



Che cos'è la sicurezza informatica

Che cosa proteggiamo, da che cosa, e perché il primo anello della catena sei tu

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Indice

Come usare questa dispensa 3

1. Un lunedì mattina senza file 3

1.1 Che cosa c'è in gioco in una segreteria 4

2. Le tre proprietà da proteggere 5

2.1 Riservatezza: chi può vedere 6

2.2 Integrità: che cosa è stato cambiato 7

2.3 Disponibilità: ci sono quando servono 7

3. Da che cosa ci difendiamo: minacce tecniche e umane 8

3.1 Minacce tecniche 9

3.2 Minacce umane 9

3.3 Spesso le due famiglie si incontrano 9

4. L'errore umano: dove nascono davvero gli incidenti 10

4.1 Primo caso: la mail del «direttore» 10

4.2 Secondo caso: la chiavetta del fornitore 11

4.3 Perché sbagliamo, e come se ne esce 12

5. Perché la formazione è la difesa più efficace 13

5.1 Che cosa significa essere formati 13

5.2 Che cosa vedremo nel corso 14

5.3 Come appare una giornata ben protetta 14

5.4 Un limite onesto 16

Esercitazione: la mappa dei tuoi dati 17

Le domande che arrivano in aula 18

Glossario 18

Per approfondire 19

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Capire che cosa significa davvero «sicurezza informatica»: le tre proprietà dell'informazione da proteggere, le minacce tecniche e umane, il peso dell'errore umano e ciò che è in gioco quando lavori con i dati delle persone.

Che cosa saprai fare alla fine

- Spiegare con parole tue riservatezza, integrità e disponibilità, con un esempio per ciascuna.
- Distinguere una minaccia tecnica da una minaccia umana.
- Riconoscere le situazioni di lavoro in cui un piccolo errore può diventare un incidente.
- Individuare quali dati di persone passano dal tuo computer ogni giorno.
- Spiegare perché la formazione è la difesa più efficace.

1. Un lunedì mattina senza file

Immagina di accendere il computer del lunedì e di scoprire che l'elenco degli iscritti non si apre più.

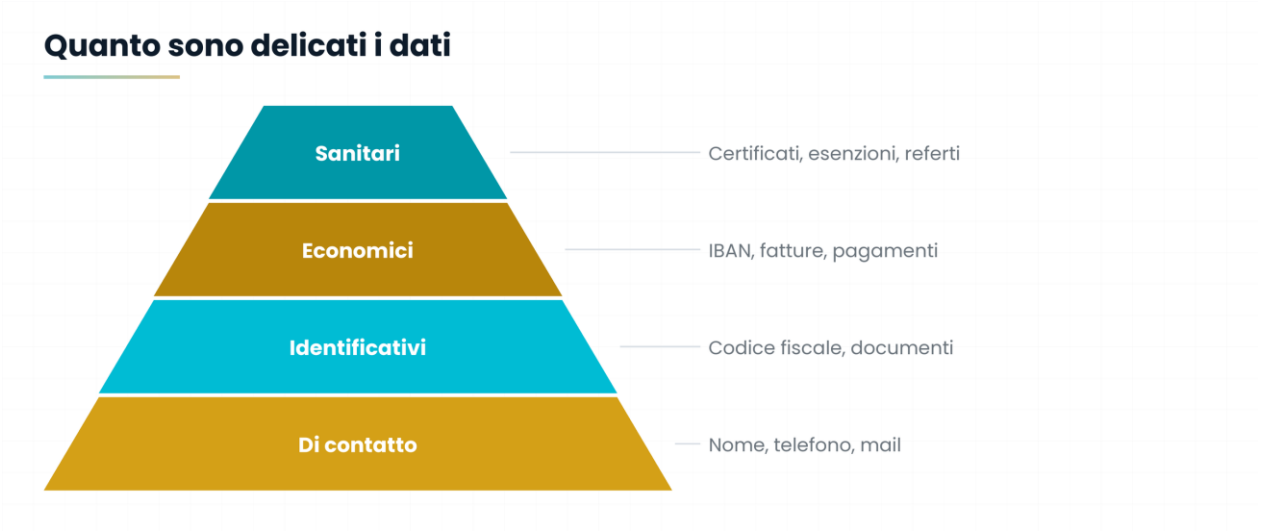
Nella segreteria di una piccola scuola di musica, la signora Marta (nome di fantasia) apre la cartella delle iscrizioni. I file ci sono, ma hanno un'estensione strana e nessun programma li legge. Sul desktop c'è un messaggio che non aveva mai visto.

