

Seguretat Informatica (SI)

Introducción a la asignatura: primavera 2021-2022

Davide Careglio

Introducción

- ▶ Davide Careglio

- ▶ careglio@ac.upc.edu
- ▶ Campus Nord, D6-I03
- ▶ Castellano pero ...
- ▶ Información asignatura
 - Atenea, Racó, web personal
 - <http://people.ccaba.upc.edu/careglio>

- ▶ Horario teoría

- ▶ Lunes de 16 a 18
- ▶ Viernes de 16 a 17

Introducción

- ▶ Roberto Barreda, roberto.barreda@upc.edu
- ▶ Horario lab
 - ▶ Martes de 16 a 18 - G11 (C6-S309)
 - ▶ Martes de 18 a 20 - G12 (C6-S309)
- ▶ Publicaremos el calendario de los labs a lo largo de la próxima semana en Atenea y Racó
 - ▶ Empezarán en Marzo

Guía docente

Objetivos del curso

- ▶ Ser capaç d'entendre les **amenaces i riscos** de seguretat dels sistemes informàtics.
 - ▶ Ser capaç d'entendre les idees generals de les implicacions legals de la seguretat informàtica.
- ▶ Ser capaç de fer servir **mecanismes criptogràfics** per a la protecció dels recursos.
 - ▶ Ser capaç d'implementar mecanismes de signatura electrònica.
- ▶ Ser capaç d'entendre, aplicar i dissenyar **infraestructures de clau pública** (PKI).
 - ▶ Ser capaç de dissenyar i gestionar certificats de clau pública.
 - ▶ Ser capaç d'entendre els mecanismes de protecció i les polítiques de seguretat
- ▶ Conèixer les **problemàtiques de seguretat** a les xarxes de computadors i ser capaç de **trobar solucions** per protegir-les.
 - ▶ Ser capaç de dissenyar tallafocs i xarxes privades virtuals.
 - ▶ Ser capaç d'entendre el funcionament dels sistemes de detecció d'intrusos.
- ▶ Ser capaç de **dissenyar mecanismes de protecció** per a les aplicacions distribuïdes.
 - ▶ Ser capaç d'identificar amenaces de seguretat i proposar solucions en app web i de e-comerç
- ▶ Ser capaç d'entendre i identificar mecanismes de **control d'accés** d'un sistema operatiu.
 - ▶ Ser capaç d'**analitzar codi maliciós**, com ara virus, troians, etc.
- ▶ Ser capaç d'entendre la necessitat i funcionament de **mecanismes forenses**

Guía docente

Objetivos del curso

- ▶ Ser capaç d'entendre les **amenaces i riscos** de seguretat dels sistemes informàtics.
 - ▶ Ser capaç d'entendre les idees generals de les implicacions legals de la seguretat informàtica. **Tema 1. Introducción**
- ▶ Ser capaç de fer servir **mecanismes criptogràfics** per a la protecció dels recursos.
 - ▶ Ser capaç d'entendre els mecanismes de signatura electrònica. **Tema 2. Criptografía**
- ▶ Ser capaç d'entendre, aplicar i dissenyar **infraestructures de clau pública (PKI)**.
 - ▶ Ser capaç de dissenyar i gestionar certificats de clau pública.
 - ▶ Ser capaç d'entendre els mecanismes de protecció i les polítiques de seguretat. **Tema 3. Infraestructura PKI**
- ▶ Conèixer les **problemàtiques de seguretat** a les xarxes de computadors i ser capaç de **trobar solucions** per protegir-les.
 - ▶ Ser capaç de dissenyar i gestionar xarxes privades virtuals. **Tema 4. Seguridad en las redes**
 - ▶ Ser capaç d'entendre el funcionament dels sistemes de detecció d'intrusos.
- ▶ Ser capaç de **dissenyar mecanismes de protecció** per a les aplicacions distribuïdes.
 - ▶ Ser capaç d'entendre les amenaces de seguretat i proposar solucions en app web i de e-comerç. **Tema 5. Seguridad en las aplicaciones**
- ▶ Ser capaç d'entendre i **identificar mecanismes de control d'accés** d'un sistema operatiu.
 - ▶ Ser capaç d'entendre i identificar **codi maliciós**, com ara virus, troians, etc. **Tema 6. Seguridad en los SO**
- ▶ Ser capaç d'entendre el funcionament de **mecanismes forenses**. **Tema 7. Análisis forense**

