1. Definició de gestor de passwords

Bàsicament, un gestor de contrasenyes és una aplicació de programari que s'utilitza per emmagatzemar i gestionar les contrasenyes que té un usuari per a diversos comptes en línia i funcions de seguretat. Aquests emmagatzemen les contrasenyes en un format xifrat i proporcionen accés segur a tota la informació de la contrasenya amb l'ajuda d'una contrasenya mestra.

Els gestors de contrasenyes existeixen com a aplicació per a telèfons intel·ligents o d'escriptori o com a extensió del navegador que omple automàticament el nom d'usuari i la contrasenya als llocs desats. Gairebé tots els gestors de contrassenyes utilitzen l'autenticació de dos factors (2FA), que requereix que els usuaris confirmin el seu inici de sessió mitjançant dos mètodes diferents, com ara una contrasenya i un codi enviat a un dispositiu.

Hi ha molts tipus de gestors de contrasenyes, que es diferencien en la forma en què xifren la informació, el tipus d'emmagatzematge i les funcions addicionals proporcionades. Segons les nostres necessitats, escollirem un tipus de gestor o altre. Hi han tres tipologies diferents:

-Els gestors de contrasenyes basats en escriptori emmagatzemen les contrasenyes localment al dispositiu, com ara el vostre ordinador portàtil, en una caixa de seguretat xifrada.
-Els gestors de contrasenyes basats en núvol emmagatzemen les vostres contrasenyes xifrades a la xarxa del proveïdor de serveis. El proveïdor de serveis és directament responsable de la seguretat de les nostres contrasenyes.
-Inici de autenticació única (SSO). A diferència d'un gestor de contrasenyes que emmagatzema contrasenyes úniques per a cada aplicació que utilitzeu, SSO us permet utilitzar una contrasenya per a cada aplicació.

2. Àmbit d'aplicació

En el nostre cas, disposem de diversos sistemes que requereixen contrasenya per a poder accedir al nostre compte (Correu electrònic, Discord, Amazon, Instagram, Facebook, Campus virtual UB, Spotify, Netflix, HBO…). Per tant, considerarem l'àmbit personal per a la realització d'aquesta activitat.

Com és evident, si volem garantir la seguretat en relació a les nostres contrasenyes, no podem utilitzar la mateixa per a tots els sistemes, hem de crear passwords únics i segurs per a l'autenticació en aquests sistemes. Això pot provocar que sigui molt complicat enrecordar-se de totes les contrasenyes que podem acabar utilitzant i que el fet de cercar-les (per exemple, si les apunten en una llibreta) pot acabar sent farragós localitzar cadascun dels passwords.

Precisament, aquesta problemàtica és la que dóna la principal necessitat de fer ús d'un gestió per a les nostres contrasenyes. En aquest sentit, un gestor ens pot ajudar a:

3. En què ens pot ajudar un gestor en el nostre cas?

Característiques generals:

- **Ja no cal que memoritzem totes les contrasenyes**. Només hem de recordar la contrasenya mestra que desbloqueja la caixa de contrasenyes. I si opteu per un gestor de contrasenyes basat en núvol, podem accedir a la vostra caixa de contrasenyes des de qualsevol lloc i des de qualsevol dispositiu.
- **Poden generar automàticament contrasenyes altament segures.** Normalment, els gestors de contrasenyes us demanaran si voleu utilitzar una contrasenya generada automàticament cada cop que creeu un compte nou amb un lloc web o una aplicació. Aquestes contrasenyes aleatòries són llargues, alfanumèriques i essencialment impossibles d'endevinar.
- **Poden avisar-nos d'un lloc de *phishing***. Aquí teniu un resum ràpid de les estafes de pesca. Els correus electrònics de correu brossa són falsificats o falsificats per semblar que provenen d'un remitent legítim, com ara un amic, un familiar, un company de feina o una organització amb la qual feu negocis. Els enllaços continguts al correu electrònic dirigeixen a llocs web maliciosos falsificats de manera similar dissenyats per recollir credencials d'inici de sessió. Si utilitzeu un gestor de contrasenyes basat en el navegador, no completarà automàticament els camps de nom d'usuari i contrasenya, ja que no reconeix el lloc web com el que està lligat a la contrasenya.

