**ACTIVITATS RECUPERACIÓ SETEMBRE**
TIC 4t d'ESO 2019/20
IES QUARTÓ DEL REI

BLOC 3. ORGANITZACIÓ, DISSENY I PRODUCCIÓ D'INFORMACIÓ DIGITAL

# 1. FULLS DE CÀLCUL: FUNCIÓ SI CONDICIONAL

En la primera unitat de reforç de la primera avaluació posareu en pràctica els coneixements adquirits en fulls de càlcul, més concretament en la Funció SI Condicional.

La seva estructura és la següent:

=Si (Condició; veritat; fals)

Això vol dir, que:

Establim una condició (per exemple, que el valor d'una cel·la sigui més gran que un número, que una data sigui anterior o posterior a una altra, etc.) i SI la condició es compleix, la fórmula ha de fer una acció (l'apartat on diu "veritat", i aquesta acció pot ser fer una operació matemàtica, mostrar un textual, etc.). En cas que la condició inicial no es compleixi, o sigui falsa, que ens faci una altra acció diferent.

Podeu observar-ho en els diferents exemples (videotutorials) i en podeu cercar més per ampliar o reforçar el vostre aprenentatge.

Videotutorials per aprendre a utilitzar la funció SI Condicional:

https://www.youtube.com/watch?v=MusQw7kTQIo&feature=emb_logo

https://www.youtube.com/watch?v=ERG_NBAzZ8Y&feature=emb_logo

## ACTIVITAT 1

Teniu 3 exercicis (A1-A, A1-B i A1-C) dins l'activitat Activitat 1 (full d'excel classroom), per a realitzar utitlitzant la funció SI en cadascun d'ells.

Us podeu ajudar del diferent material (tutorial i videotutorials que trobareu per la xarxa) a l'hora de reforçar l'aprenentatge adquirit durant la primera avaluació.

## 2. GIMP: EDICIÓ I TRACTAMENT D'IMATGE

Videotutorials per aprendre a preparar i utilitzar el programari lliure GIMP:

**2.1.** Instal·lar i personalitzar GIMP

https://www.youtube.com/watch?v=ZbLyASD_taU&feature=emb_logo

**2.2.** Obrir, guardar i exportar imatges en GIMP

https://www.youtube.com/watch?v=kxDL4UmxG5c&feature=emb_logo

**2.3.** Eines de pintura bàsiques

https://www.youtube.com/watch?v=O4Eo8QGV9To&feature=emb_logo

**2.4.** Eines i mètodes de selecció

https://www.youtube.com/watch?v=MTDNVwKuItw&feature=emb_logo

https://www.youtube.com/watch?v=ryW0pROGXQY&feature=emb_logo

## ACTIVITAT 2

Un cop finalitzada la visualització dels recursos didàctics corresponents (2.1, 2.2, 2.3 i 2.4), segueix les següents indicacions per a realitzar la tasca:

1. Descarrega la imatge Estrella.jpg (classroom)

2. Canvia el color de l'estrella del centre i el cercle que l'envolta RESPECTANT SEMPRE LA PEDRA, és a dir, que el color no tregui l'entramat (rugositat) d'aquesta.

   2.1. Fes la selecció mitjançant les eines i mètodes de selecció més adients.

   2.2. Per pintar-la, fes servir el menú de Colors/Acoloreix.

4. Després s'ha d'acabar de pintar les diferents geometries de la pedra (cercles, franges i fons) en diferents colors, utilitzant les eines i mètodes de selecció que creguis convenients. Per acolorir, menú Colors/Acoloreix.