Guía docente

Objetivos del curso

- ▶ Ser capaç d'entendre les **amenaces i riscos** de seguretat dels sistemes informàtics.
 - ▶ Ser capaç d'entendre les idees generals de les implicacions legals de la seguretat informàtica. **Tema 1. Introducción**
- ▶ Ser capaç de fer servir **mecanismes criptogràfics** per a la protecció dels recursos.
 - ▶ Ser capaç d'implementar mecanismes de signatura electrònica. **Tema 2. Criptografía**
- ▶ Ser capaç d'entendre, aplicar i dissenyar **estructures de clau pública**.
 - ▶ Ser capaç de dissenyar i gestionar certificats de clau pública. **Lab 1. Uso de certificados digitales**
 - ▶ Ser capaç d'implementar els mecanismes de protecció i les polítiques de seguretat. **Tema 3. Infraestructura PKI**
- ▶ Conèixer les **problemàtiques de seguretat** a les xarxes de computadors i ser capaç de **trobar solucions** per protegir-les.
 - ▶ Ser capaç de dissenyar i gestionar xarxes privades virtuals. **Tema 4. Seguridad en las redes**
 - ▶ Ser capaç d'entendre el funcionament dels sistemes de detecció d'intrusos. **Lab 2. iptables**
Lab 3. Snort
- ▶ Ser capaç de **dissenyar mecanismes de protecció** per a les aplicacions.
 - ▶ Ser capaç d'entendre les amenaces de seguretat i proposar solucions. **Tema 5. Seguridad en las aplicaciones**
 - ▶ Ser capaç d'entendre i identificar **SO de contro**l d'accés d'un sistema operatiu. **Lab 4. Análisis de vulnerabilidades web**
 - ▶ Ser capaç d'analitzar **codi maliciós**, com ara virus, troians etc. **Lab 5. Análisis de código malicioso**
- ▶ Ser capaç d'entendre la necessitat i funcionament de **mecanismes forenses**. **Tema 7. Análisis forense** **Lab 6. Análisis forense**

Guía docente

Competencias TI

- ▶ Definir, planificar i gestionar la instal·lació de la infraestructura TIC de l'organització.
 - ▶ Demostrar comprensió de l'entorn d'una organització i de les seves necessitats en l'àmbit de les tecnologies de la informació i les comunicacions.
 - ▶ Seleccionar, dissenyar, desplegar, integrar gestionar xarxes i infraestructures de comunicacions en una organització.
 - ▶ Seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de l'organització amb els criteris de cost i qualitat identificats.
- ▶ Garantir que els sistemes TIC d'una organització funcionen de manera adequada, són segurs i estan adequadament instal·lats, documentats, personalitzats, mantinguts, actualitzats i substituïts, i que les persones de l'organització reben un suport TIC correcte.
 - ▶ Demostrar comprensió, aplicar i gestionar la garantia i la seguretat dels sistemes informàtics.
- ▶ Dissenyar solucions que integrin tecnologies de hardware, software i comunicacions (i capacitat de desenvolupar solucions específiques de software de sistemes) per a sistemes distribuïts i dispositius de computació ubiqua.
 - ▶ Concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, tenint en compte Internet, web, comerç electrònic, multimèdia, serveis interactius i computació ubiqua.

Guía docente

Competencias TI

- ▶ Definir, planificar i gestionar la instal·lació de la infraestructura TIC de l'organització.
 - ▶ Demostrar comprensió de l'entorn d'una organització i de les seves necessitats en l'àmbit de les tecnologies de la informació i les comunicacions.
 - ▶ Seleccionar, dissenyar, desplegar, integrar i gestionar xarxes i infraestructures de comunicacions en una organització.
 - ▶ Seleccionar, desplegar, integrar i gestionar sistemes d'informació que satisfacin les necessitats de l'organització amb els criteris de cost i qualitat identificats.
- ▶ Garantir que els sistemes TIC d'una organització funcionen de manera adequada, són segurs i estan adequadament instal·lats, documentats, personalitzats, mantinguts, actualitzats i substituïts, i que les persones de l'organització reben un suport TIC correcte.
 - ▶ Demostrar comprensió, aplicar i gestionar la garantia i la seguretat dels sistemes informàtics.
- ▶ Dissenyar solucions que integrin tecnologies de hardware, software i comunicacions (i capacitat de desenvolupar solucions específiques de software de sistemes) per a sistemes distribuïts i dispositius de computació ubiqua.
 - ▶ Concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, tenint en compte Internet, web, comerç electrònic, multimèdia, serveis interactius i computació ubiqua.

Guía docente

Competencia Transversal (CT)

- ▶ Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i d'informació de l'àmbit de l'enginyeria informàtica, i valorar de forma crítica els resultats d'aquesta gestió.
 - ▶ Planificar i utilitzar la informació necessària per a un treball acadèmic (per exemple, per al treball de final de grau) a partir d'una reflexió crítica sobre els recursos d'informació utilitzats.
 - ▶ Gestionar la informació de manera competent, independent i autònoma.
 - ▶ Avaluar la informació trobada i identificar-ne les llacunes.

