



**GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI**

Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori [1574080]

Istruzioni pratiche per una cancellazione sicura dei dati: le raccomandazioni degli operatori

Nel quadro delle proprie iniziative sulla protezione dei dati rispetto allo smaltimento, dismissione e cessione a qualunque titolo di apparecchiature elettriche ed elettroniche, l'Autorità intende fornire a utenti e operatori, a complemento del provvedimento che ha adottato il 13 ottobre 2008, alcuni suggerimenti pratici e facilitare la diretta consultazione di altre indicazioni provenienti dai principali fornitori e produttori che risultano operanti in questa tematica.

Pur non assumendo una diretta responsabilità in ordine all'efficacia di questi accorgimenti che l'esperienza dimostra al momento essere utili, l'Autorità ritiene comunque opportuno darne ulteriore pubblicità e richiamare l'attenzione di operatori e utenti a contribuire alla loro corretta applicazione e ogni loro integrazione o modifica, sulla base di approfondimenti e di altre esperienze applicative.

L'Autorità si riserva quindi di aggiornare periodicamente queste istruzioni.

Il Garante, nel sottolineare come non sia responsabile in alcun modo della correttezza delle istruzioni pubblicate in rete e a cui viene qui fatto riferimento, nonché delle conseguenze della loro messa in opera da parte degli utenti, assicura la propria disponibilità a integrare queste pagine, su richiesta di produttori diversi da quelli qui citati, con l'inserimento di nuovi riferimenti utili, nonché a provvedere all'aggiornamento di quelli già presenti.

La Cancellazione sicura delle informazioni

Il problema dell'e-waste riguarda chiunque mantenga memorizzati su dispositivi elettronici dati relativi a sé o a terzi: è infatti compito del loro possessore dati assicurare che questi non possano andare dispersi e acquisiti anche in modo incontrollato da estranei.

La semplice cancellazione dei *file* o la formattazione dell'*hard disk*, infatti, non sempre realizzano una vera cancellazione delle informazioni registrate, che rimangono spesso fisicamente presenti e tecnicamente recuperabili.

Per prevenire l'acquisizione indebita di dati è necessario operare in diversi modi e tempi a seconda delle circostanze:

preventivamente, con tecniche di memorizzazione sicura;

immediatamente prima della cessione o dismissione dell'apparato elettronico, con strumenti *software* di cancellazione sicura (a condizione che l'apparato sia funzionante);

al momento della cessione o dismissione, con la demagnetizzazione (*degaussing*), che azzerava tutte le aree di memoria elettronica e rende l'apparato inutilizzabile, o con la distruzione fisica del dispositivo di memorizzazione.

Per ciascuna delle opzioni citate si forniscono qui di seguito delle informazioni per la messa in pratica o per il reperimento di informazioni più dettagliate.

Memorizzazione sicura

La memorizzazione sicura dei file si può realizzare sui più diffusi sistemi operativi con

l'attivazione di funzionalità crittografiche proprie del sistema, se disponibili, o con l'installazione di prodotti software aggiuntivi. Le concrete modalità dipendono fortemente dallo specifico sistema operativo utilizzato, e talvolta anche dalla sua versione o dall'applicazione di patch e aggiornamenti. I possessori di personal computer sono pertanto esortati a rivolgersi alle case produttrici del proprio hardware o del sistema operativo in uso per ottenere indicazioni dettagliate.

Si rinviano, in particolare, gli utenti di sistemi operativi Windows alla consultazione delle pagine informative predisposte, in lingua italiana, dalla casa produttrice Microsoft (<http://www.microsoft.com/italy/pmi/sicurezza/privacy/>).

Per i sistemi Apple, le pagine consultabili sul sito italiano del produttore illustrano le funzionalità [FileVault](#) disponibili nel sistema operativo Mac OS X per la protezione di intere directories o di volumi di dati.

Tra i sistemi "multiplatforma" (non dipendenti da uno specifico sistema operativo e perciò utilizzabili in ambiente Windows, MacOS, Unix, Linux...), è disponibile il software [TrueCrypt](#), che offre funzioni di cifratura con strong encryption di partizioni e interi dischi, comprese le partizioni "di sistema".

Cancellazione sicura

Gli utenti di sistemi operativi Microsoft Windows possono far riferimento alle già menzionate pagine informative pubblicate dal produttore (<http://www.microsoft.com/italy/pmi/sicurezza/privacy/>), che illustrano nel dettaglio le modalità per affrontare il problema della cancellazione di interi volumi di dati qualora non sia stata preventivamente adottata la soluzione della memorizzazione sicura.

Gli utenti del sistema operativo Apple MacOS X, che incorpora una funzione di "svuotamento del cestino in modalità sicura", potranno trovare dettagliate informazioni sul sito del produttore www.apple.it oppure ricorrere a utility di tipo "open source" come Permanent Eraser, che consente di effettuare cancellazioni sicure con un algoritmo avanzato.

Diversi applicativi software di tipo open source o comunque con licenze d'uso non commerciali sono poi disponibili per i sistemi Unix e Linux: tra questi, uno dei più noti ed efficaci è DBAN (www.dban.org), un sistema con cui è possibile creare un "disco di avvio" (boot disk) del proprio computer (sia in forma di floppy-disk che di CD-ROM o di USB flash storage). Si riportano qui di seguito le istruzioni per cancellare, con l'ausilio del software DBAN (Darik's Boot and Nuke), un hard-disk funzionante su un personal computer dotato di lettore di CD-ROM o di DVD.

