Guida alla cifratura dei dati

Versione 1.2 –03 marzo 2022



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

SOMMARIO

1.	Premessa	2
2.	Gli strumenti descritti nelle presenti linee guida	3
3.	Avvertenza	3
4.	BitLocker Drive Encryption	3
	3.3 Attivazione e configurazione di BitLocker	
5.	FileVault 4.1 Requisiti minimi e richieste addizionali	7 7
	4.2 Avvertenza	7
	4.3 Attivazione e configurazione di FileVault	8
6.	VeraCrypt 5.1 Requisiti minimi e richieste addizionali	9 10
	5.2 Avvertenza	
	5.3 Installazione di VeraCrypt	
	5.4 Configurazione di VeraCrypt	
	5.4.1 Creazione di un volume VeraCrypt	
	5.4.2 Mount di un volume VeraCrypt	
	5.4.3 Dismount di un volume VeraCrypt	16
7.	Gpg4win (Keopatra)	17
	6.2 Desificare file can Credwin (Kleanstra)	
	6.2 Decitrare file con Gpg4win (Kleopatra)	
	6.3 Considerazioni finali e di sicurezza di Gpg4win (Kleopatra)	
8.	Azure Information Protection	20



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

1. Premessa

I dati personali sono informazioni che identificano direttamente o indirettamente una persona fisica e che possono fornire informazioni sulle sue caratteristiche, quali i dati anagrafici, il codice fiscale, una targa, ma anche quei dati che rivelano lo stato di salute, le opinioni politiche, l'appartenenza sindacale ecc.

Viste le disposizioni di legge nazionali e le normative internazionali (Regolamento Ue 679/2016 anche "GDPR", c.d. Codice Privacy e ss.mm.ii.), nonché le <u>Istruzioni generali per il trattamento dei dati personali, ai sensi dell'Articolo 32, comma 4 del Regolamento Europeo per la Protezione dei Dati (GDPR) di Ateneo</u>, il Settore Cybersecurity, Protezione Dati e Conformità invita gli utenti che abbiano la necessità di trasmettere o trattare tali dati a leggere il seguente documento, in modo da mettere in atto azioni di prevenzione sul trattamento dei dati personali propri o di terzi.

A tal proposito ricordiamo che come previsto dalle suindicate Istruzioni Generali dell'Ateneo, è richiesta obbligatoriamente l'adozione della cifratura per tutti i supporti esterni (es. chiavette USB, dischi Esterni) e per i computer portatili utilizzati per trattare dati personali per conto dell'Ateneo al fine di ridurre il rischio collegato al data breach in caso di smarrimento o furto del computer.

Per cifratura, si intende infatti un processo crittografico (utilizzato pertanto spesso come sinonimo di "crittografia") che tramite l'utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandola e rendendola illeggibile agli utenti che non sono in possesso della chiave di decifratura. Tale processo rappresenta quindi una misura di sicurezza volta a garantire, in base alla metodologia utilizzata, la riservatezza e l'integrità delle informazioni cifrate.

La presente guida è, quindi, stata redatta con l'obiettivo di **descrivere alcuni strumenti da utilizzare al fine di cifrare i dati di cui si volesse preservare la confidenzialità** memorizzati su dispositivi di tipo Windows, MacOS o Linux o durante il loro trasferimento.

Per ulteriori approfondimenti ed indicazioni di tipo tecnico di maggior dettaglio rispetto a quelle fornite all'interno del presente documento, si rimanda alla *Guida alla cifratura dei dati* di Ateneo.

L'esecuzione di alcune delle operazioni descritte nel presente documento potrebbero richiedere il possesso di competenze di livello tecnico informatico e/o di privilegi di tipo amministrativo. In tal caso potrebbe essere necessario richiedere supporto tecnico e/o operativo al referente tecnico preposto (referente di struttura o referente tecnico del servizio) prima di procedere: il Settore Cybersecurity, Protezione Dati e Conformità, che ha curato la stesura del presente documento, non è infatti deputato a fornire assistenza operativa in tal senso.

Ulteriori informazioni utili in materia di sicurezza ICT e protezione di dati personali, in ogni caso, possono essere reperite nella sezione dedicata del portale di Ateneo raggiungibile a partire da https://work.unimi.it/servizi/security_gdpr/118582.htm

Si specifica, infine, che il Settore Cybersecurity, Protezione Dati e Conformità non risponde di alcun danno o malfunzionamento derivante dall'applicazione non corretta o non rispondente alle stesse. Si invitano i suoi destinatari delle presenti linee guida consultare periodicamente la sezione dedicata del sito di Ateneo in modo da verificare di disporre di documenti sempre aggiornati.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

2. Gli strumenti descritti nelle presenti linee guida

In ambito informatico, la crittografia può essere definita come una tecnica che converte i dati attraverso l'utilizzo di una chiave (password o pin) in un formato illeggibile al fine di minimizzare il rischio di una loro accidentale diffusione. Per ottenere dai dati cifrati quelli originali è necessaria l'applicazione della chiave di decifratura segreta. Le chiavi di cifratura e decifratura possono coincidere.