5. Per finalitzar l'edició de la imatge utilitza un pinzell per firmar en el marge inferior dret amb el vostre nom.

6. Exporteu a JPG el fitxer en finalitzar l'edició amb el següent títol: A1_NOMCOGNOM_GIMP.jpg

7. Deseu en XCF el fitxer en finalitzar l'edició amb el següent títol: A1_NOMCOGNOM_GIMP.xcf

8. Envieu els fitxers JPG i XCF al professor per poder ser avaluat.

**3.1.** Eines de transformació i degradats

https://www.youtube.com/watch?v=ZQ55mmekkYQ&feature=emb_logo

https://www.youtube.com/watch?v=RYHPDPDKTD8&feature=emb_logo

**3.2.** Eines de text

https://www.youtube.com/watch?v=UchTWJTGFXM&feature=emb_logo

https://www.youtube.com/watch?v=yoY3_jaI69k&feature=emb_logo

https://www.youtube.com/watch?v=vyMNVE-_hzo&feature=emb_logo

**3.3.** Capes i filtres bàsics

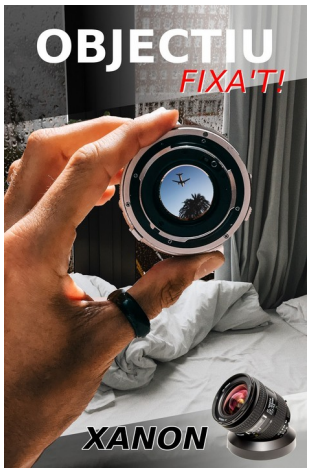
https://www.youtube.com/watch?v=y0s3Vt0LqdQ&feature=emb_logo

https://www.youtube.com/watch?v=g8bk9jmi0pc&feature=emb_logo

https://www.youtube.com/watch?v=vDPITeiuZxo&feature=emb_logo

## ACTIVITAT 3

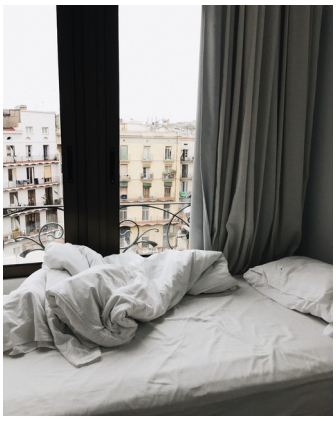
S'ha de realitzar el següent anunci publicitari per a una marquesina. Per a realitzar-ho s'han d'editar, transformar i distribuir en diferents capes un seguit d'imatges. Durant el procés s'utilitzaran diferents recursos i eines de selecció, transformació, text, gestió de les capes, degradats, etc.



S'han de crear ***12 CAPES*** en aquesta activitat distribuïdes en ***4 GRUPS*** de capes, aquests són:

*GRUP DE CAPES 1. FONS*

1. **CAPA 1.** Imatge de fons *finestra.jpg*.



   - Retallar la imatge utilitzant una eina de transformació per eliminar part del marge dret.
   - Retallar l'interior de la finestra mitjançant les eines de selecció i si cal els mètodes de selecció (Afegir canal alfa a la capa per deixar sense fons la imatge).

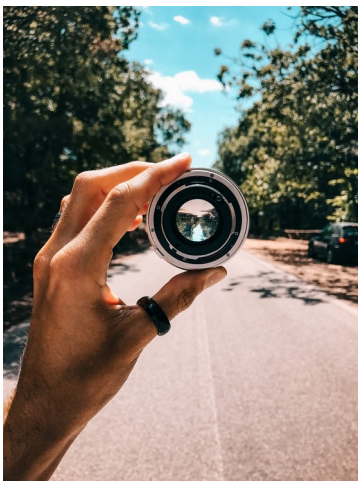
2. **CAPA 0.** Imatge *pluja.jpg*.

   - Ajustar la imatge pluja en l'interior de la finestra retallada.
   - Col·locar la capa amb anterioritat a la CAPA 1.

