

Sviluppo delle competenze digitali

Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

Coordinatore:

MMC Mediterranean Management Centre

Partner:

ПРИВРЕДНА КОМОРА РЕПУБЛИКЕ СРПСКЕ
ПОДРУЧНА ПРИВРЕДНА КОМОРА БАЊА ЛУКА

CYPRUS CERTIFICATION COMPANY

DIMITRA educational organization

CCIT

CETEOR

Asnor Associazione Nazionale Orientatori

ACT -CENTER

Obiettivi del modulo

Dal punto di vista delle conoscenze:

- Analizzare i rischi comuni per la sicurezza digitale negli ambienti di lavoro e spiegarne il potenziale impatto organizzativo.
- Interpretare e applicare i principi fondamentali del GDPR in relazione alle situazioni di gestione dei dati di routine sul posto di lavoro.
- Distinguere e giustificare approcci strutturati alla gestione delle informazioni e dei dati digitali nelle attività professionali quotidiane.
- Identificare e confrontare strumenti digitali e applicazioni di IA adeguati in base alle esigenze specifiche del posto di lavoro.
- Spiegare e giustificare gli standard professionali per la comunicazione e la collaborazione digitale negli spazi di lavoro digitali.
- Descrivere e sequenziare procedure strutturate di risoluzione dei problemi per i problemi digitali comuni, inclusi i criteri di escalation.
- Spiegare le ragioni alla base del continuo aggiornamento delle competenze digitali in ambienti di lavoro in rapida evoluzione.

Cofinanziato dall'Unione europea

Obiettivi del modulo

Per quanto riguarda le competenze:

- Attuare misure di protezione digitale adeguate per ridurre i rischi legati alla sicurezza informatica e alla protezione dei dati nelle attività lavorative quotidiane.
- Valutare criticamente le fonti e i contenuti delle informazioni digitali per determinarne l'affidabilità e l'idoneità all'uso professionale.
- Organizzare, classificare e gestire file e informazioni digitali utilizzando sistemi strutturati che migliorano l'efficienza operativa.
- Selezionare e applicare strumenti di produttività digitale adeguati per produrre autonomamente risultati standard sul posto di lavoro.
- Utilizzare gli strumenti basati sull'intelligenza artificiale in modo responsabile e strategico, garantendo la protezione dei dati sensibili e la valutazione critica dei risultati dell'IA.
- Collaborare in modo autonomo attraverso le tecnologie digitali, gestendo in modo appropriato le impostazioni di condivisione, i flussi di lavoro di co-editing e le autorizzazioni di accesso.
- Diagnosticare e risolvere i problemi tecnici comuni utilizzando una logica strutturata di risoluzione dei problemi e documentare il processo di risoluzione ove richiesto.
- Valutare i livelli di competenza digitale personale e progettare un piano di miglioramento strutturato per colmare le lacune individuate.

Cofinanziato dall'Unione europea

Obiettivi del modulo

Per quanto riguarda gli atteggiamenti:

- Dimostrare impegno nei confronti della protezione dei dati, della consapevolezza in materia di sicurezza informatica e di una condotta digitale etica negli ambienti professionali.
- Dimostrare responsabilità e professionalità nella comunicazione digitale e nelle pratiche digitali collaborative.
- Mostrare un comportamento proattivo nell'identificare e affrontare i problemi digitali all'interno dei contesti lavorativi.
- Adottare una mentalità orientata all'apprendimento continuo per lo sviluppo delle competenze digitali in risposta al cambiamento tecnologico.

Cofinanziato dall'Unione europea

Rapport

Mappa dei percorsi del modulo

Sicurezza digitale e gestione responsabile dei dati

→

Alfabetizzazione informatica e dei dati per gli ambienti professionali

→

Strumenti digitali e IA per le attività professionali quotidiane

↓

Comunicazione digitale, collaborazione e identità professionale

→

Creazione e modifica di contenuti digitali per i risultati finali sul posto di lavoro

→

Risoluzione di problemi tecnici di base

Cofinanziato dall'Unione europea

Rapport

Sicurezza digitale e trattamento responsabile dei dati

Unità 1

Cofinanziato dall'Unione europea

Perché questa unità è importante

Questa unità introduce i principi e le pratiche che garantiscono una partecipazione sicura, responsabile ed efficace negli ambienti di lavoro digitali. Si concentra sulla consapevolezza dei rischi, sulla gestione responsabile delle informazioni e sul giudizio informato nelle attività professionali quotidiane.

Nei luoghi di lavoro contemporanei, la sicurezza digitale è un requisito professionale fondamentale. Un comportamento digitale non sicuro può portare all'esposizione dei dati, all'interruzione delle operazioni, alla perdita di fiducia, a problemi legali o di conformità e a una riduzione della qualità del lavoro. Una condotta digitale responsabile è quindi parte integrante di una prestazione efficace, non una questione secondaria.

AZIONE → RISCHIO → IMPATTO

Cofinanziato dall'Unione europea

Mappa del percorso dell'unità



Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 1 – COMPRENDERE IL RISCHIO DIGITALE

Cofinanziato
dall'Unione europea

Che cos'è la sicurezza digitale?

Per **sicurezza digitale** si intende l'insieme di comportamenti, misure di controllo e decisioni che aiutano le persone e le organizzazioni a utilizzare le tecnologie digitali senza esporre inutilmente a rischi i dati, i sistemi, la privacy, il benessere o la continuità operativa.

Essa comprende:

- protezione dei dispositivi e degli account
- gestione attenta delle informazioni
- comunicazione sicura
- consapevolezza degli ambienti digitali
- capacità di giudizio responsabile



Cofinanziato
dall'Unione europea

La sicurezza digitale nella realtà del posto di lavoro

La sicurezza digitale non è rilevante solo in caso di incidenti eccezionali.

Riguarda anche attività quotidiane come:

- controllare la posta elettronica
- condivisione di file
- archiviazione di documenti
- l'utilizzo di piattaforme online
- accedere ai sistemi
- lavorare da remoto
- uso di strumenti basati sull'intelligenza artificiale

Le attività di routine possono comportare rischi significativi se svolte senza verifica o attenzione.

Cofinanziato dall'Unione europea

Che cos'è il rischio digitale?

Un **rischio digitale** è qualsiasi condizione, evento o comportamento che possa influire negativamente su:

- la riservatezza delle informazioni
- l'integrità dei dati
- la disponibilità del sistema
- la privacy
- la fiducia
- qualità del lavoro



I rischi digitali possono derivare **sia** da **vulnerabilità tecniche che dal comportamento umano**.

Esempio: *l'invio di un file al destinatario sbagliato. Un caso tipico in cui il rischio è associato a un errore umano, che potrebbe portare alla divulgazione di dati riservati.*

Rischio digitale = qualsiasi minaccia ai dati, ai sistemi, alla privacy o al flusso di lavoro causata dall'attività digitale.

Cofinanziato dall'Unione europea

Quiz1

Seleziona la risposta corretta.

Quale delle seguenti situazioni rappresenta un tipico rischio digitale sul posto di lavoro?

- **3. Utilizzare un foglio di calcolo**
- **1. Scrivere una relazione lunga**
- **2. Inviare un file al destinatario sbagliato**
- **4. Partecipare a una riunione**

Tipi di rischi digitali sul posto di lavoro

I rischi digitali sul posto di lavoro rientrano in genere in diverse categorie, ciascuna delle quali rappresenta un diverso tipo di minaccia per l'integrità dei dati, dei dispositivi e dei sistemi. La maggior parte delle minacce rientra in categorie prevedibili, il che ci aiuta a riconoscerle e a prevenirle.

Le minacce comuni sul posto di lavoro includono:

- **Phishing:** messaggi ingannevoli progettati per ottenere informazioni o indurre azioni non sicure.
- **Malware:** software dannoso che interrompe, ruba o danneggia.
- **Ingegneria sociale:** manipolazione delle persone per ottenere accesso o conformità.
- **Autenticazione debole:** pratiche inadeguate relative a password e accesso.
- **Condivisione non sicura:** accesso incontrollato a file e dati.

Le linee guida sull'igiene informatica dell'ENISA si concentrano proprio su questo tipo di pratiche di prevenzione quotidiane. Riconoscere immediatamente la categoria aiuta a determinare la risposta corretta.

Cofinanziato dall'Unione europea

Phishing

Il phishing è una forma di attacco informatico in cui gli hacker si spacciano per organizzazioni legittime (o si presentano come entità affidabili) per sottrarre informazioni sensibili quali credenziali di accesso, dati delle carte di credito o segreti aziendali.

Gli attacchi di phishing utilizzano spesso **tattiche di ingegneria sociale** per indurre il destinatario a credere che il messaggio provenga da una fonte attendibile, spingendolo ad agire senza un'adeguata verifica.

Esempio:

Un dipendente riceve un'e-mail apparentemente inviata dalla banca, in cui si afferma che il suo conto è stato compromesso e che deve cliccare su un link per aggiornare i propri dati. Questo link porta a un sito web falso progettato per rubare le informazioni di accesso.



Il rischio principale è **il furto di identità** o **la frode finanziaria**. Il phishing può anche fornire agli aggressori l'accesso ai sistemi interni, portando a violazioni dei dati più estese o infezioni da malware.

Cofinanziato dall'Unione europea

Quiz2

Seleziona la risposta corretta.

Qual è la risposta più professionale a un'e-mail urgente che richiede un intervento immediato?

- 3. Verifica il mittente prima di agire
- 4. Inoltralo ai colleghi
- 2. Clicca sul link per verificare
- 1. Agisci subito per evitare problemi

Come riconoscere il phishing

Tra gli indicatori di un messaggio sospetto figurano:

- **indirizzo del mittente insolito** → potrebbe imitare un'organizzazione affidabile ma contiene piccole incongruenze (ad es. lettere o domini in più)
- **richiesta al di fuori della normale procedura** → aggira i flussi di lavoro o i processi di approvazione consolidati
- **allegato o link inaspettato** → può reindirizzare a siti web dannosi o installare malware
- **tono urgente o minaccioso** → riduce il pensiero critico esercitando pressione sull'utente affinché agisca rapidamente senza verificare
- **incongruenze grammaticali o formattazione insolita**
- **richiesta di dati o codici riservati** → viola le politiche di sicurezza dell'organizzazione

Un messaggio può sembrare professionale e tuttavia non essere sicuro.

Regola pratica:

Non cliccare sui link né aprire allegati provenienti da e-mail sconosciute o sospette. Verifica sempre l'indirizzo e-mail del mittente e non agire mai immediatamente in seguito a richieste digitali urgenti senza aver prima effettuato una verifica.

Cofinanziato dall'Unione europea

Caso di studio: analisi di un'e-mail di phishing

Scenario: Esempio di email sospetta

Oggetto: Urgente: Problema di sicurezza rilevato sulla tua workstation
Da: Margaret Doe, Supervisore IT m.doe@ourcompanny.com
A: John Sample
Contenuto dell'e-mail:
John,
Il team di sicurezza IT ha rilevato attività insolite sulla tua postazione di lavoro nelle ore notturne. Riteniamo che il tuo dispositivo possa essere stato colpito da un problema di sicurezza individuato di recente.
Ti preghiamo di esaminare i file di log allegati e di confermare se queste azioni sono state eseguite da te.
In caso contrario, clicca sul link sottostante per aggiornare immediatamente il tuo software antivirus:
🔗 Aggiorna il software di sicurezza
Fammi sapere una volta completato.

Margaret
Responsabile IT

Analisi dell'e-mail

1. Personalizzazione

Il messaggio utilizza il nome del dipendente (“John”) → aumenta la fiducia

2. Mittente falso ma realistico

Il dominio sembra corretto ma leggermente modificato → ourcompanny.com invece di ourcompany.com

3. Autorità

Il messaggio sembra provenire dal reparto IT → aumenta la propensione a seguire le istruzioni

4. Fattore di paura

"Il tuo dispositivo potrebbe essere compromesso" → crea urgenza e preoccupazione

5. Coinvolgimento a basso rischio

“Esamina i file di log allegati” → crea fiducia prima dell’azione principale

6. Azione ad alto rischio

“Clicca sul link per aggiornare il software” → vero e proprio vettore di attacco (malware o furto di credenziali)

Cofinanziato dall'Unione europea

Malware

Il termine "malware" (software dannoso) indica un software creato per compromettere un dispositivo, un sistema o un insieme di dati. Può arrivare tramite download non sicuri, allegati dannosi, falsi aggiornamenti o siti web compromessi.

Esempio: *apertura di un allegato infetto.*

Le possibili conseguenze includono:

- perdita di file
- riduzione delle prestazioni del sistema
- accesso non autorizzato
- interruzione del servizio
- diffusione più ampia tra i sistemi

Regole pratiche:

- Assicurarsi che il software antivirus sia installato e aggiornato su tutti i dispositivi.
- Non scaricare software o aggiornamenti da fonti non affidabili e utilizzare solo piattaforme affidabili per le applicazioni relative al lavoro.



Cofinanziato dall'Unione europea

Principali tipi di malware

1. Ransomware

→ crittografa i dati aziendali e richiede un pagamento (spesso in criptovaluta)

→ prende di mira la disponibilità dei dati

2. Spyware

→ monitora silenziosamente l'attività dell'utente (digitazioni, schermo, credenziali)

→ prende di mira la riservatezza

3. Cavalli di Troia

→ si camuffano da strumenti legittimi (ad es. convertitore PDF, file di aggiornamento)

→ installa codice dannoso quando viene eseguito

Cofinanziato dall'Unione europea

Ingegneria sociale: la dimensione umana del rischio informatico

Il termine "ingegneria sociale" si riferisce alla manipolazione delle persone anziché dei sistemi. Consiste nel convincere gli individui a rivelare informazioni riservate, spesso ricorrendo a tecniche di manipolazione psicologica piuttosto che a mezzi tecnici.

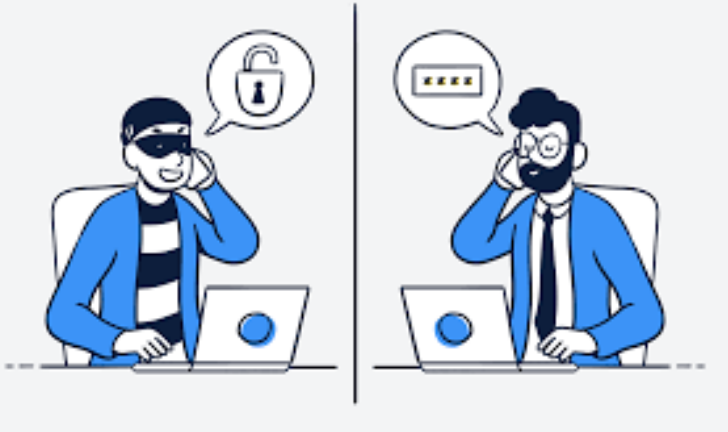
Gli aggressori possono fingersi dipendenti, fornitori o clienti legittimi per conquistare la fiducia e convincere la vittima a rivelare dati sensibili o a fornire l'accesso ai sistemi.

Esempio:

Un aggressore chiama un dipendente fingendo di appartenere al reparto Risorse Umane e lo convince a condividere i dettagli di accesso interni dell'azienda o le credenziali di accesso.

Regola pratica:

Verificare tutte le richieste non sollecitate di informazioni sensibili contattando la parte richiedente attraverso i canali di comunicazione ufficiali. Prestare attenzione quando si ricevono chiamate o e-mail non sollecitate che richiedono credenziali di accesso o l'accesso ai sistemi aziendali.



Cofinanziato dall'Unione europea

Perché il lavoro di routine è spesso vulnerabile?

I dipendenti spesso ricoprono molteplici responsabilità, lavorano sotto pressione e si affidano a modalità di comunicazione relativamente informali. Ciò può aumentare il rischio di ricorrere a scorciatoie poco sicure, di effettuare controlli insufficienti e di garantire una gestione incoerente dei dati e degli accessi.

Molti incidenti digitali non si verificano perché gli utenti non ne sanno nulla. Si verificano perché gli utenti:

- di fretta
- distratti
- impegnati in più attività contemporaneamente
- troppo sicuri di sé
- seguono l'abitudine piuttosto che il buon senso

Il rischio, quindi, emerge spesso da condizioni di lavoro ordinarie.

La sicurezza digitale dipende in gran parte dal comportamento.

Cofinanziato dall'Unione europea

Caso di studio: Il costo di un clic

Questo caso dimostra come **l'ingegneria sociale** possa portare a una violazione della sicurezza tecnica attraverso una semplice azione dell'utente.

Scenario

Un dipendente riceve un'e-mail dal titolo:

"Fattura fiscale – Revisione urgente richiesta"

- Sembra provenire da un fornitore legittimo
- Professionale e relativa al lavoro
- Chiede di aprire una fattura allegata

La richiesta sembra di routine e sicura.

Perché funziona (ingegneria sociale)

- **Fiducia** → contesto aziendale familiare (fattura)
- **Rilevanza** → parte delle attività quotidiane
- **Urgenza** → incoraggia un'azione immediata
- **Basso rischio percepito** → aprire i file sembra normale

Progressione dell'attacco, risultato e impatto

Dopo che il dipendente ha aperto l'allegato, viene eseguito un codice dannoso che infetta il sistema e consente al malware di diffondersi nella rete interna. Di conseguenza, i file dell'organizzazione vengono crittografati tramite un attacco ransomware, rendendo inaccessibili tutti i dati dei clienti e interrompendo le operazioni aziendali. L'organizzazione deve affrontare conseguenze significative, tra cui costi di ripristino superiori a 50.000 €, tempi di inattività operativa e perdita di produttività. L'impatto più critico, tuttavia, è la perdita della fiducia dei clienti, che può avere effetti a lungo termine o irreversibili.

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 2 - ACCESSO SICURO E PROTEZIONE DEI DISPOSITIVI

Cofinanziato dall'Unione europea

Perché l'autenticazione è importante

L'autenticazione è il processo di verifica dell'identità di un utente, di un dispositivo o di un'entità prima di concedere l'accesso a un sistema o a dei dati.

Un'autenticazione efficace costituisce la prima linea di difesa contro gli accessi non autorizzati. Ciò include l'uso di password, dati biometrici, smart card e altri metodi per garantire che sia la persona giusta ad accedere ai sistemi.

Esempio:

Quando si accede a un portale protetto, gli utenti devono inserire una password e confermare la propria identità utilizzando uno scanner di impronte digitali o un secondo fattore di autenticazione, come un codice mobile.

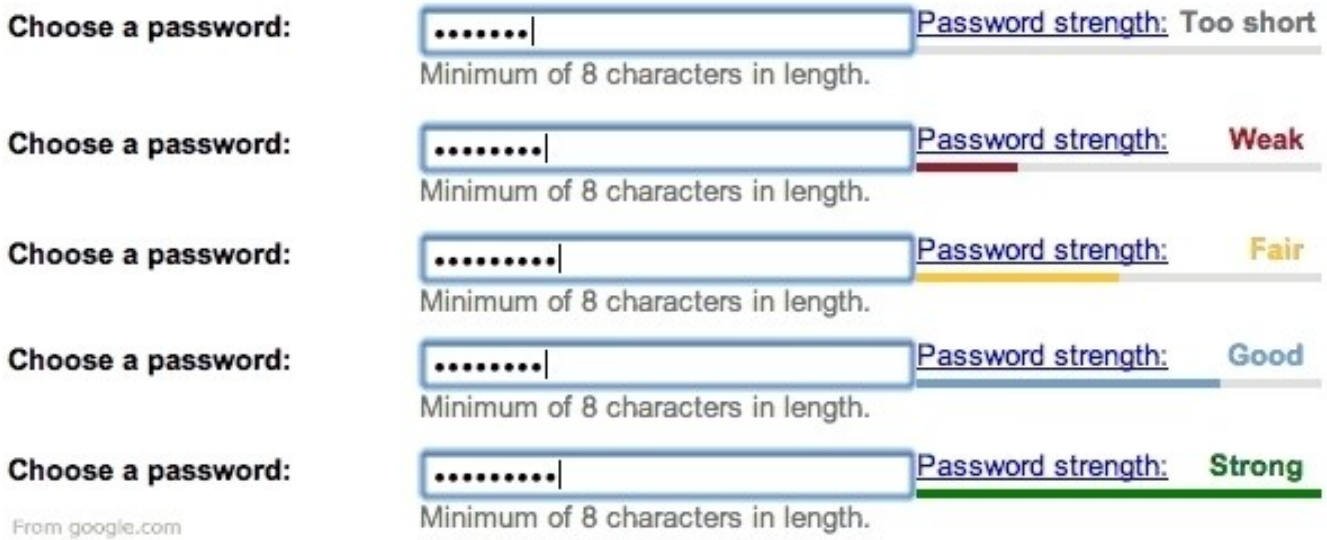


Cofinanziato dall'Unione europea

Le password come prima linea di difesa

Le password rimangono uno dei sistemi di controllo degli accessi più diffusi. La loro efficacia dipende non solo dalla complessità, ma anche dalla lunghezza, dall'unicità e dal comportamento degli utenti.

Gli attacchi di forza bruta possono violare password di 8 caratteri in pochi minuti. Pratiche inadeguate relative alle password indeboliscono anche i sistemi ben progettati.



Cofinanziato dall'Unione europea

Principi per creare password più sicure

1. La lunghezza è la priorità assoluta

- Utilizza almeno 16 caratteri.
- Le password più lunghe sono più difficili da indovinare con la forza bruta.

2. Unicità

- Non riutilizzare mai le password su siti diversi.
- Una violazione su un sito non dovrebbe comprometterne altri.

3. Complessità/Casualità

- Mescola i tipi di caratteri: lettere, numeri e caratteri speciali.
- Esempio: 6MonkeysRLooking^.

4. Usa frasi di accesso

- Combina 4–7 parole casuali non correlate (ad es., "BlueSkyCoffee*2024").
- Sono lunghe e più facili da ricordare.

5. Evita le informazioni personali

- Non utilizzare nomi, date di nascita, parole del dizionario o sequenze comuni come "123456" o "password123".

Le password devono essere lunghe, uniche e non basate su informazioni personali. Conservale in modo sicuro e non riutilizzarle su più account

Cofinanziato
dall'Unione europea

Pratiche non sicure relative alle password

1. Riutilizzo delle password

- Utilizzo della stessa password su più piattaforme.
- Una sola violazione compromette tutti gli account.

2. Password deboli/semplici

- Parole prevedibili, date di nascita, nomi di animali domestici o sequenze brevi.
- Facilmente decifrabili da strumenti automatizzati.