Esistono vari strumenti per crittografare dati in accordo con il sistema operativo utilizzato. Tra i principali annoveriamo quelli trattati in questa guida, ovvero:

- BitLocker Drive Encryption: funzionalità integrata nei sistemi Microsoft Windows Vista e successivi;
- FileVault: tecnologia presente nel sistema operativo Mac OS X, e successivi;
- *VeraCrypt:* programma applicativo open source multipiattaforma disponibile per sistemi Windows, Mac OSX e Linux;
- Kleopatra: programma applicativo gratuito per cifrare file in sistemi Windows;

Le prime due soluzioni, *BitLocker Drive Enreyption* e *FileVault*, possono essere utilizzate per la cifratura del disco, mentre le altre, *VeraCrypt* e *Kleopatra*, consentono la cifratura rispettivamente di volumi¹ e singoli file.

In calce al documento, sono inoltre riportate informazioni relative alla soluzione di Azure Information Protection che consente di classificare tramite etichettatura il livello di riservatezza di file e cartelle e, a seconda della tipologia di etichetta selezionata, cifrarne i dati.

3. Avvertenza

È opportuno sottolineare che tutti gli strumenti di seguito descritti richiedono la disponibilità di chiavi di cifratura e/o decifratura (password, pin o *passphrase*) da conservare con estrema cura in un luogo sicuro e distinto da quello in cui sono conservati i dati cifrati. Nel caso in cui le suddette chiavi fossero smarrite non sarebbe più possibile recuperare i dati. Inoltre, è importante che la chiave di decifratura rimanga segreta perché chiunque ne entri in possesso può leggere i dati.

Si raccomanda fortemente, inoltre, di effettuare un backup dei dati da cifrare prima di intervenire su di essi.

4. BitLocker Drive Encryption

Nei più recenti sistemi operativi Microsoft è integrata una funzionalità di protezione dei dati denominata *BitLocker Drive Encryption* che permette di crittografare l'intera partizione del sistema operativo o di una unità dati rimovibile.

Una volta cifrati, i dati possono essere decifrati soltanto da utenti che dispongono della chiave crittografica appropriata (ad esempio una password). Ne consegue che per cifrare un'unità di Windows è necessario accedere con un account da amministratore.

¹ Partizione o semplice cartella, salvata in locale sul PC oppure su un dispositivo esterno.

Università degli Studi di Milano - Via Festa del Perdono 7 - 20122 Milano, Italy -Tel.+39 02 5032 5032 C.F. 80012650158 - P.I. 03064870151 - <u>www.unimi.it</u> - <u>unimi@postecert.it</u>



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

Quando viene abilitato BitLocker, è necessario creare un PIN che sarà richiesto ogni volta che il computer viene acceso. Inoltre, viene generata una chiave di ripristino, utilizzata per accedere al computer quando viene dimenticata la password.

Enter the password to unl	ock this drive	
18		
Press Esc for BitLocker rec		

Figura 1- Richiesta inserimento password del BitLocker

3.1 Requisiti minimi e richieste addizionali

Per utilizzare il BitLocker il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
 - o Windows 10 nelle versioni Education, Pro, o Enterprice;
 - Windows 8 nelle versioni Professional o Enterprice;
 - Windows 7 nelle versioni Enterprice o Ultimate.
 - Per il sistema operativo Windows 7, il modulo TMP nella versione 1.2 o superiore deve essere installato, abilitato e attivato.
- Per il sistema operativo Windows 7, il modulo TMP nella versione 1.2 o superiore deve essere installato, abilitato e attivato.
- Richieste addizionali:
 - Accedere al computer come Amministratore.

3.2 Avvertenza

Qualora si perdesse o si dimenticasse sia PIN che la chiave di recupero di BitLocker, i dati cifrati non saranno più reperibili, per cui è fortemente consigliabile effettuare un backup prima di configurare il BitLocker.