Nello stesso momento, in un altro ufficio, un collega si accorge che l'importo di una fattura è cambiato. Nessuno sa chi l'abbia modificato. In un terzo ufficio, una mail con l'elenco dei genitori è partita per sbaglio verso un indirizzo esterno.

Tre episodi diversi, un solo tema: la **sicurezza informatica**. È l'insieme di regole, abitudini e strumenti che servono a proteggere le informazioni e i computer che le contengono. Non è una materia per tecnici: riguarda chiunque usi un computer per lavoro.

1.1 Che cosa c'è in gioco in una segreteria

Il computer di una segreteria contiene dati di persone: nomi, indirizzi, numeri di telefono, codici fiscali (il codice che in Italia identifica ogni cittadino ai fini fiscali), a volte documenti sanitari o economici. Sono informazioni che qualcuno ci ha affidato con fiducia.



I dati di persone in una segreteria, dai più comuni ai più delicati

Proteggerle è un obbligo di legge, ma prima ancora è una questione di fiducia. Una famiglia che iscrive il figlio a scuola, un cliente che lascia i suoi documenti a un piccolo studio, un paziente che prenota una visita: tutti si aspettano che quei dati restino al sicuro.



Proteggere i dati significa custodire la fiducia delle persone.

L'IDEA IN UNA RIGA

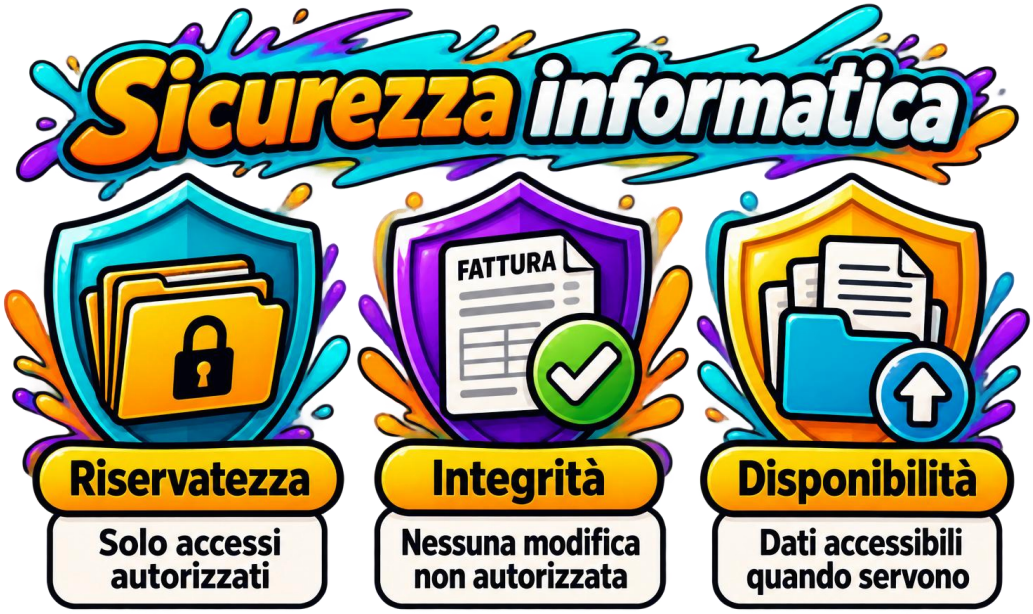
Sicurezza informatica significa far sì che le informazioni giuste siano disponibili alle persone giuste, e solo a loro, senza modifiche nascoste.

2. Le tre proprietà da proteggere

Gli esperti dicono che la sicurezza informatica protegge tre cose, chiamate le tre proprietà dell'informazione. Hanno nomi un po' tecnici, ma sono concetti che conosci già.

