CRIPTAREA HARDDISK-ULUI CU UTILITARUL WINDOWS BITLOCKER

- parte a masurilor de securitate in vederea GDPR -

Una dintre masurile care trebuie luate in vederea alinierii la GDPR este securizarea datelor care se afla pe statiile de lucru, laptopurile, tabletele sau serverele din firma.

De la bun inceput, mentionez ca acest tutorial se refera numai la device-urile pe care ruleaza sistemul de operare Microsoft Windows. Utilitare asemanatoare pentru criptare sunt disponibile si pentru MacOS, iOS, UNIX sau Android.

Eu am optat pentru folosirea utilitarului care se regaseste deja integrat in sistemul de operare, si anume ***BitLocker***. Acest utilitar este disponibil pentru Windows Professional, Windows Enterprise, Windows Server. Nu este disponibil pentru Windows Home Edition. Varianta de Windows pe care eu am lucrat este Windows 10 Professional, dar utilitarul este disponibil incepand cu Windows Vista. De asemenea, pentru toate operatiunile descrise mai jos sunt necesare drepturi de Administrator.

BitLocker este gratuit (dupa cum am mentionat vine preinstalat in Windows), algoritmul de criptare folosit este pe 128 sau 256 biti, iar criptarea se face hardware (daca device-ul este echipat cu ***Trusted Platform Module*** 1.2 minim – fig.1) sau software.

Acest tip de criptare face extrem de grea accesarea datelor de catre persoanele neautorizate, in caz de furt sau pierdere a device-ului, chiar si in eventualitatea conectarii hard-disk-ului la alt PC.

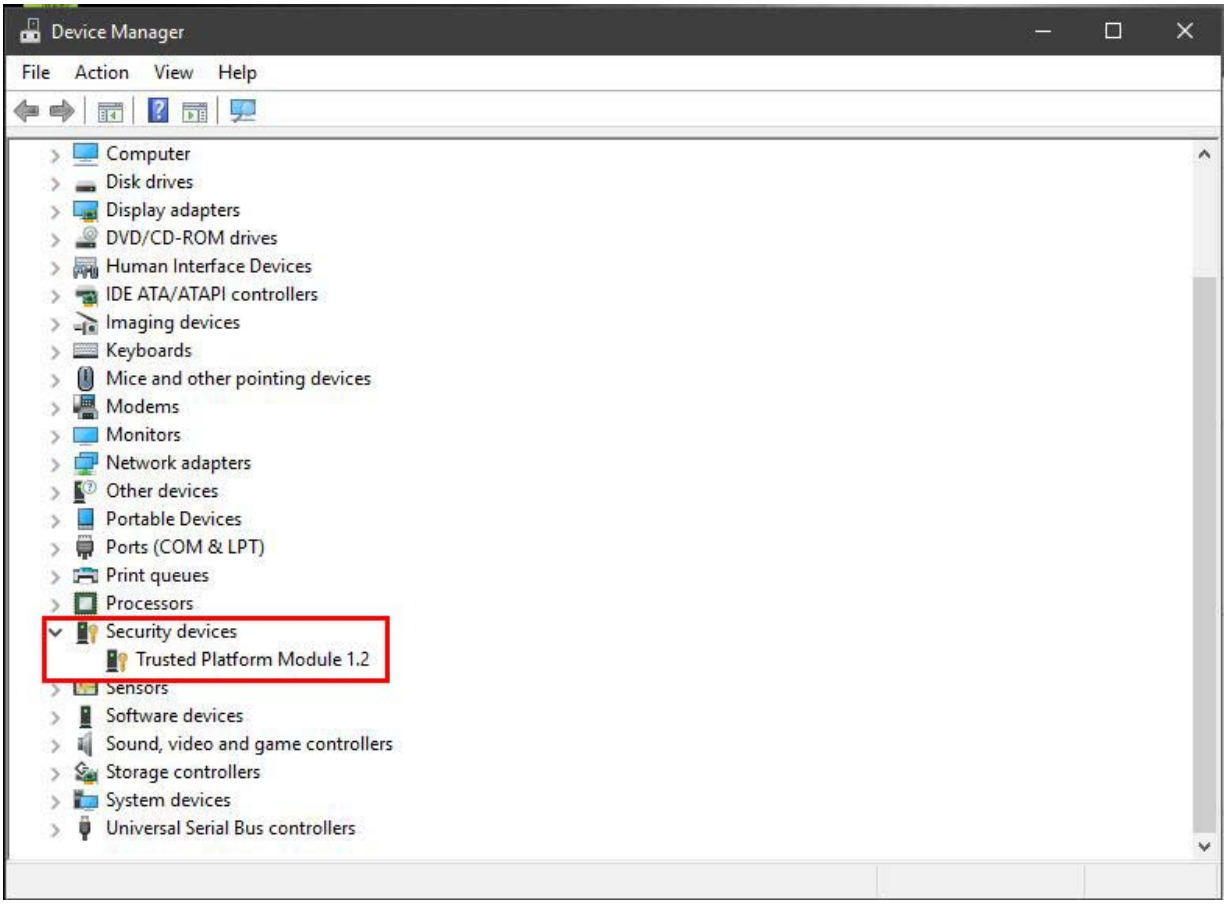

Figure 1

Inainte de inceperea criptarii, va trebui sa activati doua optiuni in ***Local Group Policy Editor***. Pentru aceasta apasati tastele Win + R, si scrieti ***gpedit.msc*** (fig.2).