3.3 Attivazione e configurazione di BitLocker

Vengono di seguito riportati i passaggi per abilitare BitLocker e procedere alla cifratura dell'unità che si desidera proteggere (hard disk interno, chiavetta USB, disco removibile, ecc.). Per le versioni da Windows Vista in poi e precedenti Windows 10 occorre:



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

- 1. Digitare nella barra di ricerca di Windows *Gestione BitLocker*, oppure aprire il **Pannello di controllo > Sistema** e sicurezza > Crittografia unità BitLocker;
- 2. Selezionare il dispositivo da crittografare e cliccare su Attiva BitLocker;

🏘 Crittografia unità BitLocker			- 🗆 ×
← → × ↑ 🏘 > Pannello	di controllo » Sistema e sicurezza » Crittografia unità BitLocker	~ Ö	Cerca nel Pannello di controllo 👂
Pagina iniziale Pannello di controllo	Crittografia unità BitLocker BitLocker consente di proteggere le unità e impedire che si verifichino accessi non autorizzati a file e cartelle.		0
	Unità sistema operativo		
	C: BitLocker disattivato		\bigcirc
	Attiva BitLocker		
	Unità dati fisse		
	Unità dati rimovibili - BitLocker To Go		
	Riservato per il sistema (E:) BitLocker disattivato		\odot
Vedere anche S Amministrazione TPM Gestione disco	F: BitLocker disattivato		\odot
Informativa sulla privacy			

Figura 2 - Attivazione del BitLocker

- 3. Attendere il termine del processo per avviare BitLocker;
- 4. Scegliere il metodo desiderato (password oppure smart card) per proteggere l'unità e cliccare su Avanti;

	 An Crittourafia unità Bitl ocker (F-) 	×
	and the process of the process (r.)	
	Scegliere il metodo desiderato per sbloccare l'unità	
(Usa password per sbloccare l'unità	
	e password devono contenere lettere maiuscole e minuscole, numeri, spazi e simboli.	
ノ	Immettere la password	
	Immettere nuovamente la password	
	CILLA smart card per shloccare l'unità	
	Sarà necessario inserire la smart card. Il PIN della smart card verrà richiesto quando si sblocca l'unità.	
		_
	Avanti Annull	a

Figura 3 - Smart card o password per sbloccare il Bitlocker

5. Scegliere dove eseguire il backup della chiave di ripristino (delle tre opzioni è preferibile scegliere la prima) e cliccare su **Avanti**;



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

		\times
←	🙀 Crittografia unità BitLocker (F:)	
	Come eseguire il backup della chiave di ripristino	
	Se si dimentica la password o si smarrisce la smart card, è possibile utilizzare una chiave di ripristino per accedere all'unità.	
	→ Salva nell'account Microsoft	
	\rightarrow Salva in un file	
	ightarrow Stampa la chiave di ripristino	
	Che cos'è una chiave di ripristino	
	Avanti Annull	

6. Figura 4 - Chiave di ripristino del BitLockerScegliere se applicare la crittografia soltanto allo spazio utilizzato del disco oppure all'intera unità (è preferibile scegliere questa seconda ipotesi) e cliccare su **Avanti**, quindi attendere il completamento dell'operazione.

		×
÷	🏘 Crittografia unità BitLocker (F:)	
	Specificare la dimensione della porzione dell'unità che si desidera crittografare	
	Per configurare BitLocker in una nuova unità o un nuovo PC, è necessario crittografare solo la parte dell'unità in uso. I nuovi dati aggiunti verranno crittografati automaticamente.	
	Se si abilita BitLocker in un PC o un'unità già in uso, prendere in considerazione la possibilità di crittografare l'intera unità. Crittografando l'intera unità si garantisce che tutti i dati siano protetti, inclusi dati che sono stati eliminati ma potrebbero ancora contenere informazioni recuperabili.	
	Applica crittografia solo allo spazio utilizzato del disco (l'operazione è più rapida ed efficace su unità e PC nuovi)	
	🔿 Applica crittografia all'intera unità (soluzone più lenta, ma consigliata per PC e unità già in uso)	
	Avanti Annull	,

Figura 5 - Dimensione dell'unità da crittografare

In Windows 10, per attivare la funzionalità BitLocker è sufficiente cliccare col tasto destro sull'unità da proteggere, scegliere il comando **Attiva BitLocker** e seguire le istruzioni.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT



Figura 6 - Attivare Bitlocker su Windows10Maggiori informazioni sono reperibili nel sito ufficiale di Microsoft.

5. FileVault

FileVault è una tecnologia Apple per criptare i dati su MacOS e hardware Mac.

Tale tecnologia permette di cifrare tutti i dati sul disco di avvio, ma consente di cifrare anche i backup *Time Machine*. Gli utenti devono inserire la password ad ogni riavvio del computer, quando il computer viene riattivato dopo uno stand-by o screensaver.