Proprietà	Significa	Esempio in segreteria
Riservatezza	Solo chi ha il diritto può vedere i dati.	L'elenco degli iscritti non finisce a un estraneo.
Integrità	I dati non vengono alterati senza autorizzazione.	Nessuno cambia di nascosto l'importo di una fattura.
Disponibilità	I dati sono accessibili quando servono.	Il lunedì mattina i file ci sono ancora, anche dopo un guasto.

Le tre proprietà dell'informazione, con un esempio quotidiano per ciascuna.



Sicurezza informatica

2.1 Riservatezza: chi può vedere

È la proprietà più intuitiva. Una scheda con i dati di un allievo deve poterla leggere chi se ne occupa, non il visitatore che aspetta in corridoio e vede lo schermo.

Si perde la riservatezza in molti modi: una mail inviata alla persona sbagliata, un foglio dimenticato sulla stampante, una password prestata al collega «tanto lui è di fiducia».



Riservatezza: i dati sono visibili soltanto alle persone autorizzate.

2.2 Integrità: che cosa è stato cambiato

Un dato può restare riservato e diventare comunque inaffidabile, se qualcuno lo cambia. Pensa a un IBAN (il codice che identifica un conto corrente) modificato in una richiesta di pagamento: la fattura sembra la stessa, ma il denaro va altrove.

Le alterazioni non sono sempre dolose. Anche un file sovrascritto per distrazione, o un programma che si blocca mentre salva, può lasciare dati sbagliati senza che nessuno se ne accorga subito.



Integrità: proteggere i dati dalle modifiche di nascosto.

2.3 Disponibilità: ci sono quando servono

I dati possono essere perfettamente riservati e corretti, ma inutili se non riesci ad aprirli. Un disco che si rompe, un virus che cifra i documenti, un account bloccato il giorno della scadenza: sono tutte perdite di disponibilità.

È la proprietà che si difende con le copie di sicurezza (i **backup**), di cui parleremo in una lezione dedicata.

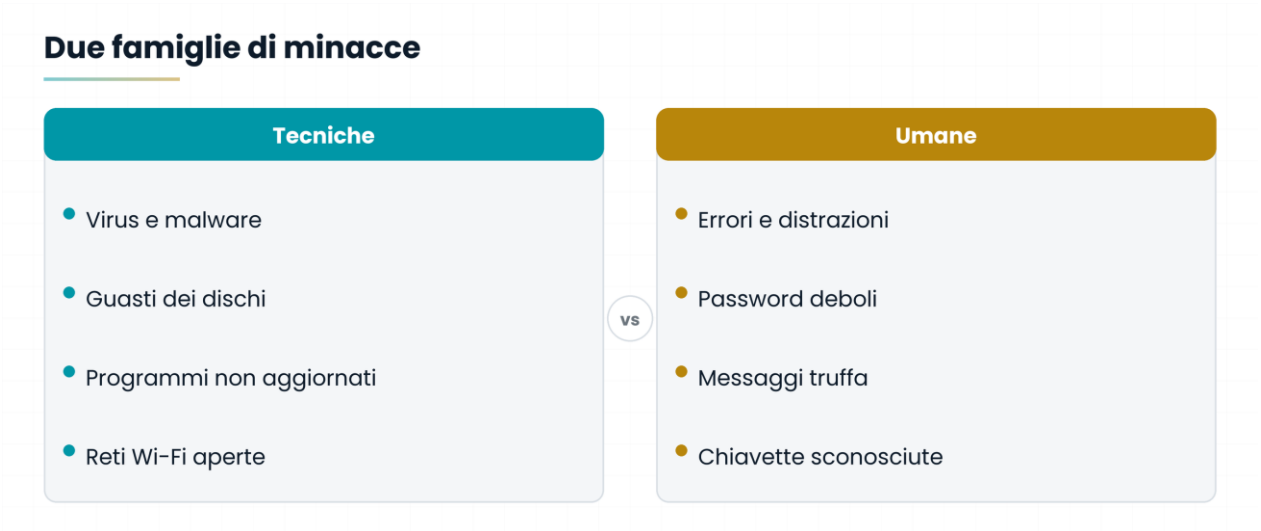


Disponibilità: ritrovare i dati quando servono.