3. Conservazione non sicura delle password

- Scrivere le password su post-it, salvarle in file di testo in chiaro o utilizzare la funzione di compilazione automatica del browser non crittografata

4. Condivisione delle credenziali

- Condivisione delle password tramite e-mail non crittografate, SMS o con altre persone.

6. Mancato aggiornamento dopo violazioni

- Continuare a utilizzare una password dopo che è stata compromessa in una violazione dei dati.

Conseguenze di una scarsa sicurezza delle password

Credential Stuffing: gli hacker ottengono l'accesso ad altri servizi utilizzando credenziali rubate.

Furto d'identità: accesso non autorizzato alle informazioni personali.

Perdita finanziaria: furto diretto o acquisti fraudolenti dai conti bancari.

Cofinanziato dall'Unione europea

Abitudini comuni relative alle password ed errori nella creazione

5 errori comuni nell'uso delle password

- Riutilizzare le password
- Conservare fisicamente le password
- Non cambiare le password dopo una violazione
- Memorizzazione delle password nel browser
- Condivisione non sicura delle password

6 errori comuni nella creazione delle password

- Includere nomi di familiari
- Inserire informazioni personali
- Inserire le proprie preferenze
- Utilizzare sequenze semplici come “56789”
- Utilizzare caratteri prevedibili o parole del dizionario
- Creazione di password brevi e semplici

Cofinanziato dall'Unione europea

Autenticazione a più fattori (MFA)

L'autenticazione a più fattori (MFA) rafforza la protezione degli accessi richiedendo più di una forma di verifica. È considerata «lo standard di riferimento in materia di protezione».

In genere combina:

- qualcosa che l'utente conosce (ad es. password/PIN)
- qualcosa che l'utente possiede (ad es. smartphone/chiave di sicurezza)
- o qualcosa che l'utente è (ad es. dati biometrici, impronta digitale/FaceID)

Non elimina tutti i rischi, ma li riduce significativamente in caso di esposizione delle credenziali. Anche se un fattore viene compromesso, l'accesso rimane comunque protetto.

Esempio: *l'uso di una password combinata con la scansione dell'impronta digitale o un codice inviato via SMS.*

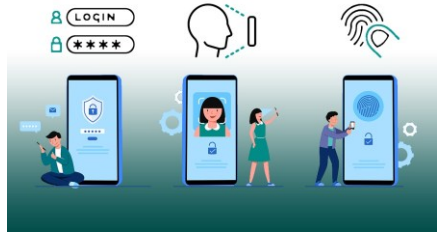


Cofinanziato dall'Unione europea

Come funziona l'autenticazione a più fattori (processo passo dopo passo)

Quando si accede a un sistema protetto, l'autenticazione avviene in più fasi:

1. L'utente inserisce **il** proprio **nome utente e la** propria **password**
2. Il sistema verifica le credenziali
3. Viene attivata una **seconda richiesta di autenticazione**
4. L'utente riceve un **codice di accesso monouso (OTP)** sul proprio dispositivo mobile o sull'app di autenticazione
5. L'utente inserisce il codice di verifica
6. L'accesso viene concesso **solo se entrambi i fattori di autenticazione sono corretti**



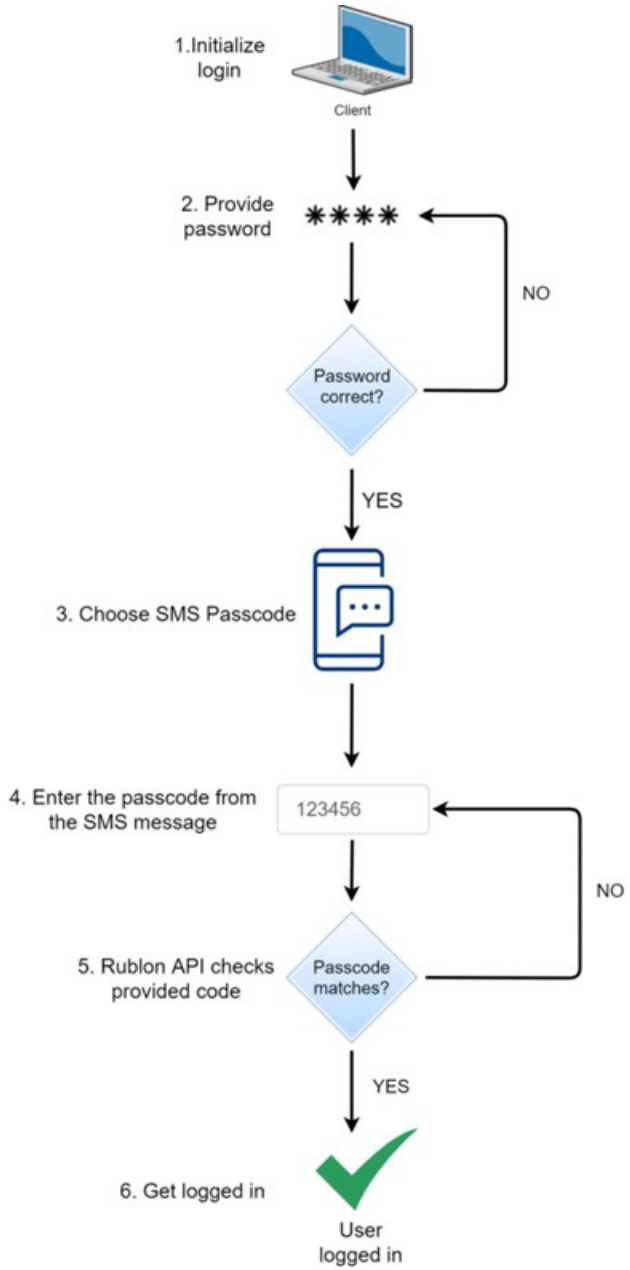
Rischio (senza MFA)

Senza autenticazione a più fattori:

- password rubate o deboli possono portare **all'accesso completo al sistema**
- gli attacchi di phishing possono facilmente compromettere gli account degli utenti
- gli aggressori potrebbero ottenere l'accesso a **dati e sistemi aziendali sensibili**

Cofinanziato dall'Unione europea

Rapport



Cofinanziato dall'Unione europea

Sicurezza responsabile dei dispositivi

La sicurezza dei dispositivi consiste nel proteggere gli endpoint, quali laptop, smartphone e computer fissi, da accessi non autorizzati, furti o malware.

Poiché **i dispositivi rappresentano i principali punti di accesso ai dati e ai sistemi**, garantirne la sicurezza è fondamentale. Ciò include l'uso di firewall, crittografia, software antivirus e configurazioni sicure.

L'uso sicuro dei dispositivi include:

- bloccare gli schermi quando ci si allontana
- l'utilizzo di software approvato
- evitare download sconosciuti e dispositivi USB
- proteggere i dispositivi durante i viaggi
- mantenere aggiornati sistemi e applicazioni



Esempio: *bloccare il computer quando ci si allontana dalla scrivania, assicurarsi che i dati siano crittografati e aggiornare regolarmente il software di sicurezza.*

Cofinanziato dall'Unione europea

Perché gli aggiornamenti sono importanti

Aggiornamenti frequenti:

- correggere le vulnerabilità note
- migliorano l'affidabilità del sistema
- ridurre i problemi di compatibilità
- rafforzano la protezione contro le minacce note

Regola pratica:
Abilitare gli aggiornamenti automatici per il software critico e dare priorità agli aggiornamenti dei sistemi operativi e del software di sicurezza.

Mantenere il software aggiornato garantisce protezione contro le vulnerabilità note e mantiene i sistemi al sicuro dalle minacce esterne.

Esempio: *aggiornare regolarmente i sistemi operativi, i programmi antivirus e i browser per correggere le falle di sicurezza.*

La mancata applicazione delle patch può lasciare i sistemi esposti allo sfruttamento da parte di malware o hacker.

Cofinanziato dall'Unione europea

Principali tipi di aggiornamenti

Tipo	Scopo	Esempio
Patch	Risolve problemi specifici che influiscono sulle prestazioni o sulla sicurezza del sistema	*Correzione di un errore di calcolo nel software di contabilità*
Hotfix	Correzione urgente di problemi critici al di fuori del ciclo di aggiornamento regolare	*Correzione immediata di un crash del sistema durante le operazioni quotidiane*
Aggiornamento di sicurezza	Risolve le vulnerabilità che potrebbero essere sfruttate dagli hacker	*Risoluzione di una vulnerabilità che consente l'accesso non autorizzato ai dati aziendali*
Aggiornamento critico	Risolve gravi errori di sistema che compromettono la funzionalità	*Risolve i problemi che impediscono l'accesso ai sistemi aziendali principali*
Aggiornamento cumulativo	Combina più correzioni e miglioramenti precedenti in un unico aggiornamento	*Installazione di un unico aggiornamento anziché di più aggiornamenti minori*
Service Pack	Pacchetto di patch, correzioni e aggiornamenti per una distribuzione più semplice	*Aggiornamento di sistema a livello aziendale su tutti i dispositivi dei dipendenti*
Aggiornamento delle funzionalità / Feature Pack	Introduce nuove funzionalità e migliora le prestazioni del sistema	*Nuovi strumenti per la collaborazione o l'efficienza del flusso di lavoro*
Aggiornamento	Cambio di versione principale del software o del sistema operativo	*Passaggio da Windows 10 a Windows 11*

Cofinanziato dall'Unione europea

Rapport

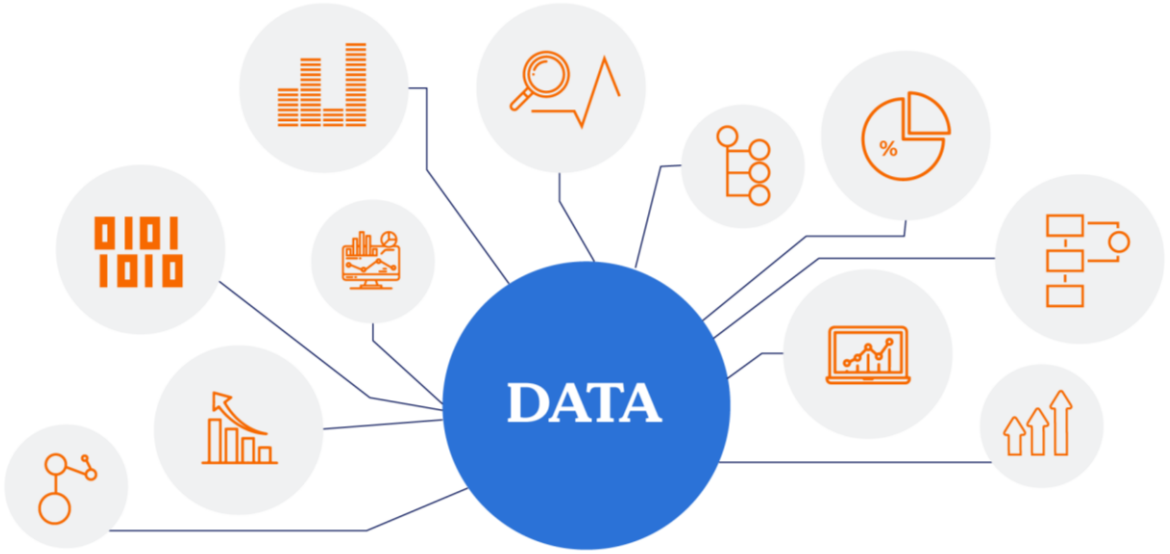
ARGOMENTO 3 – PROTEZIONE DEI DATI E SENSIBILIZZAZIONE SUL GDPR

Cofinanziato
dall'Unione europea

Cosa si intende per "dati" nella pratica lavorativa?

I dati relativi al posto di lavoro includor

- nomi e recapiti
- schede dei clienti
- informazioni sui dipendenti
- orari
- rapporti interni
- contratti
- documenti finanziari
- registri delle comunicazioni



Non tutti i dati hanno lo stesso grado di riservatezza, ma tutti richiedono un trattamento adeguato.

Cofinanziato dall'Unione europea

Dati personali

Per **"dati personali"** si intendono tutte le informazioni che consentono di identificare una persona, direttamente o indirettamente. Ciò include identificativi comuni quali nomi, recapiti, numeri di identificazione e persino identificativi online.



Esempi:

- *nome*
- *indirizzo e-mail*
- *numero di telefono*
- *dati identificativi*

Cofinanziato dall'Unione europea

Sensibilizzazione dei dipendenti sul GDPR

Il GDPR (Regolamento generale sulla protezione dei dati) è il regolamento dell'Unione Europea che tutela i dati personali e stabilisce le linee guida per il loro trattamento.

A livello dei dipendenti, la consapevolezza del GDPR non richiede competenze giuridiche. Richiede invece un comportamento professionale disciplinato, come ad esempio:

- accedere solo a ciò che è necessario
- utilizzare i dati solo per scopi lavorativi legittimi
- condivisione tramite canali approvati
- evitare l'esposizione involontaria
- segnalare tempestivamente gli errori



Le linee guida sulla protezione dei dati della Commissione Europea rappresentano la fonte pubblica di alto livello più affidabile in materia.

Linee guida della Commissione europea sulla protezione dei dati

Cofinanziato dall'Unione europea

I 7 principi fondamentali del GDPR

1. Liceità, correttezza e trasparenza

I dati devono essere raccolti e utilizzati in modo lecito e trasparente (ad esempio, informando i clienti sul motivo per cui vengono raccolti i loro dati e su come saranno utilizzati).

2. Limitazione delle finalità

I dati devono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati raccolti (ad esempio, i dati dei clienti raccolti a fini di fatturazione non possono essere utilizzati per attività di marketing senza il loro consenso).

3. Riduzione al minimo dei dati

Devono essere raccolti solo i dati necessari (ad esempio, non richiedere dettagli personali non necessari nei moduli).

4. Accuratezza

I dati personali devono essere accurati e tenuti aggiornati (ad esempio, aggiornare regolarmente i recapiti dei clienti).

5. Limitazione della conservazione

I dati non devono essere conservati più a lungo del necessario (ad esempio, cancellare i dati obsoleti relativi a dipendenti o clienti).

6. Integrità e riservatezza (sicurezza)

I dati devono essere protetti da accessi non autorizzati o dalla perdita (ad es. utilizzare sistemi sicuri, password e accesso limitato).

7. Responsabilità

Le organizzazioni devono essere in grado di dimostrare la conformità al GDPR (ad esempio, conservando registrazioni su come i dati vengono trattati e protetti).

Cofinanziato
dall'Unione europea

Perché è importante un trattamento responsabile dei dati

Una gestione inadeguata dei dati può compromettere:

- i diritti e gli interessi delle persone
- la credibilità dell'organizzazione
- la fiducia dei clienti
- la qualità delle operazioni interne
- gli obblighi legali e di conformità

La protezione dei dati è quindi al tempo stesso **una questione etica**, **operativa e normativa**.

La mancata conformità al GDPR può comportare multe significative e danni alla reputazione.

Cofinanziato dall'Unione europea

Errori comuni nella gestione dei dati sul posto di lavoro

Gli errori nella gestione dei dati si riferiscono a errori commessi durante la gestione, l'archiviazione o la condivisione dei dati.

Esempi includono:

- l'invio di file al destinatario sbagliato
- condivisione eccessiva degli accessi alle cartelle
- archiviazione di documenti in posizioni non approvate
- copiare destinatari non necessari nelle e-mail
- esposizione di dati stampati o visibili
- condivisione di dati in eccesso rispetto a quanto richiesto dall'attività

Questi errori possono portare a violazioni della privacy, fughe di dati e danni alla reputazione dell’organizzazione.

Cofinanziato
dall'Unione europea

Cosa fare dopo un errore nella gestione dei dati

Anche adottando le migliori precauzioni, possono verificarsi errori nella gestione dei dati. L'aspetto fondamentale è gestire gli errori in modo tempestivo e responsabile per ridurre al minimo i potenziali danni.

Una risposta responsabile di solito prevede:

1. valutare la situazione
2. non nascondere l'incidente
3. informare la persona o la funzione competente
4. seguire la procedura interna
5. limitare l'ulteriore esposizione, ove possibile
6. trarre insegnamento dall'evento

Cofinanziato
dall'Unione europea

Rapport

ARGOMENTO 4 – GESTIONE SICURA DI FILE E DOCUMENTI

Cofinanziato
dall'Unione europea

Perché l'organizzazione dei file è importante

Per **organizzazione dei file** si intende il metodo sistematico di archiviazione, denominazione e accesso ai file digitali, volto a garantire che questi possano essere facilmente recuperati, protetti e gestiti in modo sicuro.

Una corretta organizzazione dei file riduce al minimo rischi quali l'esposizione accidentale dei dati, la comunicazione errata e il recupero inefficiente. Assicura che le informazioni sensibili siano accessibili solo alle persone autorizzate e contribuisce a mantenere l'efficienza operativa.

Esempio: *utilizzare strutture di cartelle e convenzioni di denominazione chiare per organizzare i documenti per progetto o reparto, anziché archiviare i file in cartelle arbitrarie o generiche.*

Denominazioni chiare, cartelle strutturate, versioni controllate e archiviazione approvata riducono:

- confusione
- duplicazione
- condivisione accidentale
- l'utilizzo di documenti obsoleti
- l'esposizione non necessaria



L'organizzazione dei file è quindi sia una **questione di produttività che di sicurezza**.

Cofinanziato
dall'Unione europea

Principi fondamentali per l'organizzazione dei file digitali

1. Creare una struttura logica

- Crea una gerarchia basata sul tuo flusso di lavoro (ad esempio, per cliente, progetto o data).
- Mantieni le sottocartelle poco profonde (3–4 livelli) per evitare clic eccessivi.

2. Convenzioni di denominazione coerenti

- Sviluppa un sistema di denominazione standard (ad es. AAAA-MM-GG_NomeDocumento_Versione).
- Utilizza il camel case o i trattini bassi al posto degli spazi.
- Evita di usare caratteri speciali.

3. Controllo delle versioni

- Evita nomi come final_v2_updated.doc. Usa _v01, _v02 per le revisioni sequenziali.
- Valutare l'utilizzo di modifiche tracciate dal software.

4. Archivia/Pulisci regolarmente

- Sposta i progetti completati in una cartella di archivio per ridurre l'ingombro.

Riepilogo delle migliori pratiche

- **Non andare in profondità**: limita le sottocartelle a 3-4 livelli.
- **Utilizza nomi descrittivi**: pensa in anticipo: cosa cercherai in seguito?
- **Agisci immediatamente**: salva i file direttamente nella loro posizione finale, non sul desktop.
- **Archivia in modo coerente**: sposta regolarmente i vecchi file in una cartella di archivio o su un servizio di archiviazione cloud.

Cofinanziato
dall'Unione europea

Principi per una condivisione dei file più sicura

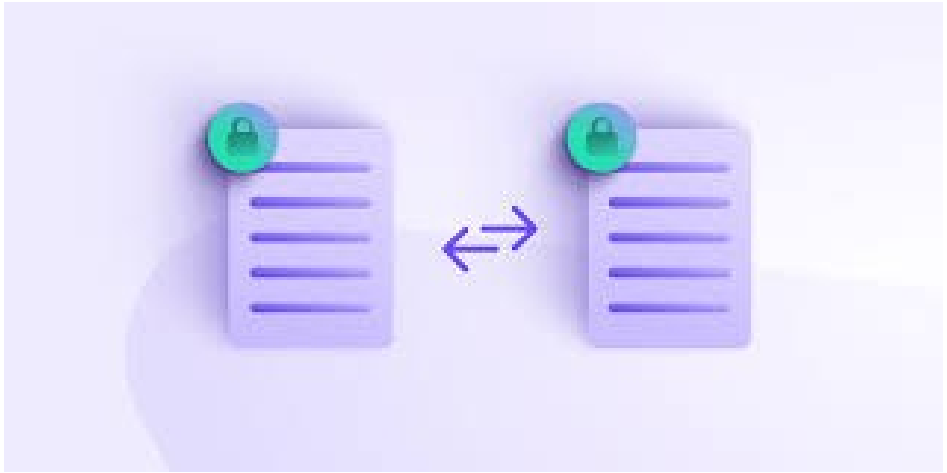
La condivisione dei file indica il processo di trasferimento dei file da una posizione a un'altra, sia all'interno di un'organizzazione che all'esterno, garantendo che i file vengano condivisi in modo sicuro e appropriato.

La condivisione dei file diventa rischiosa quando si utilizzano impostazioni non corrette o quando i file vengono condivisi con persone non autorizzate. Per proteggere sia l'integrità dei dati che la loro riservatezza, è fondamentale seguire un processo strutturato che includa il controllo degli accessi, la crittografia e la condivisione tramite piattaforme approvate.

Esempio: *inviare un file a un partner esterno tramite un servizio di posta elettronica crittografata, invece di utilizzare un link pubblico non protetto.*

Prima di condividere un file, considera:

- chi ha effettivamente bisogno di accedervi
- quale livello di autorizzazione è necessario
- se il file è la versione corretta
- se la piattaforma utilizzata è approvata
- se l'accesso debba essere limitato nel tempo



Cofinanziato dall'Unione europea

Mantenere il controllo sui documenti negli ambienti digitali

A differenza della condivisione tradizionale dei file (ad esempio, gli allegati e-mail), i sistemi di accesso controllato garantiscono che il file **rimanga all'interno di un ambiente gestito**, anziché essere duplicato su più dispositivi.

Piattaforme moderne come OneDrive, Google Drive e SharePoint forniscono meccanismi per controllare:

- **l'accesso** (chi può aprire il file)
- **la visibilità** (chi può vedere che esiste)
- **l'utilizzo** (visualizzazione, commento, modifica, download)

Questo trasforma la condivisione dei file da **distribuzione ad accesso controllato**.

Esempio: *invece di inviare un rapporto finanziario via e-mail, un dipendente condivide con un cliente un link ad accesso limitato.*

- L'accesso è limitato a utenti specifici
- Il download è disabilitato
- L'accesso può essere revocato in qualsiasi momento

La condivisione sicura dei file non riguarda l'invio dei file, ma il mantenimento del controllo sui dati durante tutto il loro ciclo di vita.

Rischi

- perdita di controllo una volta inviati i file
- inoltro o duplicazione incontrollati
- archiviazione di dati sensibili in luoghi non protetti
- impossibilità di tracciare l'accesso o l'utilizzo

Buone pratiche

- Condividere link anziché allegati
- Utilizzare solo piattaforme approvate dall'organizzazione
- Limitare l'accesso a utenti specifici
- Rivedere regolarmente e revocare l'accesso quando non è più necessario

Cofinanziato dall'Unione europea

Protezione dei documenti sensibili

La protezione dei documenti sensibili comporta la messa in sicurezza sia dei contenuti visibili che dei dati nascosti (metadati) all'interno di un file, al fine di impedire la divulgazione involontaria di informazioni.