Quando viene abilitato FileVault, è necessario creare una password che sarà richiesta ogni volta che il computer viene acceso. Inoltre, il sistema chiederà di generare una chiave di ripristino, utilizzata per accedere al computer quando viene dimenticata la password, oppure utilizzare l'account iCloud come una chiave.

4.1 Requisiti minimi e richieste addizionali

Per utilizzare il FileVault il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
 - o OS X Lion o versioni successive.
- Richieste addizionali:
 - Accedere al computer come Amministratore.

4.2 Avvertenza

Qualora di perdesse o si dimenticasse sia la password del proprio account che la chiave di recupero di FileVault, i dati cifrati non sarebbero più reperibili, per cui è fortemente consigliabile effettuare un backup prima di utilizzare FileVault.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

4.3 Attivazione e configurazione di FileVault

Vengono di seguito riportati i passaggi per abilitare FileVault:

1. Scegliere menu Apple > Preferenze di Sistema, quindi cliccare su Sicurezza e Privacy e cliccare su FileVault;

• • L			Sicurezza	e Privacy		Q Ricerca
		Generali	FileVault	Firewall	Privacy	
0	FileVault forni contenuti auto AVVISO: per acc generata autom	sce sicurezza ai omaticamente. redere ai dati, ti oc aticamente durant	i dati del disc ccorre la passw e questa confi	o codificar	ndone i o una chiave di r e dimentichi la p	Attiva FileVault
	recupero, i dati	andranno persi. attivato per il di	sco "Macinto	osh HD".		
	Filevault e dis	attivato per il di	sco macinu	Shind .		
0						Augusta

Figura 7 - Attivazione FileVault

Cliccare su , quindi immettere un nome e relativa password di amministratore;

2. Cliccare su Attiva FileVault;

Se un messaggio avvisa che il computer deve riavviarsi, cliccare su **Riavvia**. Dopo il riavvio, eseguire il login e tornare al pannello **FileVault**.

Se sul Mac sono presenti account di altri utenti, cliccare su **Abilita utente** e inserire la password dell'utente. Gli account utente aggiunti dopo l'attivazione di FileVault vengono abilitati automaticamente.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT



Figura 8 - Abilitazione utente su FileVault

3. Scegliere come sbloccare il disco e reimpostare la password di login se dimenticata (sono disponibili due opzioni), poi cliccare su **Continua** e successivamente su **Riavvia**.



Figura 9 - Accesso ad iCloud

Maggiori informazioni sono reperibili nel sito ufficiale della Apple.

6. VeraCrypt

VeraCrypt è un programma applicativo *opensource* multipiattaforma, disponibile per Windows, MacOSX e Linux.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

È un software utilizzato per creare e mantenere cifrato un volume, cioè un supporto di memorizzazione dei dati. I dati sono automaticamente cifrati prima di essere salvati e sono decifrati dopo che sono caricati, senza alcun intervento dell'utente.

Le principali caratteristiche di VeraCrypt sono:

- creazione di contenitori di file cifrati;
- cifrare interi volumi o partizioni;
- cifrare l'intero sistema operativo;
- può essere eseguito in modalità portatile, consentendo l'utilizzo dalla chiavetta USB senza alcuna installazione.

5.1 Requisiti minimi e richieste addizionali

Per utilizzare VeraCrypt il computer deve soddisfare alcuni requisiti:

- Sistemi operativi supportati:
 - o Windows Xp e successivi (e.g. Vista, 7, 8 e 8.1,10);
 - Windows Server (2003, 2008, 2012);
 - o MacOsX Lion e successivi;
 - o Linux x86 (32-bit e 64 bit, kernel 2.6 o compatibile);
 - FreeBSF x86 (32-bit e 64 bit, dalla versione 11).
- Richieste addizionali:
 - o Accedere al computer come Amministratore.

5.2 Avvertenza

Qualora si perdesse o si dimenticasse sia la password del proprio account che la chiave di recupero di VeraCrypt, i dati cifrati non sarebbero più reperibili, per cui è fortemente consigliabile effettuare un backup prima di utilizzare VeraCrypt.

5.3 Installazione di VeraCrypt

Il seguente tutorial si riferisce al sistema operativo Windows 10, per sistemi operativi diversi si consiglia di consultare la documentazione presente nel sito di VeraCrypt: <u>https://www.veracrypt.fr</u>.

Prima di utilizzare il software VeraCrypt, scaricabile dalla sezione *Domnload* del sito del produttore, è opportuno verificare la versione stabile compatibile con il proprio sistema operativo.

Dopo aver scaricato l'installer, provvedere ad avviare l'eseguibile.

Accettati i termini della licenza effettuare l'installazione, seguendo le indicazioni fornite dal software.



