Azzarone Antonio

IT SECURITY

Il modulo sull'IT security definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell' I.T. C. nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

Comprendere l'importanza di rendere sicure informazioni e dati, e identificare i principi per assicurare protezione, conservazione e controllo dei dati e della riservatezza (privacy). • Riconoscere le minacce alla sicurezza personale, quali il furto di identità, e le potenziali minacce ai dati, derivanti ad esempio dal cloud computing. • Saper usare password e cifratura per mettere in sicurezza i file e i dati. • Comprendere le minacce associate al malware

- Dato ⟶ Informazione non ancora elaborata
- Informazione ⟶ Risultato dell'utilizzo dei dati
- Crimine informatico ⟶ Attività illecita nell'utilizzo del mezzo informatico
- EULA ⟶ End User License Agreement contratto con l'utente finale

- Hacking ⟶ Attività di accesso alla rete senza autorizzazione.
- Cracking ⟶ Violazione del sistema a scopo di lucro

Cracking di password

↓

Attività di pirateria per il recupero delle password in maniera manuale o con programmi

Cracking di software

↓

Attività di pirateria che rimuove le protezioni dei programmi

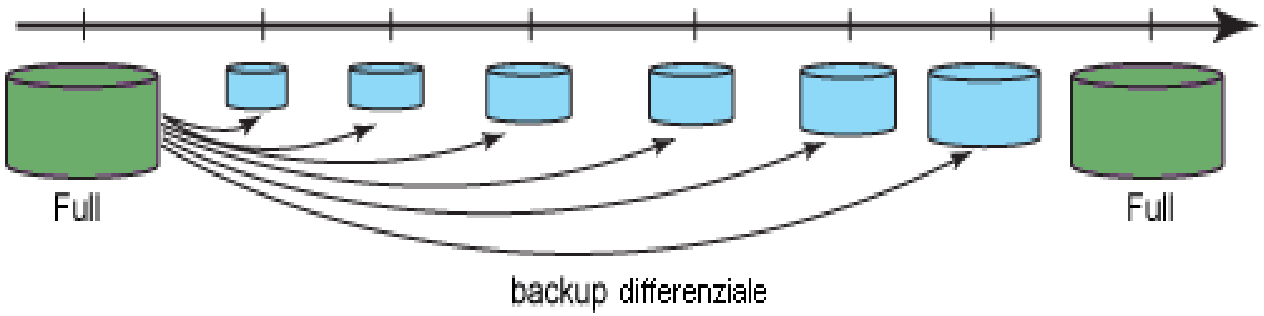
- Hacking etico ⟶ Violazione del sistema informatico a scopo di bene

Salvataggio dei dati dati

- Causa di forza maggiore ⟶ Furto, cause naturali, incendi

Backup

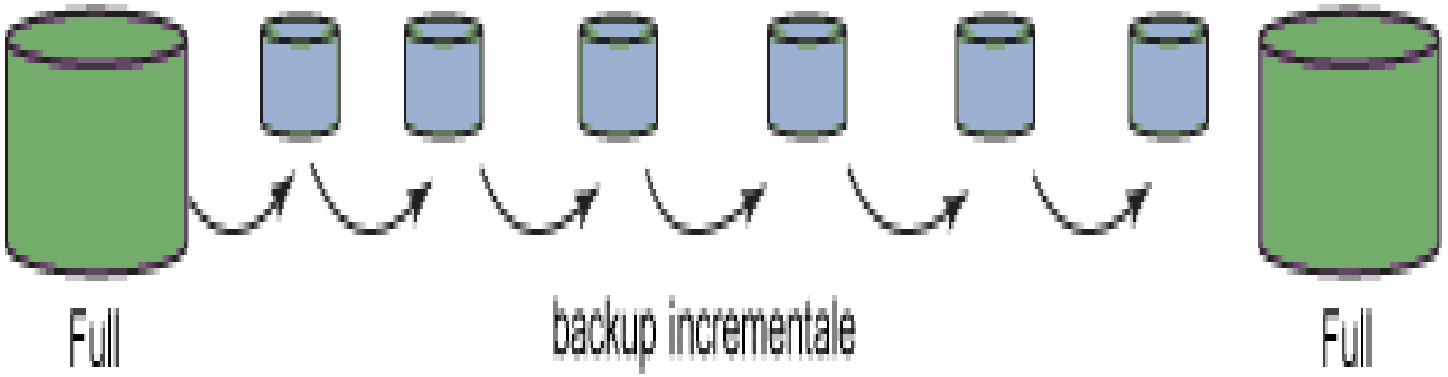
- Backup completo ⟶ Copia di tutti i dati
- Backup differenziale ⟶ solo le modifiche che sono state apportate dall'ultima immagine completa



- **Vantaggi**
- Le immagini differenziali create dopo l'iniziale immagine completa sono create molto velocemente, perché vengono salvate solo le modifiche apportate ai file dall'ultimo backup completo.
- La quantità di spazio su disco utilizzato dalle immagini differenziali è significativamente inferiore a quella di immagini complete
- Sono necessari due soli file di immagine per ripristinare il sistema (quello full + l'ultimo differenziale)
- **Svantaggi**
- Man mano che aumenta il tempo dall'ultimo backup completo, la dimensione dell'immagine differenziale crescerà, così come crescerà il tempo necessario per la sua creazione. Per ridurre questo tempo, è necessario eseguire occasionalmente una immagine completa per diminuire nuovamente la dimensione delle immagini differenziali successive.

Backup incrementali

- Backup incrementali necessitano che sia eseguito prima un backup completo.
- La differenza principale è che sono memorizzate solo le ultime le modifiche del file dall'ultima immagine, sia essa completa o incrementale. Il set di backup risultante sarà quindi costituito da una immagine completa e da un numero di immagini incrementali che devono essere tutte presenti per poter ripristinare il sistema correttamente.



- **Vantaggi**
- Nei backup incrementali sono memorizzate le sole modifiche che sono state apportate dall'ultima immagine completa o incrementale. Sono sempre piccole e molto veloci da effettuare, soprattutto se fatte spesso.
- **Svantaggi**
- Il solo svantaggio di utilizzare le immagini incrementali è che tutti i file devono essere conservati. Infatti se dovesse mancare anche una sola delle immagini intermedie incrementali, non sarà possibile ripristinare il sistema all'ultimo backup.

Minacce ai dati

- Provocate da:
- Impiegati.
- Fornitori di servizi
- Persone esterne

Protezione dei dati personali

- Furto di identità

- Ingegneria sociale ⟶ attività di carpire informazione ingannando l'utente allo scopo di realizzare frodi od accedere sistemi informatici in modo non autorizzato.

Tecniche di ingegneria sociale

- Phishing ⟶ Furto di dati via mail
- Finte promozioni o vincite
- Bin – raiding ⟶ Documenti cartaci scartati
- Contatti indesiderati.
- Furto o smarrimento del portafogli.
- Skimming ⟶ clonazione della carta di credito
- Rubare identità di un deceduto.
- Tramite noi stessi
- Shoulder surfing ⟶ Osservare la vittima mentre si inseriscono le credenziali.

