

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

XXXXXXXXXXXXXXXXXXXX  
06.503 15 01 14 PV

Enganxeu en aquest espai una etiqueta identificativa  
amb el vostre codi personal  
Prova



**Aquesta prova només la poden realitzar els  
estudiants que han aprovat  
l' Avaluació Continuada**

**Aquest enunciat correspon també a les assignatures següents:**

- 05.563 - Competència comunicativa per a professionals de les TIC
- 11.513 - Competència comunicativa per a professionals de les TIC

### Fitxa tècnica de la Prova

- Comprova que el codi i el nom de l'assignatura corresponen a l'assignatura en la qual estàs matriculat.
- Només has d'enganxar una etiqueta d'estudiant a l'espai corresponent d'aquest full.
- No es poden adjuntar fulls addicionals.
- No es pot realitzar la prova en llapis ni en retolador gruixut.
- Temps total: 1 h.
- En cas que els estudiants puguin consultar algun material durant la prova, quin o quins materials poden consultar?  
Es pot consultar un diccionari de llengua en paper.
- Valor de cada pregunta: Activitat 1 (100%)
- En cas que hi hagi preguntes tipus test: Descompten les respostes errònies? NO Quant?
- Indicacions específiques per a la realització d'aquesta prova:  
Tal com s'especifica al pla docent, i com s'ha aplicat en totes les PAC i la PR, les activitats de producció textual es poden redactar en català o castellà.

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

### Enunciats

La prova de síntesi consisteix en l'elaboració d'un text breu en què l'estudiant ha de demostrar tant el domini de les propietats textuais com la capacitat de síntesi, competència essencial per a qualsevol estudiant universitari.

**Enunciat: Redacteu una conclusió de 120 paraules per a l'article següent.**

#### Com pagar amb seguretat a Internet?

El comerç electrònic a Espanya no creix al ritme que seria desitjable. Entre les principals raons que els usuaris esgrimeixen per no comprar a la Xarxa, hi ha el recel a la seguretat dels sistemes de pagament. L'empresa EROSKI CONSUMER ha analitzat, a petició d'HISPA COOP (Confederació Espanyola de Cooperatives de Consumidors i Usuaris), els sistemes de pagament i les seves tècniques de seguretat amb la finalitat de saber si són totalment segures. La principal conclusió ha estat que el taló d'Aquilles de la compra no es troba en els sistemes, completament segurs, sinó en les cauteles de l'usuari a l'hora de deixar les seves dades en pàgines no fiables, i en la falta de cures de l'ordinador. Per assegurar al màxim la compra en línia, els experts que han elaborat aquest estudi han creat un detallat protocol d'actuació que detecta el frau, valora la seguretat dels comerços i manté l'ordinador lliure de programes espia. Si se segueixen els consells dictats a continuació, el risc de sofrir problemes en l'apartat de la seguretat en els pagaments fets a Internet es reduirà de manera notable.

Sempre que l'usuari compra en un comerç en línia selecciona el producte o el servei que vol comprar, n'especifica el nombre d'unitats i prem el botó d'anar "a la pàgina de compra". D'aquesta manera, arriba a una pàgina on se li demana que hi deixi alguns de les seves dades personals –nom, cognoms, document nacional d'identitat, telèfon de contacte, etc.–, a més de les dades de la targeta de crèdit o dèbit. El comprador emplena llavors els camps requerits, escriu les dades de la seva targeta i prem el botó d'executar "la compra". A partir d'aquí, perd el control de la informació que ha dipositat.

Significa això que un perill imminent de robatori, ús fraudulent o estafa amenaça l'usuari? Per descomptat, no des del punt de vista tècnic. Almenys fins que no es demostrï el contrari, i encara no s'ha demostrat. Els sistemes de pagament més usuals a la Xarxa són segurs al 100%. És a dir, cap "ciberdelinqüent" es pot colar en l'operació de pagament ni robar les claus de la targeta i els comptes de l'usuari mentre viatgen des de la pàgina de pagament al comerç. Això és vàlid sempre que es compleixin una sèrie de supòsits: que el comerç no actuï de mala fe –cosa que també pot passar en els establiments físics– i que el sistema de pagament, també anomenat *passarel·la*, que utilitzi aquest comerç no segueixi un protocol segur SSL.

Ara bé, moltes persones pensaran: "Doncs jo he llegit en la premsa que hi ha casos d'ús fraudulent de targetes en què els titulars havien fer compres a Internet". Fins i tot pot ser que alguna d'aquestes persones hagi experimentat en la pròpia carn aquesta mala experiència. On és el problema si els sistemes són infal·libles? D'una banda, encara que no serveixi d'excusa, cal matisar que aquests casos són poc habituals malgrat l'exagerada ressonància mediàtica que adquireixen. D'altra, s'ha d'assumir que tota compra té un punt feble en l'actitud de l'usuari. No es tracta de culpar el comprador, per descomptat, sinó de fer-lo conscient que la seguretat de la compra depèn en un 99% d'ell.

Els "ciberdelinqüents" existeixen i estan sempre a l'aguait, però els seus mètodes d'engany no són tècnics sinó psicològics. Juguen amb les debilitats, els desitjos i les pors de les persones per aconseguir les seves claus bancàries. Són grans experts, però no en tècniques de xifratge o d'informàtica, sinó en psicologia humana. Per començar, no arriben a l'usuari amb les mateixes arts que els comerços seriosos.

Aquests lladres d'última generació accedeixen a l'usuari per mitjà de correus electrònics no desitjats que superen els filtres de *spam* dels serveis –encara que cada vegada són menys els que ho aconsegueixen–, i que entabanen l'internauta perquè obri un arxiu que instal·larà un programa espia a l'ordinador. O bé l'inciten a punxar en un enllaç que porta a una pàgina web falsa amb la finalitat d'oferir-li diversos productes a un

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

preu molt reduït o difícil de trobar al país. Altres vegades, la seva tàctica consisteix a donar una falsa alarma a l'usuari perquè mitjançant una adreça URL que li ofereixen entri en una pàgina falsa del seu banc i hi deixi les claus.

Saben que la majoria de vegades fracassaran en l'intent i seran descoberts, però també és cert que un petit percentatge de persones caurà en el parany i els deixarà robar els seus comptes bancaris o els pagarà uns diners pels quals no rebrà res. Com que l'esforç que fan és mínim i l'estafa arriba a centenars de milers de bústies, amb uns pocs incauts que piquin és fàcil recuperar la inversió.

“Com pagar amb seguretat a Internet?”, *Consumer*, 01/01/2011 (text adaptat)

**Redacteu aquí la conclusió**

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

CONCLUSIÓSPAI EXTRA PER A LA

## Prova de Síntesi 2013/14-1

Assignatura	Codi	Data	Hora inici
Competència comunicativa per a professionals de les TIC	06.503	15/01/2014	20:00

CONCLUSIÓSPAI EXTRA PER A LA