I documenti contengono spesso **informazioni nascoste** che non sono visibili durante la normale visualizzazione, tra cui i dettagli dell'autore, la cronologia delle modifiche, le revisioni, i commenti interni, i percorsi dei file o i riferimenti di sistema.

- Questi metadati possono rivelare informazioni aziendali riservate se non vengono rimossi.
- Esempio: *un dipendente condivide un documento Word con un destinatario esterno senza averlo ripulito. Il destinatario può vedere le discussioni interne, le modifiche precedenti e i nomi dei dipendenti o dei clienti.*

La sicurezza non riguarda solo la protezione di ciò che è visibile, ma richiede anche il controllo delle informazioni nascoste e di contesto.

Rischi

- divulgazione di strategie o comunicazioni interne
- divulgazione di informazioni riservate sui clienti
- danno alla reputazione e rischi di non conformità al GDPR

Buone pratiche

- Utilizzare la crittografia dei documenti per i file sensibili
- Applicare la protezione con password quando necessario
- Rimuovere i metadati utilizzando strumenti come "Inspect Document"
- Condividere le password tramite un canale di comunicazione separato

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 5 – USO RESPONSABILE DEGLI STRUMENTI DI INTELLIGENZA ARTIFICIALE

ChatGPT

Grok

Gemini

deepseek

perplexity

Copilot

Cofinanziato
dall'Unione europea

Intelligenza artificiale: strumento di produttività o fattore di rischio?

Gli strumenti di IA sono software che utilizzano l'apprendimento automatico e l'intelligenza artificiale per elaborare dati, automatizzare attività e generare approfondimenti.

L'IA può aumentare la produttività, ma può anche comportare dei rischi, specialmente quando si tratta di dati personali o sensibili. Utilizzare l'IA in modo responsabile significa garantire la privacy dei dati, la sicurezza e il rispetto della legge.

Gli strumenti di IA possono aiutare a:

- riassumere le informazioni,
- strutturare il testo,
- generare prime bozze,
- organizzare le idee.

Rischio

Ogni richiesta inserita in un sistema di IA pubblico rappresenta un potenziale trasferimento di dati verso un sistema esterno

Esempio:

Se si utilizza l'IA per riassumere il feedback dei clienti, assicurarsi che nel set di dati non siano incluse informazioni di identificazione personale (PII).

L'IA non è solo uno strumento, è un ambiente di elaborazione dei dati.

Cofinanziato dall'Unione europea

Rischi legati all'uso degli strumenti di IA

Rischio 1: Utilizzo non autorizzato dei dati personali

Condivisione o utilizzo di informazioni personali senza il consenso adeguato o misure di sicurezza.

Rischio 2: Uso improprio delle informazioni fornite dall'IA

L'IA può generare informazioni, ma se utilizzata in modo improprio, queste informazioni potrebbero portare a decisioni parziali o inique.

Rischio 3: Mancato rispetto delle leggi sulla protezione dei dati

Violazione di leggi come il GDPR a causa di una gestione impropria dei dati personali o sensibili.

Esempio: *utilizzo dell'IA per analizzare il feedback dei clienti includendo però dati sensibili come numeri di telefono o indirizzi e-mail.*

L'IA dovrebbe essere utilizzata per:

- supportare il processo decisionale
- migliorare la produttività

NON per:

- sostituire il giudizio professionale
- trattare dati sensibili senza controllo

Cofinanziato dall'Unione europea

Migliori pratiche per un uso responsabile dell'IA

Esercizio 1: Anonimizzare i dati

Assicurarsi sempre di rendere anonimi i dati prima di inserirli negli strumenti di IA.

Pratica 2: Evitare di condividere dati sensibili

Condividere i dati personali con gli strumenti di IA solo se assolutamente necessario e assicurarsi che sia esplicitamente approvato.

Pratica 3: Scegliere strumenti di IA conformi

Utilizza strumenti di IA conformi alle leggi sulla protezione dei dati (ad es. il GDPR).

Esempio:

Per l'analisi del sentiment dei clienti, rimuovere o rendere anonimi tutti i dati di identificazione personale (ad es. nomi, e-mail) prima di inviarli.

Cofinanziato dall'Unione europea

Allucinazioni dell'IA e uso incontrollato degli strumenti di IA

Si parla di "**allucinazione dell'IA**" quando l'IA genera informazioni errate o fuorvianti presentate come accurate.

L'IA ombra consiste nell'uso di strumenti di IA non autorizzati al di fuori del controllo dell'organizzazione.

Gli strumenti di IA possono comportare due rischi principali:

1. Risultati non verificati (allucinazioni)

L'IA può sembrare affidabile ma fornire informazioni incomplete o errate oppure generare contenuti senza fonti valide.

2. Uso incontrollato (Shadow AI)

I dipendenti potrebbero utilizzare strumenti di IA personali per risparmiare tempo, automatizzare attività o elaborare dati relativi al lavoro.

Entrambi i rischi incidono sul processo decisionale e sulla protezione dei dati.

Rischi

- decisioni aziendali o tecniche errate
- errori professionali e responsabilità
- perdita del controllo dei dati
- mancanza di una traccia di audit
- divulgazione di dati aziendali o personali
- utilizzo dei dati in modelli di addestramento di IA esterni

Buone pratiche

- verificare sempre i contenuti generati dall'IA
- effettuare un controllo incrociato con fonti affidabili e ufficiali
- non affidarsi mai ciecamente ai risultati dell'IA
- utilizzare solo strumenti di IA (aziendali) approvati
- evitare di utilizzare account personali di IA per le attività lavorative

Cofinanziato dall'Unione europea

Quando la comodità porta all'esposizione dei dati

Scenario

Un dipendente utilizza uno strumento di IA pubblico per analizzare il feedback dei clienti e include dati reali quali nomi, indirizzi e-mail e dettagli delle transazioni. L'azione sembra efficiente, ma comporta rischi nascosti.

Cosa succede → I dati vengono elaborati al di fuori dell'organizzazione, con conseguente perdita di controllo ed esposizione di informazioni personali sensibili.

Perché questo è un problema

- dati personali condivisi senza una base adeguata
- violazione della riservatezza e del principio di minimizzazione dei dati
- crea un rischio diretto di non conformità al GDPR

Impatto

- violazione dei dati
- conseguenze legali e finanziarie
- perdita della fiducia dei clienti

Buona pratica

- non inserire mai dati personali in strumenti di IA pubblici
- Anonimizzare i dati prima dell'uso
- utilizzare solo soluzioni di IA approvate

L'utilizzo dell'IA con dati reali senza controllo equivale a condividerli con una terza parte

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 6 – LAVORO DA REMOTO E BENESSERE DIGITALE



Cofinanziato
dall'Unione europea

Il posto di lavoro è ovunque

Il lavoro a distanza estende l'ambiente organizzativo oltre l'ufficio, fino alle abitazioni, agli spazi pubblici e alle situazioni di mobilità.

Quando si lavora da remoto, l'organizzazione perde il controllo diretto su:

- reti
- dispositivi
- ambiente fisico

Ciò aumenta l'esposizione ai rischi per la sicurezza.

La sicurezza digitale dipende non solo dai sistemi, ma anche da **dove e come viene svolto il lavoro.**

Cofinanziato dall'Unione europea

Rischi del lavoro da remoto
Comprendere l'esposizione

I rischi legati al lavoro da remoto si riferiscono alle sfide in materia di sicurezza e alle potenziali vulnerabilità che sorgono quando si lavora al di fuori di un ambiente d'ufficio tradizionale, spesso utilizzando dispositivi personali o reti non protette.

Il lavoro da remoto può **esporre gli studenti a**:

- reti Wi-Fi pubbliche o non sicure
- schermi visibili in spazi pubblici
- dispositivi condivisi o personali
- conversazioni ascoltate per caso
- apparecchiature incustodite
- ambienti che distraggono

Rischi

- intercettazione dei dati
- accesso non autorizzato
- divulgazione accidentale di informazioni sensibili

Lavorare da remoto richiede quindi un comportamento protettivo consapevole.

Esempio: *lavorare da un bar e accedere ai file aziendali tramite una rete Wi-Fi aperta.*

Cofinanziato dall'Unione europea

Comportamenti più sicuri nel lavoro da remoto

Tra le pratiche più sicure figurano:

- utilizzare reti più sicure, ove possibile
- proteggere la visibilità dello schermo
- bloccare i dispositivi quando ci si allontana
- separare l'uso lavorativo da quello personale
- maneggiare i file con cura al di fuori del luogo di lavoro principale
- evitare, quando possibile, di svolgere attività delicate in ambienti esposti

Il lavoro da remoto richiede un comportamento deliberato e consapevole, non routine automatiche.

Dalla rete domestica alla protezione dei dispositivi

- modificare le password predefinite del router
- abilitare una crittografia Wi-Fi forte (WPA2/WPA3)
- utilizzare reti separate per i dispositivi di lavoro
- Attivare la VPN quando si lavora da remoto

Cofinanziato dall'Unione europea

Il benessere digitale come parte della sicurezza digitale

Il benessere digitale si riferisce all'uso sostenibile e salutare delle tecnologie digitali, garantendo che le persone non soffrano di sovraccarico digitale, stress o esaurimento a causa di un uso eccessivo degli strumenti digitali.

L'uso eccessivo delle tecnologie digitali, specialmente per motivi di lavoro, può portare all'affaticamento digitale, che riduce la produttività, aumenta gli errori e porta a un processo decisionale inadeguato.

Esempio:

controllare costantemente le e-mail o le notifiche durante il giorno, causando distrazione sul lavoro e affaticamento mentale.

Cofinanziato dall'Unione europea

In che modo il sovraccarico digitale influisce sulla sicurezza

Il sovraccarico digitale può portare a:

- decisioni affrettate
- controlli superficiali prima dell'invio
- clic incauti
- scarsa concentrazione
- cambi di attività costanti
- errori evitabili più frequenti

Il benessere digitale non è quindi solo una questione di comfort personale, ma anche una **questione di sicurezza**.

Cofinanziato
dall'Unione europea

Abitudini pratiche per il benessere digitale

1. Fai delle brevi pause regolari

→ riduce la stanchezza e migliora la concentrazione

2. Gestisci le notifiche

→ limita le interruzioni per evitare continui cambi di attività

3. Utilizza blocchi di lavoro dedicati

→ dedica del tempo senza interruzioni a compiti complessi o delicati

4. Rallenta prima di inviare o cliccare

→ verificare destinatari, link e allegati prima di agire

5. Prestare particolare attenzione ai dati sensibili

→ ricontrolla il contenuto, l'accesso e il contesto prima di condividere

Un utente attento è un utente più sicuro.

La sicurezza digitale non dipende solo dagli strumenti, ma anche dall'attenzione, dalla disciplina e dall'autogestione.

Cofinanziato
dall'Unione europea

Riferimenti e ulteriori letture

- Commissione europea (2024) *Norme dell'UE in materia di protezione dei dati (GDPR)*. Disponibile all'indirizzo: https://commission.europa.eu/law/law-topic/data-protection_en (Consultato il: 26 marzo 2026)
- OCSE (2023) *Panoramica dei principi dell'OCSE sull'IA*. Disponibile all'indirizzo: https://oecd.ai/en/ai-principles (Consultato il: 27 marzo 2026)
- Commissione europea (2024) *Linee guida etiche per un'IA affidabile*. Disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Consultato il: 27 marzo 2026)
- OCSE (2022) *Produttività e digitalizzazione sul posto di lavoro*. Disponibile all'indirizzo: https://www.oecd.org/digital (Consultato il: 26 marzo 2026)
- ENISA (Agenzia dell'Unione europea per la sicurezza informatica) (2023) *Igiene informatica: Linee guida per le PMI e le organizzazioni*. Disponibile all'indirizzo: https://www.enisa.europa.eu/topics/cyber-hygiene (Consultato il: 24 marzo 2026)
- Centro nazionale per la sicurezza informatica (NCSC) (2023) *Autenticazione a più fattori (MFA): come configurarla e utilizzarla*. Disponibile all'indirizzo: https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services (Consultato il: 25 marzo 2026)

Cofinanziato dall'Unione europea

Rapport

Competenze informatiche e di gestione dei dati per gli ambienti professionali

UNITÀ 2

Cofinanziato dall'Unione europea

Struttura dell'unità

Comprendere i dati e le informazioni → Ricerca e valutazione delle informazioni → Organizzazione e gestione di informazioni e dati → Applicazione dei dati utilizzando gli strumenti di lavoro → Applicazione e processo decisionale basati su casi concreti

Cofinanziato dall'Unione europea

Perché questa unità è importante

Nei luoghi di lavoro odierni, l'informazione non è semplicemente «qualcosa a cui accedere». È una risorsa operativa che determina l'azione, la qualità e la fiducia.

Pratiche inadeguate in materia di informazioni e dati possono portare a:

- **Problemi operativi** quali ritardi, duplicazioni, confusione, versioni errate, rendicontazione incoerente.
- **Conseguenze finanziarie** quali scelte errate dei fornitori, calcoli imprecisi, uso inefficiente di tempo e risorse.
- **Rischi di conformità ed etici** quali l'uso improprio di informazioni sensibili, un controllo insufficiente sui file condivisi, scarsa tracciabilità.
- **Danni alla reputazione,** come una minore fiducia da parte di manager, colleghi, clienti o partner esterni.

Nelle microimprese questi rischi sono amplificati perché un errore spesso influisce su più processi contemporaneamente.

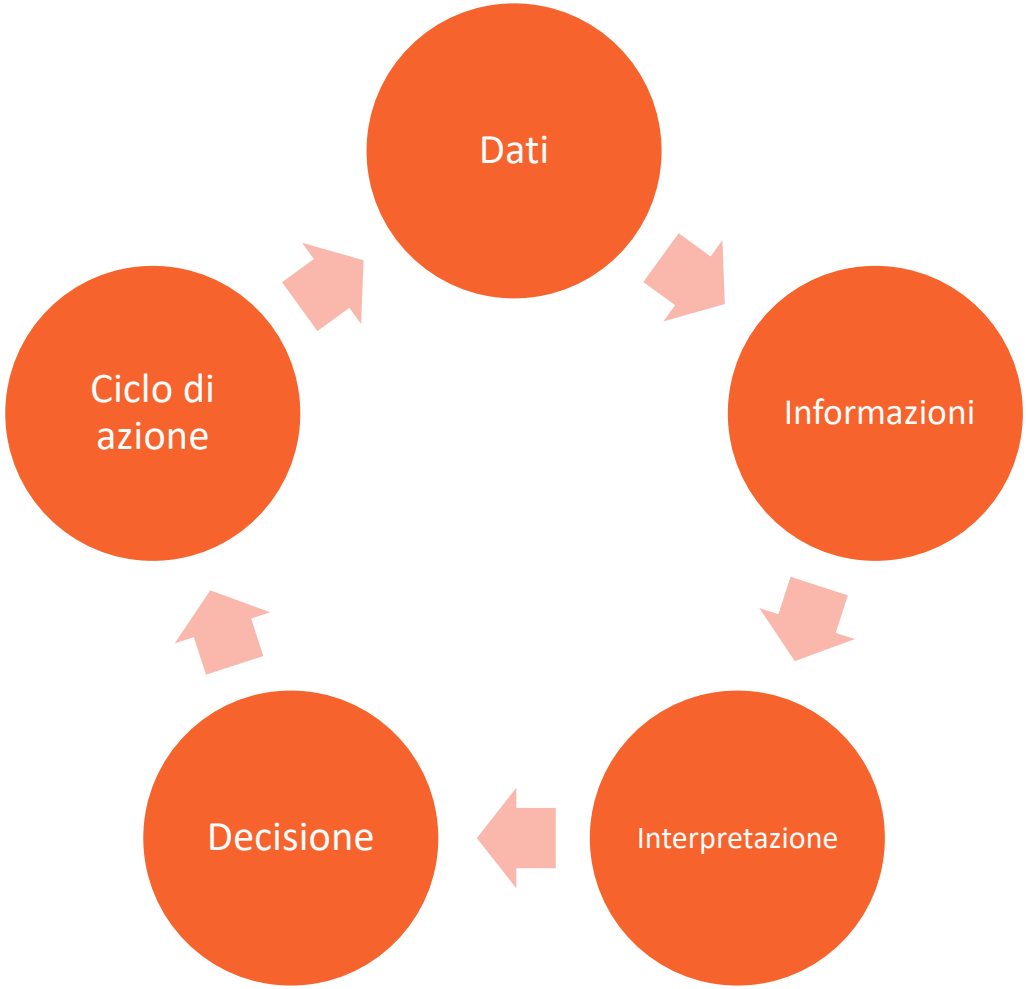
Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 1 - COMPRENDERE I DATI E LE INFORMAZIONI

Cofinanziato
dall'Unione europea

Dal ciclo di vita delle informazioni al ciclo di vita delle decisioni



Cofinanziato dall'Unione europea

L'alfabetizzazione informativa come risorsa professionale

L'alfabetizzazione informativa è la capacità di **individuare, valutare, organizzare e utilizzare le informazioni** in modo efficace ed etico. Si tratta di una competenza applicabile a qualsiasi settore, fondamentale per prendere decisioni informate, risolvere problemi e far progredire le conoscenze sul posto di lavoro.

Componenti chiave dell'alfabetizzazione informativa:

- **Ricerca delle informazioni**: sapere dove cercare, quali banche dati o piattaforme utilizzare e come filtrare le informazioni irrilevanti.
- **Valutare le informazioni**: valutare la credibilità, l'accuratezza e la pertinenza delle informazioni.
- **Organizzazione delle informazioni**: creare sistemi per la gestione delle informazioni che garantiscano accessibilità e tracciabilità.
- **Utilizzo delle informazioni**: applicare le informazioni per risolvere problemi, supportare il processo decisionale o creare nuove conoscenze.

Essere informaticamente alfabetizzati significa andare oltre il semplice accesso ai dati. Si tratta di sviluppare la capacità di **interagire criticamente** con le informazioni per utilizzarle efficacemente sul posto di lavoro. Nei luoghi di lavoro moderni, l'informazione non è neutra o passiva. È una **risorsa lavorativa fondamentale** che influisce direttamente sulle decisioni (quali azioni vengono intraprese e perché), sulle operazioni (come il lavoro viene organizzato ed eseguito) e sui risultati (qualità, efficienza e risultati).

Cofinanziato dall'Unione europea

Dati vs Informazioni vs Conoscenza

- **Dati:** fatti e cifre grezzi che di per sé hanno scarso significato.

  Esempio: *"25, 10, 35" sono solo numeri privi di contesto.*

- **Informazioni:** dati organizzati o elaborati in modo da acquisire un significato.

  Esempio: *un rapporto che mostra i dati di vendita dell'ultimo trimestre fornisce un contesto ai numeri, come tendenze o approfondimenti.*

- **Conoscenza:** informazioni interpretate, comprese e applicate nel processo decisionale o nell'azione.

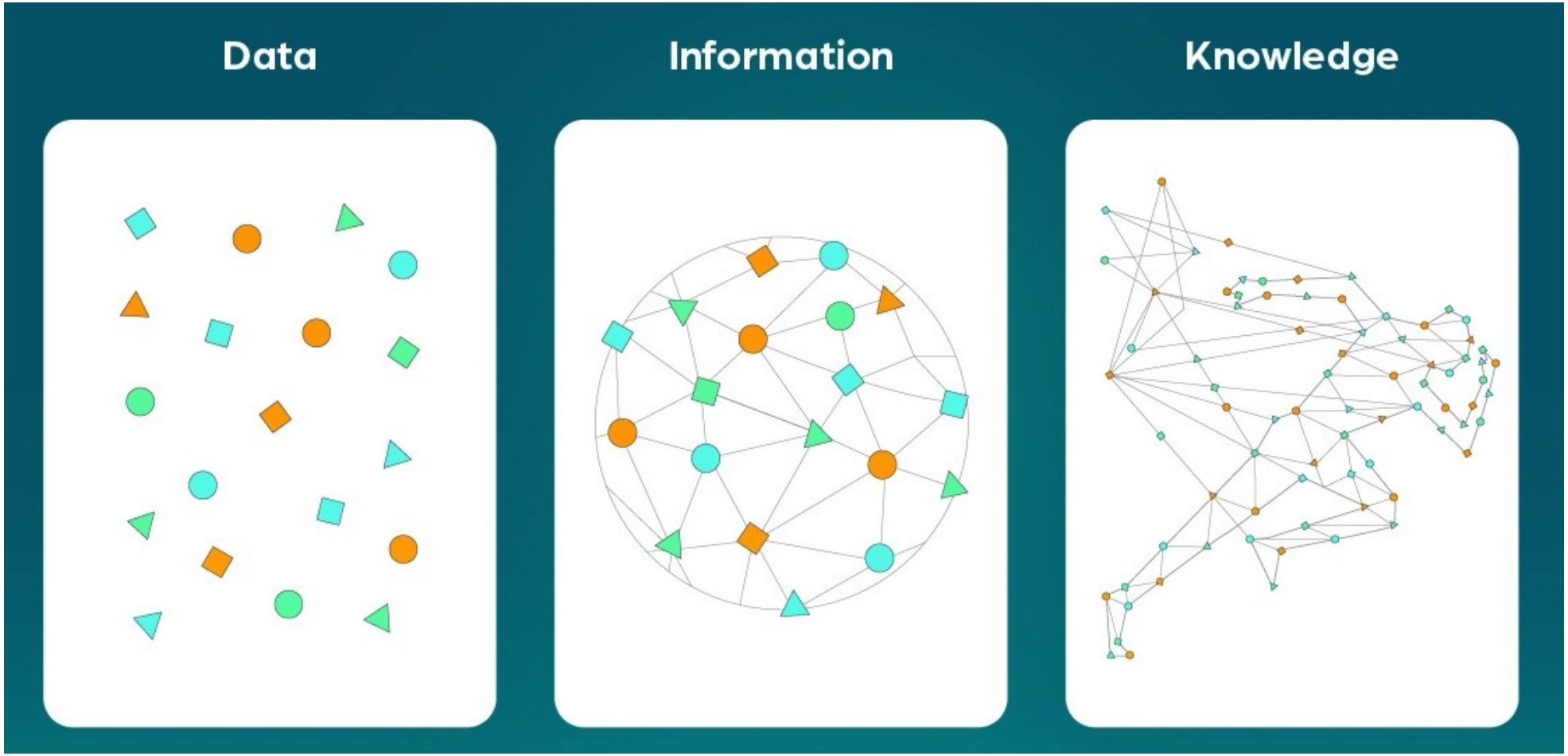
  Esempio: *un manager che utilizza il rapporto sulle vendite per prevedere le vendite del prossimo trimestre e adeguare di conseguenza la strategia di marketing.*

Comprendere la differenza tra questi concetti è fondamentale per prendere decisioni informate.