Crittografia

- Identificazione ⟶ Nome Utente
- Autetificazione ⟶ Password
- Cifratura ⟶ Tecnica che offusca il messaggio ai non autorizzati

Caratteristiche fondamentali della crittografia

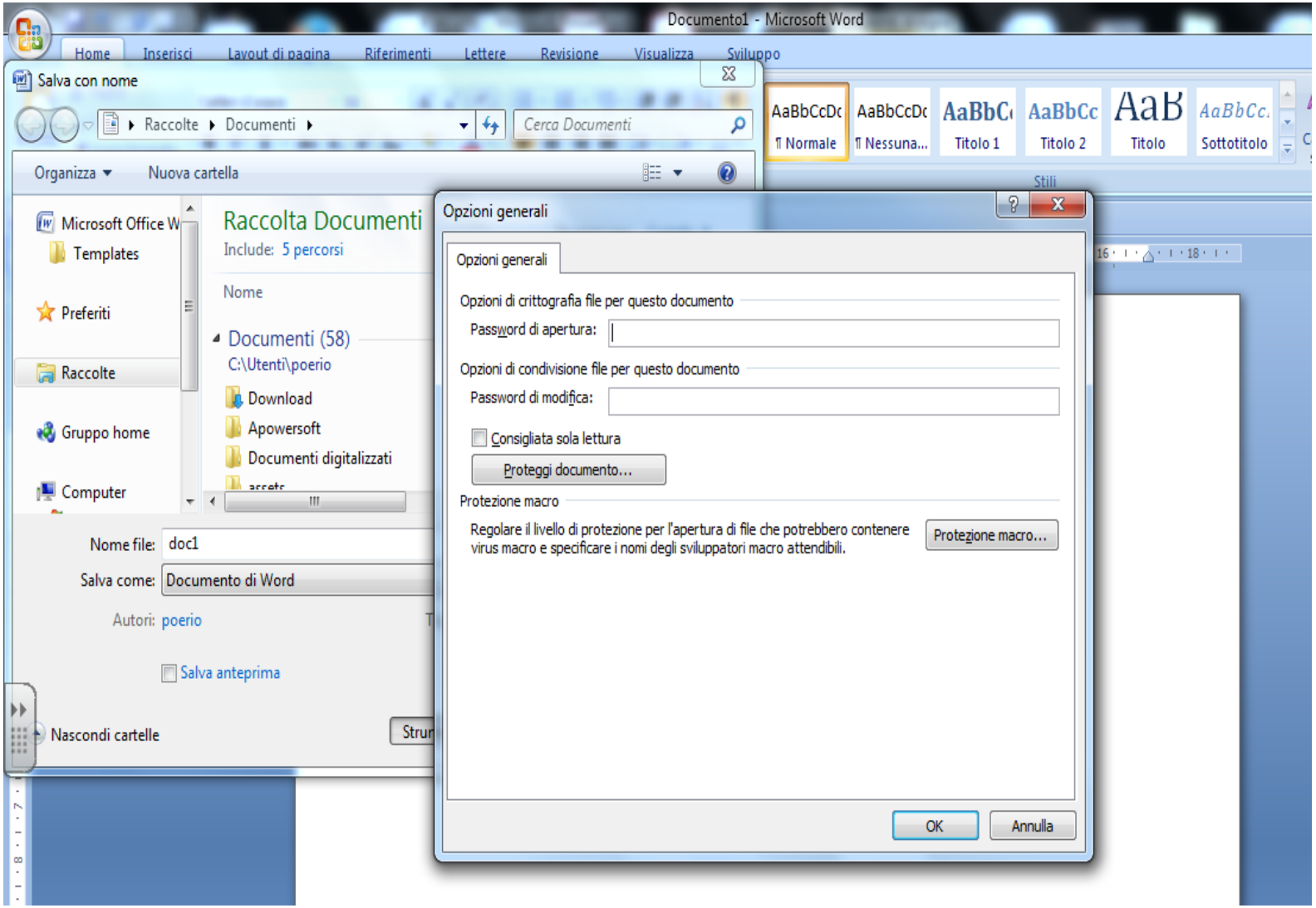
- Confidenzialità ⟶ i dati personali devono essere protetti da divulgazioni o accessi non autorizzati.
- Integrità ⟶ l'informazione deve essere integra cioè senza modifiche rispetto all'originale.
- Disponibilità ⟶ dei dati al momento del bisogno

Linee guida politiche per l'uso delle ITC

- Non lasciare che i dettagli dei principali conti delle aziende siano di pubblico dominio.
- Predisporre un'accurata gestione e archiviazione dei documenti.
- Distruggere i dati sensibili.
- Mettere i dipendenti a conoscenza dei rischi di frode.
- Assicurarsi che la procedura di gestione dei documenti sia eseguita correttamente dai dipendenti.
- Assicurarsi che il sistema antivirus e firewall siano tenuti aggiornati.

Sicurezza dei file

- Macro ⟶ Automazioni scritte in linguaggio visual BASIC da attivare solo se la provenienza è sicura.
- Impostare la password ai file office.
- File ⟶ salva con nome ⟶ strumenti ⟶ opzioni generali
- Impostare password per file compressi


Documento1 - Microsoft Word
Home
Inserisci
Layout di pagina
Riferimenti
Lettere
Revisione
Visualizza
Sviluppo
Salva con nome
Raccolte ▸ Documenti ▸
Cerca Documenti
Organizza
Nuova cartella
Microsoft Office W
Templates
Preferiti
Raccolte
Gruppo home
Computer
Raccolta Documenti
Include: 5 percorsi
Nome
Documenti (58)
C:\Utenti\poerio
Download
Apowersoft
Documenti digitalizzati
Nome file: doc1
Salva come: Documento di Word
Autori: poerio
Salva anteprima
Nascondi cartelle
AaBbCcDc ¶ Normale
AaBbCcDc ¶ Nessuna...
AaBbC Titolo 1
AaBbCc Titolo 2
AaB Titolo
AaBbCc. Sottotitolo
Stili
Opzioni generali
Opzioni generali
Opzioni di crittografia file per questo documento
Password di apertura:
Opzioni di condivisione file per questo documento
Password di modifica:
Consigliata sola lettura
Proteggi documento...
Protezione macro
Regolare il livello di protezione per l'apertura di file che potrebbero contenere virus macro e specificare i nomi degli sviluppatori macro attendibili.
Protezione macro...
OK
Annulla

Malware

- Software dannoso fatto per creare danni al software o/e all'hardware o per prelevare dati.
- Si trasmette tramite rete e_mail o chiave USB
- Virus programma che per infettare ha bisogno dell'intervento umano

Dove si nasconde il malware

- Troian ⟶ file malizioso che si nasconde all'interno di programma apparentemente
- Rootkit ⟶ software o insiemi di software capace di controllare il PC
- Backdoor ⟶ "porte sul retro" consentono di superare le procedure di sicurezza.

- Virus: programma che si attiva e si diffonde quando si verifica l'evento atteso (per esempio si apre un file).
- Vorm: (verme) duplica se stesso si attiva in modo automatico quando viene acceso il PC non ha bisogno di attaccarsi ad altri file per propagarsi.
- Adware: Programma che propone messaggi pubblicitari attraverso aperture finestre pop-up rallentato il sistema e possono inviare informazioni sulla navigazione, modifica la pagine del browser

- Spyware: Non attacca il PC ma raccoglie informazione (password, dati di carta di credito o informazioni sulla navigazione)
- Botnet: "rete di bot" permette ad un acker di prendere possesso del PC lo stesso diventa uno "zombie" permette di attaccare PC in massa anche ad enti governativi si possono sferrare attacchi di "Denial of Service".
- Keylogger: Programmi che possono copiare quello che si digita sulla tastiera del PC trasferendo i dati all'esterno copiando PIN o password

- Dialler: Programma che si installa sul PC deviando la connessione verso numeri a pagamento molto costosi.
- Ransomware: Software che si installano nel PC bloccando i file chiedendo un riscatto in danaro per sboccarli.

Antivirus

- Programmi per combattere i virus.
- Protezione "real time" scanzione in tempo reale mentre si naviga.
- Aggiornare l'antivirus: aggiornare le definizione dei virus.
- Scansione veloce: I virus sono cercato solo su alcuni punti del PC.
- Completa: Tutto il PC
- Personalizzata: solo alcune cartelle.
- Quarentena: file messi in attesa di essere rimossi.

