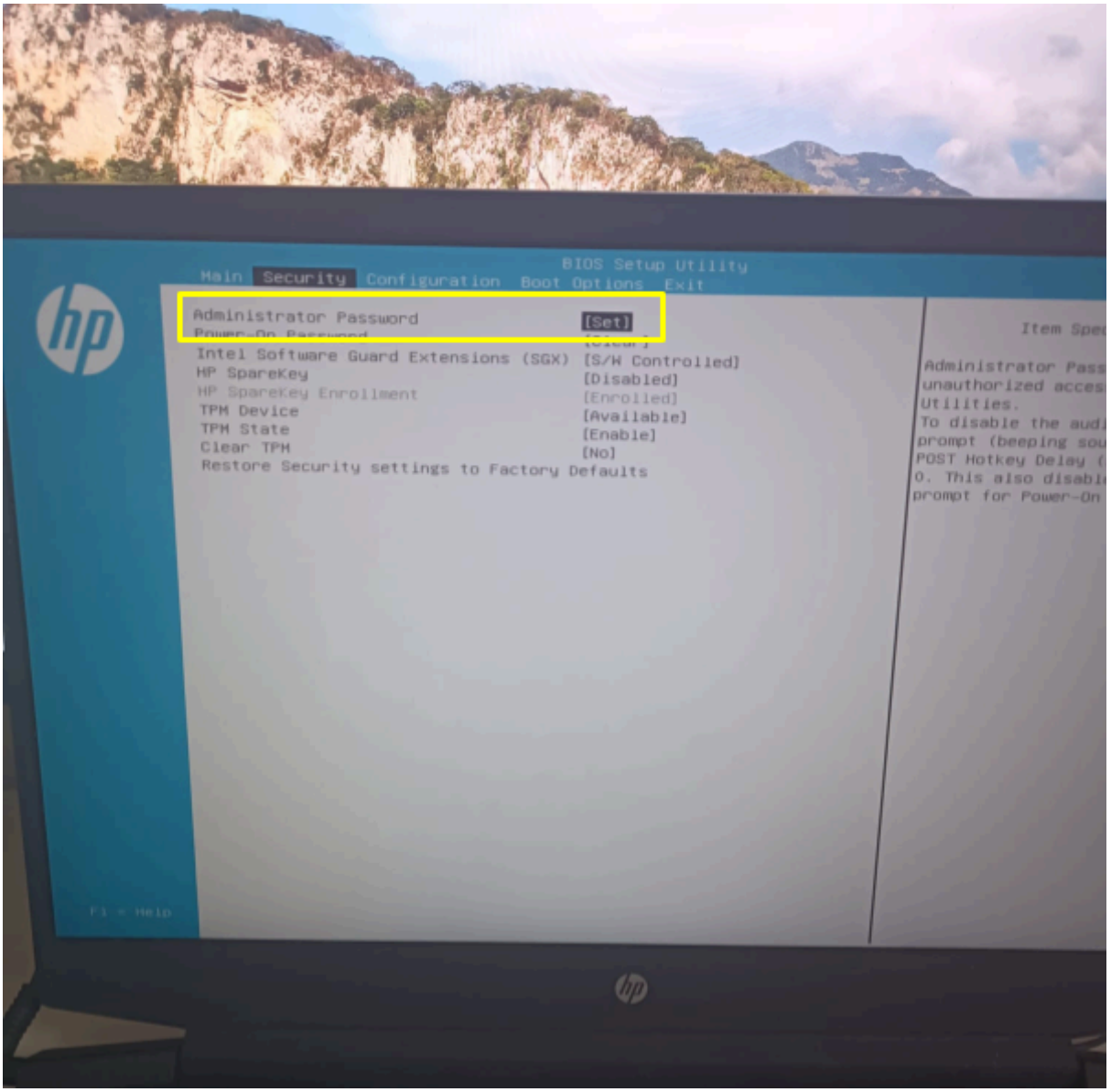
Álvaro Almellones Fernández

PRACTICA Nº 17-B, BIOS-SECUENCIA DE ARRANQUE.