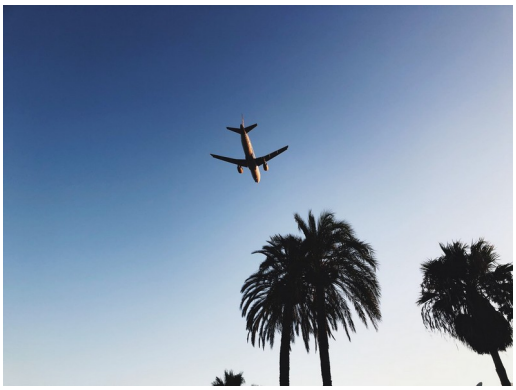
*GRUP DE CAPES 2. OBJECTIU*

3. **CAPA 3.** Imatge *mà.jpg*.

   - Seleccionar mitjançant l'eina i mètode de selecció més adient la mà i l'objectiu de la imatge i suprimir la resta.
   - Escalar la mà i l'objectiu a la imatge de fons.



4. **CAPA 2.** Imatge *avió.jpg*.
    - Col·locar la capa per sota la de la capa mà.
    - Escalar la imatge fins poder situar l'avió i part d'algunes palmeres en l'interior de l'objectiu.
    - Utilitzar l'eina de selecció el·lipse per a esborrar la resta de la imatge fora de l'objectiu.



*GRUP DE CAPES 3. ESLÒGAN*

5. **CAPA 4.** Crear una capa a la part superior del cartell amb un degradat.
6. **CAPA 5.** Introduir una capa de text amb el següent anunci: "OBJECTIU"
7. **CAPA 6.** Introduir una capa de text amb el següent anunci: "FIXA'T!"
8. **CAPA 7.** Aplicar un ombrejat al text "FIXA'T!" creant una nova capa.

*GRUP DE CAPES 4. MARCA*

9. **CAPA 8.** Crear una capa a la part inferior del cartell amb un degradat.
10. **CAPA 9.** Imatge *objectiu.jpg*.
    - Utilitza l'eina "Eina de selecció de regió contigua" per tal de eliminar el fons blanc.
    - Escala l'objectiu resultant per situar-lo en el marge inferior dret de l'anunci.
11. **CAPA 10.** Introduir una última capa de text amb la marca "INVENTADA" de l'objectiu.
12. **CAPA 11.** Aplicar un perfil al text de la marca creant una nova capa.

***REQUISITS ESPECÍFICS*** a complir:

- Cada capa o grup de capes ha de tenir el seu nom assignat i diferenciat en el diàleg de capes.
- En acabar: ***FITXER/ANOMENA I DESA*** el projecte amb el següent nom: **A2_NOMICOGNOM_GIMP.xcf**
- També: ***FITXER/ANOMENA I EXPORTA*** el projecte a **jpg** amb el següent nom: **A2_NOMICOGNOM_GIMP.jpg**
- ***Enviar al professor els arxius en finalitzar.***

BLOC 2. ORDINADORS, SISTEMES OPERATIUS I XARXES

# 4. MAQUINARI I PROGRAMARI DE L'ORDINADOR

## ACTIVITAT 4

**ELABORACIÓ D'UN PRESSUPOST A MIDA PER A UN ORDINADOR DE SOBRETAULA**

Agafant com a referència els continguts desenvolupats durant el curs, s'ha d'elaborar un **PRESSUPOST** a mida d'un ordinador de sobretaula per a un usuari fictici, tenint en compte les següents consideracions:

- És plantegen 2 perfils d'usuari amb diferents necessitats específiques de maquinari i programari.
- A elegir **1** únic perfil per a realitzar el pressupost.
- Elegir tots els components o perifèrics per satisfer les necessitats del perfil d'usuari elegit.
- Cada component ha d'anar acompanyat del seu nom, imatge, preu, enllaç de la pàgina web i amb la corresponent justificació d'elecció.
- JUSTIFICACIÓ: Tenint en compte criteris de compatibilitat, preu, adaptació al perfil.
- Per tenir en compte els diferents aspectes que pot haver a l'hora de triar els components disposem d'una guia perquè us pugueu orientar correctament i triar els components que siguin compatibles entre ells. Guia per comprar un ordinador
- Botigues en línia on podeu consultar els components, encara que es pot triar altres llocs web: AppInformàtica, https://cat.beep.es/, ...