Le reti

- LAN: Local Area Network piccola rete locale non attraversa suolo pubblico.
- MAN: Metropolitan Area Network rete più estesa che attraversa il sulo pubblico
- WAN: Wide Area Network: rete estesa con molti calcolatori collegati quella a livello mondiale è Internet.
- VPN: Virtual Private Network reti lan distanti che comunicano tra loro come se fossero vicine usando la rete pubblica

Amministratore di rete

- L' amministratore di rete è la figura professionale che si occupa della gestione e manutenzione della rete e si occupa degli aspetti legali per la protezione dei dati.
- E' responsabile delle politiche di accesso decide chi deve accede a cosa.
- La gestione degli accessi avviene con la creazione di account (nome utente e password)

Firewall

- Firewall (muro taglia fuoco) può essere un software, un hardware un computer o un insieme di computer.
- E' situato al confine tra un computer o una rete e l'esterno
- Serve per proteggere la rete da attacchi esterni o attraverso opportuni filtri impedisce a programmi di accedere ad internet senza in consenzo

Connessione delle reti

- Connessione via
- Connessione wireless
- Connessione via cavo possono essere di tipo elettrico.
- Doppino telefonico due cavi di rame 9600bps.
- Cavo coassiale 10Mbps.
- Cavi ottici

Sicurezza per reti wireless

- SSID: (Service Set Identifier) nome della rete.
- WEP: Password alfanumerica a 64 128 o 256 bit.
- WPA: sostituisce la WEP usa un algoritmo per offuscare e la crittografia.
- WPA2: ha sostituito la WPA ed è un'evoluzione della WPA. Usa chiavi da 10 a 64 caratteri

- WPA-PSK: Usa una chiave di autentificazione come in WEP, metodo di cifratura come in WPA.
- MAC: Media Access Control = Codice univoco assegnato dal produttore.

Controllo degli accessi

- Account di rete: credenziali (nome utente e password) per accedere alle risorse a cui è autorizzato.
- Rete paritetico: Rete senza server ogni PC funziona da server e da client.
- Client/server: Il server offre le sue potenzialità al client.

- Attacco “a forza bruta” mediante software che prova tutte le combinazioni possibili, o a “dizionario” prova una serie di termini usuali.
- Tecniche di phishing o “ingegneria sociale” usano messaggi di mail ma anche contatti telefonici ingannando l’utente.
- Installare programmi in grado di trefugare informazioni.

- Tecniche biometriche: Permettono di autenticare le persone in base a caratteristiche fisiche.
- Riconoscimento vocale: Rileva il timbro e la tonalità della voce.
- Impronte digitali: rileva le impronte umane.
- Scansione dell'Iride dell'occhio: Fotografa l'iride, salva l'immagine in un data base per potere effettuare il riconoscimento.

Uso sicuro del web

- Siti web protetti protezione con certificato rilasciati da enti certificatori.
- Pharming: Link ad un sito clone.
- One Time Password: password che si usa una sola volta.

Uso del brower sicuro

- Completamento Automatico: Propone valori inseriti in moduli simili o in navigazioni precedenti.
- Per disattivare il completamento automatico

Explorer

•Strumenti
•Opzione internet
•Scheda contenuti
•Impostazione (completamento automatico)
Selezionare gli elementi da abilitare/disabilitare

Chrome

Premere sul pulsante con tre punti verticali in alto a destra

Impostazioni.
scorrere in basso e premere su "Avanzate".
Sotto la sezione *Privacy e sicurezza* si deve spegnere l'interruttore alla voce: "*Utilizza le previsioni per completare i termini di ricerca e gli URL digitati nella barra degli indirizzi*" per disattivare la funzione dei suggerimenti automatici.

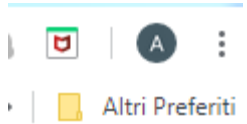
- Cookie: piccoli file di testo scritti dai siti web per memorizzare informazioni utili a velocizzare la navigazione.
- Per visualizzare i cookie

Explorer

Strumenti
Opzione internet
Scheda generale
Impostazione
Visualizza files

Chrome

Premere sul pulsante con tre punti verticali in alto a destra
Impostazioni
scorrere in basso e premere su "Avanzate“
Sotto la sezione *Privacy e sicurezza*
Impostazioni contenuti
Cliccare su cookie
Mostra tutti i cookie



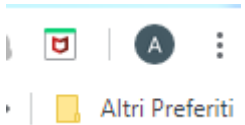
Eliminare i cookie

Explorer

Strumenti
Opzione internet
Scheda generale
Cronologia esplorazione
Elimina
Cliccare su cookie
Elimina

Chrome

Premere sul pulsante con tre punti verticali in alto a destra
Impostazioni
scorrere in basso e premere su "Avanzate“
Sotto la sezione *Privacy e sicurezza*
Cancella dati di navigazione
Cliccare su cookie
Elimina i dati



Personalizzare le impostazioni dei cookie

Explorer

Strumenti
Opzione internet
Scheda Privacy
Utilizzare il cursore per aumentare/ diminuire la protezione
Cliccare su SITI per bloccare /consentire siti specifici

Chrome

Premere sul pulsante con tre punti verticali in alto a destra
Impostazioni
scorrere in basso e premere su "Avanzate“
Sotto la sezione *Privacy e sicurezza*
Impostazione contenuti
Cliccare su “COOKIE”

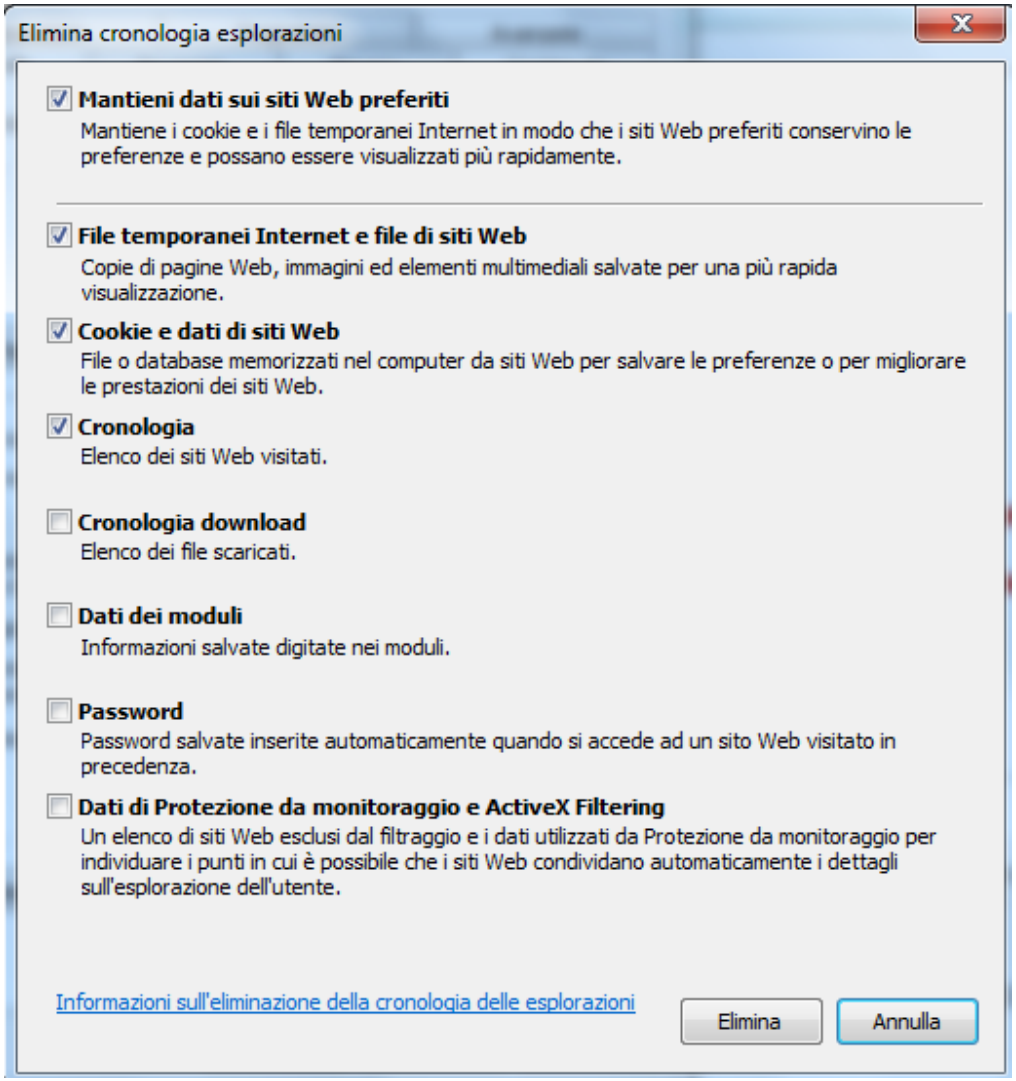
Tipi di cookie

cookie di sessione, i quali vengono cancellati immediatamente alla chiusura del browser
cookie persistenti, rimangono all'interno del dispositivo continuando ad operare anche successivamente alla chiusura del browser e fino al decorso di un determinato periodo di tempo
cookie di prima parte ossia cookie generati e gestiti direttamente dal soggetto gestore del sito web sul quale l'utente sta navigando
cookie di terza parte, i quali sono generati e gestiti da soggetti diversi dal gestore del sito web sul quale l'utente sta navigando