La chiave per utilizzare efficacemente le informazioni è comprenderne il contesto e trasformarle in conoscenza utilizzabile. I dati da soli sono spesso inutili senza un'interpretazione adeguata.

Cofinanziato dall'Unione europea

Dati, informazioni e conoscenza



Cofinanziato
dall'Unione europea

Dati strutturati vs dati non strutturati

Dati strutturati: dati organizzati in righe e colonne, che si trovano spesso nei database o nei fogli di calcolo. Sono facili da inserire, cercare, filtrare, archiviare, interrogare e analizzare.

Esempio: *un database clienti con campi per nome, numero di telefono e indirizzo e-mail del cliente.*

Dati non strutturati: dati che non seguono un formato predefinito. Possono essere più difficili da organizzare e analizzare.

Esempio: *e-mail, post sui social media, file di testo, PDF e file multimediali.*

I dati non strutturati possono spesso contenere informazioni preziose, ma richiedono un'elaborazione adeguata per sbloccare il loro pieno potenziale. I dati strutturati sono più facili da elaborare e analizzare, mentre i dati non strutturati contengono spesso informazioni preziose che richiedono un lavoro aggiuntivo per essere interpretate e organizzate.

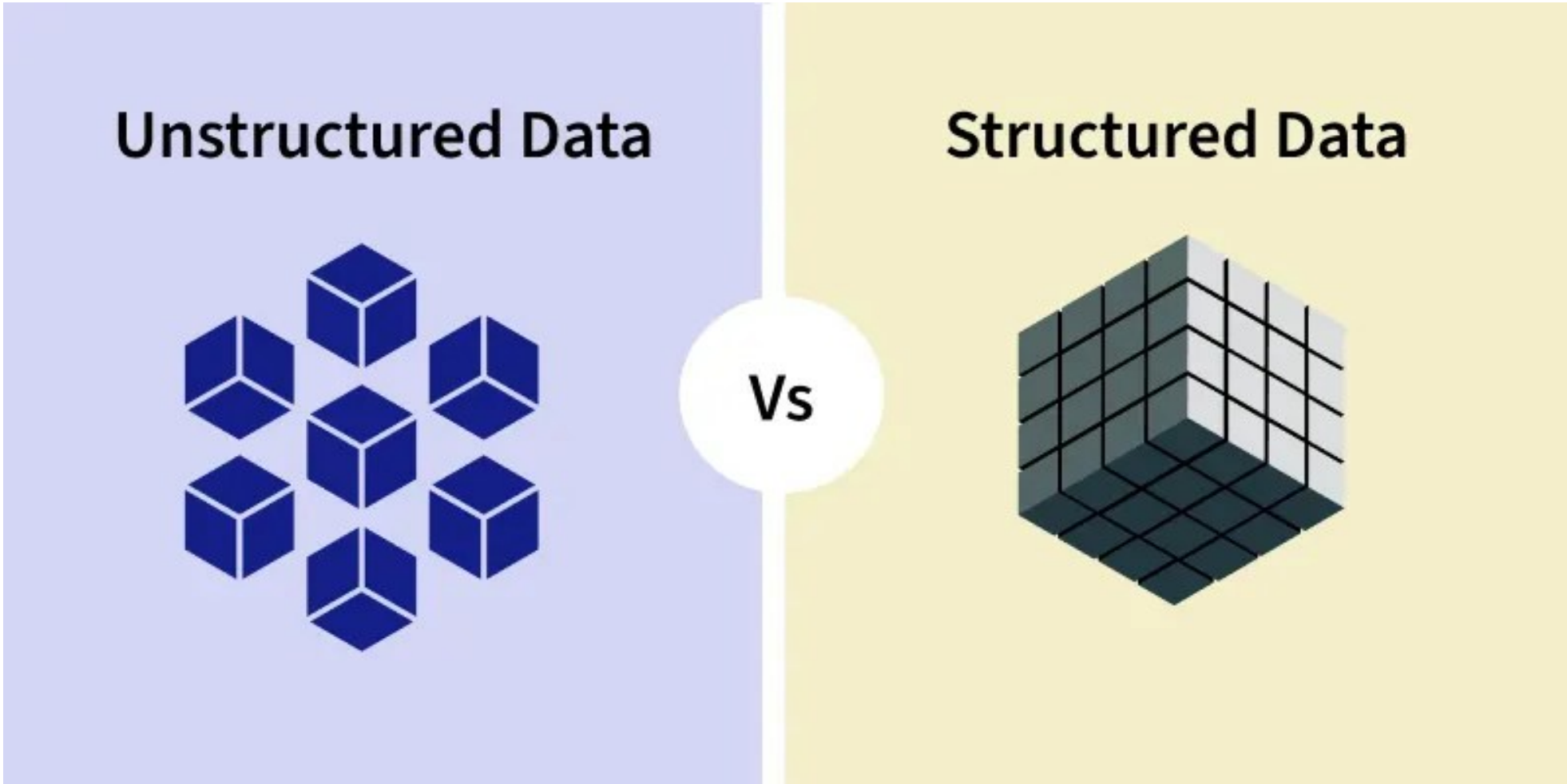
I professionisti devono comprendere come gestire sia i dati strutturati che quelli non strutturati, poiché entrambi svolgono un ruolo cruciale nel processo decisionale e nell'analisi.

Una guida completa che mette a confronto i dati strutturati e quelli non strutturati. Esplora le differenze chiave in termini di formato, archiviazione e analisi, spiegando al contempo come le moderne architetture Lakehouse gestiscono tutti e tre i tipi per promuovere la business intelligence e l'intelligenza artificiale.

Dati strutturati vs dati non strutturati

Cofinanziato dall'Unione europea

Rapport



Cofinanziato
dall'Unione europea

La realtà sul posto di lavoro

I datori di lavoro si aspettano sempre più spesso:

- Capacità di pensiero critico
- Capacità di valutare le informazioni
- Flessibilità nella gestione di diverse fonti di dati
- Apprendimento pratico e risoluzione dei problemi

In un ambiente di lavoro tipico, specialmente nelle PMI, i dipendenti spesso devono destreggiarsi tra più compiti e sono tenuti a prendere decisioni rapide. Questo contesto comporta spesso **un accesso limitato a dati perfetti** e **informazioni incomplete**.

Esempio: *un responsabile delle vendite potrebbe dover analizzare le tendenze di mercato, il feedback dei clienti e i dati interni sulle prestazioni, ma potrebbe avere accesso solo a informazioni frammentarie.*

Le decisioni informate richiedono spesso di mettere insieme vari tipi di dati e informazioni provenienti da fonti diverse. Comprendere la natura delle informazioni a disposizione e organizzarle in modo sistematico è fondamentale per evitare errori e inefficienze.

Cofinanziato dall'Unione europea

Rischi di una gestione inadeguata delle informazioni

Conseguenze di una cattiva gestione delle informazioni:

- **Decisioni errate**: l'utilizzo di informazioni errate o inaffidabili può portare a decisioni aziendali sbagliate.
- **Ritardi operativi**: una gestione inadeguata dei dati può causare ritardi nei processi o il mancato rispetto delle scadenze.
- **Rischi di conformità**: l'utilizzo di informazioni obsolete o errate può comportare il mancato rispetto dei requisiti normativi.
- **Perdite finanziarie**: dati finanziari errati possono portare a investimenti sbagliati o a opportunità mancate.

Esempio: *un dipendente potrebbe formulare previsioni finanziarie errate basandosi su dati di vendita obsoleti, portando a decisioni di bilancio sbagliate e a perdite finanziarie.*

La mancata gestione efficace delle informazioni crea un **effetto domino** che può portare a inefficienze operative e a rischi aziendali significativi.

Scopri di più sui rischi di una cattiva gestione dei dati in questa Guida IBM alla gestione dei dati

Cofinanziato dall'Unione europea

Cosa significa questo per te

Per gestire efficacemente le informazioni, è necessario:

- Capire cosa **è e cosa non è** un'informazione
- Riconoscere quando le informazioni sono **incomplete o inaffidabili**
- Organizzare i dati in modo da favorire **l'azione e la tracciabilità**
- Applicare le informazioni con **giudizio e responsabilità**

I datori di lavoro stanno dando maggiore importanza **alle meta-competenze**, quali l'adattabilità, l'iniziativa e il pensiero critico, rispetto alle competenze tecniche strettamente definite. La gestione delle informazioni non riguarda più solo la raccolta dei dati, ma anche il loro utilizzo efficace.

Sviluppare un **approccio olistico all'informazione** che includa non solo competenze di gestione dei dati, ma anche pensiero critico e adattabilità, è essenziale per soddisfare le esigenze del mondo del lavoro moderno.

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 2 – RICERCA E VALUTAZIONE DELLE INFORMAZIONI

Cofinanziato dall'Unione europea

Quiz

Click the **Quiz** button to edit this object

Seleziona la risposta corretta.

A quale fonte si dovrebbe dare la priorità quando si tratta di prendere decisioni professionali?

- **2. Post sui social media**
- **4. Sintesi generata dall'intelligenza artificiale**
- **3. Fonte ufficiale istituzionale**
- **1. Articolo di blog**

Tipi di esigenze informative sul posto di lavoro

In ogni ambiente professionale, i dipendenti devono reperire ed elaborare informazioni per portare a termine i propri compiti, risolvere problemi o prendere decisioni. Queste esigenze possono variare a seconda del settore e del ruolo ricoperto.

I principali tipi di esigenze informative includono:

- **Informazioni operative**: informazioni necessarie per gestire in modo efficiente le operazioni quotidiane (ad es. dettagli sui fornitori, prezzi, livelli delle scorte).
- **Informazioni normative**: informazioni relative a leggi, regolamenti e requisiti di conformità (ad es. linee guida in materia di salute e sicurezza, politiche GDPR).
- **Informazioni tecniche**: informazioni relative a strumenti, macchinari o software specifici (ad es. manuali d'uso, guide alla risoluzione dei problemi).
- **Informazioni relative** ai clienti: informazioni sulle esigenze, i feedback, le preferenze e la cronologia dei clienti (ad esempio, sistemi CRM, richieste di assistenza clienti).

Il tipo di informazioni necessarie può variare notevolmente a seconda dell'attività da svolgere e capire quale tipo di informazioni è richiesto vi aiuterà a indirizzare la vostra ricerca in modo più efficace.

Cofinanziato dall'Unione europea

Fonti professionali

Cosa rende una fonte professionale?

- **Credibilità**: le fonti affidabili sono redatte da esperti o da organizzazioni riconosciute nel settore. Ad esempio, articoli tratti da riviste accademiche, pubblicazioni governative o istituzioni autorevoli.
- **Autorità**: fonti provenienti da autori o editori riconosciuti, come leader del settore, professori o associazioni professionali.
- **Accuratezza**: informazioni che possono essere verificate attraverso più fonti, garantendo che siano oggettive e affidabili.
- **Rilevanza**: le informazioni devono essere aggiornate e pertinenti all'argomento specifico o alla domanda su cui stai effettuando la ricerca.

Esempi di fonti professionali:

- Riviste accademiche (ad es. ResearchGate, Academia.edu)
- Rapporti di settore (ad es. di grandi aziende come Deloitte)
- Pubblicazioni governative (ad es. regolamenti UE, linee guida ufficiali)

Affidarsi a fonti professionali garantisce che le informazioni utilizzate siano **accurate**, **affidabili** e **valide**, il che è fondamentale per prendere decisioni informate sul posto di lavoro.

Cofinanziato dall'Unione europea

Comprendere i diversi tipi di fonti di informazione

Negli ambienti professionali, le informazioni vengono prodotte e consultate attraverso diversi tipi di fonti, ciascuna con livelli diversi di affidabilità, autorevolezza e finalità:

- **Fonti ufficiali / istituzionali** (ad es. Commissione europea, legislazione, organismi di regolamentazione, politiche interne) → Elevata affidabilità, convalida formale, rilevanza giuridica
- **Fonti professionali / di settore** (ad es. documentazione tecnica, dati dei fornitori, rapporti di settore) → Pratiche, specializzate, ma possono includere un orientamento commerciale
- **Fonti interne all'organizzazione** (ad es. file aziendali, rapporti, banche dati, lavori precedenti) → Specifiche al contesto, rilevanti dal punto di vista operativo, ma possono essere obsolete o incoerenti
- **Fonti web aperte** (ad es. siti web, blog, forum, articoli) → Facile accesso, qualità variabile, spesso non convalidate
- **Contenuti generati dall'IA** (ad es. ChatGPT, Gemini, copiloti) → Rapidi e strutturati, ma richiedono verifica e giudizio critico

Il valore delle informazioni dipende in larga misura dalla loro provenienza.

Cofinanziato dall'Unione europea

Strategie di ricerca

Una ricerca efficace è fondamentale per ottenere informazioni pertinenti e accurate. Le strategie chiave includono:

- **Utilizzare parole chiave precise**: quando si effettua una ricerca online o nei database, l'uso di parole chiave specifiche e mirate fornirà risultati più pertinenti.
- **Applicare filtri**: la maggior parte dei motori di ricerca e delle banche dati consente di filtrare i risultati in base a vari fattori quali data, autore o tipo di risorsa (ad es. articoli accademici, relazioni).
- **Utilizzare più fonti**: non affidarsi a una sola fonte. Il controllo incrociato tra fonti diverse aumenta l'accuratezza e la credibilità.

Una strategia di ricerca efficace richiede molto più che digitare semplicemente alcune parole in un motore di ricerca.

Definire chiaramente la domanda prima di effettuare la ricerca.

Una buona ricerca inizia con una chiara definizione del problema, non con uno strumento.

Cofinanziato
dall'Unione europea

Rischi nella ricerca

Possibili insidie nella ricerca di informazioni:

- **Informazioni obsolete**: l'utilizzo di dati o ricerche datati può portare a decisioni basate su fatti ormai superati.
- **Parzialità delle fonti**: alcune fonti potrebbero presentare le informazioni con una particolare parzialità (ad esempio, siti web commerciali che promuovono i propri prodotti).
- **Informazioni incomplete**: una fonte potrebbe omettere un contesto importante o tralasciare fatti chiave, causando malintesi o errori.

Rischi comuni:

- Utilizzo di **fonti online non verificate** come blog o siti web personali.
- Affidarsi ai **social media** o a **contenuti generati dagli utenti** che potrebbero non essere affidabili.

Per prendere decisioni ben informate, è fondamentale essere consapevoli dei **rischi** connessi alla ricerca e all'utilizzo delle informazioni. Valutare la credibilità delle fonti è una parte essenziale del processo di raccolta delle informazioni.

Cofinanziato
dall'Unione europea

Strumenti per la ricerca di informazioni: motori di ricerca tradizionali

Motori di ricerca tradizionali:

Google è il motore di ricerca più utilizzato al mondo. Utilizza una combinazione di **algoritmi** per classificare le pagine web in base alla loro rilevanza e qualità.

Come funziona Google:

1. **Crawling**: Google utilizza dei bot per esplorare Internet e indicizzare le pagine web.
2. **Indicizzazione**: le pagine vengono classificate in base a parole chiave, link e contenuti.
3. **Classificazione**: sulla base di algoritmi, Google classifica le pagine in base alla rilevanza e all'autorevolezza, tenendo conto di criteri quali parole chiave, backlink, sicurezza del sito e coinvolgimento degli utenti.

Suggerimenti per la ricerca:

- Utilizza **parole chiave specifiche** per ottenere risultati migliori.
- Applica **dei filtri** (ad es. intervallo di date) per restringere i risultati.
- Utilizza **Google Scholar** per le risorse accademiche.
- Utilizza **Google News** per informazioni aggiornate.

I primi risultati non sono sempre:

- i più accurati
- i più affidabili

Quindi dovresti:

- controllare più risultati
- andare oltre la prima pagina
- verificare l'affidabilità delle fonti

Rischio

- Presupposto: “primo risultato = risultato migliore”
- I motori di ricerca ottimizzano per rilevanza e coinvolgimento, non sempre per veridicità o affidabilità.

Cofinanziato dall'Unione europea

La nuova tendenza: strumenti basati sull'IA per la ricerca di informazioni

Gli strumenti basati sull'intelligenza artificiale, come ChatGPT e Google Gemini, stanno cambiando il modo in cui interagiamo con i motori di ricerca.

Invece di limitarsi a restituire un elenco di link web, questi strumenti utilizzano **tecniche** avanzate **di elaborazione del linguaggio naturale (NLP)** per fornire risposte dirette, riassumere rapidamente argomenti complessi, comprendere le query in linguaggio naturale o persino partecipare a ricerche conversazionali.

Come funzionano gli strumenti di IA:

- **Comprensione dell'input**: l'utente inserisce una domanda o una query e l'IA la analizza per comprenderne il contesto e l'intento.
- **Recupero dei dati**: l'IA attinge da una vasta quantità di **conoscenze** e **dati pre-addestrati** (libri, siti web, rapporti, ecc.).
- **Generazione della risposta**: genera una risposta basata su modelli, fatti e sul proprio addestramento, offrendo una risposta chiara e diretta piuttosto che dei link.
- Esempio: *chiedendo a ChatGPT "Quali sono le principali differenze tra dati strutturati e non strutturati?", si ottiene una risposta diretta e ben strutturata, piuttosto che un elenco di link ad articoli.*

Perché la ricerca con l'IA è rivoluzionaria:

- **Efficienza**: fornisce risposte dirette, facendo risparmiare tempo agli utenti che hanno bisogno di informazioni immediate.
- **Comprensione contestuale**: è in grado di interpretare query più complesse e articolate in più passaggi e di fornire risposte sfumate.
- **Interazione personalizzata**: questi strumenti possono ricordare le conversazioni passate (in una certa misura) e affinare le risposte nel tempo.

Cofinanziato dall'Unione europea

Valutazione delle informazioni: criteri fondamentali

Prima di utilizzare le informazioni, valutare:

- **Accuratezza**
  Le informazioni sono corrette e prive di errori? Possono essere verificate tramite altre fonti attendibili?
- **Rilevanza**
  Le informazioni rispondono direttamente alla domanda o alla questione in esame? Sono tempestive e utili per il tuo processo decisionale?
- **Autorevolezza**
  Chi è l'autore o la fonte? Possiede le competenze o le credenziali necessarie per parlare dell'argomento?
- **Attualità**
  Le informazioni sono aggiornate? In settori in rapida evoluzione, l'utilizzo di informazioni obsolete può portare a decisioni sbagliate.
- **Scopo**
  Qual è l'intento dietro l'informazione? È oggettivo, o sta cercando di persuaderti o venderti qualcosa?

Ignorare la valutazione porta a:

- un uso improprio delle informazioni
- decisioni errate

Applicare sempre almeno **2-3 criteri prima dell'uso.** La valutazione è un **filtro decisionale**, non un passaggio facoltativo.

La guida alla valutazione delle informazioni dell'UNC Chapel Hill fornisce un quadro strutturato e ampiamente utilizzato per valutare la qualità, la credibilità e l'utilità delle fonti di informazione, applicabile sia in ambito accademico che lavorativo.

Cofinanziato dall'Unione europea

Quiz4

Seleziona la risposta corretta.

Qual è il comportamento corretto da adottare quando le fonti di informazione sono in contrasto tra loro?

- **3. Confronta e verifica più fonti**
- **2. Scegli la risposta più veloce**
- **4. Ignora la questione**
- **1. Scegli la fonte più semplice**

Identificare le informazioni inaffidabili

Segnali di informazioni inaffidabili:

- **Assenza di fonte o citazione**: la mancanza di una fonte chiara significa che l'informazione non può essere verificata, rendendola sospetta.
- **Linguaggio di parte o emotivo**: le informazioni che utilizzano un linguaggio eccessivamente emotivo o di parte per promuovere una causa dovrebbero essere trattate con cautela.
- **Autore poco chiaro o fuorviante**: se le credenziali dell'autore sono vaghe o non direttamente correlate all'argomento, siate scettici.
- **Affermazioni esagerate**: dichiarazioni che promettono risultati estremi o troppo belli per essere veri senza prove adeguate.
- **Informazioni incoerenti o contraddittorie**: se le informazioni contraddicono fatti accertati o il consenso degli esperti, dovrebbero essere esaminate con attenzione.

Essere in grado di identificare **i segnali di allarme** aiuta a evitare la disinformazione e a concentrarsi su fonti affidabili.

Cofinanziato dall'Unione europea

Valutazione delle informazioni generate dall'IA

Gli strumenti di intelligenza artificiale, come ChatGPT o Google Gemini, sono progettati per rispondere alle domande e fornire informazioni rapidamente, ma **non verificano i fatti** in tempo reale.

L'IA può generare contenuti che **sembrano accurati** ma che potrebbero basarsi su dati obsoleti, incompleti o distorti.

Limiti dell'IA nella valutazione delle informazioni:

- **Nessuna convalida in tempo reale**: l'IA non accede a dati in tempo reale per garantire l'attualità delle informazioni.
- **Distorsioni nei dati di addestramento**: l'IA viene addestrata su vasti set di dati, alcuni dei quali potrebbero includere informazioni distorte o inaccurate.
- **Mancanza di contesto**: l'IA potrebbe non comprendere appieno situazioni complesse e ricche di sfumature che richiedono l'interpretazione umana.

Migliori pratiche per l'utilizzo delle informazioni generate dall'IA:

- **Verificare** sempre le informazioni generate dall'IA con altre fonti credibili.
- Comprendere che **gli strumenti di IA** sono lì per assistere, ma non per sostituire **la valutazione critica**.
- Utilizzare l'IA in modo responsabile per **supportare il processo decisionale**, ma non come unica fonte di verità.

La responsabilità dell'accuratezza rimane a carico dell'utente umano, non dello strumento.

Cofinanziato dall'Unione europea

Cosa fare quando le fonti sono in conflitto?



Si legge:

- La fonte A dice una cosa
- La fonte B dice un'altra cosa

In quel caso dovresti:

- verificare l'autorevolezza della fonte
- confrontare più riferimenti
- dare priorità ai dati ufficiali o convalidati
- rimandare la decisione se necessario

Scegliere la risposta più facile o più veloce non è la pratica corretta.