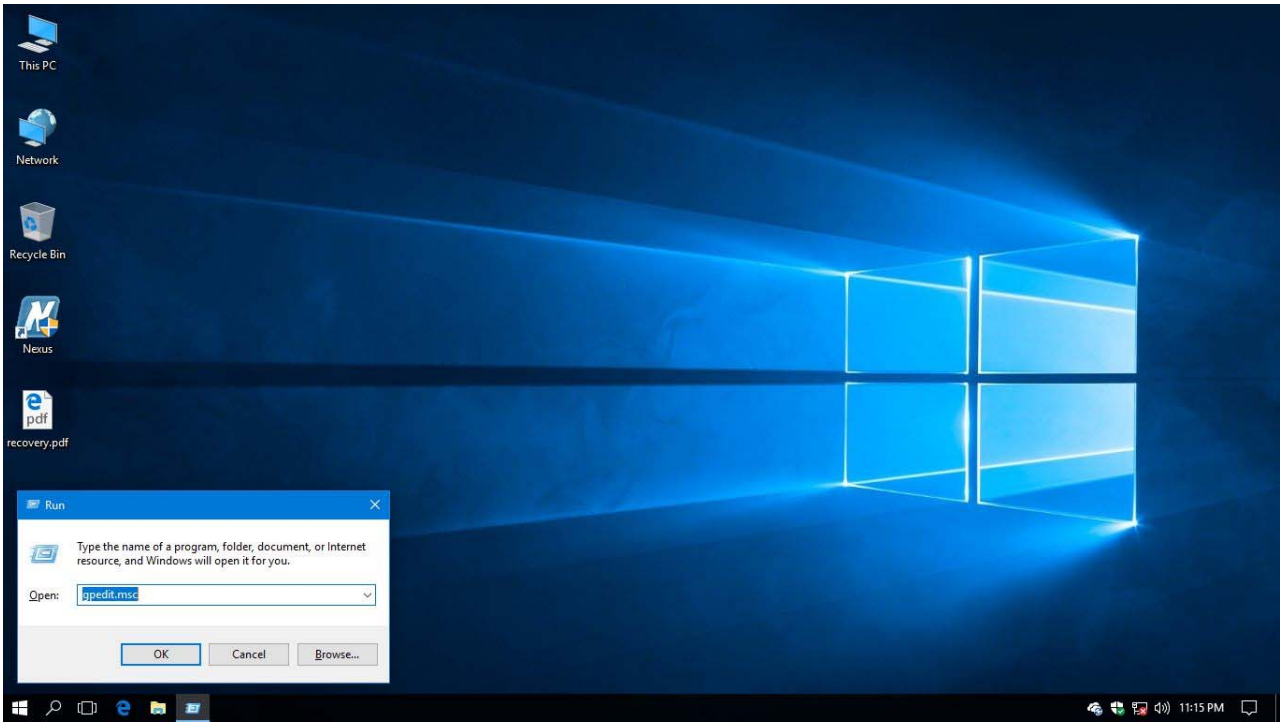

Figure 2

In ***Local Group Policy Editor***, navigati la ***Computer Configuration – Administrative Templates – Windows Components – BitLocker Drive Encryption – Operating System Drive***.

Aici trebuie sa setati ***Enable*** doua optiuni (fig.3):

1. ***Require additional authentification at startup***
2. ***Enable use of BitLocker authentification requiring preboot keyboard input on slates*** (fig.5)

