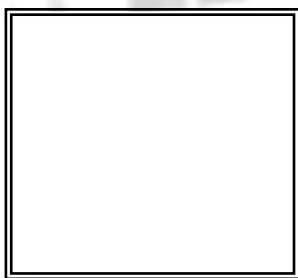




Pla docent de *Estratègies de Seguretat en Xarxes i Serveis*

Pla docent



Curs acadèmic: 2012/2013

Trimestre: Tercer

Nom de l'assignatura: Estratègies de Seguretat en Xarxes i Serveis

Codi de l'assignatura: 21743

Estudis: Grau en Enginyeria Telemàtica

Nombre de crèdits ECTS: 4 ECTS

Nombre total d'hores de dedicació: 100

Temporalització:

Curs: Tercer

Tipus: Trimestral

Període: Tercer Trimestre

Professorat: Vanesa Daza, Matteo Signorini

Pla Docent

1. Dades descriptives de l'assignatura

- **Curs acadèmic:** 2012/2013
- **Nom de l'assignatura:** Estratègies de Seguretat en Xarxes i Serveis **Codi:** 21743
- **Tipus d'assignatura:** Optativa
- **Titulació / Estudis:** Grau en Enginyeria Telemàtica (tot i que la poden cursar estudiants del Grau en Enginyeria en Informàtica i del Grau en Enginyeria de Sistemes Audiovisuals)
- **Nombre de crèdits ECTS:** 4
- **Nombre total d'hores de dedicació a l'assignatura:** 100 h
- **Temporalització:**
 - Curs: 3er curs
 - Tipus: trimestre
 - Període: 3er trimestre
- **Coordinació:** Vanesa Daza
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Professorat:** Vanesa Daza, Matteo Signorini
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Llengua de docència:** Català – Anglès
- **Edifici on s'imparteix l'assignatura:** Edifici 52 – Roc Boronat
- **Horari:**
 - Dilluns 10:30 – 12:30
 - Dimarts 8:30 – 10:30
 - Dimecres 12:30 – 14:30

2. Presentació de l'assignatura

Actualment no és difícil trobar al diari notícies que expliquen com les dades i els serveis de les empreses s'han vist compromesos per hackers. Inclús les principals companyies de tots els àmbits (webs, jocs en línia, e-banking, xarxes socials, ...), que operen principalment a través de la xarxa, s'han vist sotmeses a nombrosos atacs. Així, atacs de denegació de servei distribuïts (DDoS) poden afectar considerablement algun dels serveis oferts per una empresa, mentre que d'altres com els atacs de segrest de sessió posen el perill la privadesa dels usuaris.

Podríem pensar que una solució per garantir la seguretat de la xarxa d'ordinadors d'una empresa és que s'abstinguin de posar-los connectats a Internet, i mantenint-los darrera d'una porta tancada amb clau. Però encara hi ha atacs que poden realitzar els propis treballadors des de dintre (les estadístiques indiquen que d'un 70% o 80% es fan per personal de la pròpia empresa). Per tant, desafortunadament, aquesta no és una solució molt pràctica.

Avui dia, els equips són més útils si estan connectats en xarxa per compartir informació i recursos, però les empreses que posen els seus equips en xarxa necessiten fer ús d'eines i protocols que permetin reduir les amenaces i el risc a que estaran sotmesos.

L'objectiu principal d'aquesta assignatura és treballar els principals aspectes implicats en el desplegament de mecanismes i procediments de gestió de la seguretat en les xarxes de telecomunicació, establint els principals principis de la seguretat de la informació, així com els principals atacs i contra-mesures coneguts.

L'aproximació de l'assignatura és que, en algunes parts, l'alumne aprengui dels propis errors. Així, a partir d'algunes vulnerabilitats, els alumnes veuran la necessitat de garantir mecanismes de seguretat.

Tal i com es descriurà a l'apartat corresponent, l'assignatura inclou tant activitats pràctiques com estudi de casos.