- **Poden ajudar els teus beneficiaris quan moris.** Això s'anomena herència digital. En cas de defunció, la vostra família o qui designeu per administrar el vostre patrimoni tindrà accés a la vostra caixa de contrasenyes.
- **Els gestors de contrasenyes estalvien temps**. Més enllà d'emmagatzemar contrasenyes per a tu, molts gestors de contrasenyes també omplen automàticament les credencials per accedir més ràpidament als comptes en línia. A més, alguns poden emmagatzemar i emplenar automàticament el nom, l'adreça, el correu electrònic, el número de telèfon i la informació de la targeta de crèdit. Això pot suposar un gran estalvi de temps quan compres en línia, per exemple.
- **Molts gestors de contrasenyes se sincronitzen amb diferents sistemes operatius**. Si sou un usuari de Windows a la feina i un usuari de Mac a casa, feu servir el vostre Android de dilluns a divendres i utilitzeu iOS els caps de setmana, podreu accedir ràpidament a les vostres contrasenyes independentment de la plataforma en què us trobeu. Idem per a tots els navegadors web més populars; és a dir, Chrome, Firefox, Edge, Internet Explorer i Safari.
- **Ajuden a protegir la teva identitat**. De manera indirecta, els gestors de contrasenyes ajuden a protegir-se del robatori d'identitat, i aquí teniu el perquè. En utilitzar una contrasenya única per a cada lloc, bàsicament esteu segmentant les vostres dades a cada lloc web i aplicació que utilitzeu. Si un criminal pirateja un dels vostres comptes, no necessàriament podrà accedir a cap dels altres. No és infal·lible, però és una capa addicional de seguretat que sens dubte apreciareu després d'una violació de dades.

4. Quins requisits hauría de tenir el gestor que necessitem?

Multiplataforma: Requerirem que el gestor de contrasenyes que utilitzem sigui multiplataforma, és a dir, que el poguem usar en diferents sistemes operatius com macOS, IOS, Windows o Android. I que, en la mesura del possible, també estigui disponible per navegadors com Firefox, Chrome o Edge. És un requisit important, ja que en l'ús personal és probable que tinguem diferents dispositius amb diferents sistemes operatius, per exemple, un ordenador Windows i una tableta MAC. També en l'àmbit estudiantil, segurament, utilitzarem dispositius que no siguin els nostres, per tant, necessitarem que pugui encaixar en el màxim nombre per no quedar-nos penjats en ninguna ocasió.

Multidispositiu i dispositius il·limitats: És important que el gestor que utilitzem no estigui limitat només a un dispositiu, i estigui disponible a un nombre ilimitat d'ells. Actualment fem servir aplicacions, com podria ser el campus virtual o xarxes socials, en diferents dispositius com el telefòn mòbil i l'ordinador o diferents ordinadors, per tant que el gestor que adquirim gaudeixi d'aquesta funcionalitat és imprescindible.

Català o Castellà: Les llengues que utilitzem diàriament de forma social o escolar en el web són el català i el castellà, per comoditat i fluidesa necessitarem que el nostre gestor de contrasenyes estigui disponible en una d'aquestes dues llengües.

Basat en el núvol: Un gestor de contrasenyes basat en el núvol significa que emmagatzemen les contrasenyes xifrades a la xarxa del proveïdor de serveis. El principal avantatge dels gestors de contrasenyes basats en núvol, és que podeu accedir a la vostra caixa de contrasenyes des de qualsevol dispositiu sempre que tingueu una connexió a Internet. Així no depenem d'una aplicació externa que hauríem de descarregar en cada dispositiu, tot i que també, poden presentar-se en diferents formes, més habitualment com a extensió del navegador, aplicació d'escriptori o aplicació mòbil.

Facilitat d'ús (Interfície amigable): Ens serà de molta utilitat que el gestor de contrasenyes tingui una interfície amigable, és a dir, de fàcil ús i que hi hagi una bona portabilitat cap a altres dispositius. Necessitarem aquesta facilitat d'ús, ja que a l'hora de controlar varies contrasenyes requerirem d'una interfície on la qual puguem ubicar de forma directe quines són les contrasenyes en cada portal.