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

VeraCrypt Setup 1.23	
Modo guidato Selezionare uno dei modi. Se non siete sicuri di quello che volete scegliere, usate la mod rvarlafinita	alità
© Installa	
Selezionare questa opzione se volete installare VeraCrypt in questo sistema	l.
Estrai Se selezionate questa opzione, tutti i file saranno estratti da questo pacche installati nel sistema. Non selezionaria se intendete cifrare la partizione di si nell'unità di sistema. La scelta di questa opzione può essere utilissima, per e volete eseguire VeraCrypt in modalità driamata Portabile. VeraCrypt non vi nel sistema operativo nel quale esso viene eseguito. Dopo che tutti file sor potete eseguire direttamente il file estratto VeraCrypt.exe' (quindi VeraCry eseguito in modalità portabile).	itto ma non stema sempio, se ene installato no estratti, /pt verrà
VeraCrypt Installer	Annulla
Figura 10 - Setup di VeraCrypt	

La parte finale dell'installazione consiste nel definire la posizione dove installare il programma.

🥪 VeraCrypt Setup 1.23	
Opzioni di installazione Qui potete impostare varie opzioni per controllare il processo di installazione.	¥
Selezionare o digitare la posizione dove volete installare i file di programma di VeraCr directory specificata non esiste, sarà creata automaticamente.	ypt. Se la
C: \Program Files\VeraCrypt\	Sfoglia
🔽 Installa per tutti gli utenti	
📝 Aggiungi VeraCrypt al menu di avvio	
📝 Aggiungi icona di VeraCrypt al desktop	
Associa i file con estensione .hc con VeraCrypt	
Crea punto di ripristino del sistema	
VeraCrypt Installer	
Guida <indietro installa<="" td=""><td>Annulla</td></indietro>	Annulla

Figura 11 - Opzioni di setup di VeraCrypt

5.4 Configurazione di VeraCrypt

Di seguito vengono riportate le operazioni principali da eseguire per creare, montare ed utilizzare un volume VeraCrypt.

5.4.1 Creazione di un volume VeraCrypt

1. Dopo aver aperto il software cliccare su Create Volume;



SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

- 2. A questo punto sono disponibili tre diverse opzioni:
 - **Create an encrypted file container** permette di cifrare un disco all'interno di un file ed è raccomandato per i principianti;
 - Encrypt a non-system partition/drive permette di cifrare unità interne/esterne e dà anche la possibilità di creare un volume nascosto;
 - Encrypt the system partition or entire system drive permette di cifrare l'intero sistema operativo (quindi per avere accesso al computer sarà necessario inserire la password corretta prima dell'inizializzazione del computer).

In questa guida si è scelto di mostrare come creare un volume VeraCrypt all'interno di un file, quindi occorre selezionare la prima opzione e cliccare su **Next**.



Figura 12 - Selezione del volume in VeraCrypt

- 3. Scegliere se creare un volume VeraCrypt standard (Standard VeraCrypt) o nascosto (Hidden VeraCrypt volume);
- 4. Scegliere dove creare il volume di VeraCrypt cliccando su **Select File** (apparirà una finestra di selezione di file; la finestra della creazione guidata del volume di VeraCrypt rimarrà aperta sullo sfondo);
- Selezionare il percorso desiderato (dove si desidera creare il contenitore), digitare in File name il nome del file contenitore desiderato e cliccare su Save (sparirà la finestra di selezione di file), in questo esempio My Volume in F:\Data\;

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

Organize 🔻 New folder					• ==	0
Git	*	Name	^		Date modified	
J Music			NI- Server and the			
Pictures			No items match	your search.		
Subversion						
Videos						
· Commuter	Ξ					
Local Dick (C)						
Local Disk (D:)						
Local Disk (F:)		. F	222 1			
Local Disk (C:) Local Disk (D:)	-	٠ [m			
File name: My Volu	ıme					_
Save as type: All Files	(* *)					

Figura 13 - Creazione del volume in VeraCrypt

Quando viene creato un contenitore di file, VeraCrypt non effettua alcuna operazione di cifratura ad alcun file esistente. Se si seleziona un file esistente in questo passaggio, tale file verrà sovrascritto e sostituito dal volume appena creato, perdendo il file precedente. In seguito sarà possibile cifrare i file esistenti spostandoli sul volume VeraCrypt creato.