**Perfil 1:** Dissenyador gràfic amb les següents necessitats específiques en maquinari (tauleta gràfica, tauleta digital, impressora, escàner d'alta qualitat, webcam) i en programari (Gimp, Inkscape, scribus, libreoffice, foxit reader).

**Perfil 2:** Dissenyador industrial amb les següents necessitats específiques en maquinari (doble pantalla, ratolí 3D, Impressora 3D, impressora A3, webcam) i en programari (Solidworks, CATIA, FreeCAD, Cura 4.5, Inkscape).

P.D. El pressupost ha d'incloure tot component i programari ben referenciat i el preu final amb IVA.

BLOC 4. SEGURETAT INFORMÀTICA

# 5. CIBERSEGURETAT

## ACTIVITAT 5

Tria una de les paraules que apareixen en el glossari del document "glossari_ciberseguretat_yomo.pdf" en el material didàctic "5. CIBERSEGURETAT"

Una vegada triada, realitza un vídeo on expliquis el concepte amb les teves pròpies paraules, recomanacions i conclusions.

El vídeo ha de tenir una durada mínima de 1:30 min i màxima de 2:00 min i ha de gravar-se en posició horitzontal. Recorda fer un guió previ.

Una vegada realitzat el vídeo, guarda'l i envia-ho al professor.

# 6. ANTIVIRUS, TALLAFOCS I ANTIESPIES

## SEGURETAT D'UN SISTEMA INFORMÀTIC

POLÍTIQUES DE SEGURETAT

La política de seguretat d'un sistema informàtic és el conjunt de normes i procediments que defineixen les diferents formes d'actuació recomanades, per tal de garantir un cert grau de seguretat.

És impossible parlar de sistemes 100% segurs perquè, entre altres aspectes, el cost de seguretat total és molt alt. Per aquesta raó, moltes empreses, a més d'utilitzar eines de seguretat, creen plans d'acció en les seves polítiques de seguretat, amb el propòsit de conscienciar cada un dels membres de l'organització sobre la importància i la sensibilitat de la informació, ja que una de les peces clau per preservar la seguretat d'una empresa són les actuacions dels seus empleats.

SOLUCIONS ANTIVIRUS

Un antivirus és un programari que té com a finalitat prevenir, detectar i eliminar virus, programari maliciós i altres atacs al sistema. Resideix a la memòria, analitzant constantment els arxius executats, els correus entrants, les pàgines visitades, les memòries USB introduïdes, etc. En cas d'amenaça, els antivirus mostren un missatge a l'usuari amb les possibles accions a realitzar, els antivirus actualitzen constantment les seves definicions de virus incloent noves amenaces que van apareixent; per aquesta raó, és imprescindible que estiguin instal·lats en equips amb connexió a internet.

Disposem de diferents antivirus, els més populars són els programes que instal·lem per controlar les intrusions, però també existeixen antivirus en línia. Els més populars són: Avast, Avira, Bitdefender, ESET, GData, karspesky, McAfee Norton.

SÍMPTOMES D'UNA INFECCIÓ

- Alentiment de l'equip durant l'arrencada, el funcionament o la connexió a internet.
- Desaparició de carpetes o arxius, o distorsió dels seus continguts.
- Aparició de publicitat, missatges d'error o sons no habituals.
- Moviment automàtic del ratolí, dels menús o de les finestres.
- Errors o comportaments estranys en les aplicacions i els dispositius.
- Intents de connexió a Internet inesperats o redireccionaments no desitjats.
- Segrest de la pàgina d'inici del navegador i canvi del cercador predeterminat.
- Aparició de barres d'eines estranyes al navegador web.
- Enviament de correus electrònics o de missatges als contactes d'una llista.
- Augment de l'activitat en l'equip i del trànsit a la xarxa.