5. Cercar quins són els gestors que més s'adapten a les nostres necessitats. Justificació de la tria.

   Bitwarden: és un gestor de contrasenyes potent i flexible, amb la capacitat no només d'emmagatzemar contrasenyes bàsiques, sinó també contrasenyes d'una sola vegada (dos factors), elements que no són contrasenyes (com ara targetes de crèdit i documents d'identificació) i notes segures. Bitwarden té extensions de navegador per a tots els grans navegadors (Chrome, Firefox, Safari, etc.) que funcionen molt bé, permetent no només introduir contrasenyes de manera automàtica als llocs web, sinó generar automàticament contrasenyes i emmagatzemar-les directament a Bitwarden.

   A més, Bitwarden ofereix tant un nivell gratuït, amb un conjunt de funcions menor (específicament en no permetre l'emmagatzematge de contrasenyes d'un sol ús) com un nivell de subscripció extremadament econòmic (10 dòlars anuals). Finalment, de manera predeterminada, totes les contrasenyes

s'emmagatzemen al núvol de Bitwarden (cosa que ens interessa per al nostre àmbit d'aplicació) amb una sincronització fàcil de configurar entre tots dispositius; tanmateix, si no ens trobéssim còmodes amb emmagatzemar totes les vostres contrasenyes al núvol, Bitwarden ofereix una potent opció d'allotjament automàtic (tot i que és difícil de configurar). Disposa de "Single Sign On" o inici de sessió únic. Com que és un gestor de contrasenyes de codi obert, Bitwarden es considera extremadament segur: milers d'experts en seguretat de tot el món han revisat de manera independent cada fragment del seu codi font.

Lastpass: Molt senzill i fàcil de configurar i desplegar. L'extensió del navegador i les aplicacions del telèfon fan que l'ús de LastPass sigui una manera fàcil perquè la majoria de la gent tingui accés segur a totes les contrasenyes des de qualsevol dispositiu que puguin utilitzar, les opcions d'emplenament automàtic acabaran fent que l'entrada de contrasenyes úniques segures sigui més fàcil que escriure manualment una contrasenya. Omple automàticament el nom d'usuari/contrasenya a la majoria de llocs d'Internet. LastPass també proporciona una comprovació de contrasenyes per revisar totes les teves contrasenyes i dir-te quantes són antigues, si s'han compromès (llocs piratejats públics on has introduït la contrasenya), s'utilitzen en diversos llocs, etc. Reps un avís al correu que una combinació de correu electrònic/contrasenya estava compromès. Et dona la opció canviar-la per a aquest lloc, verificar quins altres llocs també utilitzen aquesta contrasenya (cosa que no hauríem de fer) i canviar-la per ser més segur i evitar que els pirates informàtics entrin als nostres llocs, ens robin la identitat, etc. També ofereix una versió gratuïta i "Single Sign On" (SSO)

LogMeOnce: La pantalla d'inici de sessió de LogMeOnce ofereix diverses opcions diferents per accedir al vostre compte, com ara l'inici de sessió amb fotos, reconeixement facial, empremta digital, PIN i una contrasenya tradicional, que us ofereix moltes opcions per trobar un equilibri entre facilitat d'ús i seguretat. Doble factor d'autentificació (2FA) també és una opció, així com el reconeixement facial i els inicis de sessió biomètrics en dispositius mòbils. Aquestes opcions i un nivell de xifratge de 256 bits fan que sigui increïblement difícil que els usuaris no autoritzats accedeixin al vostre compte. El sistema de seguretat propietari té moltes patents pendents, cosa que deixa clar que l'empresa ha posat moltes investigacions originals en el desenvolupament del programari. La versió mòbil del programa també us demana un PIN, que es pot restablir (tot i que és un procés bastant complicat, a la pràctica). LogMeOnce permet emmagatzemar les contrasenyes a l'ordinador o utilitzar la seva còpia de seguretat al núvol. És molt recomanable la còpia de seguretat al núvol, ja que permet accedir al nostre compte des de qualsevol dispositiu mitjançant les credencials d'inici de sessió del vostre gestor de contrasenyes, però podeu canviar entre les dues utilitzant l'opció

"Configuració" a la qual s'accedeix a través de la icona "Menú intel·ligent" a la pantalla d'inici.