Creazione del disco di avvio DBAN

Per prima cosa, occorre "scaricare" sul proprio computer il file immagine di DBAN, scegliendo quello adatto a essere "masterizzato" su CD o su DVD (<http://www.dban.org/download>). Il file dban-*_i386.iso va quindi salvato sul proprio computer e trasferito su CD (o DVD) utilizzando un software di masterizzazione. Il CD (o DVD) risultante sarà utilizzabile come "disco di avvio" del proprio computer.

Avvio della procedura di cancellazione sicura

Il computer che contiene il disco da cancellare dovrà essere avviato utilizzando il CD o DVD precedentemente creato, inserendo questo nel corrispondente lettore (drive) e procedendo al riavvio del sistema. Affinché il computer si avvii dal CD o DVD potrà rendersi necessario modificare l'ordine di scelta del dispositivo di avvio, tramite il cosiddetto BIOS setup solitamente accessibile poco dopo l'accensione del computer e prima che venga caricato il sistema operativo.

Cancellazione degli hard-disk con DBAN

Una volta avviato il computer con il disco di avvio DBAN, viene presentata una schermata di scelta tra diverse opzioni di avvio:

```
Darik's Boot and Nuke
-----
Warning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied
warranty of merchantability or fitness for a particular purpose. In no event
shall the software authors or contributors be liable for any damages arising
from the use of this software. This software is provided "as is".

http://www.dban.org/

* Press the F2 key to learn about DBAN.
* Press the F3 key for a list of quick commands.
* Press the F4 key for troubleshooting hints.
* Press the ENTER key to start DBAN in interactive mode.
* Enter autonuke at this prompt to start DBAN in automatic mode.

boot: _
```

Figura 1: Avvio di DBAN

Premendo il tasto INVIO (RETURN) della tastiera si avvierà la procedura interattiva di cancellazione. Successivamente viene presentata la scelta del disco da cancellare, tra quelli installati nel computer e riconosciuti da DBAN.

```
Darik's Boot and Nuke 1.0.7
-----
Options                               Statistics
Entropy: Linux Kernel (urandom)       Runtime:
PRNG: Mersenne Twister (mt19937ar-cok) Remaining:
Method: DoD Short                      Load Averages:
Verify: Last Pass                     Throughput:
Rounds: 1                              Errors:

-----
Disks and Partitions
-----
▶ [wipe] (SCSI 1,0,0,0,-) VMware, VMware Virtual S
[ ] (IDE 0,0,1,-,-) VMware Virtual IDE Hard Drive

P=PRNG M=Method U=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start
```

Figura 2: Scelta del disco da cancellare

Effettuata la scelta, occorrerà specificare quale metodo di cancellazione si vuole applicare. Per la maggior parte degli utilizzatori sarà sufficiente il cosiddetto "DoD short", derivato da standard militari USA: altri metodi, teoricamente ancora più sicuri, hanno lo svantaggio di richiedere tempi di elaborazione significativamente più lunghi, soprattutto se applicati a dischi di grande capacità.

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime:
Remaining:
Load Averages:
Throughput:
Errors:

----- Wipe Method -----

Quick Erase syslinux.cfg: nuke="dwipe --method dodshort"
RCMP TSSIT OPS-II Security Level: Medium (3 passes)
▶ DoD Short
DoD 5220.22-M
Gutmann Wipe
PRNG Stream

The American Department of Defense 5220.22-M short wipe.
This method is composed of passes 1,2,7 from the standard wipe.

J=Up K=Down Space=Select

```

Figura 3: Scelta del metodo di cancellazione

Successivamente il programma mostrerà lo stato di avanzamento della cancellazione:

```

Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG: Merseenne Twister (mt19937ar-cok)
Method: DoD Short
Verify: Last Pass
Rounds: 1
----- Statistics -----
Runtime: 00:00:11
Remaining: 00:00:19
Load Averages: 0.33 0.09 0.02
Throughput: 18260 KB/s
Errors: 0

(SCSI 1,0,0,0,-) VMware, VMware Virtual S
[34.01%, round 1 of 1, pass 2 of 3] [writing] [18260 KB/s]

```

Figura 4: Cancellazione in corso

fino al suo completamento:

```
DBAN succeeded.  
All selected disks have been wiped.  
Remove the DBAN boot media and power off the computer.  
  
Hardware clock operation start date: Sun Aug 13 15:24:36 2006  
Hardware clock operation finish date: Sun Aug 13 15:27:00 2006  
Saving log file to floppy disk... a floppy disk in DOS format was not found.  
DBAN finished. Press ENTER to save the log file._
```

Figura 5: Fine della cancellazione con DBAN

A questo punto, si potrà spegnere il computer con sufficiente certezza di non aver lasciato dati sul disco, potendo così procedere alla sua integrale o parziale cessione o smaltimento.

Demagnetizzazione e distruzione

Nel caso in cui il dispositivo elettronico da sottoporre a smaltimento non sia più funzionante, e non siano pertanto applicabili le misure software, allo scopo di garantire l'impossibilità di recupero dei dati da parte di terzi estranei occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (degausser), o con la distruzione fisica.

I degausser permettono l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.

In determinati casi è necessario ricorrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con appositi macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superfici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.