Eliminare i dati da un browser

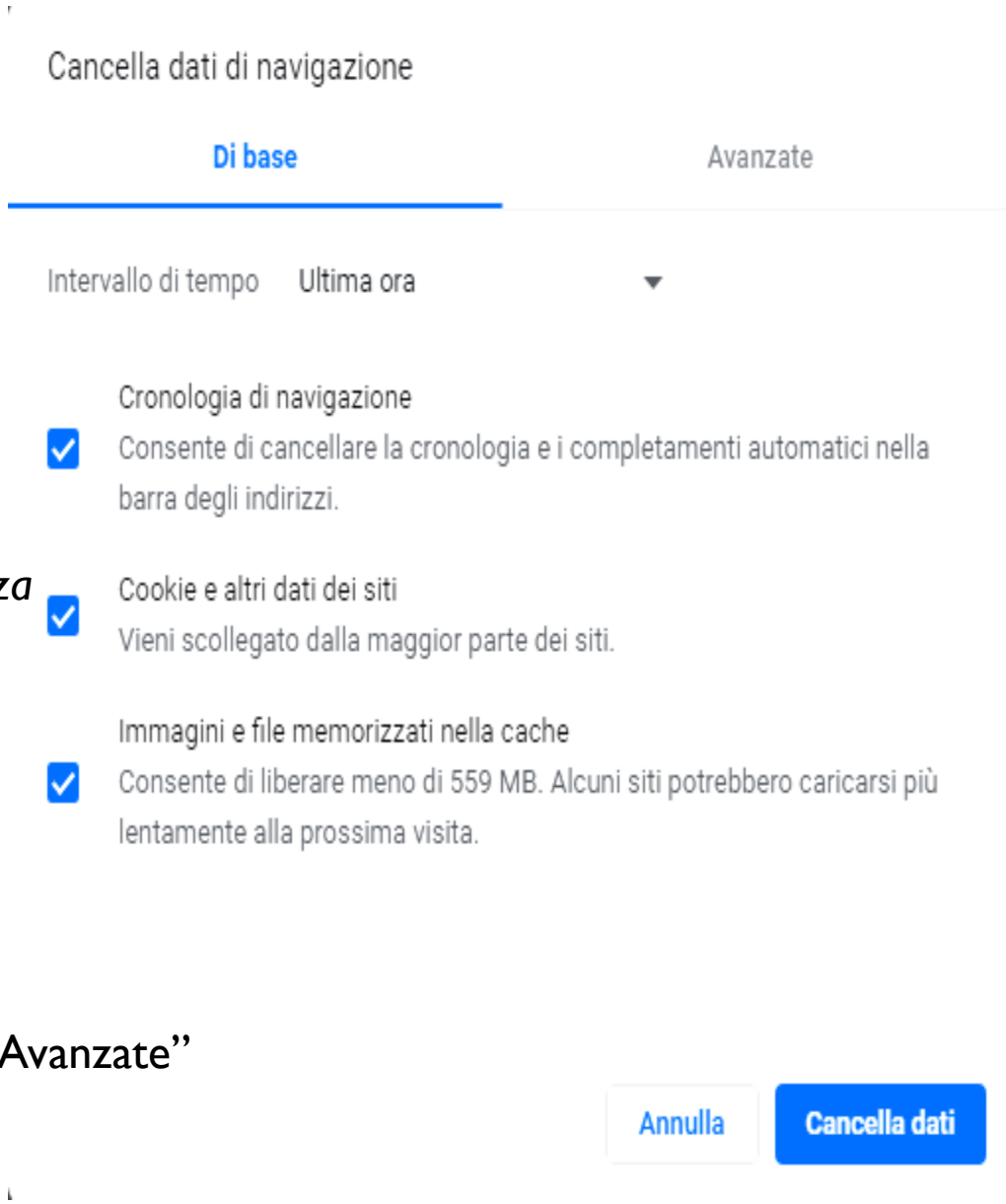
Explorer

Strumenti
Opzione internet
Scheda Generale
Cliccare su ELIMINA
Selezionare gli elementi da eliminare



Chrome

Premere sul pulsante con tre punti verticali in alto a destra
Impostazioni
scorrere in basso e premere su "Avanzate“
Sotto la sezione *Privacy e sicurezza*
Impostazione contenuti
Cliccare su
“Cancella dati di navigazione“



Si può scegliere “Di Base” o “Avanzate”
E l’intervallo di tempo

Controllo dei contenuti dei siti

- Opzioni Internet ⟶ Sicurezza

Quattro aree di sicurezza

- Internet: Il livello di sicurezza è applicato a tutti i siti web.
- Intranet locale: siti web archiviati nella rete aziendale.
- Siti attendibili: siti che si reputano attendibili e non pericolosi.
- Siti con restrizione: siti che potrebbero danneggiare il PC.
- Livello personalizzato: Disabilitare alcune funzioni ad esempo il download

Controllo genitore (W7)

- Pannello di controllo ⟶ Controllo genitore
- Restrizione di orario.
- Restizione di giochi
- Restrizione di programmi.

Controllo genitore (W10)

- Per utilizzare Windows' parental controls, accedere s con un account Microsoft (che non è un account locale). Questo è un cambiamento rispetto alle precedenti versioni di Windows, ma consente di applicare le impostazioni di controllo genitori su tutti i dispositivi Windows.
- Verrà chiesto di crearne uno quando si imposta l'account del figlio.

- Una volta che il bambino ha creato l' account in Windows, è possibile iniziare a utilizzare il controllo genitori disponibili da Microsoft Family portale web.
- 1. **Accedi al https://account.microsoft.com/family#/** con il tuo account Microsoft.
- **Scegliere il nome del vostro bambino.**
- **Rivedere e regolare l'Attività di reporting** sulla principale pagina account per il vostro bambino. Attività di reporting e-mail settimanale. I rapporti sono attivati per impostazione predefinita. È possibile deselezionare o alternare queste impostazioni e anche visualizzare l' attività di navigazione web.

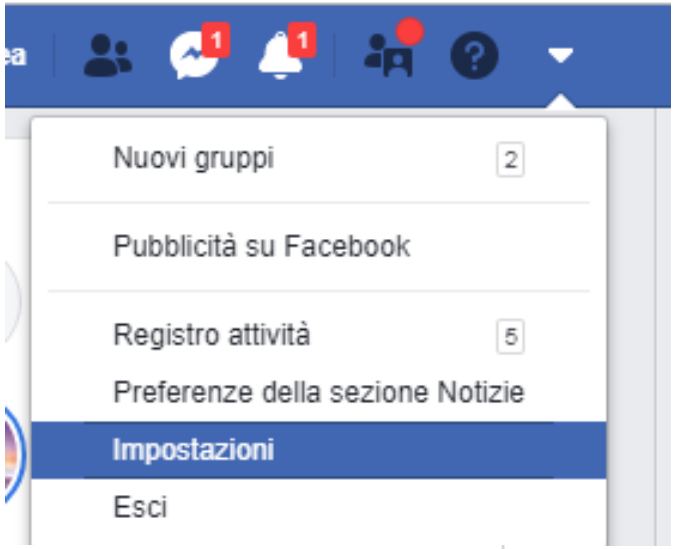
- **Bloccare siti specifici o applicazioni.**
- **Alterna contenuti inappropriati blocco off o on.** Contenuti per adulti è bloccato per impostazione predefinita.
- **Aggiungere gli Url** per i siti web che si desidera consentire al bambino.
- **Permettere o non permettere ai bambini di scaricare apps** e giochi
- **Accendere limiti di tempo.**
- **Scegliere gli orari in cui il vostro bambino può utilizzare il computer**
- **Revisione del vostro bambino di spesa nel Negozio.** Questa pagina mostra l'elenco degli acquisti con Microsoft Store e Xbox store.
- .**Aggiungere i soldi per il vostro bambino account Microsoft**