Il giudizio professionale viene messo alla prova quando le informazioni sono **incerte o contraddittorie**.

Cofinanziato dall'Unione europea

Impatto del rischio derivante da una valutazione inadeguata delle informazioni

Conseguenze di una valutazione inadeguata:

- **Rischi legali**: l'utilizzo di informazioni di conformità obsolete può comportare **multe** o **azioni legali**.
- **Rischi operativi**: un'errata interpretazione della documentazione tecnica può causare guasti alle attrezzature o ritardi nella produzione.
- **Rischi finanziari**: un'analisi di mercato inadeguata può portare a decisioni di investimento sbagliate o a opportunità mancate.
- **Rischi reputazionali**: affidarsi a informazioni parziali o false può danneggiare la reputazione dell'azienda e portare alla sfiducia dei clienti.

Valutare la qualità e l'affidabilità delle informazioni **mitiga i rischi** e garantisce che le decisioni siano prese in linea con gli standard professionali e le normative del settore.

Dati del fornitore errati → contratto sbagliato → perdita finanziaria

Cofinanziato dall'Unione europea

Flusso di lavoro professionale per la valutazione delle informazioni

Un approccio strutturato:

- **Verifica delle informazioni**: confronta fatti e dati con più fonti affidabili.
- **Porre domande chiave**: Chi è l'autore? Qual è la sua autorevolezza? Quando è stato pubblicato? Perché viene utilizzata questa fonte?
- **Documentare i risultati**: tenere traccia delle fonti utilizzate, specialmente quando si prendono decisioni basate sulle informazioni.
- **Utilizzare gli strumenti**: utilizzare in modo responsabile strumenti di fact-checking, banche dati e IA per integrare il processo di valutazione delle informazioni.

Un **approccio professionale** alla valutazione delle informazioni comprende un'attenta verifica, il pensiero critico e un approccio strutturato all'organizzazione e alla documentazione dei risultati. Ciò tutela sia la credibilità personale che quella organizzativa.

Non saltare mai la valutazione a causa di:

- la mancanza di tempo
- routine
- supposizioni

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 3 – ORGANIZZAZIONE E GESTIONE DI INFORMAZIONI E DATI

Cofinanziato
dall'Unione europea

Perché l'organizzazione è una competenza professionale

Negli ambienti professionali, **l'organizzazione delle informazioni** non è un semplice dettaglio tecnico, ma una competenza lavorativa fondamentale che incide direttamente sulle prestazioni.

L'organizzazione dei dati è essenziale per l'efficienza, la produttività e la sicurezza dei dati. Sul posto di lavoro, garantisce che:

- Le informazioni siano facilmente accessibili in modo rapido e sicuro quando necessario.
- Gli errori siano ridotti al minimo perché i dati sono ben strutturati e facilmente verificabili.
- Si collabori in modo efficace con i colleghi
- I rischi per la sicurezza siano ridotti, poiché i dati organizzati impediscono l'esposizione accidentale.

Cofinanziato dall'Unione europea

Logica della struttura delle cartelle

Strutture di cartelle efficaci: uno dei modi migliori per organizzare i dati consiste nel creare una struttura di cartelle chiara e coerente. Ecco alcune linee guida fondamentali:

- **Categorizzazione**: raggruppa i file per progetto, reparto o data per trovare facilmente ciò che ti serve.
- **Coerenza**: segui sempre lo stesso sistema di denominazione e archiviazione per ogni progetto, in modo che i file siano più facili da individuare.
- **Sottocartelle**: suddividere i progetti di grandi dimensioni in sottocartelle per attività specifiche, in modo da facilitare il monitoraggio dei diversi aspetti di un progetto.

Una struttura di cartelle professionale dovrebbe riflettere la logica del lavoro:

- **Per progetto** → quando il lavoro è basato su progetti
- **Per funzione** → quando le attività sono ripetitive (ad es. finanza, risorse umane)
- **Per fase del processo** → quando i flussi di lavoro seguono delle fasi

Esempio di struttura: *Progetto → Fase → Tipo di documento → Versione*

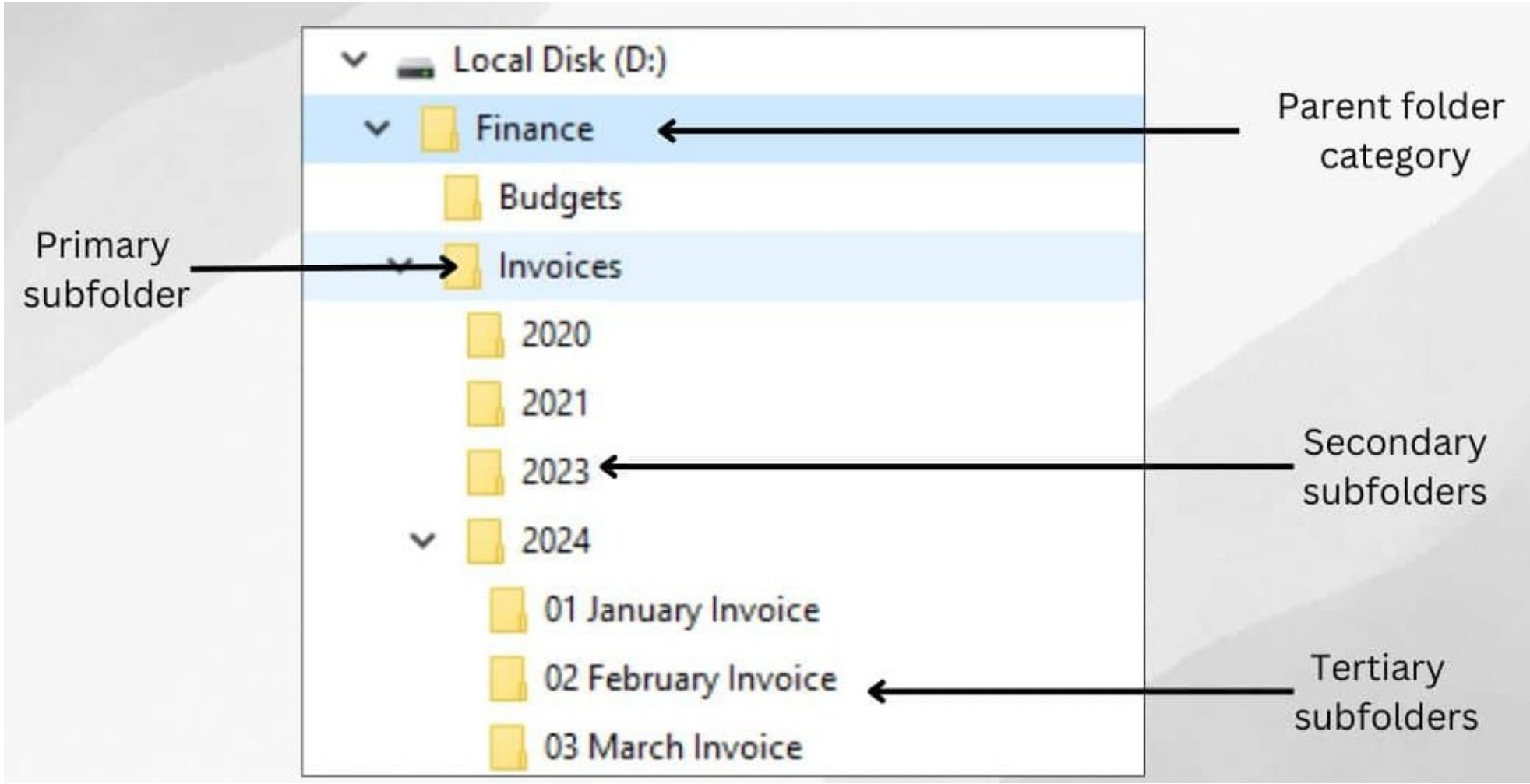
Un sistema di cartelle ben strutturato riduce la confusione, garantisce un recupero efficiente dei dati e aiuta a prevenire la perdita di file importanti.

Migliori pratiche:

- Mantienila semplice e intuitiva.
- Utilizza nomi descrittivi per cartelle e file per rendere chiaro il loro contenuto.
- Evita sottocartelle inutili e gerarchie complesse che rendono più difficile la navigazione nel sistema.
- Assicurati che la struttura delle cartelle supporti la collaborazione, con permessi e livelli di accesso appropriati.

Cofinanziato dall'Unione europea

Un esempio di raggruppamento delle cartelle per categoria



Cofinanziato dall'Unione europea

Convenzioni di denominazione dei file

L'adozione di convenzioni di denominazione coerenti contribuisce a garantire che i file siano facili da identificare e recuperare.

Si prega di seguire queste linee guida:

- **Siate descrittivi**: includete dettagli chiave come il nome del progetto, la data, il numero di versione e il tipo di contenuto. Esempio: *"ClientXYZ_ProjectReport_2023-10-15_V1".*
- **Sii semplice**: evita nomi troppo lunghi e dettagli superflui. L'obiettivo è rendere il file facilmente identificabile a colpo d'occhio.
- **Evita i caratteri speciali**: i caratteri speciali (ad es. !, @, #) possono causare problemi in alcuni sistemi. Utilizza solo lettere, numeri e trattini.
- **Utilizza formati di data coerenti**: utilizza sempre lo stesso formato di data (ad es. AAAA-MM-GG) in modo che i file siano organizzati in ordine cronologico.

Perché le convenzioni di denominazione sono importanti:

- **Chiarezza**: i file con nomi corretti sono più facili da comprendere e da trovare.
- **Coerenza**: una denominazione standardizzata previene la confusione quando più persone gestiscono i file.
- **Controllo delle versioni**: includere i numeri di versione nei nomi dei file consente di tracciare facilmente le modifiche.

Cofinanziato dall'Unione europea

Che cos'è la gestione delle versioni?

La gestione delle versioni consiste nell'organizzare i file in modo da poter seguire **l'evoluzione** di un documento nel tempo. Ciò consente di:

- **Evitare confusione** quando esistono più versioni dello stesso documento.
- **Tenere traccia** delle modifiche apportate al file.
- **Tracciare la versione più recente** di un documento.

Migliori pratiche per il controllo delle versioni:

- **Includere i numeri di versione**: etichettare sempre ogni versione del file (ad es. "v1", "v2", "final") per tenere traccia degli aggiornamenti.
- **Utilizza sistemi cloud con controllo delle versioni integrato**: le piattaforme di archiviazione cloud come Google Drive o OneDrive tengono automaticamente traccia della cronologia delle versioni.
- **Limita le revisioni**: evita di creare troppe versioni a meno che non sia necessario. Fai aggiornamenti chiari e ben ponderati per garantire la chiarezza.

Esempio: *un team di marketing che lavora su una proposta dovrebbe etichettare i propri file come "Proposta_ClienteXYZ_v1", "Proposta_ClienteXYZ_v2", ecc. Ciò consente a tutti di essere allineati ed evita confusione sulla versione corrente.*

Utilizzando il controllo delle versioni, vi assicurate di lavorare sempre sul file più recente e aggiornato, riducendo al minimo errori e confusione. Esempio: *Report_v1 → Report_v2 → Report_final*

Cofinanziato dall'Unione europea

Errori comuni nell'organizzazione dei dati

Errori comuni nell'organizzazione dei dati:

- **Struttura delle cartelle troppo complessa**: creare troppe sottocartelle o divisioni non necessarie può rendere più difficile trovare i file.
- **Denominazione incoerente**: cambiare le convenzioni di denominazione o utilizzare nomi vaghi può rendere difficile capire cosa contiene un file.
- **Archiviazione dei file in posizioni casuali**: salvare i file in posizioni casuali invece che in una struttura di cartelle coerente porta alla perdita o allo smarrimento dei file.
- **Mancanza di backup**: non eseguire il backup dei dati può portare a una perdita permanente in caso di guasti del sistema.

Come evitare gli errori:

- Mantenere la struttura delle cartelle **semplice** e **intuitiva**.
- Utilizzare un **sistema di denominazione coerente** per tutti i file e i documenti.
- **Eseguire backup regolari** per evitare la perdita di dati.

Gli errori comuni nell'organizzazione dei dati portano a inefficienze e frustrazioni. Seguire semplici best practice può migliorare significativamente la gestione dei dati.

Cofinanziato dall'Unione europea

Cosa sono i dati strutturati? (Versione estesa)

Per "**dati strutturati**" si intendono dati organizzati secondo un **formato predefinito,** come righe, colonne e tabelle, che ne facilitano l'elaborazione e l'analisi.

Caratteristiche dei dati strutturati:

- **Organizzati:** i dati sono organizzati in righe e colonne, il che ne facilita l'inserimento, l'interrogazione e l'analisi.
- **Coerenti:** ogni voce segue un formato simile, come date, numeri o testo.
- **Facili da elaborare:** poiché i dati sono prevedibili, possono essere facilmente elaborati utilizzando strumenti automatizzati come Excel o Google Sheets.

Esempio: *un **database clienti** con colonne per nome, e-mail, numero di telefono e cronologia degli acquisti è un esempio di dati strutturati.*

I dati strutturati sono **ideali per l'analisi** perché la loro uniformità consente di interrogarli, ordinarli e analizzarli facilmente.

Cofinanziato dall'Unione europea

Cosa sono i dati non strutturati? (Versione estesa)

Per "**dati non strutturati**" si intendono le informazioni che non seguono un formato predefinito e che sono difficili da organizzare e analizzare in modo sistematico.

Esempi: *e-mail, PDF, messaggi di chat, note*

La maggior parte delle informazioni esiste inizialmente come **dati non strutturati.**

Tuttavia, presentano alcuni problemi:

- difficili da cercare
- difficili da confrontare
- facilmente persi

Esempio: *richieste dei clienti nelle e-mail rispetto al sistema CRM strutturato.*

Convertire i dati non strutturati importanti in formati strutturati.

I dati non strutturati sono utili per la comunicazione, ma rischiosi per le decisioni.

Cofinanziato dall'Unione europea

Da dati non strutturati a dati strutturati

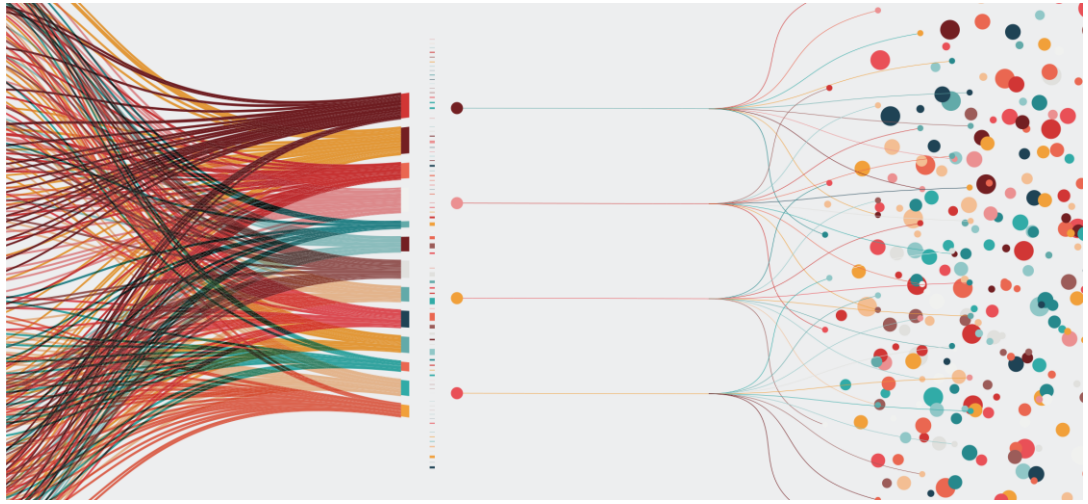
Il lavoro professionale richiede la trasformazione delle informazioni: **Input → Elaborazione → Utilizzo**

Esempio: E-mail / note → Foglio di calcolo / sistema → Decisione

Esempio di flusso di lavoro: Ordini dei clienti (e-mail) → inseriti nel foglio di calcolo → analizzati per individuare le tendenze

Perché questo passaggio è importante

- riduce l'ambiguità
- migliora la tracciabilità
- supporta l'automazione



Saltare la strutturazione porta a:

- decisioni incoerenti
- perdita di informazioni

Il passaggio dai dati non strutturati a quelli strutturati è il punto **di partenza del controllo professionale**.

Cofinanziato dall'Unione europea

I fogli di calcolo come strumenti per i dati strutturati

I fogli di calcolo (Excel, Google Sheets) sono strumenti fondame

- organizzare dati strutturati
- analizzare modelli e tendenze
- supportare le decisioni operative e finanziarie

Funzioni principali

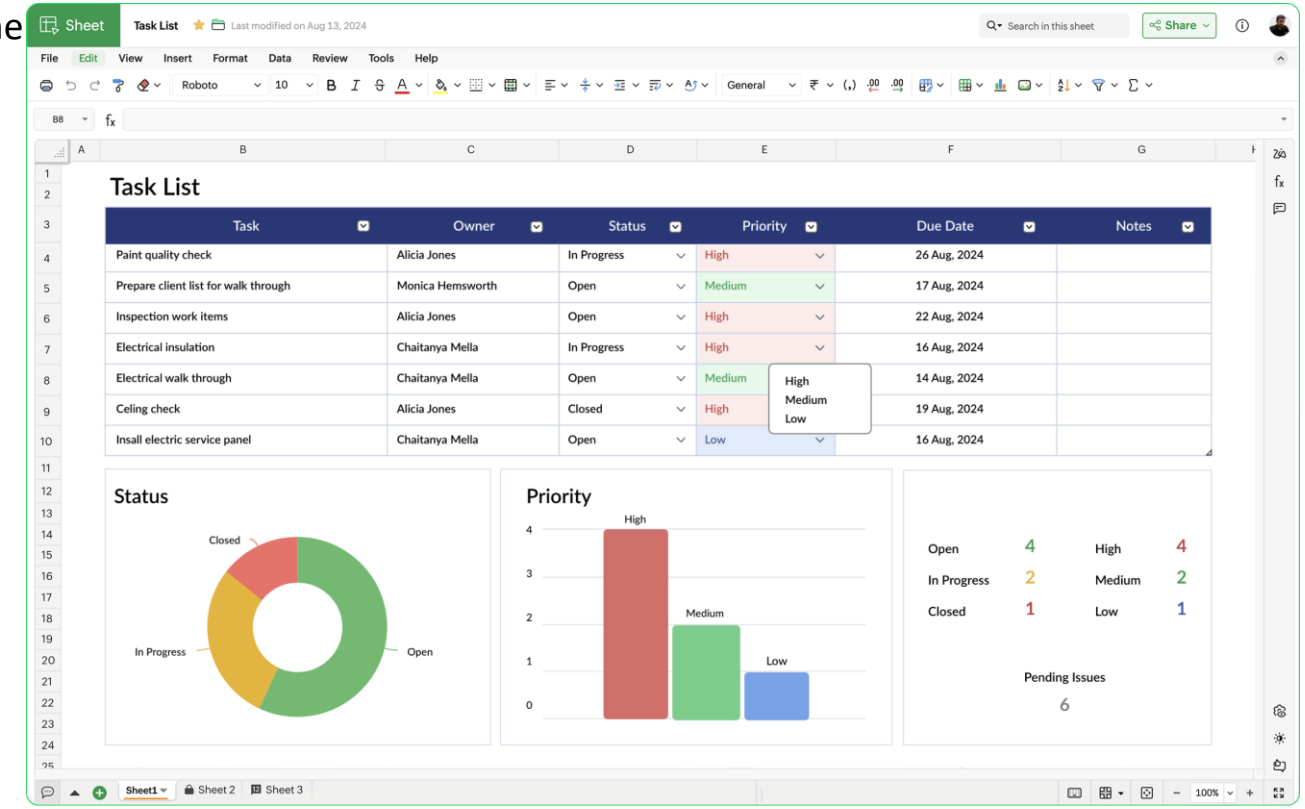
- inserimento dati
- ordinamento e filtraggio
- formule e calcoli
- visualizzazione dei dati

Applicazioni sul posto di lavoro

- monitoraggio delle vendite
- gestione delle scorte
- bilanci
- reportistica

L'uso di fogli di calcolo senza una struttura porta a:

- dati incoerenti
- risultati inaffidabili



I fogli di calcolo non sono solo strumenti di archiviazione: sono **sistemi di supporto decisionale**.

Su Microsoft Excel Training (Guida ufficiale) puoi trovare tutorial ufficiali su come strutturare, analizzare e gestire i dati in modo efficace.

Cofinanziato dall'Unione europea

Progettare correttamente un foglio di calcolo

Principi fondamentali di progettazione

- **Una colonna = un tipo di dati**
- (ad es. Data, Importo, Nome del cliente – mai mescolati)
- **Formato coerente per ogni colonna**
  (ad es. tutte le date nello stesso formato, tutti i valori numerici)
- **Nessun campo vuoto o misto** (evitare spazi vuoti, celle unite o dati combinati)
- **Utilizzare intestazioni chiare** (ogni colonna deve descrivere esattamente ciò che contiene)

- Esempio:
  - ❌ Errato: “12/03 – John – 250€” in un’unica colonna
  - ✅ Corretto: Data | Nome | Importo (colonne separate)

Una buona struttura:

- consente l'ordinamento e il filtraggio
- supporta formule e automazione
- riduce gli errori di interpretazione

La maggior parte dei problemi dei fogli di calcolo non ha origine nelle formule, ma nella progettazione della struttura.

Rischi

Una progettazione inadeguata porta a:

- errori di calcolo
- analisi incoerenti
- impossibilità di riutilizzare i dati

Buona pratica

- pianificare la struttura prima di inserire i dati
- mantenere i formati semplici e standardizzati
- controllare il layout prima dell'uso

Cofinanziato dall'Unione europea

Qualità e coerenza dei dati

Disporre di dati di alta qualità è fondamentale per garantire analisi e processi decisionali affidabili. Anche i dati ben strutturati perdono di efficacia se non se ne preserva la qualità.

Dimensioni fondamentali della qualità dei dati

- **Accuratezza** → i valori sono corretti e verificati
- **Completezza** → nessuna voce mancante o parziale
- **Coerenza** → stesso formato in tutti i record
- **Affidabilità** → i dati sono attendibili ai fini decisionali

Problemi comuni nella pratica

- formati di data misti (ad es. GG/MM vs MM/GG)
- valute incoerenti (€ vs $ vs testo)
- valori mancanti o righe incomplete
- voci duplicate o in conflitto

Buone pratiche

- standardizzare i formati prima dell'uso
- applicare regole di convalida (ad es. campi solo numerici)
- Rivedere e ripulire i dati regolarmente
- verificare la presenza di duplicati e incongruenze

Una scarsa qualità dei dati porta a:

- calcoli errati
- report fuorvianti
- decisioni errate o rischiose

La qualità dei dati non è una questione tecnica, ma una **questione di affidabilità delle decisioni**.