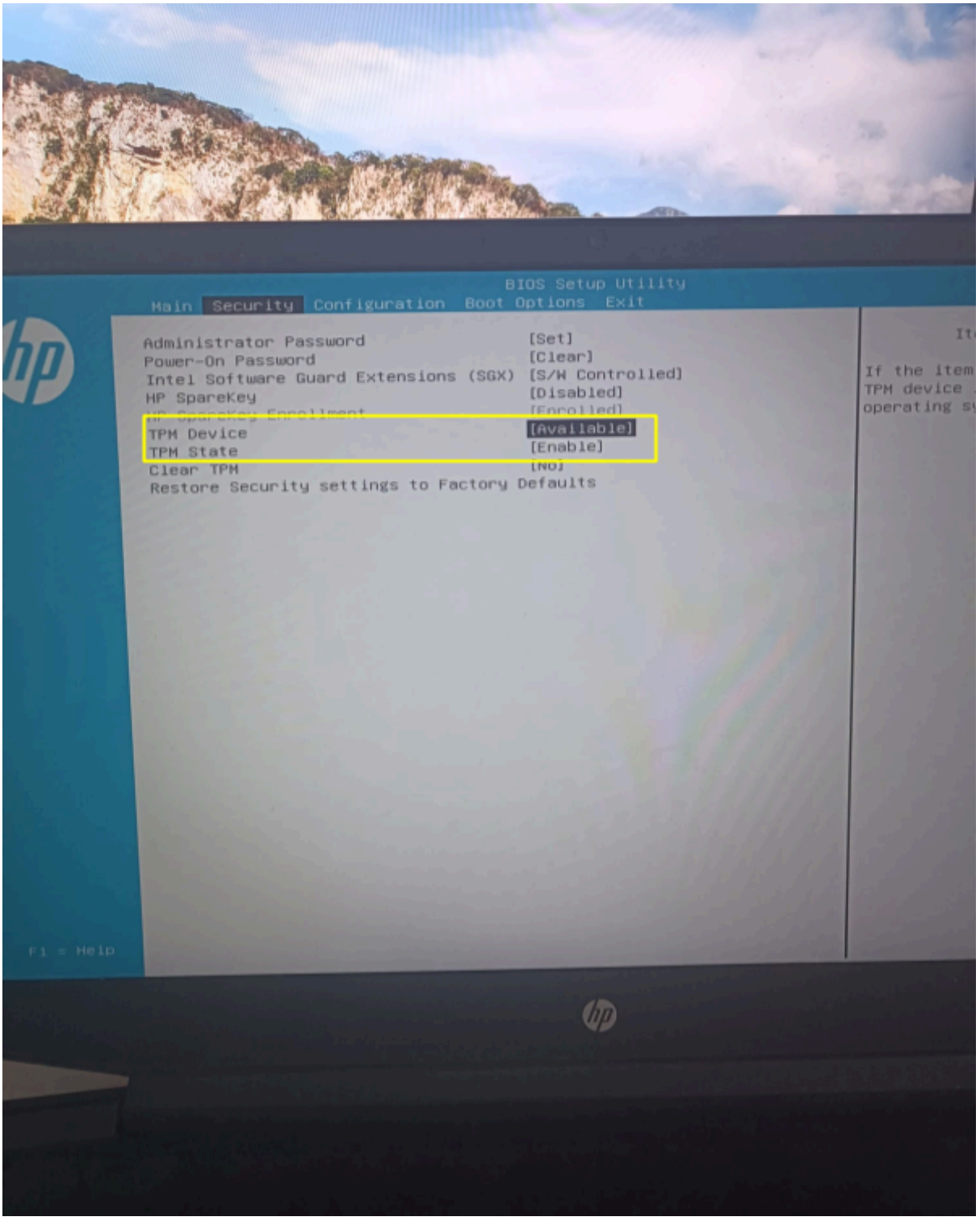
Ejercicio de enunciado y resolución abierto teniendo en cuenta el criterio de evaluación 6.c.