Social network

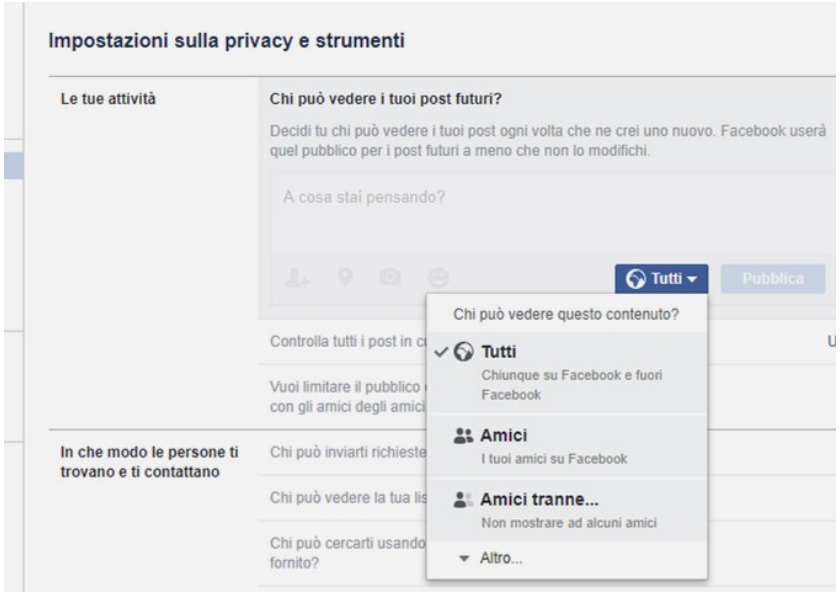
- Comunità virtuale: Gruppi di persone che si riuniscono via Internet per valori o interessi comuni.
- Scopo dei social network è di comunicare e condividere con altre persone.
- Mettere in contatto persone e far nascere relazioni.
- E' possibile creare la propria pagina web, pubblicare link, immagini video, testo.
- Per iscriversi bisogna compilare un modulo e fornire i propri dati personali standard.

Impostazione per la privacy

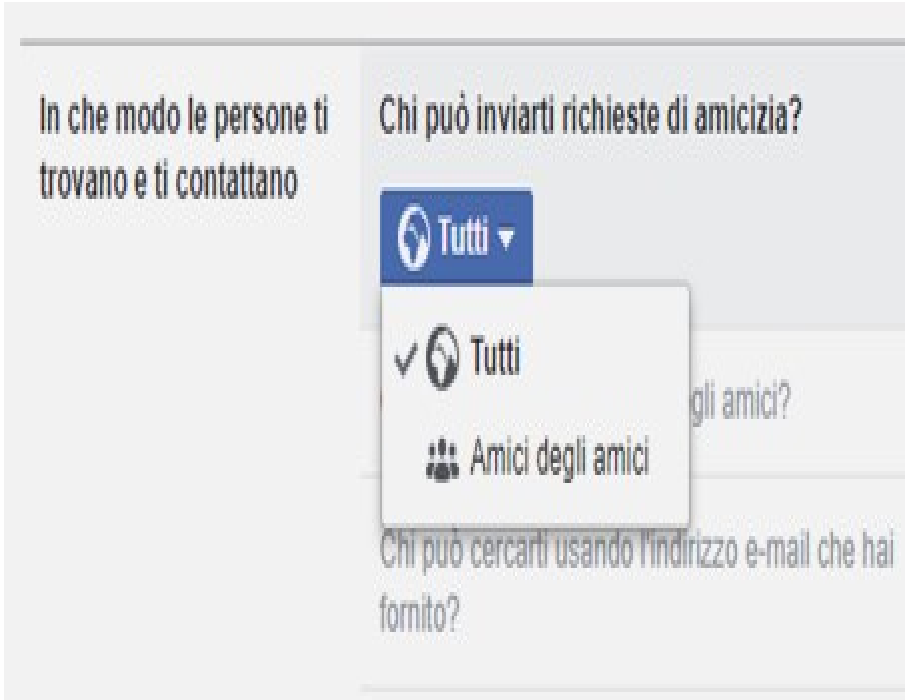
- In alto sulla destra cliccare sul triangolo e su impostazione.
- Sulla sinistra scheda privacy



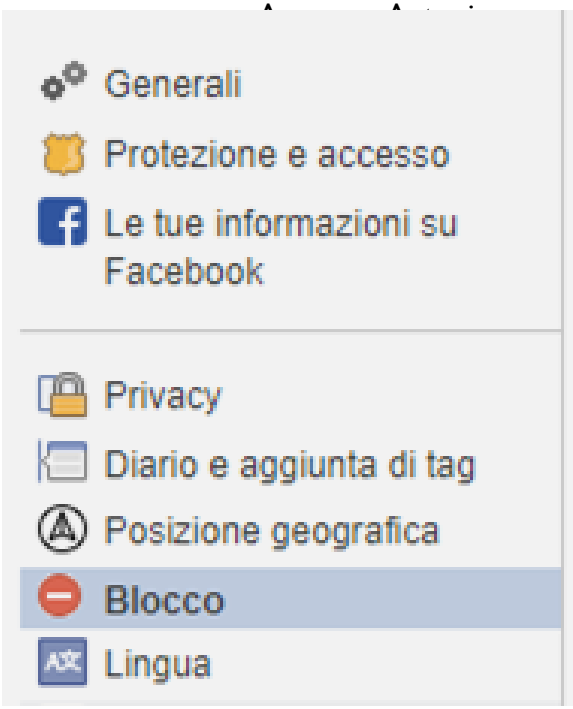
- “Chi può vedere le mie cose”: si configura la visibilità dei post futuri.



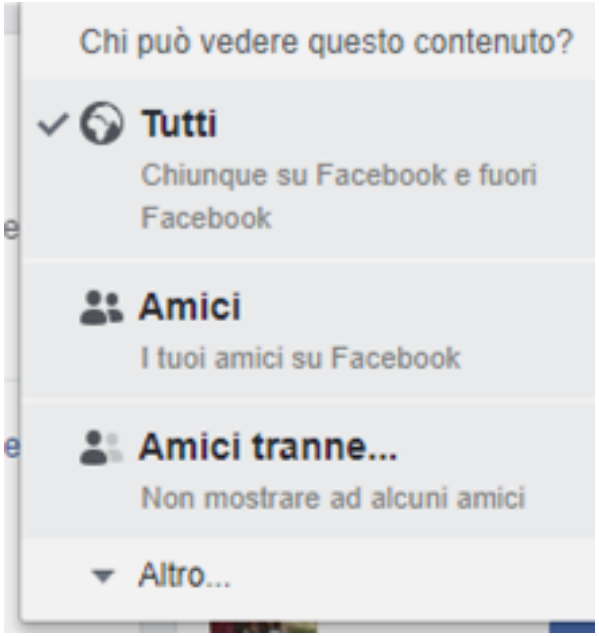
- “Chi può contattarmi” la possibilità di altre persone di contattare o inviare richieste di amicizia



- Sulla destra “blocco” per bloccare una persona



- Impostare limitazioni a singoli elementi del profilo (es, foto)



Rischi nell'uso dei social network

- Cyberbullismo: Utilizzo della rete per attaccare ripetutamente un individuo.
- Adescamento o grooming: Tecnica psicologica per l'adescamento di minori per ottenere comportamenti inappropriati.
- Reato recentemente introdotto nel nostro codice penale non è necessario che l'incontro con il minore avviene basta solo che l'adulto conquista la fiducia di un bambino.
- False identità o "fake": Creare falsi profili.