	Bitwarden	LastPass	LogMeOnce
Còpia de seguretat al núvol	Sí	Sí	Sí
Codi Obert	Sí	No	No
Single Sign On	Sí	Sí	Sí
2FA	Sí	Sí	Sí
Emmagatzematge de dades xifrat	Sí	Sí	Sí
Preus mínims	3$ al mes	48$ a l'any	3$ al mes
Versió gratuïta	Sí	Sí	No
Prova gratuïta	Sí	Sí	Sí
Gestió de privilegis dels comptes	Sí	No	No
Atenció a l'usuari	Email/FAQs	Email/FAQs/Assistència telefònica/Xat	Email/Xat
Arquitectura de coneixement zero	Sí	Sí	Sí
Biometria	Sí	Sí	Sí
Múltiples comptes d'usuari	No	Sí	Sí
Seguretat SSL	Sí	No	Sí
Autoritzacions basades en rols	Sí	Sí	Sí
Emmagatzematge de contrassenyes ilimitat	Sí	Sí	No
Sincronització multi-dispositiu	Sí	Sí	Sí
Billetera digital (per guardar targetes de crèdit i	Sí	Sí	No

comptes bancaris)			
Canviador automàtic de contrassenyes	No	Sí	No
Mugshot	No	No	Sí
Català o Castellà	Si	Si	Si

6. Després de la comparació, seleccionar només 1, i justificació de la tria.

LastPass, LogMeOnce i Bitwarden tenen una seguretat excel·lent. Tanmateix, en quant a seguretat informàtica, Bitwarden té un lleuger avantatge perquè és de codi obert, ofereix emmagatzematge de dades local i mai ha estat piratejat. No obstant, LastPass és compatible amb més aplicacions d'autenticació TOTP que Bitwarden, i el seu autenticador integrat és molt més còmode que el de Bitwarden.
LastPass, Bitwarden i LogMeOnce ofereixen bàsicament les mateixes funcionalitats bàsiques de gestió de contrasenyes. Tot i que Bitwarden té una extensió per a més navegadors i pot generar contrasenyes una mica més llargues, LastPass és molt millor en tots els aspectes essencials, com ara la importació, l'emmagatzematge automàtic i l'emplenament automàtic de contrasenyes.
Tant LastPass com Bitwarden tenen excel·lents eines d'auditoria de contrasenyes i inclouen 1 GB d'emmagatzematge encriptat, la nova funció d'intercanvi de contrasenyes de Bitwarden és una mica més intuïtiva. Tanmateix, LastPass té diverses funcions addicionals que Bitwarden no ofereix, com ara una àmplia gamma d'opcions de recuperació del compte, accés d'emergència amb un període d'espera de fins a 30 dies i un canviador automàtic de contrasenyes.
Els plans gratuïts de LastPass i Bitwarden són dos dels millors del mercat: tots dos ofereixen emmagatzematge il·limitat de contrasenyes, sincronització entre diversos dispositius i fins i tot compartir contrasenyes un a un. Tanmateix, pel que fa al preu, Bitwarden és un clar guanyador, cobrant gairebé una quarta part del que cobra LastPass per una protecció similar. I Bitwarden ofereix més funcions al seu pla gratuït. LogMeOnce no és molt car i les eines que ofereix poden ser ben apreciades pels usuaris avançats i els usuaris empresarials, però possiblement el consumidor mitjà buscarà un altre gestor de contrassenyes, tot i tenir una funcionalitat única com el *Mugshot*[1].

Justificació de la tria

Per concloure, en termes de seguretat informàtica, Bitwarden és el millor per tot l'esmentat en l'apartat anterior, però LogMeOnce i LastPass són millors en termes de

[1] Ajustant la configuració a les preferències mitjançant el menú de la pantalla d'inici, permet que el dispositiu faci fotos d'intrusos, fent un seguiment de qualsevol intent d'inici de sessió desde dispositius desconeguts.

compatibilitat, usabilitat i atenció a l'usuari. Però com que estem en l'assignatura de Seguretat Informàtica, ens quedem amb Bitwarden.