> **UN CASO, TRE PROPRIETÀ**
>
> Uno studio commerciale di fantasia, «Studio Esempio», conserva le buste paga dei dipendenti di un cliente.
>
> **Riservatezza:** solo due persone dello studio possono aprirle. **Integrità:** nessuno può cambiare un importo senza lasciare traccia. **Disponibilità:** il giorno della scadenza dei pagamenti i file devono aprirsi, anche se il computer si è rotto la sera prima.

3. Da che cosa ci difendiamo: minacce tecniche e umane

Le minacce sono tutto ciò che può far perdere una delle tre proprietà. Le dividiamo in due grandi famiglie, e conviene tenerle distinte perché si combattono in modo diverso.



Due famiglie di minacce, due modi di difendersi

3.1 Minacce tecniche

Sono quelle che nascono dalle macchine e dal software. Un virus, cioè un programma dannoso, ne è l'esempio più noto. Ma ci sono anche un guasto del disco, un programma non aggiornato che ha una falla già conosciuta, una rete Wi-Fi pubblica senza protezione.

Contro queste minacce servono strumenti: aggiornamenti, antivirus, copie di sicurezza. Li vedremo uno per uno nelle prossime lezioni.

3.2 Minacce umane

Sono quelle che passano dalle persone: un errore, una distrazione, oppure un inganno. Un truffatore non ha bisogno di forzare il computer se riesce a convincerti a spalancargli la porta.

- **l'errore:** una mail inviata al destinatario sbagliato, un file cancellato per distrazione;
- **la dimenticanza:** il computer lasciato acceso e sbloccato, la password scritta su un post-it;
- **l'inganno:** un messaggio che finge di essere della banca, del corriere o del direttore;
- **la leggerezza:** una chiavetta USB trovata nel parcheggio e infilata nel computer «per vedere cosa c'è».

3.3 Spesso le due famiglie si incontrano

Un attacco riuscito di solito unisce le due cose. Il truffatore usa un trucco umano (una mail convincente) per far partire una minaccia tecnica (un programma dannoso). Per

questo non basta comprare un buon antivirus: bisogna anche sapere che cosa non cliccare.



Minacce tecniche e umane si incontrano spesso.

> **ATTENZIONE**
> Nessuno strumento tecnico ferma una persona che consegna volontariamente la propria password a un estraneo convinto di parlare con l'assistenza.

4. L'errore umano: dove nascono davvero gli incidenti

Nella realtà, la maggior parte degli incidenti nasce da un errore umano.

Un clic sbagliato, una password debole, una chiavetta persa. Non è una colpa da addossare a qualcuno: è la normale conseguenza del fatto che lavoriamo di fretta, in mezzo a mille cose, con la posta che arriva a ondate.

Chi attacca lo sa bene. Per questo i messaggi truffa sono scritti per far sentire urgenza, paura o curiosità: sono le emozioni che ci fanno cliccare prima di pensare.

4.1 Primo caso: la mail del «direttore»

Giulia (nome di fantasia) lavora nella segreteria di un piccolo ente. Un giovedì pomeriggio riceve un messaggio che sembra del direttore: «Sono in riunione, non posso

telefonare. Devi fare subito un bonifico a questo fornitore, ti spiego dopo». Il nome è giusto, il tono è quello di sempre.

Se Giulia esegue, il denaro è perso. Se si ferma e legge l'indirizzo del mittente, nota che il dominio (la parte dell'indirizzo dopo la chiocciola) è leggermente diverso da quello dell'ente. Se telefona al direttore sul numero che già conosce, in pochi secondi scopre che è un inganno.



Una richiesta urgente di denaro merita una verifica.

4.2 Secondo caso: la chiavetta del fornitore

In un negozio di fantasia, un rappresentante lascia una chiavetta USB con «il listino aggiornato». Il commesso la inserisce nel computer della cassa per stamparlo. Se la chiavetta contiene un programma dannoso, ora si trova nel computer dove passano gli incassi e i dati dei clienti.



Anche un gesto in buona fede può introdurre un rischio.

Il gesto era in buona fede. La buona fede però non basta: serve una regola semplice, nota a tutti, per esempio **non si inserisce nei computer di lavoro nulla che non sia stato controllato dal referente informatico**.