Cofinanziato dall'Unione europea

Il fattore umano nella gestione dei dati

La maggior parte dei problemi legati ai dati non è causata dagli strumenti, ma dal **comportamento umano e dai modelli decisionali**.

Comportamenti comuni

- inserimento affrettato dei dati
- trascurare la struttura o la convalida
- affidarsi alla memoria anziché ai sistemi
- abitudini di lavoro incoerenti

Cause sottostanti

- pressione del tempo
- routine (“facciamo sempre così”)
- sovraccarico cognitivo
- mancanza di consapevolezza o formazione

Impatto sul posto di lavoro

- errori ripetuti
- set di dati incoerenti
- riduzione della fiducia nelle informazioni
- maggiore necessità di correzioni

Pratica corretta

- seguire procedure chiare e coerenti
- applicare regole standard in tutte le attività
- verificare i dati prima di utilizzarli
- sviluppare l'abitudine di controllare e rivedere

La tecnologia non elimina il rischio: trasferisce la responsabilità al **giudizio e** al **comportamento umano**.

Cofinanziato dall'Unione europea

Sintesi: dai dati alle decisioni affidabili

Una gestione efficace dei dati è un processo strutturato che collega la gestione delle informazioni al processo decisionale professionale.

Processo integrato

1. Strutturare correttamente i dati

2. Garantire qualità e coerenza

3. Individuare e prevenire gli errori

4. Applicare pratiche di lavoro disciplinate

5. Consentire un recupero rapido e affidabile

Flusso operativo:

Dati → Struttura → Qualità → Analisi → Decisione → Azione

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 4 – ARCHIVIAZIONE NEL CLOUD E GESTIONE DEI DATI

Cofinanziato
dall'Unione europea

Comprendere l'archiviazione cloud sul posto di lavoro

Il cloud storage consiste nel salvare i dati in un ambiente online anziché su dispositivi fisici (ad esempio, dischi rigidi locali). Piattaforme cloud come **Google Drive**, **OneDrive** e **Dropbox** consentono agli utenti di archiviare, accedere e condividere file da remoto. In parole semplici, il cloud storage consiste nell'archiviazione e nella gestione dei dati su **server remoti accessibili tramite Internet**, anziché su dispositivi locali.

Vantaggi dell'archiviazione cloud:

- **Accessibilità**: i file sono accessibili da qualsiasi dispositivo connesso a Internet, garantendo flessibilità per il lavoro da remoto e i viaggi.
- **Collaborazione**: più utenti possono accedere, modificare e collaborare sui documenti in tempo reale. Ciò è essenziale per il lavoro di squadra, specialmente nelle PMI in cui i dipendenti possono lavorare in sedi diverse.
- **Scalabilità**: l'archiviazione cloud consente alle aziende di **adattare** le proprie esigenze di archiviazione man mano che l'azienda cresce, senza dover investire in hardware fisico aggiuntivo.

Esempio: *un team di progetto che lavora su un **documento condiviso** in **Google Drive** può apportare aggiornamenti in tempo reale, garantendo a tutti la versione più recente senza dover inviare manualmente i file avanti e indietro.*

Cofinanziato dall'Unione europea

Come l'archiviazione cloud cambia il nostro modo di lavorare

Approccio tradizionale (archiviazione locale)

- file memorizzati su computer personali
- accesso limitato
- condivisione manuale (e-mail, USB)
- versioni multiple dello stesso file

Approccio basato sul cloud

- accesso condiviso in tempo reale
- versione unica e attendibile
- aggiornamenti continui
- collaborazione integrata

Esempio sul posto di lavoro:

- *Prima: File_v1 → File_v2 → Finale_v3 → FINALE_FINALE*
- *Ora: Un unico documento condiviso → aggiornato continuamente*

Il cloud trasforma il lavoro da attività individuali → processi collaborativi.

Cofinanziato dall'Unione europea

Funzioni principali, collaborazione e controllo nella gestione dei dati nel cloud

I sistemi cloud non sono semplici sistemi di archiviazione: influenzano attivamente il modo in cui si svolgono il lavoro, la collaborazione e il processo decisionale.

Funzioni principali (Cosa consentono i sistemi cloud)

- **Archiviazione e organizzazione:** cartelle strutturate, denominazione e categorizzazione coerenti
- **Accesso e autorizzazioni:** controllo di chi può visualizzare, modificare o condividere le informazioni
- **Controllo delle versioni:** tracciare, rivedere e ripristinare le modifiche nel tempo
- **Ricerca e recupero:** accesso rapido e affidabile ai file quando necessario

Collaborazione nella pratica

- più utenti che lavorano sullo stesso file
- aggiornamenti in tempo reale e visibilità condivisa
- monitoraggio continuo attraverso la cronologia delle versioni

L'efficienza del cloud dipende da **come viene gestito, non solo da come viene utilizzato**.

Negli ambienti cloud: **Collaborazione + Controllo = Risultati affidabili**

Buone pratiche

- Assegnare ruoli chiari (proprietario / editore / visualizzatore)
- controllare e gestire sempre i permessi di accesso
- utilizzare attivamente la cronologia delle versioni
- evitare la modifica simultanea non controllata
- mantenere una struttura chiara e convenzioni di denominazione

Cofinanziato dall'Unione europea

Rischi nell'archiviazione cloud e nella condivisione dei dati

Gli ambienti cloud comportano rischi specifici legati **all'accesso, alla condivisione e al controllo**.

Rischi comuni

- autorizzazioni di accesso non controllate
- condivisione accidentale con utenti sbagliati
- esposizione dei dati tramite link pubblici
- perdita di controllo sulle versioni dei file
- esposizione dei dati
- accesso esterno

La maggior parte dei problemi deriva da:

- fraintendimento delle autorizzazioni
- azioni di condivisione affrettate
- mancanza di verifica

Negli ambienti cloud, **accesso = controllo = responsabilità.**

Buone pratiche

- controllare sempre le impostazioni di accesso
- evitare l'opzione "chiunque abbia il link" a meno che non sia necessario
- rivedere la condivisione prima dell'invio
- verificare regolarmente i file condivisi

Cofinanziato dall'Unione europea

Best practice per la gestione dei dati nel cloud

Per lavorare in modo efficace con i sistemi cloud, i professionisti devono seguire procedure strutturate:

- definire ruoli e responsabilità
- comunicare chiaramente i cambiamenti
- utilizzare i documenti condivisi in modo responsabile

Disciplina del flusso di lavoro

- verificare prima di condividere
- aggiornare i file in modo coerente
- mantenere la chiarezza delle versioni

L'efficienza del cloud dipende da **disciplina, coerenza e responsabilità**.

Pratiche chiave

- Organizzare le cartelle in modo chiaro e coerente
- utilizzare convenzioni di denominazione standard
- controllare attentamente i permessi di accesso
- evitare la duplicazione dei file
- Rivedere e ripulire regolarmente lo spazio di archiviazione

Cofinanziato dall'Unione europea

Rapport

ARGOMENTO 5 – APPLICAZIONE AVANZATA BASATA SU CASI CONCRETI

Cofinanziato
dall'Unione europea

Scenario 1: Gestione dei dati dei fornitori per il processo decisionale

Lavori come assistente operativo junior in una piccola società commerciale.

Le tue responsabilità sono:

- gestire i registri dei fornitori
- aggiornare i dati sui prezzi nei fogli di calcolo
- archiviare i documenti nel sistema cloud aziendale

Il tuo responsabile ti chiede di:

- aggiornare le informazioni sui prezzi dei fornitori
- preparare un rapporto di confronto
- caricarlo e condividerlo nel cloud

Stai lavorando con:

- diverse versioni di fogli di calcolo
- e-mail con prezzi aggiornati
- file archiviati in cartelle diverse
- convenzioni di denominazione poco chiare

Devi completare l'attività **rapidamente** perché una decisione di acquisto dipende dal tuo report.

Nelle situazioni lavorative reali, i dati sono spesso **incompleti, sparsi e urgenti**.

Qual è la tua priorità principale prima di iniziare l'attività?

Cofinanziato dall'Unione europea

Analisi dello scenario 1: Gestione dei dati dei fornitori

Per gestire questa situazione in modo professionale, è opportuno seguire un approccio strutturato:

Fase 1 – Chiarire l'obiettivo	• Cosa è necessario? → Confronto tra fornitori per il processo decisionale • Cosa è fondamentale? → Accuratezza e prezzi aggiornati
Fase 2 – Convalidare le fonti di informazione	• confrontare i dati del foglio di calcolo con gli aggiornamenti via e-mail • Individuare le informazioni obsolete o incoerenti • dare priorità alle fonti più recenti e affidabili
Fase 3 – Strutturare i dati	• creare un foglio di calcolo pulito • definire colonne chiare (fornitore, prezzo, data, condizioni) • garantire la coerenza nel formato
Fase 4 – Garantire la qualità dei dati	• controllare la presenza di valori mancanti o errati • verificare i calcoli • evitare duplicazioni
Fase 5 – Archivia e condividi correttamente	•salvare nella cartella cloud corretta •utilizzare una convenzione di denominazione adeguata •controllare le autorizzazioni prima di condividere

Un professionista non lavora con i primi dati disponibili, ma li convalida, li struttura e li verifica prima di agire.

Decisioni affidabili dipendono da dati controllati, non da supposizioni affrettate.

Cofinanziato dall'Unione europea

Scenario 2: Gestione dei dati dei clienti in un foglio di calcolo

Lavori come **assistente amministrativo junior** in un'azienda di servizi.

Le tue responsabilità sono:

- aggiornare i dati dei clienti
- tenere un foglio di calcolo con le transazioni
- preparare riepiloghi di base sulle prestazioni

Ti viene chiesto di:

- aggiornare i dati relativi alle transazioni dei clienti
- calcolare i totali mensili
- inviare un rapporto di sintesi al proprio supervisore

Notate che:

- valori mancanti in alcune righe
- formati di data incoerenti
- voci duplicate
- formule poco chiare già utilizzate nel foglio di calcolo

Il report verrà utilizzato per **la pianificazione finanziaria**, quindi l'accuratezza è fondamentale.

Qualsiasi errore potrebbe portare a:

- decisioni finanziarie errate
- perdita di fiducia

Spesso ci si fida dei fogli di calcolo anche quando contengono **errori nascosti**.

Qual è l'azione più importante da compiere prima di utilizzare i dati?

Cofinanziato dall'Unione europea

Analisi dello scenario 2: Gestione dei dati dei clienti

Questa situazione richiede un'attenta gestione della qualità dei dati e dell'integrità dei fogli di calcolo.

Fase 1 – Individuare i problemi relativi ai dati	• individuare i valori mancanti • rilevare i duplicati • verificare i formati incoerenti
Fase 2 – Pulizia dei dati	• standardizzare i formati (date, valuta) • rimuovere i duplicati • inserire o contrassegnare i dati mancanti
Fase 3 – Controllare la struttura del foglio di calcolo	• verificare che le colonne siano definite correttamente • assicurarsi che ci sia un solo tipo di dati per colonna • evitare campi misti o poco chiari
Fase 4 – Convalida i calcoli	•controllare le formule e gli intervalli •verificare i risultati con dati di esempio
Fase 5 – Preparare un output affidabile	•assicurarsi che il rapporto finale rifletta i dati corretti •Rivedere prima di condividere

Non fidarti mai di un foglio di calcolo senza averne verificato **la struttura, la qualità e le formule**.

I fogli di calcolo creano un'illusione di precisione, ma l'affidabilità dipende dal **controllo della qualità dei dati**.

Cofinanziato dall'Unione europea

Scenario 3: Lavorare con file condivisi nel cloud

Lavori come **assistente di team** in una piccola azienda che opera su base progettuale.

Le tue responsabilità sono:

- supportare la preparazione dei documenti
- collaborare con i membri del team
- gestire i file in una cartella cloud condivisa

Il tuo team sta preparando una relazione di progetto.

Devi:

- rivedere il documento
- apportare modifiche
- condividerlo con il responsabile del progetto

Trovi:

- versioni multiple dello stesso file
- nomi dei file poco chiari (Final_v2, Final_NEW, Final_Updated)
- membri del team che modificano versioni diverse

Non sei sicuro:

- quale versione sia quella corretta
- chi ha apportato le ultime modifiche
- quale file debba essere inviato

Il rapporto deve essere consegnato **entro la prossima ora**.

Gli strumenti cloud semplificano la collaborazione, ma possono creare confusione se non vengono gestiti.

Qual è il tuo primo passo prima di modificare o condividere il file?

Cofinanziato dall'Unione europea

Analisi dello scenario 3: Collaborazione nel cloud e controllo delle versioni

Questa situazione evidenzia l'importanza del **controllo negli ambienti cloud**.

Passaggio 1 – Identificare la versione corretta	• controllare la cronologia delle versioni • identificare l'ultimo aggiornamento • verificare con il team se necessario
Fase 2 – Stabilire il controllo	• identificare il proprietario del file • garantire che vengano apportate solo modifiche autorizzate
Fase 3 – Evitare la duplicazione	• smettere di lavorare su più file • unire il tutto in un'unica versione condivisa
Fase 4 – Applicare una denominazione chiara	• rinominare i file in modo coerente • rimuovere i duplicati che creano confusione
Fase 5 – Verifica prima della condivisione	• confermare la versione corretta • controllare i permessi • garantire l'accuratezza finale

Nei sistemi cloud, la chiarezza e il controllo sono più importanti della velocità. La collaborazione richiede **struttura, responsabilità e disciplina**.

Cofinanziato dall'Unione europea

Scenario 4: Ricerca e valutazione delle informazioni per un compito

Lavori come **dipendente junior in una piccola azienda**.

Le tue responsabilità sono:

- ricerca di informazioni esterne
- supportare le decisioni operative
- raccogliere e sintetizzare i dati

Ti viene chiesto di:

- trovare informazioni su un nuovo fornitore
- verificare i requisiti di conformità
- fornire una raccomandazione

Trovi:

- informazioni diverse sui siti web
- un articolo di blog con dettagli utili
- un riassunto generato dall'intelligenza artificiale
- una fonte ufficiale con contenuti complessi

Difficoltà

- le informazioni sono incoerenti
- alcune fonti sono più facili da comprendere
- altre sono più affidabili ma complesse

Il tuo responsabile si aspetta una **risposta rapida e chiara**. Scegliere la fonte sbagliata può portare a:

- decisioni errate
- problemi di conformità

Le informazioni più semplici non sono sempre le **più affidabili**.

A quale fonte ti affideresti per prima e perché?

Cofinanziato dall'Unione europea

Analisi dello scenario 4: Valutazione delle fonti di informazione

Questa situazione richiede **una valutazione critica e un giudizio professionale**.

Fase 1 – Identificare i tipi di fonte	• fonte ufficiale → alta affidabilità • blog / IA → affidabilità inferiore • fonti miste → richiedono una verifica
Fase 2 – Valutare le informazioni	• verificare l'accuratezza • verificare autore e origine • confermare la data di aggiornamento
Fase 3 – Confronta le fonti	• Individuare le differenze • dare priorità alle informazioni autorevoli • verificare i fatti chiave
Fase 4 – Evitare errori comuni	• non scegliere la fonte più facile • non affidarti a una sola fonte • Non fidarti dei risultati dell'IA non verificati
Fase 5 – Formulare una raccomandazione motivata	• Basa la decisione su informazioni verificate • spiega il ragionamento

Un professionista non seleziona le informazioni in base alla convenienza, ma in base **all'affidabilità e alla rilevanza**.

Il pensiero critico è la capacità di **mettere in discussione, confrontare e giustificare le decisioni**.

Cofinanziato dall'Unione europea

Fonti

- Commissione europea (2022) *Indice dell'economia e della società digitali (DESI) 2022: Capitale umano*. Disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/policies/desi (Consultato il: 31 marzo 2026)
- Università della Carolina del Nord (UNC) (2023) *Valutazione delle fonti di informazione*. Disponibile all'indirizzo: https://guides.lib.unc.edu/evaluating-info/evaluate (Consultato il: 31 marzo 2026)
- IBM (2023) *Gestione dei dati: rischi di una cattiva gestione delle informazioni*. Disponibile all'indirizzo: https://www.ibm.com/topics/data-management (Consultato il: 31 marzo 2026)
- Microsoft (2024) *Formazione su Excel: strutturare e gestire i dati in modo efficace*. Disponibile all'indirizzo: https://support.microsoft.com/en-us/excel (Consultato il: 31 marzo 2026)

Cofinanziato dall'Unione europea

Rapport

Strumenti digitali e intelligenza artificiale per le attività professionali quotidiane

Unità 3

Cofinanziato dall'Unione europea

Identificare le esigenze digitali: iniziare dall'attività

Un uso efficace degli strumenti inizia dall'analisi del compito, non dalla scelta dello strumento.

Fattori chiave da considerare:

- **Frequenza:** con quale frequenza viene eseguita questa attività?
- **Collaborazione:** coinvolge più persone?
- **Complessità:** richiede dati complessi o semplici testi?
- **Risultato:** come si presenta il prodotto finale?

L'utilizzo di uno "strumento potente" (come un CRM complesso) per un'attività che richiede uno "strumento manuale" (un semplice elenco di contatti) aumenta lo sforzo e riduce l'efficienza.

Strumento giusto + attività giusta = efficienza

Strumento sbagliato + Compito sbagliato = Costi aggiuntivi e tempo sprecato

Cofinanziato
dall'Unione europea

Categorie di lavoro digitale

Le mansioni lavorative si suddividono in quattro categorie funzionali:

1. **Produzione: creazione e sintesi di contenuti**
   - *La sala macchine dove le idee si trasformano in risorse tangibili.*
   - **Elaborazione testi:** redazione di documenti di lunga durata, relazioni e proposte (ad es. **Microsoft Word, Google Docs**).
   - **Visual Storytelling:** creazione di presentazioni di grande impatto per gli stakeholder (ad es. **PowerPoint, Canva**).
   - **Progettazione creativa:** contenuti multimediali di livello professionale, prototipazione e risorse di marca (ad es. **Adobe Creative Cloud, Figma**).
2. **Comunicazione: flusso di informazioni e connettività**
   - *Il "tessuto connettivo" che garantisce che la persona giusta abbia le informazioni giuste al momento giusto.*
   - **Sincrono (in tempo reale):** messaggistica istantanea per la risoluzione rapida dei problemi e le "chiacchierate in ufficio" (ad es. **Slack, Microsoft Teams**).
   - **Asincrono (differito):** corrispondenza formale e archiviazione dei documenti che non richiedono una risposta immediata (ad es. **Outlook, Gmail**).
   - **Presenza virtuale:** colmare il divario per i team remoti attraverso l'interazione faccia a faccia (ad es. **Zoom, Google Meet**).

Cofinanziato dall'Unione europea

Categorie di lavoro digitale

3. Organizzazione: Pianificazione e gestione delle risorse

- *Il quadro di riferimento che gestisce le due risorse più scarse: tempo e concentrazione.*
- **Gestione del tempo:** gestione della disponibilità individuale e del team (ad es. **Google Calendar, Calendly**).
- **Gestione di progetti e attività:** monitoraggio dei progressi, assegnazione delle responsabilità e rispetto delle scadenze (ad es. **Asana, Trello, Monday.com**).
- **Gestione della conoscenza:** centralizzazione della "conoscenza tribale" e della documentazione interna (ad es. **Notion, Obsidian, Confluence**).

4. Analisi e dati: approfondimenti e processo decisionale

- *Il livello analitico che converte i numeri grezzi in azioni strategiche.*
- **Modellazione su fogli di calcolo:** quantificazione della logica, definizione del budget e organizzazione dei dati strutturati (ad es. **Excel, Google Sheets**).
- **Business Intelligence (BI):** visualizzazione di set di dati complessi tramite dashboard interattive (ad es. **Tableau, Power BI**).

Ogni categoria richiede strumenti e logiche diverse.

Cofinanziato dall'Unione europea

Scegliere gli strumenti per la produttività in modo strategico

La scelta degli strumenti deve basarsi sulla logica aziendale, non sulla popolarità. Valutate ogni strumento in base a questi quattro pilastri fondamentali:

- **Efficienza in termini di costi vs. Prezzo di acquisto:** non limitarti a considerare il costo dell'abbonamento. Calcola il **ritorno sull'investimento (ROI).** Il tempo risparmiato dal team nelle attività manuali giustifica il costo mensile?
- **Interoperabilità e integrazione:** lo strumento "comunica" con il vostro ecosistema esistente? Uno strumento è produttivo solo se si sincronizza perfettamente con i vostri sistemi principali (ad esempio, Google Workspace, Microsoft 365 o CRM/ERP esistenti).
- **Curva di apprendimento e usabilità:** quanto è intuitiva l'interfaccia? Stima il "tempo totale necessario per acquisire competenza". Uno strumento complesso che richiede settimane di formazione può causare un calo temporaneo della produttività del team.
- **Sicurezza e conformità al GDPR:** i dati vengono gestiti secondo gli standard UE? Verifica che lo strumento offra archiviazione crittografata, autenticazione a più fattori (MFA) e politiche chiare sulla gestione dei dati.

Cofinanziato dall'Unione europea

Quiz5

Seleziona la risposta corretta.

Qual è l'approccio corretto da seguire nella scelta di uno strumento digitale?

- 3. Scegli lo strumento in base alle esigenze del compito
- 4. Utilizza sempre strumenti gratuiti
- 2. Scegli lo strumento più complesso
- 1. Scegli lo strumento più diffuso

La trappola degli strumenti "gratuiti" negli ambienti professionali

Gli strumenti gratuiti sembrano spesso convenienti, ma comportano rischi nascosti.