Posta elettronica in sicurezza

- Chiunque può spedire un messaggio falsificando il nome, per sopperire a questa c'è la firma digitale.
- **Integrità**: Il destinatario non può alterare il contenuto del documento ne creare uno nuovo facendolo risultare firmato da qualcun altro
- **Autenticità**: Il destinatario è sicuro del mittente.
- **Non ripudiabilità:** Il mittente non può negare di aver inviato il documento da lui firmato

Firma Digitale

- Si basa su una coppia di chiavi asimentriche.
- Una chiave A corrisponde ad una sola chiave B
- Delle due chiavi una è pubblica.
- Codificato un documento con la chiave privata il destinatario potrà prelevare la chiave "pubblica" e decodificarlo
- Il meccanismo prevede l'utilizzo di una funzione Hash per ricavare l'impronta (digest)del documento circa 160byte indipendente dalla lunghezza del documento

Mail indesiderati

- Spam: Messaggi pubblicitari non richiesti per indurre ad acquistare qualcosa.
- Pishing: Messaggio simile ad un avviso ufficiale inviato da una fonte attendibile (es. Banca).
- Malaware. Software dannoso in allegato alla mail.

Sicurezza della messaggistica istantanea e VOIP

- Anche l'IM comporta rischi di ricevere un malawere all'apertura di file allegati o link che porta ad un sito infetto.
- Bloccare i mittenti indesiderati.
- Non fornire informazioni personali.
- Non aprire colleganti o allegati non richiesti
- VOIP è il trasporto di voce sotto forma di dati, un‘ intruso può intercettare i pacchetti dati e trasformarli in file audio, inoltre è possibile attivare i microfono ed intercettare le conversazioni

Autorizzazione delle applicazioni

- Ogni app per potere funzionare ha bisogno delle autorizzazioni.
- La visualizzazione delle autorizzazioni ha lo scopo di impedire la diffusione di app dannose.
- Le app possono accedere a molte informazioni di carattere personale.
- E' sempre opportuno verificare se l'applicazione che si sta utilizzando è coerente per il proprio scopo

- Alcune autorizzazioni possono trasmettere i codici IMEI e IMSI che potrebbero rintracciare il telefono.
- IMEI (International Mobile Equipment Identity)è un codice numerico che identifica il terminale mobile ed è salvato nella memoria non volatile del cellulare.
- IMSI (International Mobile Subscriber Identity): numero memorizzato nella SIM che identifica una coppia SIM-operatore, ossia la SIM.

Messa in sicurezza dei dispositivi

- Per prevenire il furto di dati è necessario mettere in sicurezza i dispositivi.
- Bisogna valutare di volta in volta la situazione dove è situato il PC (casa, ufficio, laboratorio, rivendita di PC)
- Molti PC hanno una fessura sul case per potere mettere in sicurezza il PC.
- Inserire un password nel BIO per evitare il ravvio della macchina.

Copie di sicurezza

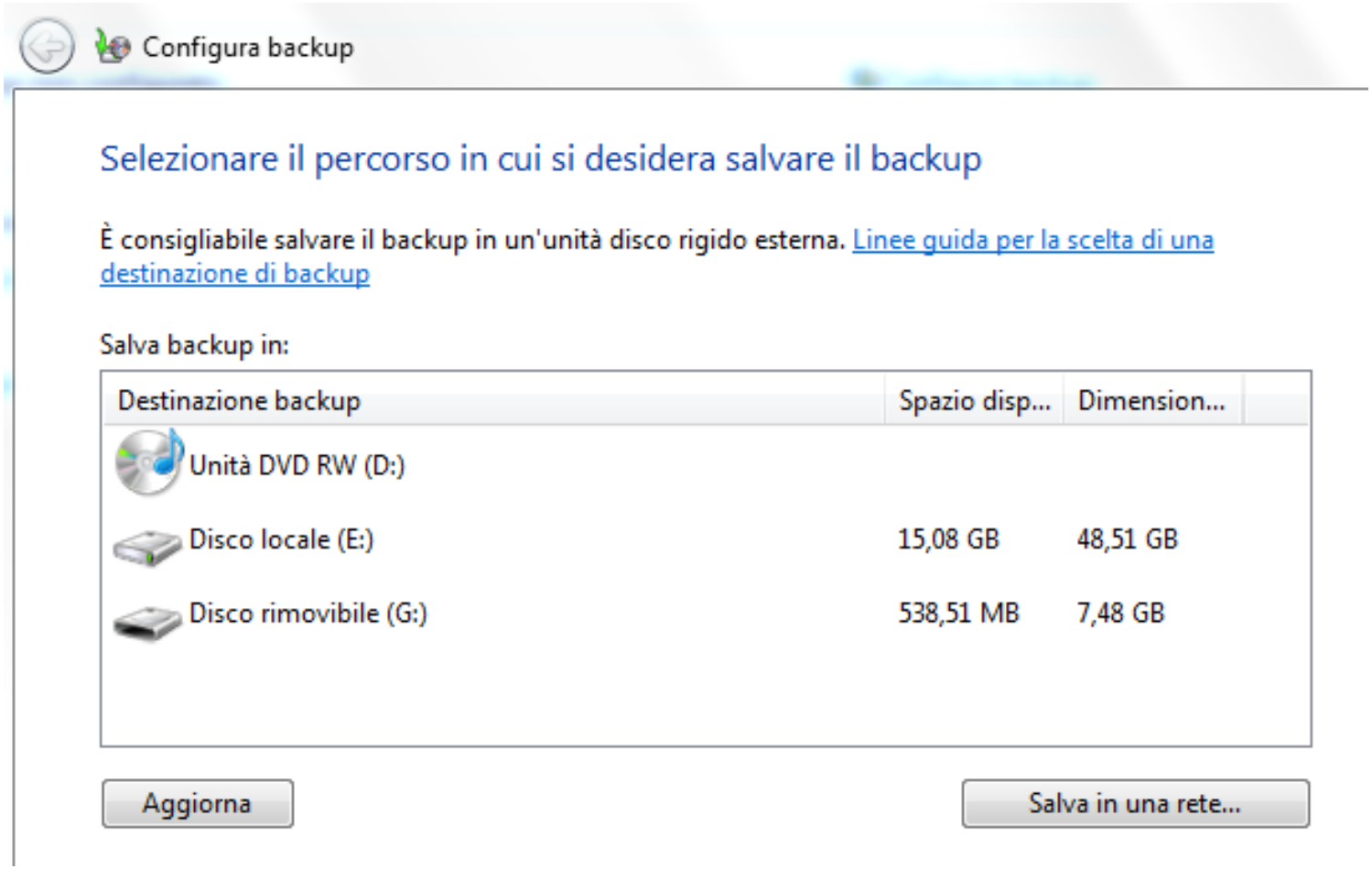
- E' opportuno impostare un programma di copia in modo che questa avvenga quando il PC non è utilizzato.
- Le copie vanno conservate in un luogo diverso da quello dove è situato la macchina.
- La frequenza delle copie dipende dalla rapidità con cui cambiano i dati.
- E' importante valutare quali dati salvare.
- Esistono diversi tipi dispositivi di memorizzazione con vantaggi e svantaggi è preferibile fare la copia su di un unico dispositivo.

Come effettuare un backup

- Primo passo da fare è configurare il backup
- Star ⟶ Pannello di controllo ⟶ Backup e ripristino

