Política de Seguridad

Nicolás A. Ortega Froysa

19 de octubre de 2022

Índice

1. Introducción

Buscamos una forma de guardar los datos personales importantes de mi ordenador personal (sobremesa) en casa de una forma segura. Esta política me ha de proteger de los riesgos más comunes y posibles.

2. Posibles Riesgos

Históricamente los mayores problemas que he tenido de pérdida de datos han sido por error humano – e.g. `dd` –, además del riesgo de que mi sobremesa se encuentra justo al lado de una ventana por la que puede entrar agua cuando llueve, y así estropear los dispositivos de almacenamiento. También hemos tenido un caso hace trece años de robo, aunque esto se ve menos posible ya que (por ahora) siempre hay gente en casa.

Dicho lo cual, en el caso de un robo también será necesario evitar que tengan acceso a los datos del dispositivo robado.

3. Almacenamiento Ordinario de Datos

En primer lugar, para evitar la vulnerabilidad de acceso a datos personales de forma no autorizada, se cifrará el disco. Esto, aunque conlleva una pérdida en rendimiento – la lectura y escritura de datos –, tampoco es tanto que sea notable (tal, uso una NVMe).

4. Las Copias de Seguridad

En primer lugar, para tratar el riesgo primario – el error humano – esto lo solucionamos simplemente con tener un servidor de copias de respaldo dentro de la misma casa – también con el disco cifrado. A este servidor mandaremos de forma semanal una copia de respaldo del sistema. Se hará de forma semanal ya que tampoco hago muchos cambios importantes entre semanas, sino que suelen haber más cambios en fin de semana. En concreto la copia se hará el domingo por la noche a las 23:30, hora y media después de que me vaya a dormir. De esta forma hay copia de seguridad de todos los cambios que se han hecho ese fin de semana. También si hay algún problema con el servidor durante la semana, la puedo arreglar el fin de semana.

En segundo lugar, para protegernos ante la posibilidad (pequeña) de un robo, también guardaremos una copia en un almacenamiento remoto masivo. Como el robo es menos probable, tampoco es necesario hacer esta copia con

tanta frecuencia. Por lo tanto se hará de una forma mensual. Y como el servidor de copias está siempre encendida, enviará esta copia el lunes por la noche, para asegurarnos de que se haya acabado de hacer copia de la noche anterior.

5. Recuperación

En caso de que haya pérdida de datos en el escritorio, podremos bajar la copia del servidor interno e instalarlo de nuevo en la máquina principal. En caso de robo, se puede acceder a los datos del almacenamiento remoto una vez que haya comprado un ordenador nuevo.

6. Vulnerabilidades

Aunque este sistema me pueda proteger de los casos más comunes, no queda sin vulnerabilidades. Quizá la más peligrosa es que el punto débil es el servidor de respaldo local, que sirve como punto medio entre mi ordenador y el almacenamiento remoto. Una vulnerabilidad bastante posible es que, por cualquier motivo, el servidor se quede deshabilitado – por ejemplo, mi abuela limpia los cables y accidentalmente desenchufa el servidor – y por lo tanto ya no se puede sincronizar entre el servidor local y el almacenamiento remoto. Esto se podría solventar haciendo que sea el mismo ordenador el que envíe copia de seguridad al almacenamiento remoto, pero entonces tendría que tener todo un ordenador con CPU AMD encendido todo el rato, y sinceramente a luz está muy cara.

7. Derechos de Autor y Licencia