→ Practica específica dedicada a esta CT

**Lab CT. Uso solvente de los
recursos informáticos**

Organización

- ▶ **Parte teórica**

- ▶ 7 temas (presentaciones + pizarra de vez en cuando)
- ▶ Resolución de problemas
- ▶ Tres controles (uno cada mes +/-)
- ▶ Material disponible en Atenea
- ▶ Comunicación vía Racó

- ▶ **Parte práctica**

- ▶ 1 practica con personal de la biblioteca (CT)
- ▶ 6 laboratorios presenciales
- ▶ 1 examen final

Temario: parte teórica

- ▶ Tema 1. Introducción
- ▶ Tema 2. Criptografía
- ▶ Tema 3. Infraestructura PKI

→ Primer control (1C)

33,3% nota de teoría

- ▶ Tema 4. Seguridad en la red
- ▶ Tema 5. Seguridad en las aplicaciones

→ Segundo control (2C)

33,3% nota de teoría

- ▶ Tema 6. Seguridad en los sistemas operativos
- ▶ Tema 7. Análisis forense

→ Tercer control (3C)

33,3% nota de teoría

Temario: parte práctica

- ▶ 6 clases prácticas en el lab (coordinadas con teoría)
 - ▶ Lab 1. Uso de certificados digitales y apache (HTTPS)
 - ▶ Lab 2. Configuración de firewall y NAT con iptables
 - ▶ Lab 3. Detección de intrusos con Snort
 - ▶ Lab 4. Análisis de vulnerabilidades web
 - ▶ Lab 5. Análisis de código malicioso
 - ▶ Lab 6. Análisis forense
- ▶ I practica sobre uso solvente de los recursos de información
 - ▶ Practica coordinada con la biblioteca del CN
 - ▶ A la espera de confirmar fechas
- ▶ I examen final sobre las practicas
 - ▶ La última semana de clase, probablemente durante una clase de teoría

Temario: parte práctica

Metodología laboratorios

- ▶ Calendario será disponible en Atenea y Racó (próxima semana)
- ▶ Los enunciados se publicarán en Atenea
- ▶ Hay que leerse el enunciado de cada sesión antes de venir a clase
- ▶ Las practicas son individuales
 - ▶ Se empezarán en clase de lab
 - ▶ Si no se consiguen acabar, se pueden continuar en casa
- ▶ Se usarán máquinas virtuales
 - ▶ Para poder trabajar en casa se recomienda un ordenador con software capaz de ejecutar maquinas virtuales como por ejemplo VMWarePlayer o VirtualBox
- ▶ Evaluación a través de entregas y/o cuestionario
 - ▶ La evaluación del laboratorio se realizan a través de Atenea
 - ▶ La data límite para las entregas y/o contestar al cuestionario es dos semanas después de cada lab

Evaluación

- ▶ **Tres componentes**
 - ▶ Nota de Teoría (NT)
 - ▶ Nota de Laboratorio (NL)
 - ▶ Nota Competencia Transversal (CT)
- ▶ **Nota de Teoría (NT)**
 - ▶ Tres controles, 1C, 2C, 3C (uno cada mes +/- y tienen el mismo peso)
 - ▶ $NT = (1C + 2C + 3C) / 3$
- ▶ **Nota de Laboratorio (NL)**
 - ▶ Todas las practicas valen lo mismo
 - ▶ Es obligatorio entregarlas, de lo contrario, no hay examen de laboratorio (EL)
 - ▶ $NL = 50\% (Lab1 + Lab2 + Lab3 + Lab4 + Lab5 + Lab6) / 6 + 50\% EL$
- ▶ **Nota Competencia Transversal (CT)**
 - ▶ Cuestionario en Atenea después de la clase con el personal de la biblioteca
- ▶ **Nota final (NF)**
 - ▶ **$NF = 70\% NT + 25\% NL + 5\% CT$**

Consultas

- ▶ Hacer preguntas en clase: probablemente muchos compartáis las mismas dudas y necesitáis las mismas aclaraciones
- ▶ Por correo: davide.careglio@upc.edu
- ▶ Online, concordar data y hora por correo
- ▶ Presencialmente en mi despacho D6-I03, si será posible

Bibliografía

- ▶ **Network security essentials: applications and standards**
Stallings, W, Pearson Education, 2011. ISBN: 0136108059
- ▶ **Cryptography and network security: principles and practice**
Stallings, W, Prentice Hall, 2014. ISBN: 9780273793359
- ▶ **Computer Security: Principles and Practice**
Stallings, W, Prentice Hall, 2014. ISBN: 9780132775069
- ▶ **Handbook of applied cryptography**
Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A, CRC Press, 1997.
ISBN: 0-8493-8523-7
- ▶ **Understanding PKI: concepts, standards, and deployment considerations**
Adams, C.; Lloyd, S, Addison-Wesley, 2003. ISBN: 0-672-32391-5
- ▶ **Material online: videos, documentos, artículos, etc.**
Enlaces disponibles en las presentaciones



Seguretat Informatica (SI)



Introducción a la asignatura



Davide Careglio