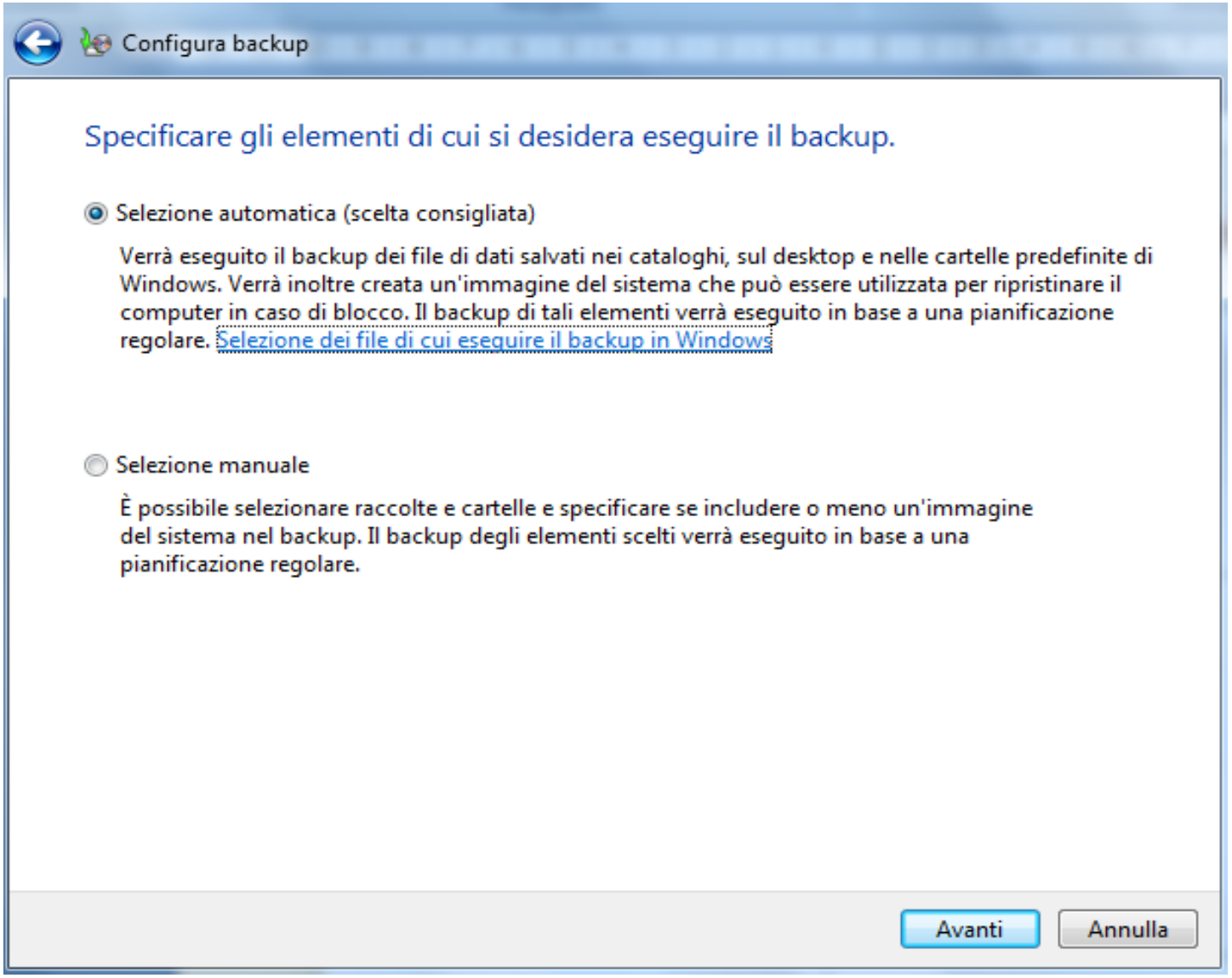
- Cliccare su Configura backup
- Bisogna indicare il supporto dove memorizzare il salvataggio

- Bisogna indicare il supporto dove memorizzare il salvataggio



- Evitare di salvare nello stesso disco rigido dove è installato Windows.

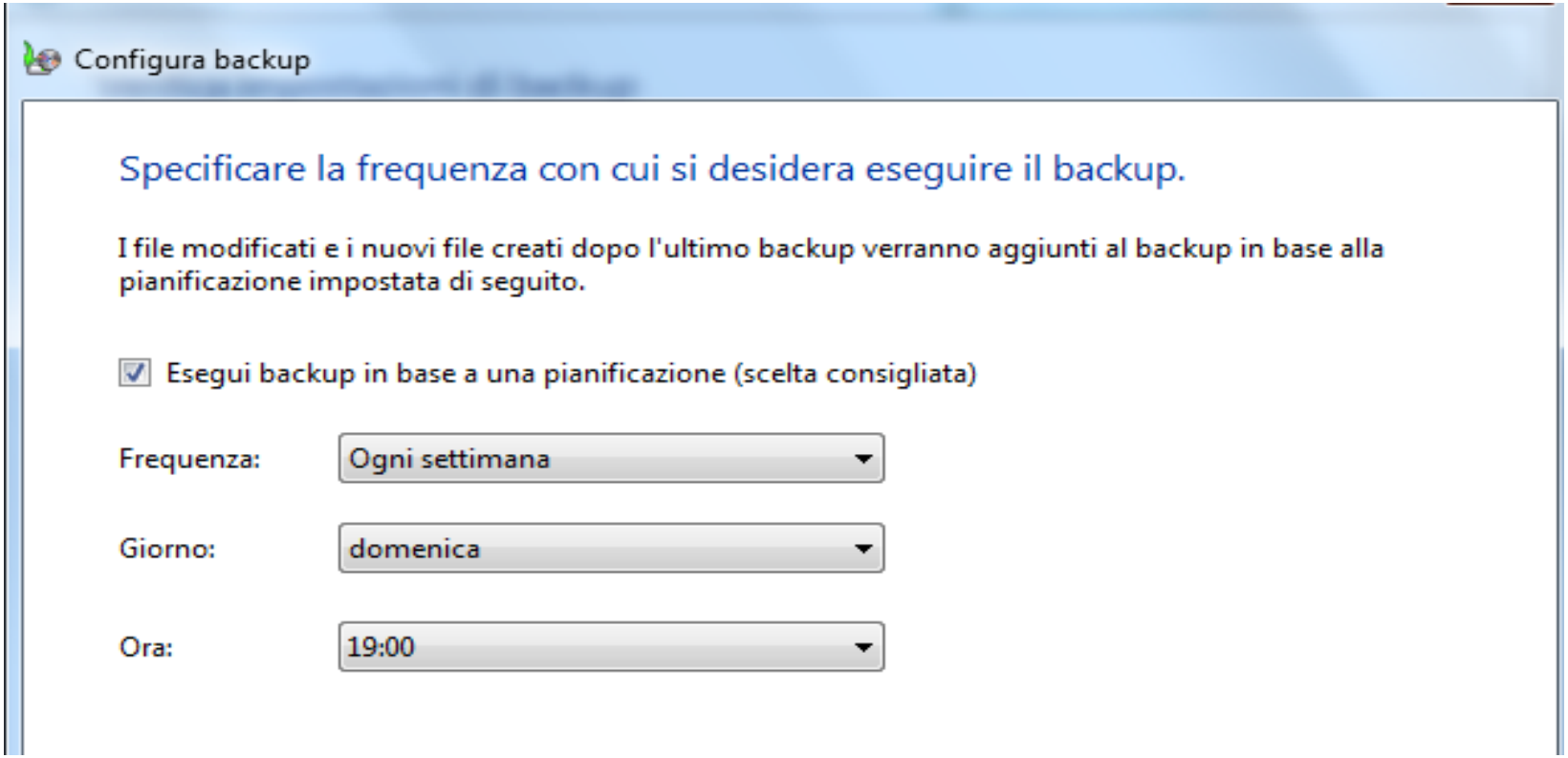
- Selezionare gli elementi da copiare con il backup



- Nella selezione automatica saranno inclusi i file salvati nelle raccolte (Documenti, Immagine, Video, Musica), sul desktop e nelle cartelle specifiche di windows.
- Nella selezione manuale si possono scegliere delle cartelle specifiche.

Pianificare il backup

- Con la pianificazione non è necessario ricordarsi di fare il backup, le impostazioni si possono cambiare in qualsiasi momento.