6. Nella finestra della creazione guidata del volume di VeraCrypt cliccare su Next;

Figura 14 - Creazione del volume su VeraCrypt

7. Scegliere un algoritmo di cifratura e di hash per il volume e cliccare su Next;

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

9 VeraCrypt Volume Creation Wizard	
VeraCrypt Volume Creation Wizard	Encryption Options Encryption Algorithm AES Test FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect dassified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS. More information on AES Benchmark Hash Algorithm SHA-512 Information on hash algorithms
F: 45 0	Help < Back Next > Cancel

Figura 15 - Opzioni di cifratura su VeraCrypt

- 8. Specificare la dimensione del contenitore VeraCrypt e cliccare su Next (es. 250 megabyte);
- 9. Scegliere una password per il volume, digitarla in **Password** e successivamente in **Confirm**, quindi cliccare su **Next**;
- 10. Muovere il mouse il più casualmente possibile all'interno della finestra della creazione guidata (almeno finché l'indicatore di casualità diventa verde), quindi cliccare su **Format**;

Si consiglia di muovere il mouse per almeno 30 secondi.

SeraCrypt Volume Creation Wizard	
	Volume Format Options Filesystem FAT Cluster Default Dynamic Random Pool: *,*+.+-*,/+-***/+,,+*,+ Header Key: Master Key:
VeraCrypt	Abort Done Speed Left IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the crybtorraphic strength of the encryption keys. Then click Format to create the volume. Randomness Collected From Mouse Movements Help < Back Format Cancel

Figura 16 - Creazione del volume in VeraCrypt

Università degli Studi di Milano - Via Festa del Perdono 7 - 20122 Milano, Italy -Tel.+39 02 5032 5032 C.F. 80012650158 - P.I. 03064870151 - www.unimi.it - unimi@postecert.it

DICT_IO_GuidaCifraturadeiDati _rev.1.2 del 03/03/2022

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

11. Attendere la creazione del volume (il processo potrebbe richiedere molto tempo, a seconda delle dimensioni del volume), al termine verrà visualizzata la finestra di dialogo di seguito riportata, quindi cliccare su **OK**;

In questo passaggio VeraCrypt crea un file chiamato *My Volume* nella cartella *F:\Data* (come specificato al punto 5). Tale file sarà un contenitore VeraCrypt:

12. Una volta creato il volume VeraCrypt cliccare su Exit per chiudere la finestra della procedura guidata.

5.4.2 Mount di un volume VeraCrypt

1. Avviare VeraCrypt e selezionare l'unità dall'elenco sulla quale montare il contenitore VeraCrypt e cliccare su **Select File**, cercare il file contenitore e selezionarlo, quindi cliccare su **Open**;

olumes	System	Favorites	Tools	Settings	Help		Homepa
Drive	Volume				Size	Encryption Algorithm	Туре
B:							
E:							
K:							
M:							
-N:							
0:							
P:							
Q:							
R:							
S:							
- T:							
—т:							
<u>с</u>	reate Volur	ne		Volume	Properti	es	Wipe Cache
T:	reate Volur	ne		Volume	Properti	ies	Wipe Cache
T:	ireate Volur	ne		Volume	Properti	ies	Wipe Cache
Volume	P ^t Volum	me	tory	Volume	Properti	v	Wipe Cache Select File Select Device

Figura 17 - Mount del volume in VeraCrypt

			1.11		
Organize 🔻 New	folder			III • 🗂	
	^	Name		Date modified	Ту
Cibraries		My Volume		12/30/2014 11:28	Fil
Long and					
Music Victures Videos Computer Computer Cocal Disk (D:)	E				

Figura 18 - Selezione del volume in VeraCrypt

2. Nella finestra principale di VeraCrypt cliccare su Mount;

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

orannes	System	Favorites	Tools	Settings	Help		Homepa
Drive	Volume				Size	Encryption Algorithm	Туре
B:							
E:							
K:							
M:							
N:							
0:							
-P:							3
Q:							
R:							
-S:							
- T:							
	Create Volur	me		Volume I	Propert	ies	Wipe Cache
Volume	Create Volur	ne		Volume I	Propert	les	Wipe Cache
Volume	Create Volur	me ata∖My Volur	ne	Volume I	Propert	es	Wipe Cache Select File
Volume VeraCr	F:\p	ne ata My Volur ever save his	ne tory	Volume I	Propert	volume Tools	Wipe Cache Select File Select Device
Volume	F:\D	ne lata (My Volur ever save his	ne tory	Volume I		rolume Tools	Wipe Cache Select File Select Device

Figura 19 - Drive del volume in VeraCrypt

- 3. Inserire la password nell'apposito campo, selezionare l'algoritmo PRF (Pseudo-Random Function) che è stato usato durante la creazione del volume, è possibile usare l'*autodetection*, ma il processo di montaggio richiederà più tempo, il default è HMAC-SHA512
- 4. creazione del volume

Password	•••••		ОК
PKCS-5 PRF	HMAC-SHA-512 T	rueCrypt Mode	Cancel
	Use PIM		
	Cache passwords and keyfile	s in memory	

Figura 20 - Password del volume in VeraCrypt

5. Il contenitore è stato montato con successo come disco virtuale *M*;

Nel disco virtuale si possono salvare (copiare, spostare, ecc.) file che vengono cifrati nel momento in cui sono scritti.