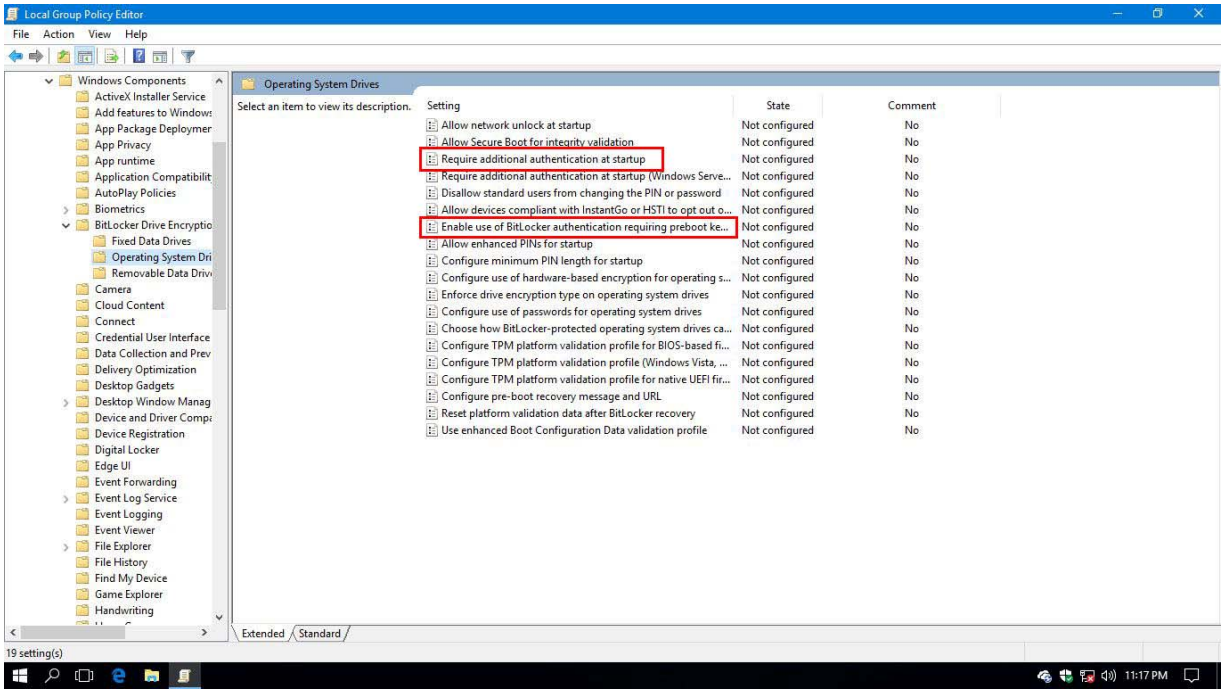

Figure 3

La optiunea nr.1, trebuie sa avem grija ca, odata bifat ***Enable***, sa fie bifat si ***Allow BitLocker without a compatible TPM*** (aceasta bifa este necesara in cazul in care sistemul nu este prevazut cu un modul de criptare hardware) (fig.4)