Come un piccolo errore diventa un incidente, e dove si può fermare

4.3 Perché sbagliamo, e come se ne esce

Che cosa ci fa sbagliare	Che cosa aiuta
La fretta e le scadenze	Un attimo di pausa prima di cliccare o di eseguire un pagamento.
L'abitudine («l'ho sempre fatto così»)	Regole scritte, semplici, uguali per tutti.

Che cosa ci fa sbagliare	Che cosa aiuta
La fiducia nel nome del mittente	Controllare l'indirizzo e, nel dubbio, richiamare su un numero noto.
La vergogna di chiedere	Un ambiente dove si può dire «non sono sicuro, controlli con me?».

Le cause più comuni dell'errore e la contromisura che funziona.

L'IDEA IN UNA RIGA

Un errore non diventa un incidente grave se lo segnali subito. Il silenzio, invece, lo peggiora.

5. Perché la formazione è la difesa più efficace

Se la maggior parte degli incidenti passa dalle persone, anche la difesa più efficace passa dalle persone. Un buon antivirus ti protegge da ciò che conosce. Una persona attenta ti protegge anche da ciò che nessun programma ha ancora visto.

Questo non vuol dire che gli strumenti siano inutili. Vuol dire che funzionano insieme: gli strumenti fermano il grosso, le persone fermano il resto.



Le difese lavorano insieme: nessuna basta da sola

5.1 Che cosa significa essere formati

- **sapere** che cosa si rischia e perché i dati delle persone vanno trattati con cura;
- **riconoscere** i segnali di un inganno prima di cliccare;
- **conoscere** poche regole semplici e applicarle sempre, anche quando si ha fretta;

- **sapere chi avvisare** se qualcosa va storto, e farlo subito.

5.2 Che cosa vedremo nel corso

Questa lezione è la mappa. Nelle prossime vedremo il malware e il ransomware, il phishing e le sue varianti, i siti-trappola e l'ingegneria sociale, le password e la verifica in due passaggi, la protezione di dispositivi e reti, il backup, la privacy e che cosa fare se succede.

Ogni lezione parte da un problema reale e finisce con una breve esercitazione che puoi fare con ciò che hai già sul tuo computer.



Quali dati di persone passano dal tuo lavoro? Chi deve poterli vedere?

5.3 Come appare una giornata ben protetta

Non è una giornata eroica: è una giornata normale, con qualche gesto in più. Accendi il computer e lo sblocchi con la tua password, che nessun altro conosce. Quando ti alzi dalla scrivania, blocchi lo schermo. Una mail che mette fretta la rileggi con calma e, se riguarda soldi, telefoni a chi dovrebbe averla scritta.

A fine giornata, i documenti importanti sono anche in una copia al sicuro. Nessuno di questi gesti richiede competenze tecniche. Richiede un'abitudine, e le abitudini si costruiscono: è proprio ciò che faremo lezione dopo lezione.



Bloccare, rileggere, verificare e conservare una copia: piccoli gesti quotidiani.

C'è poi un effetto che si nota col tempo: chi lavora in un ambiente dove queste abitudini sono condivise si sente meno solo davanti al dubbio. Sa a chi chiedere e sa che chiedere non è una debolezza.



Fermati, controlla, segnala. Chiedere aiuto fa parte della sicurezza.

5.4 Un limite onesto

Nessuna difesa dà sicurezza assoluta. L'obiettivo non è non sbagliare mai, ma ridurre molto le occasioni di errore e limitare i danni quando uno sbaglio succede. Una segreteria che ha copie di sicurezza recenti e persone abituate a segnalare i problemi è già molto più al riparo di una che confida nella fortuna.

> **ATTENZIONE**
>
> Le regole di questo corso sono basi di buon senso. Se lavori in un ente o in un'azienda, segui anche le procedure interne e le indicazioni del tuo referente informatico: hanno la precedenza.

Esercitazione: la mappa dei tuoi dati

Una breve esercitazione, con carta e penna e il computer che usi di solito. Nessuno strumento da installare.