Problemi principali relativi agli strumenti gratuiti:

1. Mancanza di funzionalità di sicurezza essenziali

- Gli strumenti gratuiti spesso non dispongono delle **funzionalità di sicurezza** necessarie per proteggere i dati aziendali.
- Esempio: *una piattaforma di archiviazione cloud gratuita potrebbe non offrire **la crittografia dei dati**, lasciando le informazioni aziendali sensibili vulnerabili alle violazioni.*

2. Assenza di assistenza tecnica

- Gli strumenti gratuiti offrono in genere **un'assistenza tecnica limitata o assente**, il che significa che eventuali problemi potrebbero rimanere irrisolti per periodi più lunghi.
- Esempio: *se si verifica un problema con uno strumento gratuito, potresti dover affrontare tempi di inattività prolungati senza un team di assistenza dedicato, con conseguente **perdita di produttività**.*

Cofinanziato dall'Unione europea

La trappola degli strumenti "gratuiti" negli ambienti professionali

3. Creazione di "silos di dati" e mancanza di integrazione

- Molti strumenti gratuiti **non si integrano** con altri sistemi aziendali o software. Ciò crea **silos di dati**, rendendo difficile la condivisione delle informazioni tra le piattaforme e causando inefficienze e malintesi all'interno dei team. **I silos di dati** si riferiscono a situazioni in cui i dati sono archiviati in sistemi isolati che non comunicano né si integrano tra loro.
- Esempio: *l'utilizzo di uno strumento gratuito di gestione dei contatti che non si sincronizza con la tua posta elettronica o con il tuo sistema CRM comporta* ***una frammentazione dei dati****, causando errori e ritardi.*

4. Aumento dei costi nascosti in termini di tempo e rischi per la sicurezza

- Sebbene gli strumenti gratuiti possano sembrare convenienti inizialmente, i costi nascosti, come **le lacune di sicurezza** e la mancanza di assistenza, possono comportare **spese maggiori** nel lungo periodo. Il tempo dedicato alla risoluzione dei problemi, alla risoluzione dei problemi di integrazione e alla gestione dei rischi di sicurezza può costare più di uno strumento a pagamento.
- Esempio: *se il tuo strumento gratuito diventa inadeguato man mano che la tua attività cresce, potresti dover passare a una versione a pagamento o a un altro strumento, con conseguenti* ***costi nascosti di passaggio****.*

Cofinanziato dall'Unione europea

Collegare l'uso degli strumenti all'efficienza

Il principio: Efficienza = (Valore del risultato) / (Tempo + Sforzo)

L'obiettivo è garantire che gli strumenti utilizzati aiutino a ottenere risultati di alta qualità con il minimo dispendio di tempo e fatica. Gli strumenti dovrebbero migliorare la produzione senza aggiungere inutili complessità.

Gli errori operativi sono costosi e spesso derivano da processi manuali, come:

- Errori nell'inserimento manuale dei dati
- E-mail perse
- Conflitti di versione nel lavoro collaborativo

Esempio: *aggiornando automaticamente le informazioni di contatto nel tuo CRM, eviti di aggiornare manualmente i record, riducendo gli errori e risparmiando tempo. Questa integrazione garantisce che i dati siano coerenti tra i sistemi e aggiornati.*

Cofinanziato dall'Unione europea

Categoria	Strumenti professionali
Ragionamento AI e progettazione avanzata	ChatGPT, Gemini, Claude.ai, MS Word
Ricerca e sintesi delle informazioni	Perplexity, Google Scholar, Claude (PDF)
Competenze informatiche e analisi dei dati	MS Excel, Fogli Google, Power BI
Progettazione visiva e storytelling	MS PowerPoint, Canva, Adobe Express, Midjourney
Flussi di lavoro e gestione delle conoscenze	Trello, Asana, Notion, MS Planner
Collaborazione e gestione delle riunioni	MS Teams, Slack, Otter.ai, Fireflies.ai

Cofinanziato dall'Unione europea

Logica di ottimizzazione del posto di lavoro

L'ottimizzazione inizia con l'identificazione dei colli di bottiglia nel flusso di lavoro.

I colli di bottiglia sono gli ostacoli nel flusso di lavoro che rallentano il processo complessivo. Questi possono derivare da strumenti inefficienti, attività manuali o scarsa collaborazione.

- **La regola dell'80/20**
  - "Probabilmente il 20% dei tuoi strumenti produce l'80% del tuo valore."
  - Identificate e concentratevi sugli strumenti che migliorano davvero il vostro lavoro e valutate la possibilità di ridurre o eliminare quelli che aggiungono poco valore.
- **Automazione vs. lavoro manuale**
  - **Automazione**: ottimizzazione delle attività tramite strumenti digitali per eliminare il lavoro manuale ripetitivo.
  - **Lavoro manuale**: attività che richiedono l'intervento umano, spesso causando processi più lenti e un maggior rischio di errore.

Cofinanziato dall'Unione europea

Il ruolo dell'IA nei flussi di lavoro moderni come partner per la produttività

L'intelligenza artificiale non è più un optional: è ormai un elemento fondamentale per la produttività.

Per sfruttare efficacemente l'Intelligenza Artificiale, i professionisti devono cambiare il proprio modello mentale: l'IA generativa (ChatGPT, Claude e Gemini) non è un motore di ricerca, ma un **motore di ragionamento**.

- **Funzionalità principali (il "Cosa"):**
  - **Sintesi:** riassumere rapporti complessi o lunghe catene di email.
  - **Produzione:** stesura di bozze iniziali di e-mail, proposte o contenuti per i social media.
  - **Ideazione:** brainstorming di soluzioni creative e bozze di progetti.
  - **Supporto tecnico:** Generazione e debug di codice o riformattazione di strutture di dati.
- **Limiti critici (il "Cosa non"):**
  - **Realtà:** non garantisce la verità; prevede modelli (rischio di "allucinazioni").
  - **Contesto:** manca di "buon senso" e non è in grado di comprendere il contesto interno specifico delle PMI a meno che non venga esplicitamente fornito.
  - **Autorità:** non può assumersi la responsabilità professionale dei propri risultati.

Considerate l'IA generativa come uno stagista altamente capace ma leggermente inaffidabile. È in grado di svolgere l'80% del lavoro pesante in pochi secondi, ma richiede un supervisore umano per verificare, perfezionare e autorizzare il restante 20%.

Cofinanziato dall'Unione europea

L'IA per la sintesi

L'intelligenza artificiale riduce il carico cognitivo nelle attività di routine:

- Riassumere documenti lunghi
- Scrivere e-mail e relazioni
- Strutturazione dei contenuti

Esempio: *ti viene presentato un rapporto di settore di 50 pagine, ma hai solo 10 minuti prima di una riunione strategica cruciale.*

- **Azione dell'IA:** carica il documento o fornisci il testo a un LLM con un prompt specifico per il contesto: "Estrai da questo rapporto i 5 risultati chiave principali e i 3 rischi concreti per un'azienda manifatturiera di piccole dimensioni".
- **Vantaggi:** riduzione immediata del sovraccarico di informazioni.
- Usa l'IA per risparmiare tempo sulle attività di scarso valore: concentrati sulle decisioni.

Quanto tempo potresti risparmiare ogni settimana utilizzando l'IA per la sintesi?

Cofinanziato dall'Unione europea

L'IA per l'organizzazione del lavoro

Gli strumenti di IA possono facilitare l'organizzazione del lavoro strutturando le informazioni, le attività e i processi in formati più chiari e gestibili.

L'IA può essere utilizzata per strutturare:

- **Elenchi di attività** → suddividendo attività complesse in passaggi più piccoli e realizzabili
- **Flussi di lavoro** → organizzando i processi in sequenze logiche (ad es. procedure passo dopo passo)
- **Formati dei dati** → trasformando le informazioni non strutturate in tabelle, riepiloghi o categorie

- L'IA favorisce:
  - **Chiarezza** → migliora la comprensione dei compiti e delle responsabilità
  - **Definizione delle priorità** → aiuta a identificare ciò che è urgente o importante
  - **Pianificazione** → supporta una migliore gestione del tempo e il coordinamento del flusso di lavoro

Un dipendente utilizza l'IA per:

- convertire gli appunti delle riunioni in un elenco strutturato di attività
- assegnare priorità e scadenze

Ciò migliora l'efficienza e riduce il rischio di tralasciare delle azioni.

Cofinanziato dall'Unione europea

IA per la stesura e l'ideazione

L'intelligenza artificiale è particolarmente utile per:

- **Superare il blocco della "pagina bianca"** → iniziare compiti complessi o di grande importanza
- **Generare più varianti** → esplorare tono, struttura e approccio
- **Supportare lo sviluppo delle idee** → strutturare concetti e strategie di comunicazione

Esempio: *Prompt: "Genera 5 varianti di un'e-mail cortese ma decisa in cui si richiede uno sconto del 10% a un fornitore di lunga data."*

L'utente può confrontare diversi toni (formale, collaborativo, assertivo) e selezionare quello più appropriato.

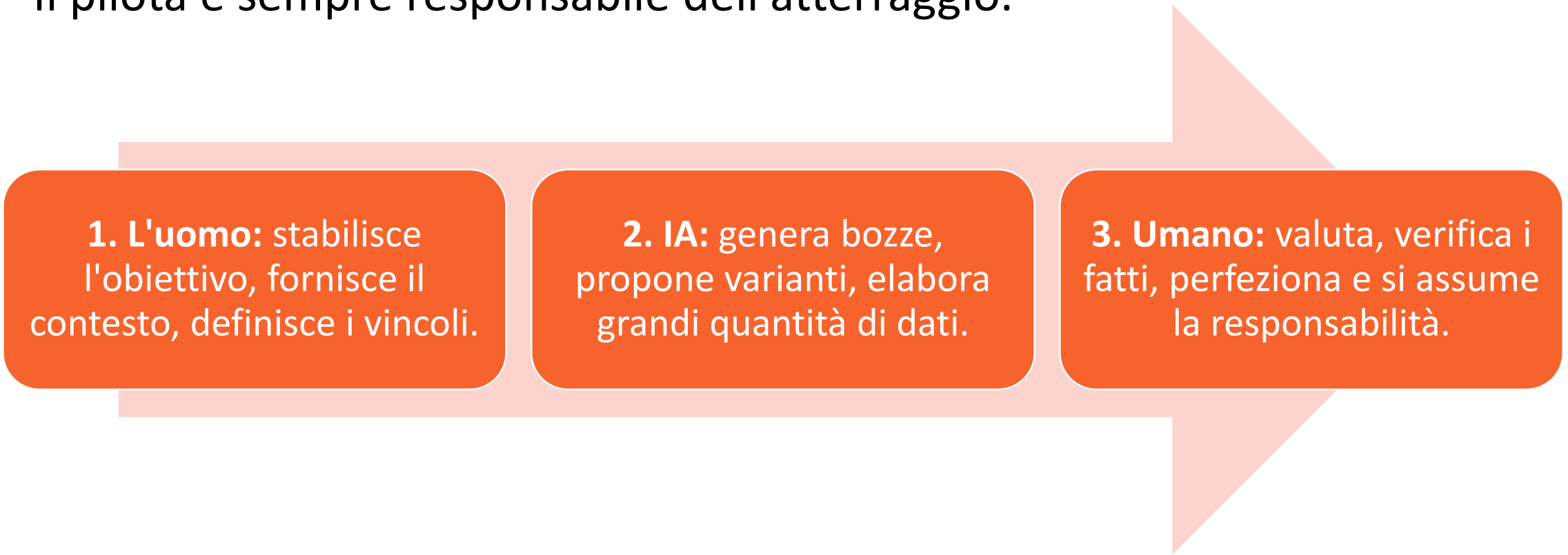
Vantaggi

- **Prototipazione rapida** → esplorare più opzioni in pochi secondi
- **Precisione linguistica** → accesso a formulazioni e vocabolario professionali
- **Sgravio cognitivo** → ridurre lo sforzo nella stesura e concentrarsi sulle decisioni

Cofinanziato dall'Unione europea

Il modello di collaborazione tra intelligenza artificiale e esseri umani (diagramma del flusso di lavoro)

Tu sei il "pilota"; l'IA è il "copilota".
Il pilota è sempre responsabile dell'atterraggio.



Cofinanziato dall'Unione europea

Prompt Engineering: l'arte dell'istruzione

Un prompt non è solo una domanda, è un **comando**. Nell'era dell'intelligenza artificiale, la qualità del risultato dipende interamente dalla precisione dell'input.

Elemento	L'approccio "vago" (debole)	L'approccio "architetto" (forte)
Il prompt	"Scrivi un business plan."	"Assumi il ruolo di **consulente senior per le startup**. Delinea una **strategia di ingresso nel mercato in tre fasi** per **un'azienda SaaS** che sta per lanciarsi **nell'UE**. Concentrati sulla **conformità al GDPR** e **sul marketing localizzato**."
Il risultato	Testo generico e "vago" che richiede un'intensa revisione.	Una strategia di alto livello e attuabile, su misura per le tue specifiche esigenze.
La differenza	Mancanza di contesto, ruolo e obiettivi specifici.	**Personaggio + Contesto + Obiettivo specifico + Vincoli.**

Cofinanziato dall'Unione europea

Quiz6

Seleziona la risposta corretta.

Qual è il rischio principale legato all'utilizzo di strumenti di IA pubblici con dati reali?

- 3. Maggiore automazione
- 4. Flusso di lavoro semplificato
- 2. Esposizione dei dati e perdita di controllo
- 1. Riduzione della velocità

Il modello CREATE per i prompt

- Personaggio: chi dovrebbe essere l'IA? (ad es., "Contabile senior")
- Richiesta: Qual è il compito? (ad es. "Analizza questo bilancio")
- Esempi: Fornire un modello o uno stile.
- Destinatari: A chi è rivolto? (ad es., "Il Consiglio di Amministrazione")
- Tipo: quale formato? (ad es., "Tabella", "E-mail")
- Extra: Vincoli (ad es. "Meno di 200 parole", "Nessun gergo tecnico")

L'utilizzo di un modello come CREATE garantisce di non dimenticare il contesto che rende utile l'IA.

Esercitati con questo framework finché non diventa una seconda natura.

Cofinanziato
dall'Unione europea

Esempio di un prompt ben strutturato utilizzando CREATE

- **Ruolo:** "Vice direttore"
- **Richiesta:** "Riassumi i risultati di vendita di questo mese."
- **Esempi:** "Fornisci il riepilogo in forma di elenco puntato con indicatori chiave quali il fatturato totale, i prodotti più venduti e le aree da migliorare."
- **Destinatari:** "Team vendite"
- **Tipo:** "Elenco puntato"
- **Extra:** "Limita il riepilogo a meno di 150 parole. Usa un linguaggio chiaro e semplice."

Spiegazione:

- **Personaggio**: Definiamo il ruolo dell'IA (Assistant Manager) per fornirle il contesto adeguato.
- **Richiesta**: Il compito è chiaro: riassumere i risultati di vendita del mese.
- **Esempi**: Specifichiamo come vogliamo che sia il risultato (punti elenco con metriche chiave).
- **Destinatari**: Definiamo il pubblico di destinazione (team di vendita) per garantire che l'IA adatti il tono e il contenuto.
- **Tipo**: Vogliamo il riepilogo sotto forma di elenco puntato, che sia facile da leggere e da assimilare.
- **Extra**: Il limite di parole e i vincoli di stile linguistico assicurano che l'output sia conciso e chiaro.

Cofinanziato dall'Unione europea

Valutazione dell'output dell'IA: la verifica in quattro punti

Per garantire risultati di livello professionale, i risultati generati dall'intelligenza artificiale non devono mai essere utilizzati così come sono.

Prima di finalizzare qualsiasi risultato, applicare una rigorosa checklist di verifica in quattro punti:

- **Accuratezza empirica e integrità dei dati:** cifre, date e nomi propri specifici sono corretti?
- **Allineamento stilistico e tono:** il testo suona "robotico" o eccessivamente generico?
- **Rilevanza contestuale e utilità:** l'output risolve effettivamente il problema specifico sul posto di lavoro o si tratta di una risposta generica?
- **Conformità etica e di sicurezza:** il contenuto rispetta le linee guida etiche dell'azienda e gli standard del GDPR?

Cofinanziato dall'Unione europea

Navigare nella curva di maturità dell'IA: Fluidità vs. Padronanza

- **Padronanza dell'IA (il "come"):** Sviluppo delle competenze linguistiche e tecniche necessarie per comunicare con il modello di IA (padronanza del Prompt Engineering e del framework CREATE).
- **Padronanza dell'IA (il "dovrebbe" e il "perché"):**
  - Sapere quando l'IA è lo strumento giusto e quando un approccio esclusivamente umano è superiore.
  - La capacità di verificare sistematicamente i risultati e individuare **le "allucinazioni"**, ovvero informazioni statisticamente plausibili ma di fatto errate.

L'IA genera spesso errori relativi a dati finanziari specifici, citazioni legali, nomi propri ed eventi verificatisi dopo il suo ultimo aggiornamento di addestramento.

"Saggezza nell'IA": la maggior parte degli utenti si ferma alla fluidità, accettando i risultati dell'IA per quello che sono. Un professionista a livello di padronanza riconosce che i modelli di linguaggio (LLM) sono motori di probabilità, non query di database. Essere "saggi nell'IA" significa mantenere un sano scetticismo e un solido protocollo di verifica.

Cofinanziato dall'Unione europea

Etica dell'IA: trasparenza e paternità

Principi fondamentali:

- **Trasparenza:** sii onesto se un risultato è stato generato al 100% dall'IA.
- **Pregiudizi:** l'IA può riprodurre i pregiudizi sociali (di genere, razziali). Un professionista deve correggerli.
- **Proprietà:** sei il proprietario del risultato solo se lo hai modificato e verificato in modo significativo.

La tua "firma" professionale significa che ti assumi la responsabilità del contenuto, indipendentemente da come è stato redatto.

➢ *A uno studente dovrebbe essere permesso di usare l'IA per un saggio? Un dipendente dovrebbe usarla per un rapporto che include dati reali? C'è una differenza?*

L'etica riguarda la costruzione della fiducia. Se nascondete il vostro uso dell'IA, danneggiate la vostra identità professionale.

Cofinanziato
dall'Unione europea

Autodiagnosi: identificare i propri divari digitali



Le piccole e medie imprese (PMI) devono affrontare sfide digitali specifiche:

- Supporto IT limitato (spesso sei tu stesso a occuparti dell'assistenza).
- Necessità di elevata versatilità (multitasking tra diversi set di strumenti).
- Impatto diretto sui ricavi (l'inefficienza costa immediatamente all'azienda)

Non si può migliorare ciò che non si può misurare. Prima di iniziare, dobbiamo misurare il "divario".

- Utilizzi solo gli strumenti che conosci o quelli migliori?
- Posso automatizzare un report ricorrente?
- Posso distinguere tra un'«allucinazione» dell'IA e un fatto?

La vera crescita professionale inizia con l'ammettere quali aree tecniche abbiamo evitato. La maggior parte dei professionisti utilizza solo il 10% delle funzionalità del proprio software.

Cofinanziato dall'Unione europea

Il Piano di miglioramento digitale (DIP) – (Parte 1: Strumenti e IA)

Fase 1: Identificazione

- Elenca 3 attività digitali che attualmente rappresentano dei colli di bottiglia, attività che richiedono troppo tempo o causano notevole frustrazione.

Fase 2: Ricerca degli strumenti

- Identifica uno strumento specifico (che si tratti di un agente AI o di un software standard) che abbia il potenziale per risolvere o automatizzare ciascuna di queste attività.

Fase 3: Obiettivi di apprendimento

- Fissa un obiettivo concreto di "micro-apprendimento" per questa settimana.
- Esempio: *guarda 3 tutorial sulle macro di Excel per automatizzare la reportistica settimanale.*

Un piano di miglioramento digitale è un documento in continua evoluzione che riflette la tua crescita professionale. Non dovrebbe essere statico, ma crescere insieme alle tue competenze.

Cofinanziato dall'Unione europea

Scenario: il flusso di lavoro "veloce ma sbagliato"

Maria lavora in una piccola PMI come assistente amministrativa. Deve preparare **un'e-mail di aggiornamento per i clienti e un breve rapporto** basato sui dati interni.

Per risparmiare tempo, lei:

- Utilizza **l'IA per redigere l'e-mail e il rapporto**
- Copia **i dati del cliente direttamente nello strumento di IA**
- Utilizza uno **strumento gratuito di condivisione file** per inviare il rapporto
- **Non controlla attentamente il risultato dell'IA**

L'attività viene completata in **15 minuti invece che in 1 ora**.

Cosa succede dopo:

- L'e-mail contiene **informazioni inesatte (allucinazione dell'IA)**
- I dati sensibili del cliente sono stati **esposti tramite lo strumento di IA**
- Il file viene condiviso con la **versione sbagliata**
- Il cliente nota delle incongruenze e mette in dubbio l'affidabilità

Cosa è andato storto in questo flusso di lavoro? Identifica almeno 3 errori critici.

Cofinanziato dall'Unione europea

Quiz

Click the **Quiz** button to edit this object

Seleziona la risposta corretta.

Qual è l'elemento fondamentale di un'e-mail professionale?

- 1. Introduzione troppo lunga
- 3. Scopo chiaro e messaggio strutturato
- 4. Uso di emoji
- 2. Tono informale

Analisi dello scenario: cosa si sarebbe dovuto fare?

1. **Errore nell'analisi delle attività**
   - Mancata valutazione della sensibilità dei dati e dell'accuratezza richiesta.
   - Ipotesi errata: “IA = scorciatoia sicura”
2. **Uso improprio dell'IA**
   - Inserimento **di dati sensibili in uno strumento di IA pubblico**
3. **Scelta inadeguata dello strumento**
   - Utilizzo di **uno strumento gratuito e non integrato**
   - Risultato: confusione tra le versioni e mancanza di controllo
4. **Mancanza di verifica dei risultati**
   - L'assenza di un controllo finale prima dell'invio comporta un rischio reputazionale

Flusso di lavoro professionale corretto:

✓ Rimuovere/anonimizzare i dati sensibili prima dell'uso dell'IA
✓ Utilizzare **solo strumenti approvati**
✓ Verificare i risultati dell'IA (accuratezza + tono)
✓ Confermare la versione finale prima della condivisione

Il lavoro professionale non è una questione di velocità. Si tratta di **risultati controllati e affidabili**.

Cofinanziato dall'Unione europea

Risorse esterne e approfondimenti

Per approfondire le tue competenze in materia di strumenti digitali e intelligenza artificiale, consulta le seguenti **risorse affidabili**:

- Principi dell'OCSE sull'IA
- 5 consigli e trucchi sull'IA per il lavoro – YouTube

Questo video mostra come gli strumenti di IA possano supportare le attività professionali quotidiane quali la stesura, la sintesi e l'organizzazione del lavoro. Evidenzia modi pratici per integrare l'IA nei flussi di lavoro quotidiani mantenendo il controllo e la qualità.