PASSOS QUE S'HAN DE SEGUIR EN CAS D'INFECCIÓ

Quan s'ha detectat una infecció o hi ha una sospita raonable que pugui haver-la, és possible adoptar les següents mesures:

- **Restaurar el sistema a un estat anterior:** Alguns sistemes operatius, com Windows, creen punts de restauració periòdicament permetent retornar l'equip a un estat segur anterior sense que es perdi informació.
- **Actualitzar la base de dades del antivirus i realitzar un anàlisis complet de l'equip:** En cas que no es detecti o s'elimini el malware, es pot optar per utilitzar aplicacions d'altres fabricants o per realitzar una anàlisi en línia.
- **Engegar l'equip amb un Live CD o Live USB.** Aquesta opció permet:
    - Analitzar l'equip amb un antivirus sense contaminar, ja que l'instal·lat podria estar infectat.
    - Extreure els arxius per recuperar la informació en cas que el sistema operatiu de l'equip hagi estat danyat i no permeti iniciar el sistema.
- **Executar utilitats de desinfecció específiques, que actuen com antídots de virus o eliminen amenaces concretes.**
- **MOLT IMPORTANT: EN CAS D'INFECCIÓ NO INTRODUIR DADES PERSONALS I ESTAR DESCONNECTAT DE LA XARXA A LA MESURA DEL POSSIBLE.**

## NAVEGACIÓ SEGURA

BONES PRÀCTIQUES DE NAVEGACIÓ

- **Configura el navegador adequadament:** El navegador permet configurar diferents nivells de seguretat, el que possibilita, entre altres opcions, fer servir filtres contra la suplantació de la identitat, bloquejar elements emergents i activar el control parental per a la protecció de menors. Tot i així, és recomanable eliminar periòdicament la informació que s'emmagatzema en l'historial i en la memòria cau.
- **No accedir a llocs web de dubtosa reputació i evitar enllaços sospitosos.**
- **Acceptar únicament les galetes desitjades.**
- **Protegir les dades personals:** No s'han de facilitar dades personals, com el nom, cognoms, adreça, número de targeta de crèdit en aquelles pàgines que NO siguin de total confiança.
- **Descarregar aplicacions de llocs web oficials.**
- **Revisar el correu electrònic.**
- **Actualitzar sistema operatiu i aplicacions:** Els ciberatacants utilitzen les vulnerabilitats detectades en els programes informàtics per llançar els seus atacs.

NAVEGACIÓ PRIVADA

La navegació privada és una mesura de privacitat perquè el navegador no emmagatzemi la informació que es genera en relació amb la navegació, per activar-la, cal utilitzar l'opció **Nova finestra d'incògnit, Navegació privada o Navegació InPrivate, en funció del navegador.**

PROTEGIR LA PRIVACITAT A LA XARXA AMB UN SERVIDOR INTERMEDIARI

Els servidors intermediaris actuen com a intermediaris entre els equips dels usuaris i els llocs web que visiten. L'usuari accedeix al proxy i utilitza el seu cercador per navegar per internet. D'aquesta manera, les pàgines visitades només poden captar dades del servidor intermediari, però no de l'usuari.

**PRIVACITAT DE LA INFORMACIÓ**

Es considera informació privada, tota aquella informació protegida per la LOPD (Llei Orgànica de Protecció de Dades) o aquella que altres usuaris o entitats no desitgen que sigui coneguda (llocs visitats, corre electrònic, etc.).