Ripristinare i dati

- La procedura inversa al backup è il **ripristino.**
- Si può ripristinare l'ultima versione di backup o una versione precedente in questo caso si chiama **Versioning.**
- Dopo avere scelto la versione si scelgono le cartelle da ripristinare

- A questo punto bisogna specificare se ripristinare i files nella posizione originale o in una posizione diversa

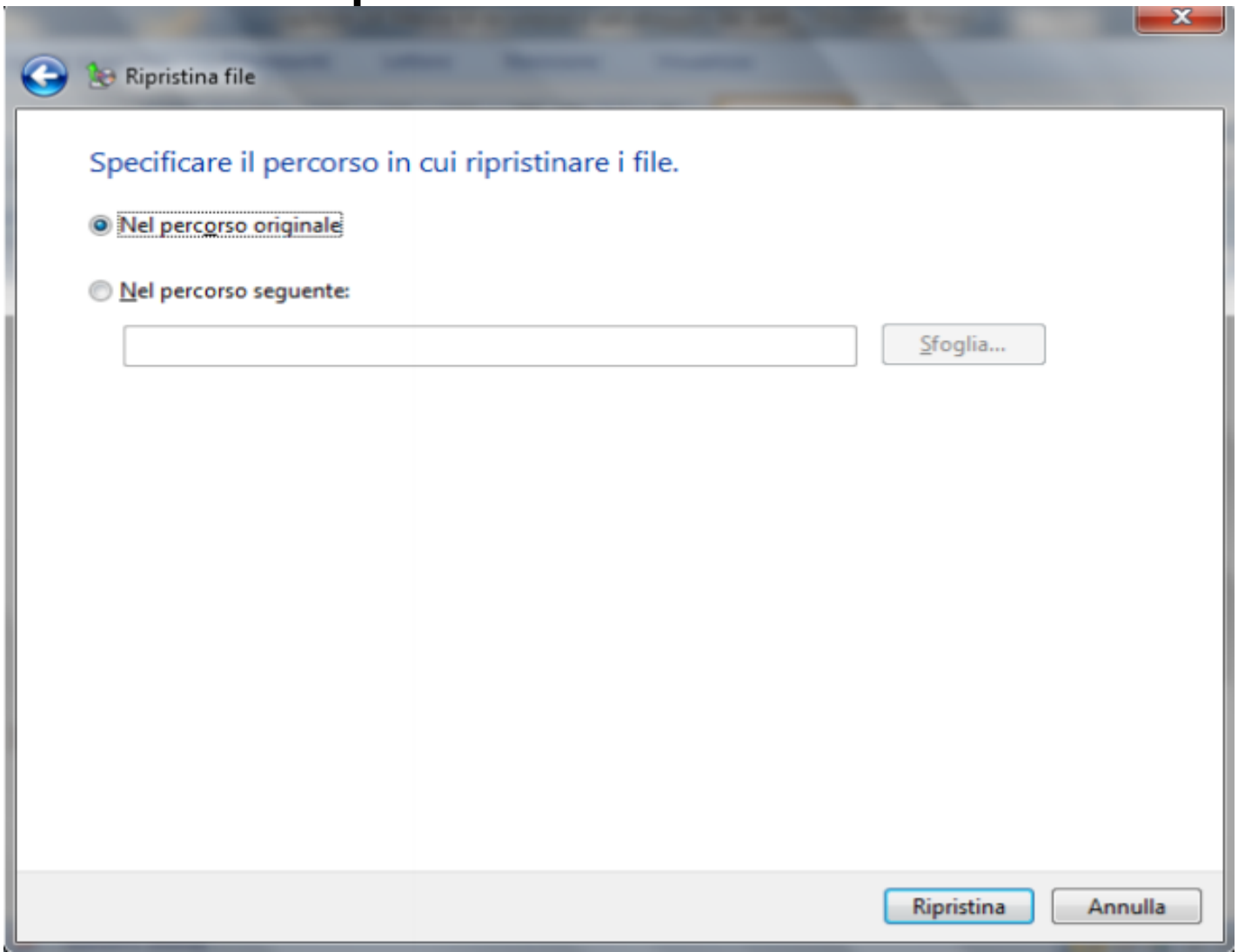
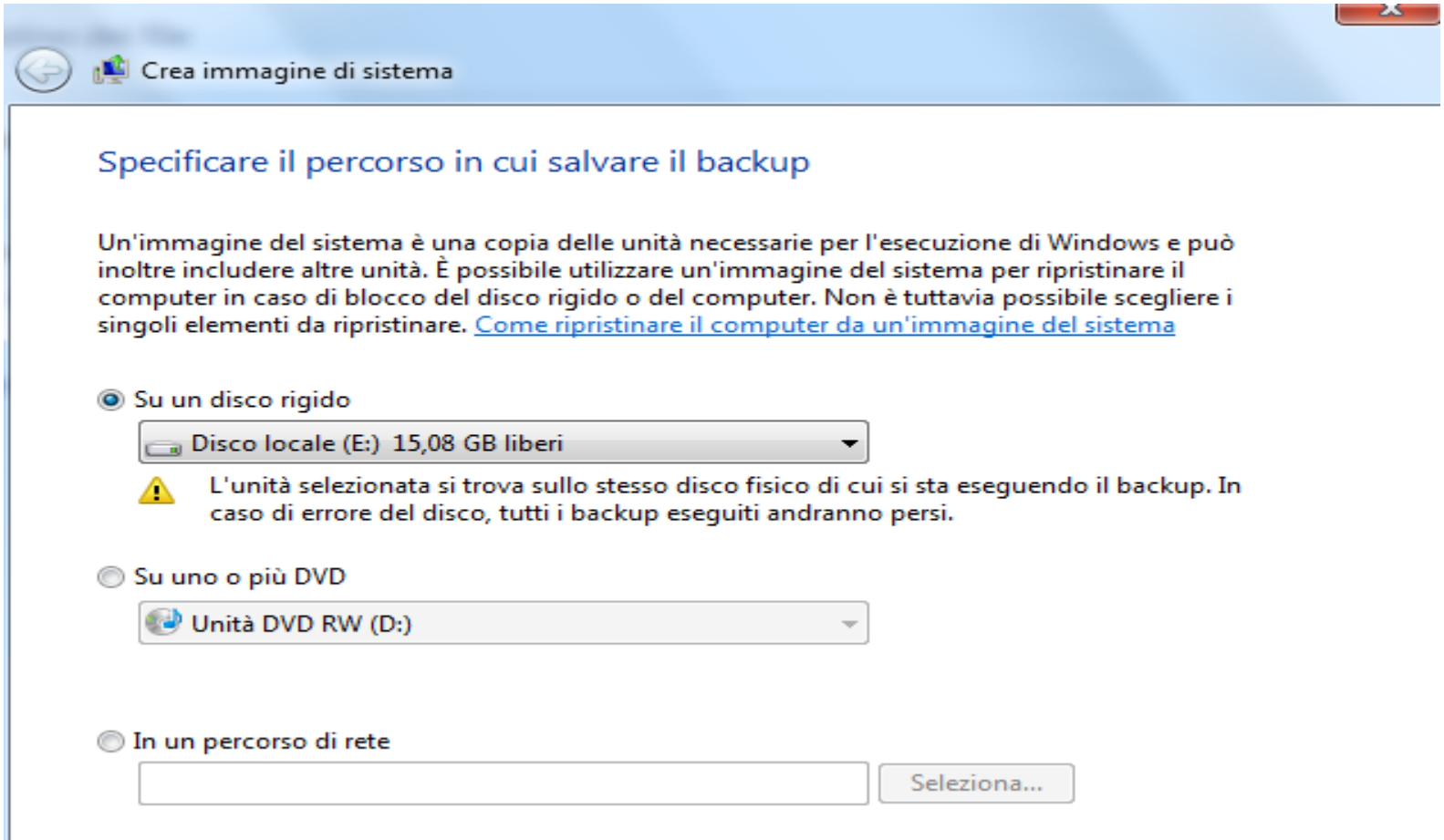


Immagine del sistema

- E' possibile creare un'immagine completa del sistema incluso windows, programmi e driver.



Cancellazione dei dati

- Quando si cancella un file viene messo in una parte della memoria "Cestino" dove è possibile recuperalo dopo un certo periodo.
- Anche quando si cancella definitivamente un file, è sempre presente perché windows non cancella il file ma segna il suo spazio come disponibile per altri dati.
- Ci sono programmi che possono recuperare i files anche dopo anni.

- Per distruggere documenti cartacei è possibile utilizzare dei tritadocumenti che riducono i documenti in striscioline o a coriandoli.
- La cancellazione avviene con la formattazione ma in realtà la formattazione veloce non intacca i files ma elimina solo la tabella di allocazione.
- La cancellazione con software non garantisce la distruzioen dei dati in quanto possono sempre rimanere della flebili tracce che possono essere intercettate con apposite strumentazioni.

- E’ possibile smagnetizzare gli Hard disk tramite l’esposizione a forti campi magnetici.
- Il metodo più economico e semplice è la distruzione fisica del supporto con colpi di martello e piccone, la trapanazione, il degaussing o l’inceneritura.
- Per quanto riguarda i CD o i DVD, si possono usare dei tritadocumenti utilizzabili anche con i CD, graffiare la superficie o spezzarli.