Si me pongo en la piel de que un atacante tiene acceso a mi ordenador de forma física y tengo que evitar que me altere la secuencia de arranque lo primero que hago es ponerle contraseña al administrador de la BIOS para que no pueda acceder a modificar nada



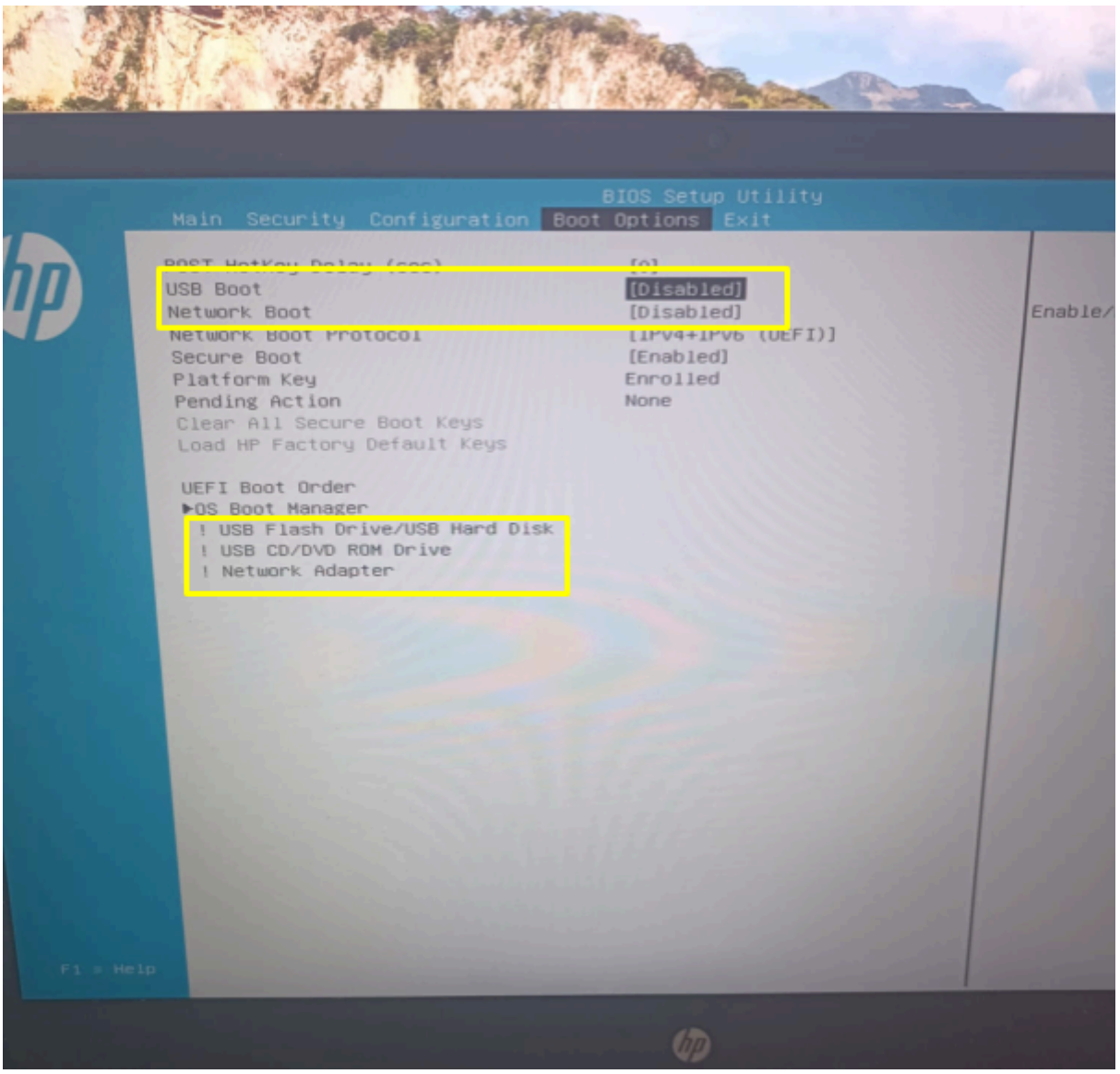
Después me aseguro de que este TPM activado que es un chip que protege el sistema desde el arranque guardando claves de cifrado y verificando que el sistema no haya sido modificado.