AMENACES A LA PRIVACITAT

- **Sistemes operatius:** La majoria de dispositius que es connecten a Internet utilitzen un sistema operatiu que, per funcionar, reuneix la informació confidencial de l'usuari, com les seves dades d'identificació biomètrica, el seu idioma, la seva ubicació, les seves recerques habituals... Els atacants podrien aprofitar alguna vulnerabilitat en aquest programari per obtenir totes aquestes dades.
- **Contrasenyes:** El mètode més estès per a la identificació dels usuaris és l'ús de contrasenyes. Per evitar que altres usuaris aconsegueixin apoderar d'aquesta informació secreta, és important utilitzar autenticacions biomètriques o, si no, generar contrasenyes fortes, amb diferents tipus de caràcters i amb una longitud mínima de vuit caràcters.
- **Registre de visites web:** Cada vegada que accedeixes a una pàgina web, el navegador proporciona dades sobre el navegador, el sistema operatiu, els dispositius, l'adreça IP, etc. Aquestes dades poden ser utilitzades fraudulentament per obtenir informació dels usuaris i llançar ciberatacs.
- **Sessions del navegador:** Alguns navegadors permeten gestionar l'historial o les adreces d'interès des de qualsevol lloc. En alguns casos, com a **Google Chrome**, la sessió oberta encara que l'usuari tanqui la aplicació.
- **Cookies:** Alguns llocs web utilitzen cookies per obtenir informació sobre els hàbits de navegació de l'usuari o les seves dades personals, per a realitzar seguiments de compres en línia, etc. En la majoria de casos, aquesta informació s'utilitza per a fins publicitaris, encara que, en altres ocasions, les galetes poden ser manipulades amb intencions fraudulentes.
- **Formularis:** El web 2.0 ofereix multitud de serveis en línia, que, en la majoria de casos, requereixen que l'usuari es registri a través d'un formulari. En cas de contenir camps amb informació confidencial, cal verificar la legitimitat del lloc. Una bona estratègia és corroborar el domini i l'ús del protocol HTTPS.
- **Xarxes socials:** Les publicacions en xarxes socials, com Instagram, Twitter, o Facebook, amaguen més perills del que la majoria d'usuaris sospiten. Per als ciberatacants, les xarxes socials constitueixen un mètode senzill i ràpid amb el qual accedir a tot el tipus d'informació personal (fotografies, vídeos, dades personals...).
- **Google:** La principal font d'ingressos de Google està relacionada amb la publicitat adaptada als gustos i necessitats de l'usuari. Aquesta multinacional ofereix gran part dels serveis que s'utilitzen habitualment a Internet en les seves diferents aplicacions (Chrome, maps, Picasa, Youtube, Store, Google+, Books, etc.) pel que és capaç de reunir una gran quantitat d'informació sobre cadascun dels seus usuaris. Una mesura de protecció consisteixen en configurar les opcions de privacitat dels serveis de Google.

ANTIESPÍES

L'espionatge es defineix com l'obtenció encoberta de dades o d'informació confidencial. Per fer-ho, s'utilitzen diverses tècniques per tal d'obtenir informació confidencial o privada, pràctica que es considera un delicte i que està penada per la llei.

Els programes espies o spyware s'introdueixen en els dispositius en forma de petites aplicacions que recopilen informació del sistema dels usuaris per enviar-la als ciberatacants.

Els programes anti-espia funcionen de manera similar als antivirus, a saber: comparen els arxius analitzats amb una base de dades de programari espia. Algunes de les aplicacions anti-espies més populars són: **CCleaner**, **ad-Aware**, **Windows Defensar**, **Malwarebytes** i **SpyBot**.

**PROTECCIÓ DE LES CONNEXIONS EN XARXA**

TALLAFOCS

Anomenat Firewall, és un dispositius maquinari o programari en que la finalitat és controlar la comunicació entre un equip i la xarxa, el qual s'ha convertit en una de les principals defenses contra atacs informàtics i una peça clau per bloquejar la sortida d'informació de l'ordinador a Internet. L'origen del terme té a veure amb la seguretat industrial, on s'utilitzaven parets gruixudes amb càmeres d'aire en aquells llocs amb perill d'incendi per aïllar ràpidament els espais i minimitzar els danys.