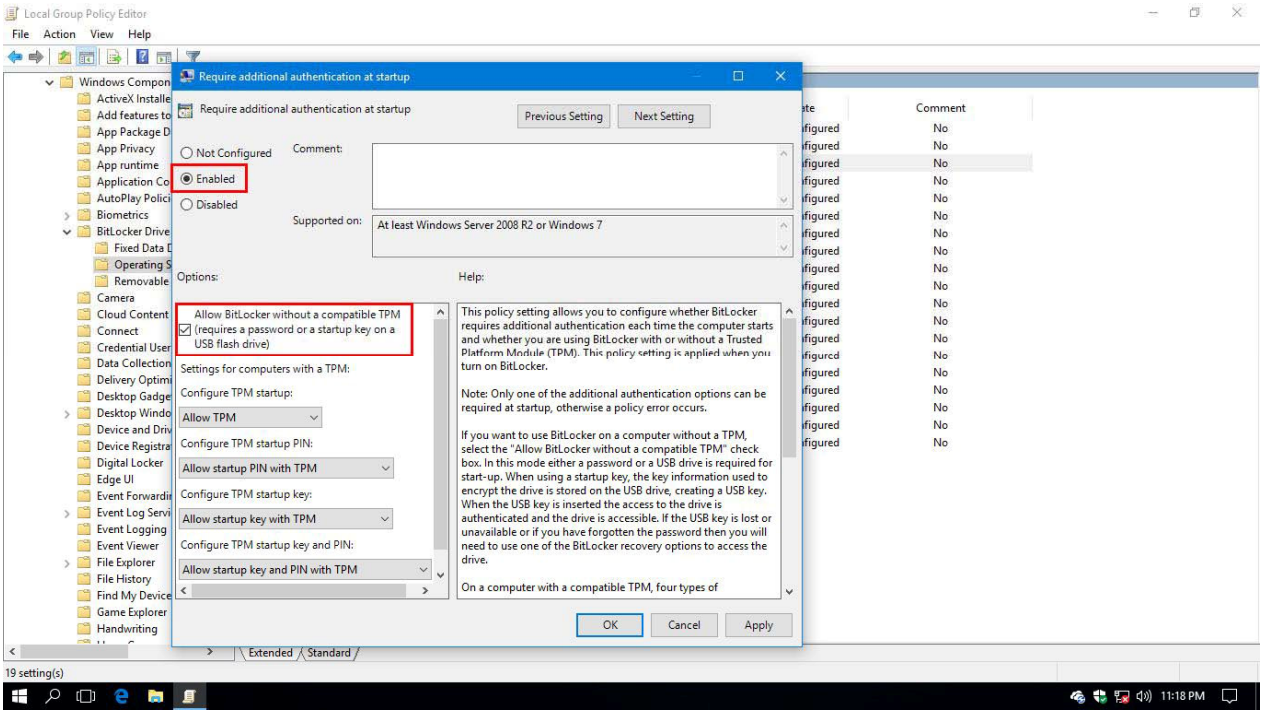

Figure 4

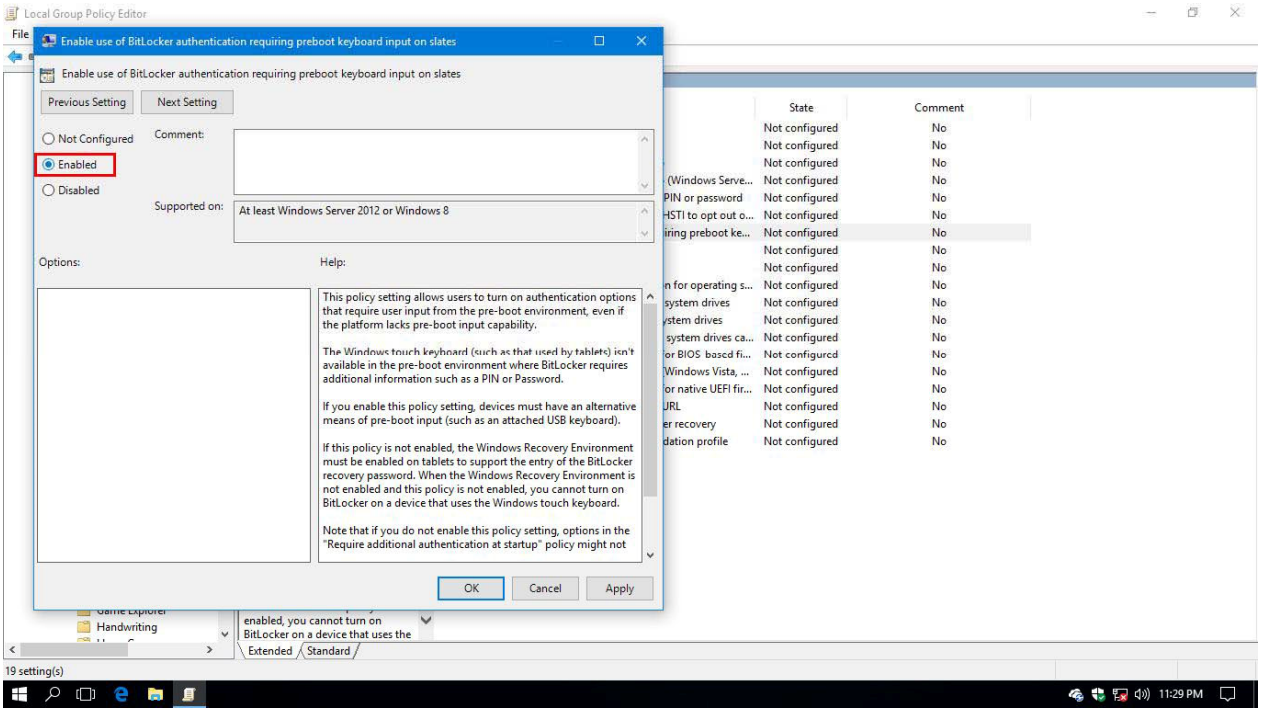

Figure 5

Odata facute aceste setari, se poate incepe criptarea hard-disk-ului.

Pentru aceasta, vom deschide ***This PC***, click dreapta pe drive-ul C, iar din meniul derulant vom selecta ***Turn On BitLocker*** (fig.6).

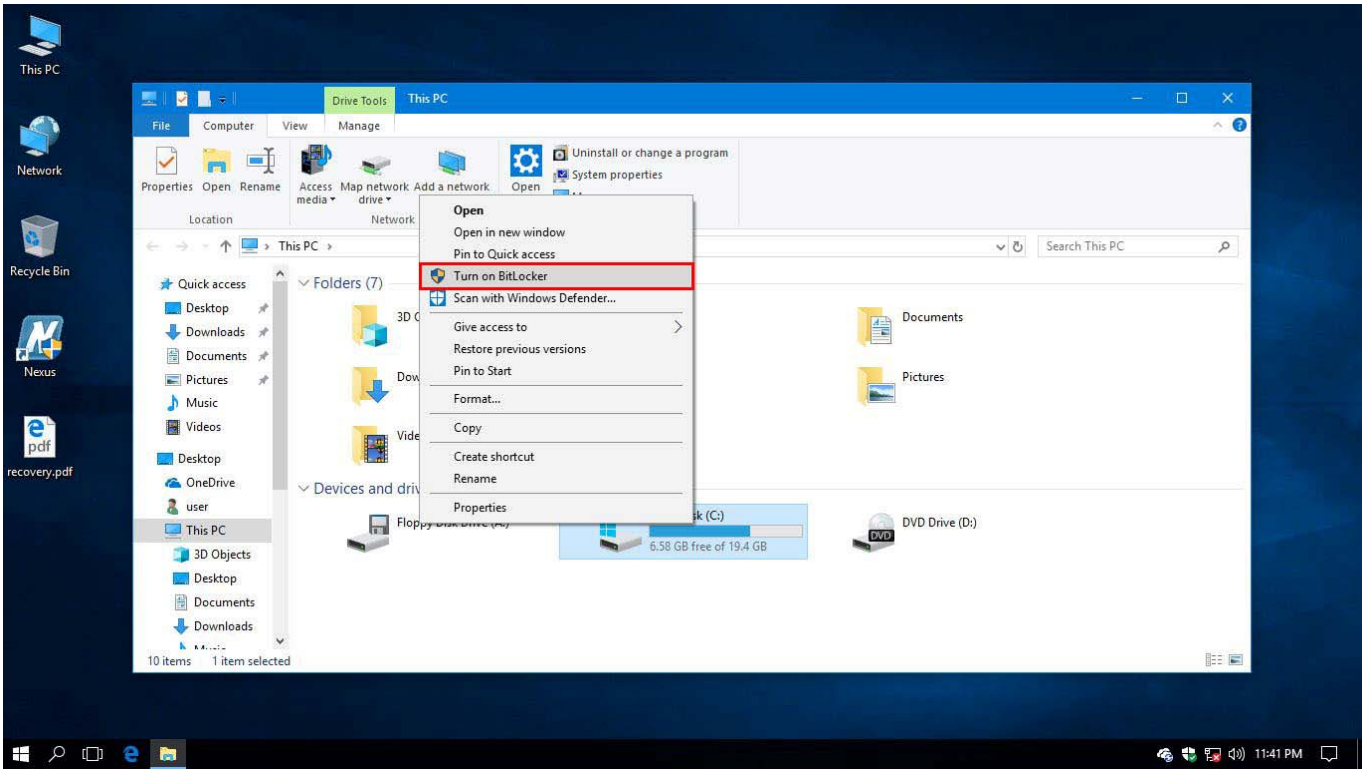

Figure 6

In continuare, se vor urma instructiunile pentru introducerea unei parole sau a unui PIN (fig. 7 si 8) si modalitatea de stocare a backup-ului parolei. Aici, eu am ales varianta printarii, dar puteti alege oricare dintre optiuni, in functie de preferinte (fig.9)