1. Elenca quali dati di persone passano dal tuo lavoro in una settimana normale: nomi, indirizzi, telefoni, codici fiscali, documenti, foto.
2. Per ciascun tipo di dato scrivi dove si trova: sul computer, in una cartella condivisa, in una mail, su carta, su una chiavetta.
3. Per tre di questi dati rispondi alle domande: chi deve poterlo vedere (riservatezza)? Che cosa succederebbe se qualcuno lo modificasse (integrità)? Che cosa succederebbe se lunedì mattina non fosse più disponibile (disponibilità)?
4. Cerca un'abitudine tua o di chi lavora con te che mette a rischio una delle tre proprietà, per esempio una password condivisa o un foglio lasciato in vista.
5. Scrivi la prima piccola regola che adotteresti per correggerla.

CONTROLLA IL RISULTATO

Hai trovato almeno cinque tipi di dato e il luogo dove si trovano?

Per ogni dato analizzato hai risposto a tutte e tre le domande?

La regola che hai scritto è abbastanza semplice da applicare anche nei giorni di fretta?

Le domande che arrivano in aula

Sono solo una segretaria (o un impiegato): perché dovrebbero attaccare proprio me?

Perché spesso non attaccano te in particolare. Inviano lo stesso messaggio a moltissime persone e vedono chi cade. Inoltre, un computer di segreteria è interessante proprio perché contiene dati di persone e ha accesso a mail, pagamenti e archivi.

Basta un buon antivirus per essere al sicuro?

No. L'antivirus è una parte importante, ma non ferma un truffatore che ti convince a consegnargli una password o a fare un bonifico. Servono insieme strumenti, regole e persone attente.

Se ho sbagliato e ho cliccato, rischio un richiamo?

Dipende dall'organizzazione, ma il messaggio giusto è questo: segnalare subito è molto meglio che tacere. Un clic sbagliato avvisato subito si rimedia spesso; lo stesso clic nascosto può diventare un danno grave.

Qual è la differenza tra sicurezza informatica e privacy?

La sicurezza informatica protegge le informazioni e i sistemi dai rischi di perdita, alterazione e accesso non autorizzato. La privacy riguarda il diritto delle persone al corretto uso dei propri dati personali. Si sovrappongono: senza sicurezza non c'è privacy. Alla privacy dedichiamo una lezione a parte.

Con il lavoro da casa o da smartphone cambia qualcosa?

I principi sono gli stessi. Cambiano i luoghi: una rete Wi-Fi di casa o di un bar, un telefono che si smarrisce. Per questo i dispositivi personali usati per lavoro vanno protetti con la stessa cura, e chiedi sempre all'organizzazione quali sono le regole.

Glossario

Termine	Che cosa significa
Backup	Copia di sicurezza dei dati, conservata in modo da poterli ripristinare se gli originali si perdono.
Dato personale	Qualunque informazione che riguardi una persona identificata o identificabile: nome, indirizzo, mail, codice fiscale, foto.
Disponibilità	La proprietà per cui i dati sono accessibili quando servono.
Dominio	Il nome di un sito o di un indirizzo di posta, per esempio ente-esempio.it.

Termine	Che cosa significa
Integrità	La proprietà per cui i dati non vengono alterati senza autorizzazione.
Malware	Dall'inglese «malicious software»: programma creato per danneggiare un computer o rubare dati.
Minaccia	Qualsiasi evento, tecnico o umano, che può far perdere riservatezza, integrità o disponibilità.
Riservatezza	La proprietà per cui solo chi ne ha diritto può vedere i dati.
Sicurezza informatica	L'insieme di regole, abitudini e strumenti che proteggono le informazioni e i dispositivi che le contengono.

Per approfondire

Regolamento (UE) 2016/679 (GDPR) - testo ufficiale su EUR-Lex

Agenzia per la cybersicurezza nazionale (ACN) - materiali informativi per cittadini e imprese, acn.gov.it

Garante per la protezione dei dati personali - guide e schede sulla sicurezza dei dati, garanteprivacy.it

> **ATTENZIONE**
>
> Informazioni aggiornate a ottobre 2026. I nomi di persone, studi e domini usati negli esempi sono di fantasia. Le regole generali di questo corso non sostituiscono le procedure della tua organizzazione.