Tots els missatges que entren o surten pel tallafocs són examinats, de manera que aquells que no compleixen els criteris de seguretat especificats són bloquejats, amb el propòsit d'evitar els atacs d'intrusos, els accessos d'empleats a llocs no autoritzats, la descàrrega de programari nociu o que els equips infectats de malware enviïn dades sense autorització fora de la xarxa.

El tallafocs s'instal·len al dispositiu que dona accés a Internet, que sol ser un servidor o un router. Els sistemes operatius i les solucions antivirus solen incloure el seu propi tallafocs, encara que és possible instal·lar eines específiques com **ZoneAlarm**, **Outpost** o **Comodo**.

- Els ports del 0 al 1023 estan assignats als protocols coneguts i més utilitzats, com **FTP (21), SMTP (25) HTTP (80) HTTPS (443), POP3 (110) etc**.
- Els ports compresos entre el **1024** i el **49151** estan registrats i poden ser usats per qualsevol aplicació.
- Els ports del 49152 al 65535 són dinàmics o privats i s'utilitzen habitualment en connexions P2P.

XARXES PRIVADES VIRTUALS

Són connexions punt a punt a través d'una xarxa privada o pública insegura, com Internet. Els clients usen protocols basats en TCP / IP, denominats protocols de túnel, per realitzar connexions amb una xarxa privada. Una vegada que el servidor VPN autentifica l'usuari, s'estableix una connexió xifrada. Hi ha dos tipus de connexions en aquest tipus de xarxes:

- **VPN d'accés remot:** S'utilitzen perquè el usuaris tinguin accés a un servidor d'una xarxa privada amb la infraestructura proporcionada per una xarxa pública. És el cas de les persones que treballen a

distància, dels alumnes que accedeixen a la xarxa d'una universitat o dels usuaris que desitgen obtenir una connexió segura des de llocs públics (**Dropbox, Google Drive, TeamViewer**...).

- **VPN de lloc a lloc:** Permeten a les organitzacions connectar xarxes a través d'Internet utilitzant comunicacions entre elles. Alguns exemples de les seves aplicacions són la connexió entre oficines, sucursals, empreses o administracions públiques.

CERTIFICATS SSL/TLS DE SERVIDOR WEB I HTTPS

El SSL (**secure sockets layer**) és un protocol criptogràfic desenvolupat per Netscape fins a la versió 3.0, quan va ser estandarditzat i va passar a denominar-se TLS (transport layer security). No obstant això, avui dia el terme SSL està molt estès, per la qual cosa es sol al·ludir a tots dos indistintament.

Aquests estàndards s'utilitzen per **emetre certificats de llocs web**, de manera **que són una peça fonamental en la seguretat, ja que garanteixen la integritat i la confidencialitat de les comunicacions.**

Quan s'utilitza el xifrat basat en **SSL/TLS** al costat del protocol de navegació web HTTP, es crea un canal xifrat segur denominat HTTPS. Aquest canal fa servir una clau de 128 bits de longitud que només coneixen el servidor i el dispositiu connectat, de manera que encripta les dades transmeses.

## ACTIVITAT 6

En un document de text, defineix les funcions principals dels antivirus, tallafocs (o Firewall) i l'antiespia.

Adjunta-hi les següents captures de pantalla:

1. Anàlisi finalitzat de l'antivirus que tinguis instal·lat en el teu equip (Si no en tens cap, descarrega i instal·la'n un de gratuït com: AVG o AVAST).

2.- Configuració del tallafocs del teu equip (Generalment els sistemes operatius en tenen un d'integrat, si ho consideres, pots descarregar-ne i instal·lar-ne un de gratuït com: comodo o mudu).

3.- Anàlisis finalitzat d'un antiespia que tinguis instal·lat en el teu equip (Si no en tens cap, pots descarregar un antiespia gratuït com: ad-aware).

Un cop finalitzada l'activitat envia l'arxiu al professor.