5.4.3 Dismount di un volume VeraCrypt

1. Avviare VeraCrypt, selezionare il volume che si vuole rendere inaccessibile e cliccare su **Dismount**:

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

lumes	System	Favorites	Tools	Settings	Help		Homepag
Drive	Volume				Size	Encryption Algorithm	Туре
в:							
- E:							
■K:							
_'M:	F:\Data\∕My	Volume		2	49 MB	AES	Normal
N:							
D:							
0:							
R:							
R:							
R: S: T:							
R: S: T:							
R: S: T:							
R: S: T:	ireate Volun	ne		Volume I	Properti	es [Wipe Cache
R: S: T: Volume	ireate Volun	ne		Volume I	Properti	es	Wipe Cache
R: S: T: Volume	F: \D	ne	ie	Volume I	Properti	es [Wipe Cache
R: S: T: C Volume	F:\D F:\D V Ne	ne ata\My Volum wer save hist	ne pory	Volume I	Properti	es	Wipe Cache Select File Select Device

Figura 21 - Dismount del volume in VeraCrypt

Il dismount di un volume avviene automaticamente al momento del riavvio o dello spegnimento del computer.

7. Gpg4win (Keopatra)

Gpg4win è una collezione di software Open Source pensati per la crittografia dei file su sistemi operativi Windows.

6.1 Installare e cifrare file con Gpg4win (Kleopatra)

È possibile scaricarlo all'indirizzo https://gpg4win.org/thanks-for-download.html. Una volta eseguita l'installazione, sarà possibile utilizzare lo strumento "Kleopatra".

Una volta avviato il programma, per cifrare un file fare click sul tasto "firma/cifra..." in alto a sinistra:

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

Ele Visualizza Certificati Spumenti Impostazioni Figestra Ajuto	
Importa Emporta Certifica Cerci aul server Emporta Emporta Benvenuti in Kleopatra Gyg4win-4.0.0 Keepatra è uninterfacca per i software d'ottografia Grafic. Re la augior perte delle autori è necessaria per destrare d'ottografia Grafic. Per la maggior perte delle autori è necessaria per destrare o fimme. La dieve privata è necessaria per doffare o fimme. La dieve privata è necessaria per dentine au autori per verificare la sua identità o offare del messaggi per te. Paua correfactoria pia questo provento in Viscodia.	
Benvenuti in Kisopatra Gpg4win-4.0.0 Kespatra é uninterfacia par la software di ottografia Goußis. Per la maggior parte delle azioni è necessaria d'aive privata (certificato) o una tua driave privata. « La diave publica può essere usato da abit per verificare la sua identità o offare dei messaggi per te. Pua doarende elutori informazioni su auctori arconte in i Viscoda.	
Benvenuti in Kleopatra Gpg4win-4.0.0 Keopatra è uninterfaccia per il software di crittografia Go <u>4PS</u> . Per la magoir parte delle asioni è necessaria chieve privata (certificato) o una tua chieve privata. • La chieve publica può essere usato da abri per verificare la tua identità o offare dei messaggi per te. • La chieve publica può essere usato da abri per verificare la tua identità o offare dei messaggi per te. Pou accorredore ulteriori informazioni su questo accorrotto in Villoceda.	
 Network ar & drivent microsol per l'avrinnar è d'intrody alla <u>vicco</u>. Per la maggior parte delle autori e concessaria driver privata (certificato) o una tua driave privata. La driave publica può essere usato da altri per verificare la tua identità o offare dei messaggi per te. La driave publica può essere usato da altri per verificare la tua dentità o offare dei messaggi per te. 	
 La chave privata è necessaria per deofrare o finare. La chave privata è necessaria per deofrare o finare. La chave publica può sere usato da altri per vertificare la tua identità o offare dei messaggi per te. Posi apprendere ulteriori informazioni su questo argomento in Vilkoedia. 	
 La critave privata e necessaria per osomare o minute. La critave pubblica pole serve suato da atilize verificare la tua identità o offare dei messaggi per te. Poui apprendere ulteriori informaziori su questo argomento in Wilcoeda. 	
Puol apprendere ulteriori informazioni su questo argomento in Weipedia.	
Nuova coppia gi chiavi Importa	