Álvaro Almellones Fernández



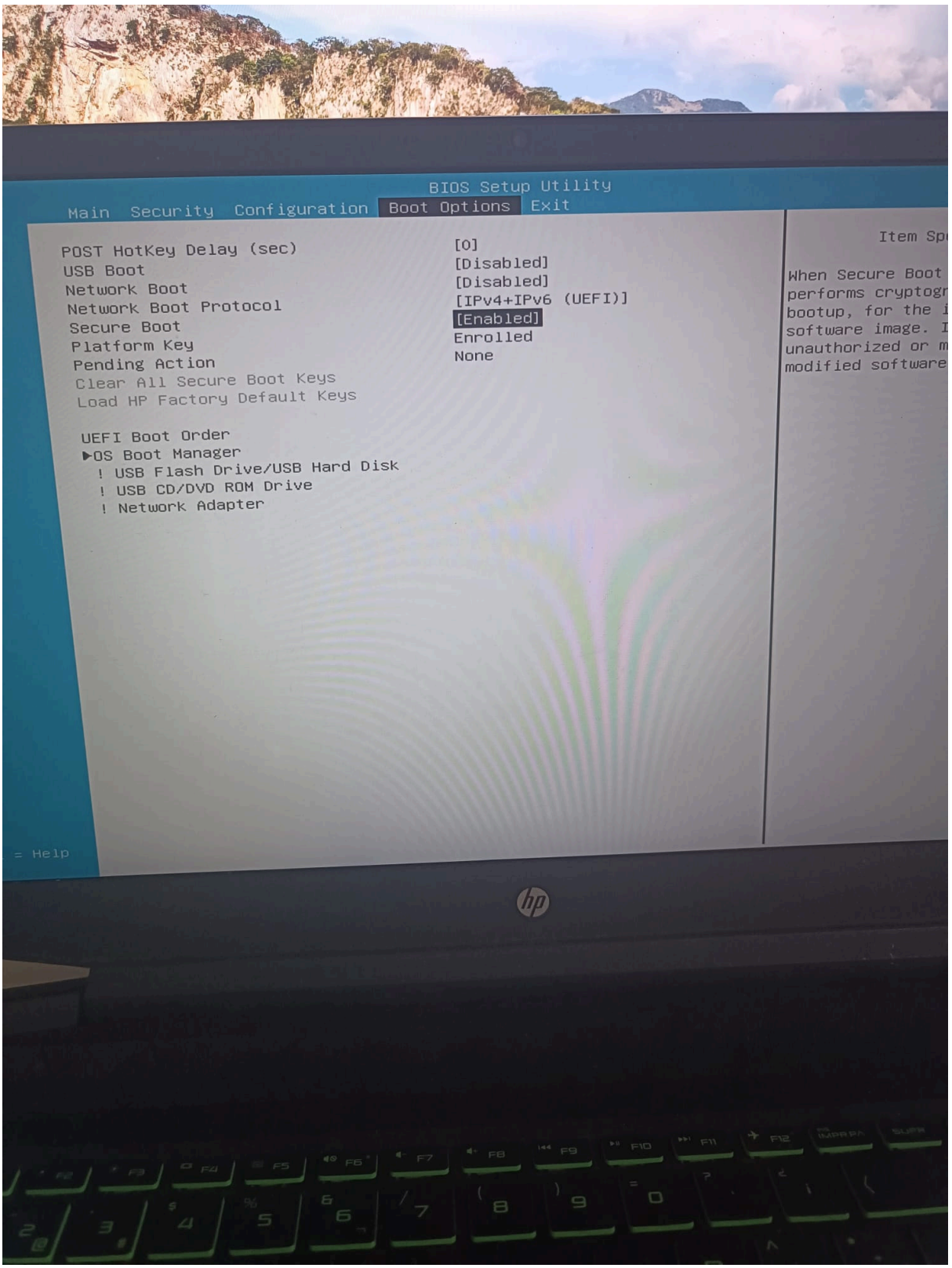
Después lo siguiente que hago es desactivar el USB Boot que deshabilita la posibilidad de arrancar otro OS desde USB o CD/DVD y Network boot evitando que se pueda arrancar otro OS desde un servidor remoto desde un adaptador red

Álvaro Almellones Fernández



Y finalmente compruebo que este Secure Boot activado que solo permite arrancar sistemas operativos firmados y verificados

Álvaro Almellones Fernández



También he visto que sería recomendable establecer el arranque desde el disco duro primario pero no he encontrado la opción para asignarlo

Álvaro Almellones Fernández

CRITERIOS DE EVALUACIÓN	
6.c	Se ha configurado un sistema informático para que un actor malicioso no pueda alterar la secuencia de arranque con acceso ilegítimo.