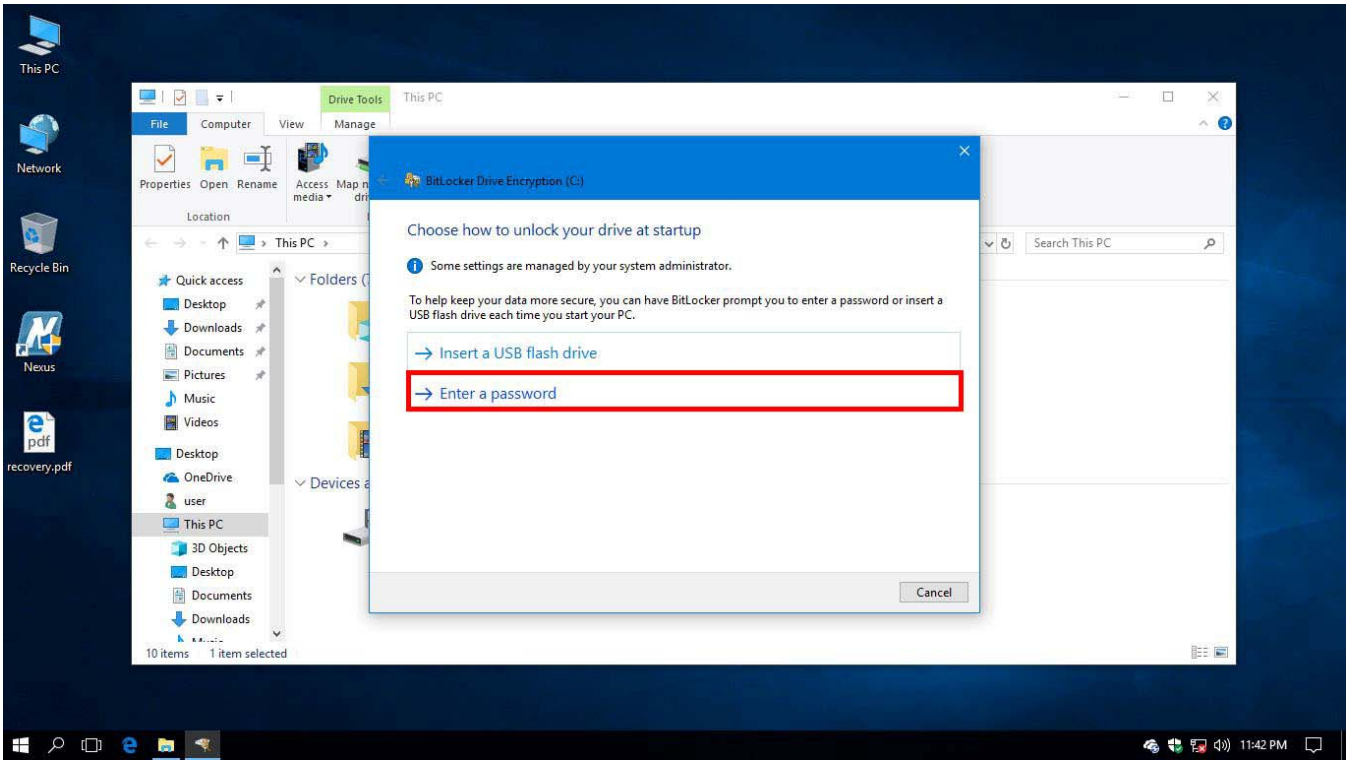

Figure 7

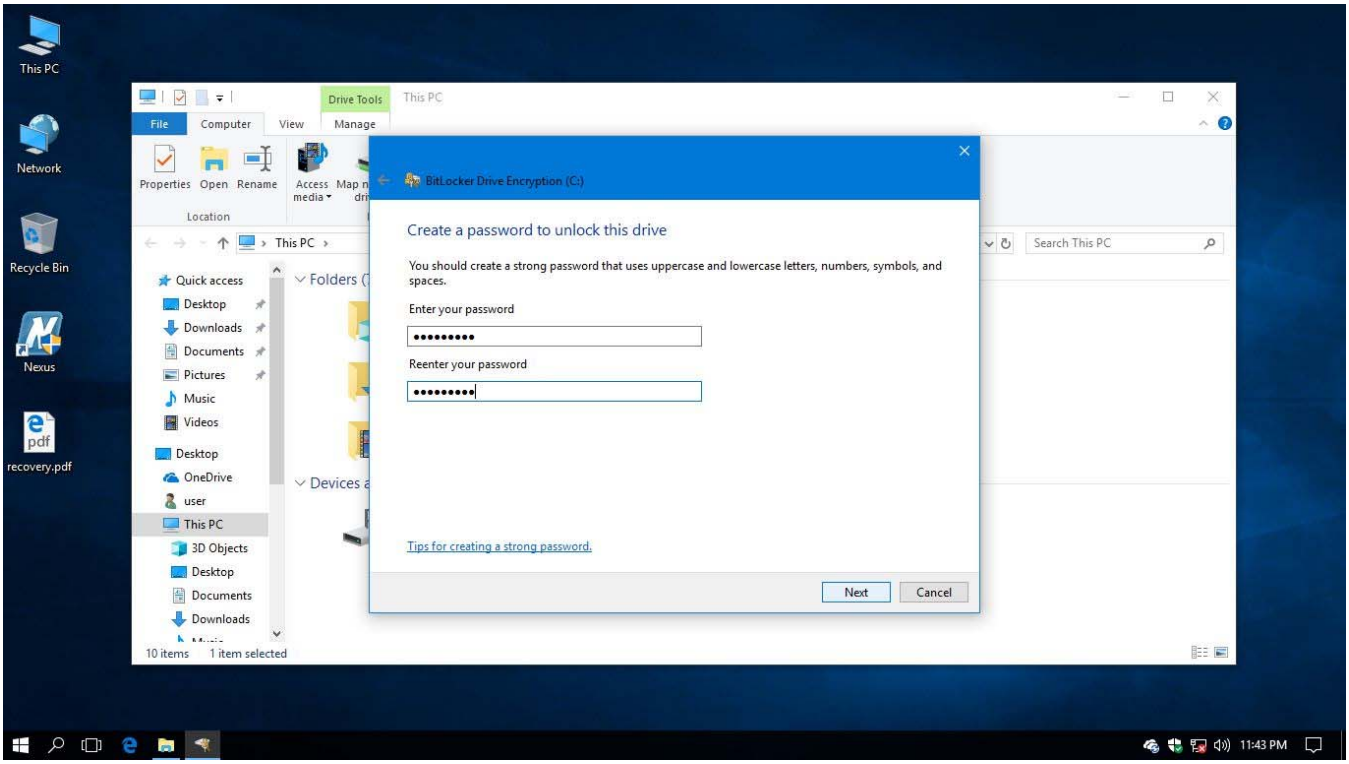

Figure 8

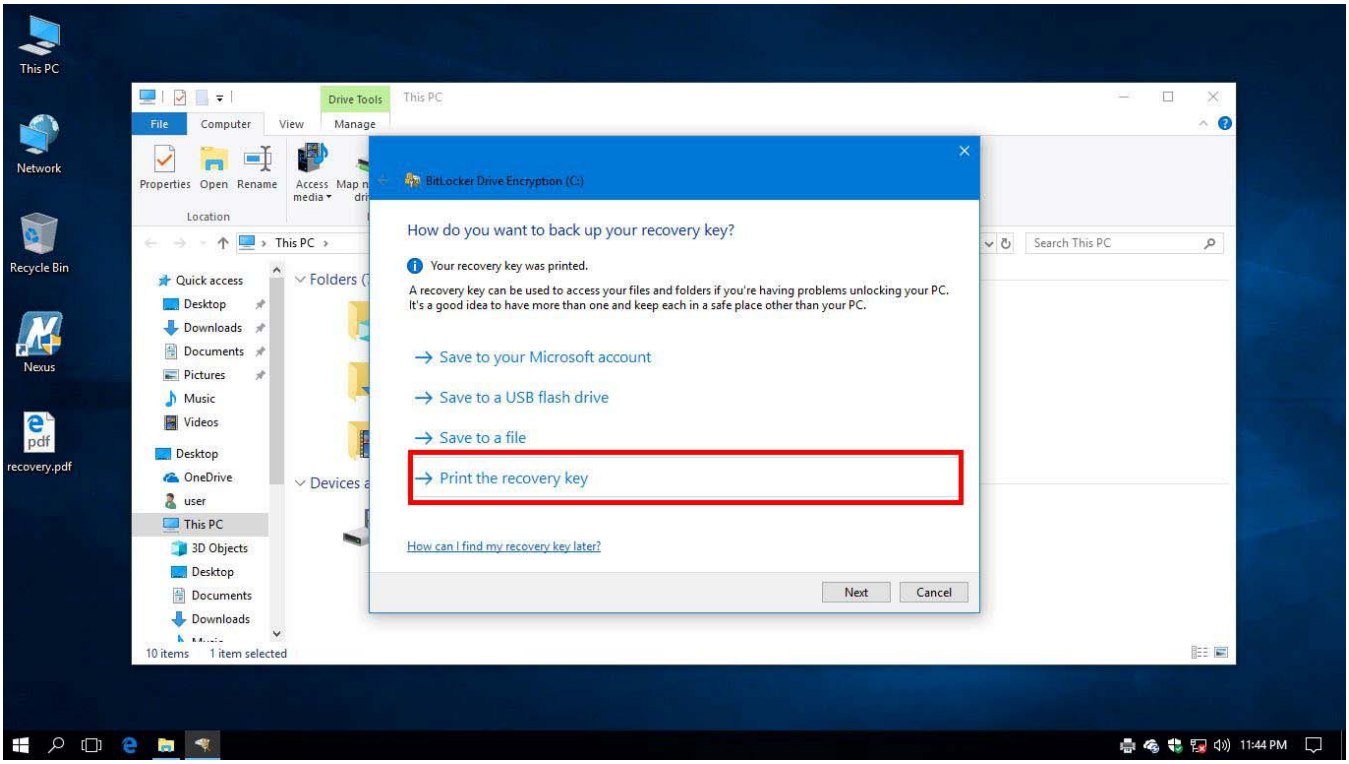

Figure 9

In ferestrele urmatoare se vor selecta optiunile ***New encryption mode*** si ***Run BitLocker System Check***, apoi ***Restart now*** (fig.10, 11 si 12).