Figura 22 - Cifrare un file in Windows con Kleopatra

E selezionare il file da cifrare (in questo esempio viene illustrato un file Excel, ma è possibile cifrare qualunque file, comprese le cartelle .zip):

👦 Seleziona uno o più file	da firmare o cifrare					×
← → ~ ↑ 📙 > Q)uesto PC → Documenti → test		~ ē) 🔎 Cerca i	n test	
Organizza 👻 Nuova	cartella					?
📃 Desktop 🛷 ^	Nome	Ultima modifica	Tipo	Dimensione		
🕂 Download 🖈	a-offuscare.xlsx	23/12/2021 13:58	Foglio di lavoro di	7 KB		
🔮 Documenti 🖈						
📰 Immagini 🖈						
SicurezzalCT 🖈						
incidenti_202 🖈						
Luca						
procedure						
screenshot						
screenshot						
OneDrive						
Questo PC						
Desktop						
🖶 Documenti 🗸						
Nom	ne file: da-offuscare.xlsx			✓ Tutti i file (*)	\sim
				Apri	Annulla	

Figura 23 - Selezionare file da cifrare con Kleopatra

Successivamente compare una finestra di riepilogo come quella seguente:

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

👦 Firma/Cifra file -	Kleopatra	?	×
Firma / cifra	file		
Prova l'autenticità (firm	na)		
Eirma come:			\sim
Cifra			
Cifra per me:			\sim
Cifra per gli altri:	😤 Inserisci un nome o un indirizzo di posta elettronica		
	Tutti quelli che ricevana la password possono leggere i dati		
en a con passion	. Tata dacili che neevono la passivora possono leggere r'ada.		
Risultato			
File/cartella <u>d</u> ei risultat	i:		
C:/Users	Documents/test/da-offuscare.xlsx.gpg	×	
Cifra/firma separat	amente ogni file.		
	Cifra	Ann	ulla
	2		

Figura 24 - Salvare file da cifrare in Kleopatra

Fare click su "Cifra" e inserire la password nel campo passphrase quando compare la relativa finestra (si faccia riferimento alle linee guida presenti all'indirizzo <u>https://work.unimi.it/servizi/servizi tec/59030.htm</u> per indicazioni sui requisiti sulle creazioni delle password):

🔒 piner	ntry-qt		-		×
0	Inserisci la pa	issphrase			
	Passphrase:	•••••	•••••	•••••	۲
	Ripeti:	0	ĸ	Canc	el
		<u> </u>			

Figura 25 - Inserimento passphrase in Kleopatra

Se la passphrase inserita risulta "debole", il software ne darà un avviso e si raccomanda di sceglierne una più forte. Un'ultima finestra comunicherà l'avvenuta cifratura del file. Fare click su Fine.

Il file cifrato avrà come estensione standard il formato .gpg appeso in fondo al nome del file.

6.2 Decifrare file con Gpg4win (Kleopatra)

Per decifrare un file in formato gpg su Windows sarà sufficiente aprirlo con Kleopatra, facendo doppio click sullo stesso o premendo il tasto "Decifra/verifica...". A questo punto sarà sufficiente inserire la password nell'apposito campo e dare indicazione di salvataggio al programma. In ogni caso, una volta selezionato il file si aprirà la seguente finestra in cui verrà richiesto di inserire la password:

SETTORE CYBERSECURITY, PROTEZIONE DATI E CONFORMITA' - Direzione ICT

Operazione 1: Decifrazio	ne: offuscato.txt.gpg	
	Please enter the passphrase for decryption. Passphrase: CKCancel	

Figura 26 - Decifrare file con Kleopatra

6.3 Considerazioni finali e di sicurezza di Gpg4win (Kleopatra)

Se viene aperto un file che è stato cifrato sul proprio computer da Kleopatra, è possibile che il software non chieda il reinserimento della password. Non si tratta di un errore, ma di una funzionalità del software che è in grado di riconoscere quali file ha cifrato ed è in grado di decifrarli senza chiedere il reinserimento della password.

La condivisone della password scelta in momento di cifratura col destinatario deve avvenire attraverso un canale di comunicazione sicuro, che sia telefonico o verbale, avendo cura che l'informazione non venga ascoltata da terzi. È assolutamente da evitare lo scambio di password via mail.

8. Azure Information Protection

Azure Information Protection è una soluzione cloud Microsoft che consente agli utenti di proteggere i documenti mediante l'applicazione di etichette al contenuto.

Per ulteriori informazioni su Azure Information Protection è possibile consultare le Linee Guida di Ateneo dedicate: *Azure Information Protection: le etichette*.