3. Recomanacions

Es recomana que l'alumne hagi tingut els coneixements bàsics dels principals conceptes i protocols de xarxes, i que hauran assolit a l'assignatura *Xarxes i Serveis*.

4. Competències a assolir en l'assignatura

Competències generals	Competències específiques
Instrumentals 1. Habilitat de cerca i la gestió de la informació 2. Capacitat d'anàlisi i síntesi 3. Capacitat de comunicació oral 4. Capacitat de presa de decisions 5. Capacitat d'organització i planificació 6. Capacitat per aplicar els coneixements a l'anàlisi de situacions i la resolució de problemes	12. Capacitat per aplicar les tècniques en què es basen les xarxes, serveis i aplicacions telemàtiques per a garantir la seguretat (protocols criptogràfics, tunelatje, tallafocs, mecanismes de cobrament, d'autenticació i de protecció de continguts) 13. Identificar les amenaces més representatives per a la seguretat de la informació així com els principals mecanismes de protecció. 14. Utilitzar bones pràctiques per garantir la seguretat física dels servidors i altres components de la xarxa 15. Conèixer i utilitzar els principals protocols criptogràfics per garantir la seguretat a les comunicacions 16. Conèixer i utilitzar les eines pertinents per proporcionar seguretat a la xarxa
Interpersonals 7. Capacitat crítica i autocrítica. 8. Compromís ètic.	
Sistèmiques 9. Capacitat de resoldre problemes amb iniciativa, presa de decisions, creativitat, i de comunicar i transmetre coneixements, habilitats i destreses, comprenent la responsabilitat ètica i professional de l'activitat de l'enginyer TIC 10. Capacitat de motivació per la qualitat i per l'assoliment 11. Capacitat de generació de noves idees	

5. Continguts

- Bloc 1. Fonaments Criptogràfics
 - Criptografia de clau simètrica
 - Criptografia de clau pública
- Bloc 2. Principis de Seguretat en Xarxes
 - Autenticació
 - PKIs
 -
- Bloc 3. Escenaris Reals: Atacs i Mecanismes de Protecció

6. Metodologia

Aquesta assignatura es durà a terme mitjançant sessions presencials i sessions no presencials.

Les sessions presencials seran sessions de teoria i sessions de laboratori. A continuació es detallen els trets bàsics de cada tipologia:

- **Sessions de Teoria:** Tindran una durada aproximada d'entre hora mitja i dues hores. El professor presentarà durant aquestes sessions els conceptes, procediments i processos corresponents a cada un dels blocs temàtics. Tot i que tindran un caire fonamentalment expositiu es fomentarà la interacció amb l'estudiant per a resoldre dubtes, plantejar qüestions, etc.
- **Sessions de Laboratori:** Tindran una durada de dues hores. Durant les sessions de laboratoris, es plantejaran un o diversos exercicis pràctics que els alumnes hauran de resoldre. Els estudiants comptaran amb el suport del professor per a resoldre tots els dubtes que puguin sorgir.

És important tenir present que **els laboratoris requereixen d'un treball previ** que serà degudament entregat abans de l'inici de cada sessió de laboratori. Una nota inferior a 5 a aquestes entregues comporta l'anul·lació de qualsevol nota obtinguda com a resultat d'aquest laboratori en concret. Les entregues es faran de manera individual a través de l'Aula Global de l'assignatura. Per a aquest treball previ, les entregues en grup o còpies seran penalitzades amb l'anul·lació de la nota d'aquell laboratori.