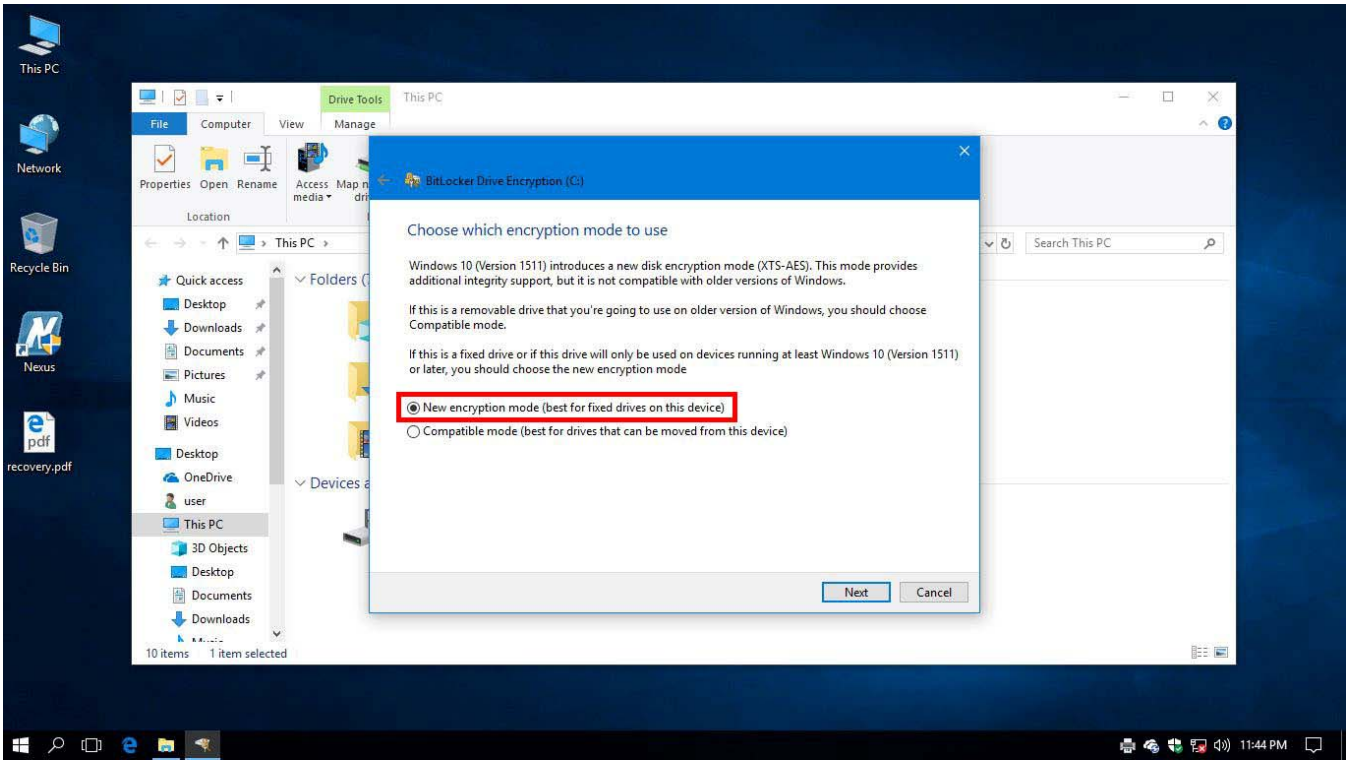

Figure 10

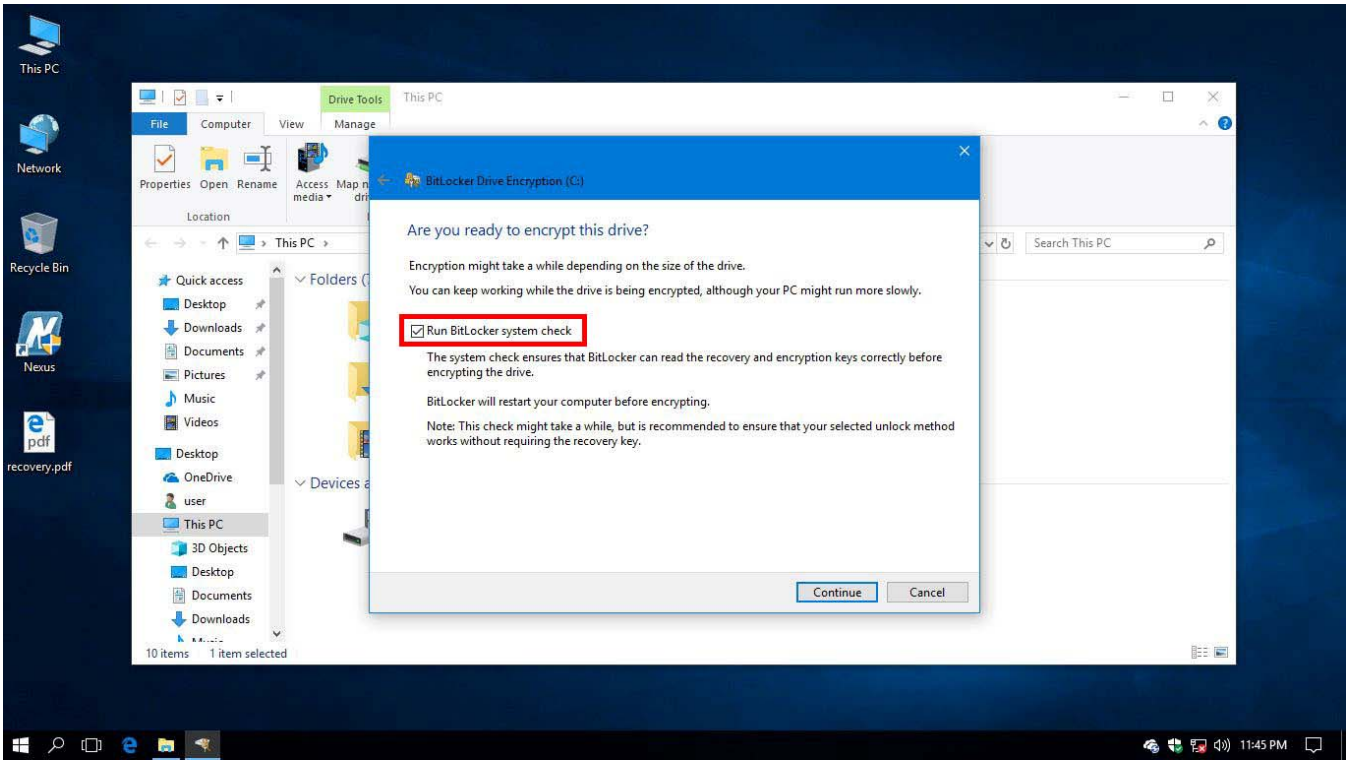

Figure 11

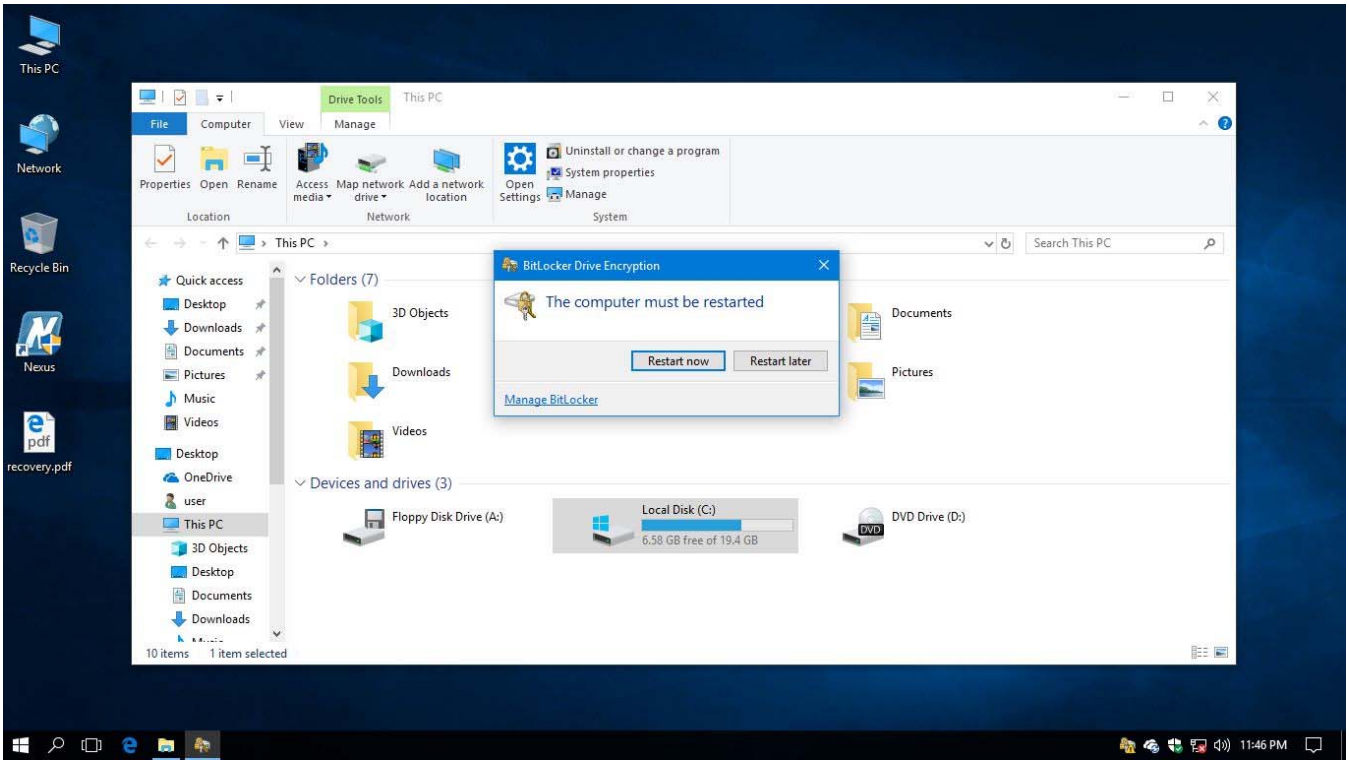

Figure 12

Dupa restart, va aparea, inainte de incarcarea sistemului de operare, o fereastra prin care se solicita parola sau PIN-ul setate mai devreme (fig.13)

Figure 13

Dupa incarcarea sistemului de operare, criptarea hard-disk-ului va continua in background.

Daca hard-disk-ul este partitionat, va trebui sa reluati procedura pentru fiecare partitie.