**CIFRADO DE DATOS**

Existen diversas herramientas y algoritmos que se utilizan para cifrar datos y garantizar su seguridad y privacidad. Algunas de las herramientas más comunes incluyen:

**TrueCrypt/VeraCrypt**: Estas son herramientas de cifrado de disco completo que permiten crear unidades virtuales cifradas y encriptar particiones enteras del disco. TrueCrypt fue descontinuado, pero VeraCrypt es un proyecto de código abierto basado en TrueCrypt y ofrece una seguridad mejorada.

**BitLocker**: Una característica de cifrado de disco completo incorporada en algunas ediciones de sistemas operativos Windows, como Windows 10 Pro y Enterprise. Permite cifrar unidades enteras y protegerlas con una contraseña o una llave USB.

**FileVault**: Una herramienta de cifrado de disco completo integrada en macOS. Permite cifrar todo el disco duro y proteger los datos en caso de pérdida o robo del dispositivo.

**PGP (Pretty Good Privacy)**: PGP es un software que proporciona cifrado y autenticación de datos mediante el uso de criptografía de clave pública. Se utiliza comúnmente para cifrar correos electrónicos y archivos.

**GnuPG (GPG)**: Es una implementación de software libre del estándar OpenPGP, que permite cifrar y firmar digitalmente datos. Es ampliamente utilizado en sistemas basados en Unix y también está disponible en otras plataformas.

**OpenSSL**: Una biblioteca de código abierto que proporciona herramientas y bibliotecas para implementar protocolos de seguridad, incluyendo SSL/TLS para comunicaciones seguras en la web.

**AES (Advanced Encryption Standard)**: Un algoritmo de cifrado simétrico ampliamente utilizado y altamente seguro. Se utiliza en muchas aplicaciones y protocolos de cifrado.

**RSA**: Un algoritmo de cifrado de clave pública que se utiliza para cifrar y firmar digitalmente datos. Es fundamental en la infraestructura de clave pública (PKI).

**OpenSSH**: Una implementación de código abierto del protocolo SSH (Secure Shell), que permite la comunicación segura y el acceso remoto a sistemas a través de redes inseguras.

**Signal**: Una aplicación de mensajería segura que utiliza cifrado de extremo a extremo para proteger las conversaciones y llamadas de voz.

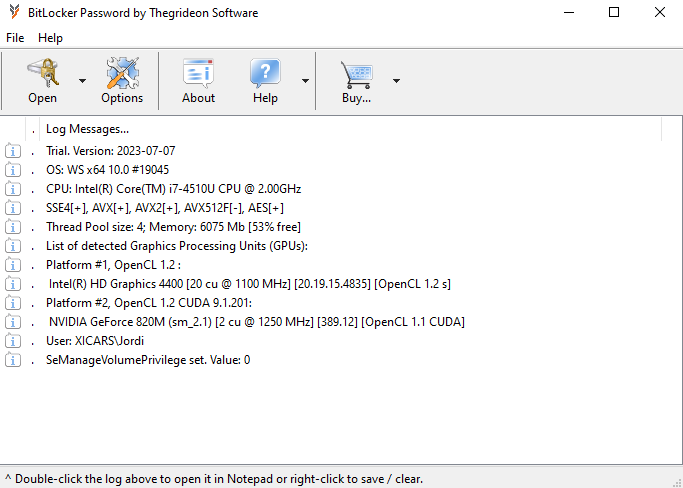
**Tresorit**: Un servicio de almacenamiento en la nube que ofrece cifrado de extremo a extremo y garantiza la privacidad de los datos almacenados.

**Cryptomator**: Una herramienta que permite crear contenedores cifrados para archivos antes de almacenarlos en la nube, asegurando que solo el usuario tenga acceso a los datos.

**BITLOCKER**

BitLocker es una función de seguridad en Windows que cifra toda la información en una unidad de almacenamiento, como discos duros o USBs. Esto protege los datos en caso de pérdida o robo. Puedes desbloquear la unidad con contraseña, clave de recuperación, tarjeta inteligente o TPM. Es parte de Windows 10 Pro, Enterprise y otras ediciones, y su objetivo es asegurar que tus datos estén a salvo.

**CIFRADO DE CONTRASEÑA**



**CIFRADO DE DATOS**