Serà a les **sessions no presencials** on:

- L'alumne treballarà els conceptes treballats a les sessions de teoria.
- L'alumne prepararà les sessions de laboratori tot consolidant els coneixements adquirits a les sessions de teoria de l'assignatura, contrastant amb fonts bibliogràfiques i enllaços facilitats pels professors.
- L'alumne finalitzarà tanmateix aquelles parts que no s'hagin pogut finalitzar al laboratori, incloent una memòria de qualitat, breu i que reflecteixi la comprensió dels principals conceptes treballats al laboratori.
- L'alumne prepararà qualsevol altra activitat proposada pel professorat tant a les sessions de teoria com de laboratori.
- Els alumnes prepararan, en grups, el joc que es proposarà al final de l'assignatura.

Tot el material de l'assignatura (diapositives i enunciats) estarà disponible a l'Aula Global.

7. Avaluació

Per a l'avaluació de l'assignatura es tindran en compte els següents elements:

- Lliurament de les *entregues pre-laboratori* (10%).
- Lliurament de les pràctiques proposades a les sessions de laboratori (40 %). És obligatori el lliurament de totes les sessions de laboratori i aprovar la nota mitja de totes elles. L'entrega endarrerida de la pràctica es penalitzarà amb 2 punts per a cada dia que passi de la data límit.
- Prova de validació que inclourà alguns dels exercicis (total o parcialment) tractats a les sessions de laboratori (30 %). Cal superar amb almenys un 5 la prova per a superar l'assignatura.
- Lliurament i proposta del joc de taula de seguretat (20%). La participació en aquesta activitat és obligatòria per a superar l'assignatura.

A més a més, es plantejaran diferents activitats optatives durant el curs que poden representar fins a un 10% extra per a la puntuació final de l'assignatura.

L'única activitat que es podrà recuperar al juliol serà la prova de validació.

8. Bibliografia i recursos didàctics

La bibliografia i recursos didàctics de l'assignatura són:

- Bibliografia bàsica
 - Network Security: Private Communication in a Public World, 2/E C. Kaufman, R. Perlman, M. Speciner, Pearson 2002.
- Bibliografia complementària
 - Introduction to Computer Security, M. T. Goodrich, R. Tamassia. Ed. Pearson, 2011.
 - Cryptovirology, A. Young, M. Yung, Wiley, 2004.
 - Network Security with openSSL: Cryptography for Secure Communications, J. Viega, M. Messier, P. Chandra, O'Really, 2002.
- Recursos didàctics i material docent
 - A l'aula Global de l'assignatura, l'alumne podrà obtenir el material docent corresponent a les sessions de teoria.
 - A l'aula Global de l'assignatura, l'alumne podrà obtenir la col·lecció d'enunciats corresponent a les sessions de laboratori.

9. Planificació

	Dilluns 10:30-12:30	Dimarts 8:30-10:30	Dimarts 14:30-16:30	Dijous 12:30-14:30
S1. 08-12 abr	T	NO CLASSE	T	T
S2. 15-19 abr	L1. P101	L1. P102	L1. P103	T
S3. 22-26 abr	L2. P102	FESTIU	L2. P103 ¹	L2. P101
S4. 29abr- 3 maig	T	L3. P101	L3. P103	L3. P102
S5. 06-10 maig	T	L4. P102	L4. P103	L4. P101
S6. 13-17 maig	L5. P101	L5. P102	L5. P103	T
S7. 20-24 maig	FESTIU	L6. P102	L6. P103	L6. P101
S8. 27-31 maig	T	L7. P101	L7. P103	L7. P102
S9. 3-7 juny	T	L8. P102	L8. P103	L8. P101
S10. 10-15 juny	JOC. P101	JOC. P102	JOC. P103	JOC. T

10. Dates de lliuraments

Entregables	Data Entrega	Data Qualificació
L1 + L2	28 abril	5 maig
L3	5 maig	13 maig
L4	13 maig	18 maig
L5	18 maig	26 maig
L6	26 maig	2 juny
L7	2 juny	9 juny
L8	9 juny	15 juny
JOC	17 juny	21 juny

¹ Aquesta sessió es realitzarà el dijous 25 d'abril en ser festiu el dia 23 d'abril.