Cofinanziato dall'Unione europea

Rapport

Comunicazione digitale, collaborazione e identità professionale

Unità 4

Cofinanziato dall'Unione europea

Il costo di una comunicazione digitale inadeguata

Una comunicazione digitale inadeguata genera inefficienze operative e incide sia sul flusso di lavoro che sui rapporti professionali.

Impatto di una comunicazione inadeguata

- **Errori di interpretazione** → messaggi poco chiari portano a fraintendimenti
- **Ritardi** → le attività richiedono chiarimenti o devono essere rifatte
- **Errori** → esecuzione errata delle istruzioni
- **Perdita di fiducia** → minore fiducia nella qualità della comunicazione

Esempio:

Email poco chiara → compito frainteso → risultato errato → perdita di tempo

Un solo messaggio poco chiaro può avere ripercussioni su più persone.

Una comunicazione poco chiara genera costi operativi nascosti.

Cofinanziato dall'Unione europea

Principi della comunicazione digitale professionale

Principi fondamentali

- **Chiaro** → nessuna ambiguità
- **Conciso** → nessuna informazione superflua
- **Strutturato** → facile da seguire
- **Orientato allo scopo** → incentrato sul risultato

Pratica corretta

- definisci il tuo messaggio prima di scrivere
- concentrati su ciò di cui il lettore ha bisogno

Esempio:

Messaggio ben strutturato → decisione più rapida → meno errori

Se il lettore deve indovinare, la comunicazione ha fallito.

Cofinanziato dall'Unione europea

Comunicazione via e-mail – Standard professionali

Struttura di un'e-mail professionale

- **Oggetto chiaro**
- **Scopo nella prima frase**
- **Messaggio strutturato (paragrafi brevi)**
- **Azione o aspettativa chiara**

Rischio

- e-mail poco chiare → ritardi e confusione
- messaggi lunghi → attenzione ridotta

- Esempio: *Oggetto: Aggiornamento richiesto – Progetto X. Si prega di esaminare e confermare le modifiche entro venerdì.*

Strumenti consigliati

- Outlook / Gmail (per domini e-mail)
- Grammarly (strumento AI per tono e chiarezza)

Cofinanziato dall'Unione europea

Come scrivere un'e-mail professionale

Struttura di base

- **Saluto** → professionale e adeguato al contesto *(Gentile [Nome], Buongiorno [Nome])*
- **Lo scopo (“Perché”)** → indicare il motivo dell’e-mail nelle prime 1–2 frasi
- **La richiesta (“Chiedere”)** → definire chiaramente ciò che serve e utilizzare elenchi puntati per richieste multiple
- **Conclusione** → chiusura professionale + firma *(Nome, Ruolo, Organizzazione, Dettagli di contatto / LinkedIn)*

Esempio:

“Ciao Maria,
ti scrivo per chiederti il file aggiornato del progetto da esaminare.
Potresti inviarmi:
- *la versione finale*
- *l'ultimo file del budget”*

Cofinanziato dall'Unione europea

Linguaggio del corpo digitale: tono nella comunicazione scritta

Nella comunicazione digitale, il tono viene trasmesso attraverso la scelta delle parole, la punteggiatura e gli elementi visivi, non tramite la voce o l'espressione facciale.

Elementi chiave

- **Emoji**
  → accettabili nella comunicazione interna informale (Teams, Slack)
  → da evitare nelle e-mail formali o esterne
- **Punteggiatura** → un uso eccessivo (!!!, ???) appare poco professionale
- **Scelta delle parole** → i messaggi brevi o bruschi possono essere fraintesi

<u>Esempio:</u>

- “Va bene.” → può sembrare brusco o negativo
- “Per me va bene.” → più chiaro e neutrale

Cofinanziato dall'Unione europea

Netiquette negli ambienti professionali

La netiquette definisce il comportamento appropriato nella comunicazione digitale.

Regole fondamentali

- utilizzare un tono professionale
- evitare un linguaggio informale in contesti formali
- rispettare i tempi di risposta

Il tono viene spesso frainteso nella comunicazione digitale

Rischio

- errata interpretazione del tono
- comportamento percepito come poco professionale

Buona pratica

- verificare il tono prima di inviare
- adattare la comunicazione al contesto

Cofinanziato dall'Unione europea

Canali di comunicazione – Scegliere quello giusto

Strumenti di comunicazione diversi hanno scopi diversi.

Scelta del canale

- **E-mail** → comunicazione formale
- **Chat (Teams, Slack)** → coordinamento rapido
- **Riunioni** → discussione complessa

Lo strumento modella il messaggio.

Rischio

canale sbagliato → risultato sbagliato

Pratica corretta

scegliere il canale in base allo scopo e all'urgenza

Cofinanziato dall'Unione europea

Collaborazione negli spazi di lavoro digitali

Il lavoro moderno si basa su strumenti digitali condivisi e interconnessi.

Elementi chiave

- documenti condivisi
- collaborazione in tempo reale
- sistemi basati sul cloud

Vantaggi

- velocità
- trasparenza
- coordinamento

Strumenti consigliati

- Google Workspace
- Microsoft Teams / SharePoint
- Notion

Cofinanziato
dall'Unione europea

Rischi nella collaborazione digitale

Rischi comuni

- conflitti di versione
- proprietà poco chiara
- sovrascrittura dei contenuti
- esposizione dei dati
- Esempio: *più utenti che modificano → modifiche perse*

Pratica corretta

- assegnare la proprietà
- tracciare le modifiche
- utilizzare l'accesso controllato

La collaborazione senza controllo crea caos

Cofinanziato dall'Unione europea

Controllare chi può fare cosa

Livelli di accesso

- **Visualizzatore** → solo lettura
- **Commentatore** → feedback
- **Redattore** → accesso completo

Rischio

- accesso eccessivo → esposizione dei dati
- accesso insufficiente → inefficienza

Buona pratica

- Assegnare le autorizzazioni con attenzione

Cofinanziato
dall'Unione europea

Pratiche sicure nella condivisione dei dati

La condivisione sicura dei file garantisce che i dati aziendali vengano consultati, utilizzati e distribuiti in modo controllato e protetto.

Una condivisione errata dei file può comportare:

- accessi non autorizzati
- fughe di dati
- perdita di controllo sulle informazioni

Migliori pratiche

- utilizzare **piattaforme approvate dall'organizzazione** → garantisce sicurezza, registrazione e conformità
- evitare **canali non sicuri** → ad es. e-mail personali, app di messaggistica
- controllare **le impostazioni di condivisione** → limitare l'accesso, disabilitare il download dove necessario

Strumenti consigliati

- **OneDrive / SharePoint** → controllo a livello aziendale
- **Google Drive** → condivisione e collaborazione flessibili

Cofinanziato dall'Unione europea

Mantenere l'accuratezza nel lavoro condiviso

Il controllo di versione garantisce che tutti gli utenti lavorino sulla versione corretta e più aggiornata di un documento.

Senza controllo delle versioni

- confusione sulla versione più recente
- file duplicati
- lavoro sovrascritto o perso

Buona pratica

- utilizzare **documenti condivisi anziché allegati**
- abilitare **il controllo delle modifiche / la cronologia delle versioni**
- evitare di scaricare e ricaricare i file

Strumenti

- Google Docs (modifica in tempo reale)
- Microsoft 365 (cronologia delle versioni e collaborazione)

Cofinanziato dall'Unione europea

Quiz

Click the **Quiz** button to edit this object

Seleziona la risposta corretta.

Qual è il vantaggio principale del controllo di versione nei documenti condivisi?

- **2. Evitare confusione riguardo all'ultima versione**
- **3. Ridurre le dimensioni dei file**
- **1. Digitazione più veloce**
- **4. Migliorare il design**

Come vieni percepito negli ambienti digitali

La tua identità digitale è l'immagine professionale che trasmetti attraverso il tuo comportamento, la tua comunicazione e la tua presenza online.

Elementi chiave

- **Stile di comunicazione** → chiarezza, tono, professionalità
- **Presenza online** → profili, post, contenuti condivisi
- **Comportamento nell'uso degli strumenti** → abitudini di collaborazione, reattività

Esempio (contesto lavorativo)

- Comunicazione coerente e chiara → professionista affidabile
- Comportamento poco chiaro o informale → credibilità ridotta

Cofinanziato dall'Unione europea

Gestire la propria impronta digitale

Ogni azione online lascia una traccia che può influire sulla tua reputazione professionale.

Cosa include

- e-mail e allegati
- messaggi interni (Teams, Slack)
- attività sui social media

Esempio:

Commento poco professionale nella chat interna → condiviso all'esterno → impatto sulla reputazione

Cofinanziato dall'Unione europea

Limiti nella comunicazione digitale

Stabilire dei confini sani nella comunicazione digitale favorisce la produttività, il benessere e un processo decisionale più sicuro.

I rischi della cultura del "sempre connessi"

- esaurimento e affaticamento
- riduzione della concentrazione
- aumento degli errori

Esempio:

- *Notifiche costanti → distrazione → errori dovuti alla disattenzione*

Buone pratiche

- definire la disponibilità e i tempi di risposta
- Gestire le notifiche
- evitare comunicazioni non urgenti al di fuori dell'orario di lavoro

Cofinanziato dall'Unione europea

Responsabilità professionale nella comunicazione

Una comunicazione etica garantisce che le informazioni vengano condivise in modo responsabile, rispettoso e tale da tutelare le persone, le organizzazioni e i dati.

Principi fondamentali

- **Rispetto** → comunicare in modo professionale, evitando un linguaggio offensivo, informale o inappropriato
- **Trasparenza** → fornire informazioni chiare, oneste e complete ed evitare messaggi fuorvianti o incompleti
- **Riservatezza** → proteggere i dati sensibili, personali o aziendali e condividere le informazioni solo con persone autorizzate
- **Esempio** Condivisione di informazioni aziendali interne su un canale pubblico o inoltro di un'e-mail senza verificare le autorizzazioni

Rischio

- violazione della riservatezza
- danno alla reputazione
- perdita di fiducia all'interno dei team o da parte dei clienti
- potenziali implicazioni legali

Buona pratica

- comunicare in modo chiaro e onesto
- verificare i destinatari prima di condividere le informazioni
- rispettare la riservatezza dei dati e le norme sulla privacy

Cofinanziato dall'Unione europea

Responsabilità condivisa negli ambienti di lavoro digitali

La collaborazione richiede che ogni partecipante si assuma la responsabilità delle proprie azioni, dei propri contributi e della propria comunicazione.

Responsabilità principali

Ogni utente è responsabile di:

- **Accuratezza** → garantire che le informazioni condivise siano corrette e affidabili
- **Gestione dei dati** → utilizzare, archiviare e condividere i dati in modo responsabile
- **Chiarezza nella comunicazione** → fornire istruzioni e aggiornamenti chiari

Esempio: *un membro del team carica dati errati in un file condiviso senza verificarli. Ciò influisce sul lavoro dell'intero team.*

Rischio

- propagazione degli errori all'interno del team
- confusione e rielaborazione
- riduzione della fiducia nei risultati condivisi

Pratica corretta

- verificare le informazioni prima di condividerle
- comunicare chiaramente le modifiche
- assumersi la responsabilità dei propri contributi
- sostenere il coordinamento del team

Nel lavoro collaborativo, le azioni individuali influenzano i risultati collettivi

Cofinanziato dall'Unione europea

Capire perché la comunicazione si interrompe

I problemi di comunicazione derivano spesso dal comportamento umano, da una struttura inadeguata o dalla scelta di strumenti non appropriati.

Cause comuni

- **Supposizioni** → aspettarsi che gli altri capiscano senza bisogno di spiegazioni
- **Mancanza di chiarezza** → messaggi vaghi o incompleti
- **Struttura inadeguata** → informazioni disorganizzate
- **Strumenti sbagliati** → utilizzo di canali di comunicazione inadeguati

Esempio: *inviare un compito complesso tramite chat invece che tramite un'e-mail strutturata porta a confusione e alla perdita di dettagli.*

Rischio

- incomprensioni
- ritardi nell'esecuzione
- risultati errati
- riduzione dell'efficienza

Pratica corretta

- comunicare in modo chiaro ed esplicito
- strutturare le informazioni in modo logico
- scegliere il canale di comunicazione appropriato
- La maggior parte dei fallimenti nella comunicazione è prevenibile

Cofinanziato dall'Unione europea

Quiz9

Seleziona la risposta corretta.

Cosa contraddistingue i contenuti digitali professionali?

- 1. Testo lungo e dettagliato
- 3. Struttura chiara, finalità ben definite e precisione
- 4. Ampio ricorso a elementi visivi
- 2. Linguaggio complesso

Migliori pratiche per la collaborazione

Linee guida fondamentali

✓ **Definire i ruoli** → assegnare le responsabilità relative alle attività e ai contenuti

✓ **Utilizzare strumenti condivisi** → garantire che tutti i membri del team lavorino nello stesso ambiente

✓ **Comunicare le modifiche** → informare gli altri di aggiornamenti o modifiche

✓ **Tracciare le versioni** → mantenere il controllo sull'evoluzione del documento

Rischi di pratiche inadeguate

- confusione e duplicazione del lavoro
- informazioni incoerenti
- perdita di controllo sui contenuti

La collaborazione è efficace solo quando è strutturata e controllata

Cofinanziato dall'Unione europea

Galateo delle riunioni virtuali: comportamento professionale nelle riunioni online

Le riunioni virtuali richiedono lo stesso livello di professionalità delle interazioni faccia a faccia.

Pratiche fondamentali

- **Preparazione** → controllare microfono, videocamera e connessione prima della riunione
- **Ambiente**
  → utilizzare uno sfondo pulito o sfocato
  → assicurarsi che l'illuminazione e la posizione siano adeguate
- **Coinvolgimento**
  → evitare di interrompere
  → usa funzioni come "Alza la mano"
- **Regole per il silenziamento** → rimanere in modalità silenziosa quando non si parla per evitare distrazioni

Esempio:

Microfono sbloccato → rumore di fondo → riunione interrotta

Cofinanziato dall'Unione europea

Scenario – Incomprensione

Scenario

- Un team collabora su un documento condiviso:
- nessun proprietario chiaro
- più utenti che modificano contemporaneamente
- nessuna comunicazione sulle modifiche

Cosa succede

- modifiche sovrapposte
- versioni in conflitto
- perdita di informazioni

Risultato

- confusione tra i membri del team
- errori nei contenuti
- ritardi nel completamento del progetto

La mancanza di struttura porta a un'inefficienza operativa

Cofinanziato
dall'Unione europea

Analisi dello scenario – Cosa è andato storto?

Questioni fondamentali

- **Mancanza di titolarità** → nessuna responsabilità per i contenuti
- **Nessuna struttura** → mancanza di un flusso di lavoro organizzato
- **Comunicazione carente** → nessun aggiornamento o coordinamento

Impatto

- duplicazione degli sforzi
- risultati incoerenti
- riduzione della produttività

Pratica corretta

✓ assegnare ruoli e responsabilità chiari
✓ utilizzare strumenti di controllo delle versioni
✓ comunicare aggiornamenti e modifiche
✓ definire il flusso di lavoro prima della collaborazione

Una collaborazione efficace richiede struttura, non solo partecipazione

Cofinanziato
dall'Unione europea

Controllo finale prima della condivisione o della collaborazione

Una revisione finale garantisce che la comunicazione e la collaborazione siano chiare, precise e adeguate.

Lista di controllo

Prima di inviare o condividere:

✓ **È chiaro?** → Il messaggio è comprensibile?

✓ **È completo?** → Include tutte le informazioni necessarie?

✓ **È appropriato?** → Il tono e il formato sono adeguati?

✓ **L'accesso è corretto?** → Le persone giuste dispongono delle autorizzazioni giuste?

Esempio:

Prima di condividere un file:

- verificare la chiarezza
- verifica il contenuto
- confermare le autorizzazioni di accesso

Previene errori e malintesi.

Cofinanziato dall'Unione europea

Rapport

Creazione e modifica di contenuti digitali per i risultati finali sul posto di lavoro

Unità 5

Cofinanziato dall'Unione europea

Cosa definisce un contenuto digitale professionale?

I contenuti professionali si caratterizzano per:

- **Chiarezza** → facile da comprendere, senza ambiguità o inutili complessità
- **Struttura** → organizzato in modo logico, con un flusso e una sequenza chiari
- **Accuratezza** → corretto e verificato sulla base di informazioni affidabili
- **Finalità** → in linea con gli obiettivi del compito, il pubblico e lo scopo

Contenuti scadenti portano a:

- Incomprensioni
- Decisioni errate
- Perdita di credibilità
- Confusione nei flussi di lavoro

Se i tuoi contenuti non sono chiari, il tuo lavoro non è chiaro. Una comunicazione professionale riflette la competenza professionale e influenza direttamente la fiducia e le prestazioni.

Cofinanziato dall'Unione europea

Strutturare i contenuti per ottenere un impatto

I contenuti professionali dovrebbero seguire un percorso semplice e coerente:

- **Scopo** → Qual è l'obiettivo di questo documento o messaggio?
- **Messaggio chiave** → Qual è il punto più importante che il lettore deve comprendere?
- **Informazioni di supporto** → Quali dati, spiegazioni o prove sostengono il messaggio?
- **Conclusione / Azione** → Cosa dovrebbe succedere dopo? Cosa ci si aspetta dal lettore?

Esempio:

- ***Struttura inadeguata*** → *testo lungo e disorganizzato, privo di titoli o di un focus chiaro*
- ***Struttura efficace*** → *sezioni chiare, flusso logico, punti chiave evidenziati*

La seconda consente una comprensione più rapida e decisioni migliori.

Cofinanziato dall'Unione europea

Equilibrio tra testo e immagini

Usi efficaci dei contenuti:

- **Testo** → per spiegare idee, fornire dettagli e garantire l'accuratezza
- **Elementi visivi** → per evidenziare i punti chiave, semplificare la complessità e guidare l'attenzione

L'obiettivo è **la complementarità**, non la competizione.

<u>Esempio:</u>

- *Un rapporto con solo testo denso → difficile da leggere e interpretare*
- *Un rapporto con testo strutturato + immagini semplici (icone, diagram*
  → più facile da comprendere e su cui agire

Rischio di squilibrio

- **Troppo testo** → sovraccarico cognitivo, attenzione ridotta, informazioni perse
- **Troppi elementi visivi** → distrazione, perdita di concentrazione, messaggio poco chiaro

- utilizzare immagini per **chiarire le idee chiave**, non per decorare il contenuto
- mantieni il testo conciso e strutturato
- evidenziare visivamente le informazioni essenziali
- assicurarsi che gli elementi visivi supportino direttamente

Cofinanziato dall'Unione europea

Progettare documenti leggibili

Principi fondamentali di leggibilità

Per migliorare la leggibilità:

- **Paragrafi brevi** → rendono il contenuto più facile da scorrere e comprendere
- **Titoli chiari** → guidano il lettore attraverso la struttura
- **Elenchi puntati** → evidenziano le informazioni chiave e migliorano la chiarezza
- **Formattazione coerente** → crea un'esperienza di lettura professionale e prevedibile

Esempio:

- *Un documento con lunghi blocchi di testo e senza struttura → difficile da seguire*
- *Un documento con titoli, spaziatura e elenchi puntati → facile da leggere e da mettere in pratica*

Cofinanziato dall'Unione europea

Creazione di presentazioni professionali

Principi fondamentali

Presentazioni efficaci:

- **Concentrati sui messaggi chiave** → evidenzia ciò che è essenziale, non tutto ciò che si sa
- **Evita il sovraccarico di informazioni** → limita il contenuto a ciò che può essere facilmente compreso
- **Utilizzare una gerarchia visiva** → guidare l'attenzione attraverso titoli, spaziatura ed enfasi

Strumenti consigliati

- **Microsoft PowerPoint** → strumento standard per presentazioni professionali
- **Canva** → modelli intuitivi e supporto alla progettazione visiva
- **Google Slides** → creazione collaborativa di presentazioni basata sul cloud

Rischio di una progettazione inadeguata della presentazione

- confusione o disinteresse del pubblico
- messaggi chiave persi o fraintesi
- credibilità e impatto ridotti

Pratica corretta

- semplificare i contenuti riducendoli ai punti essenziali
- strutturare le diapositive in modo chiaro e coerente
- supportare il testo con immagini significative
- progettare le presentazioni in modo da facilitare la comprensione, non solo per mostrare informazioni

Cofinanziato dall'Unione europea

Ingegneria dei documenti

Una progettazione efficace dei documenti comprende:

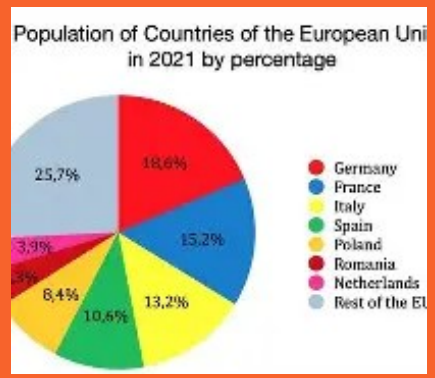
- **Modelli** → formati predefiniti che garantiscono l'uniformità tra i documenti
- **Strutture standard** → organizzazione chiara (ad es. introduzione, contenuto principale, conclusione)
- **Formattazione coerente** → caratteri, spaziatura, intestazioni e layout uniformi

- Esempio:
  - ***Documento casuale*** → *layout incoerente, struttura poco chiara, difficile da seguire*
  - ***Report aziendale basato su modello*** → *sezioni strutturate, design coerente, facile da consultare*

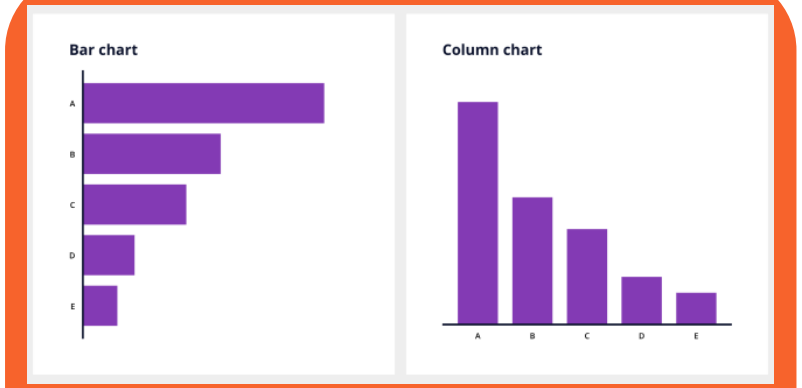
I documenti strutturati migliorano l'usabilità e la professionalità.

Cofinanziato dall'Unione europea

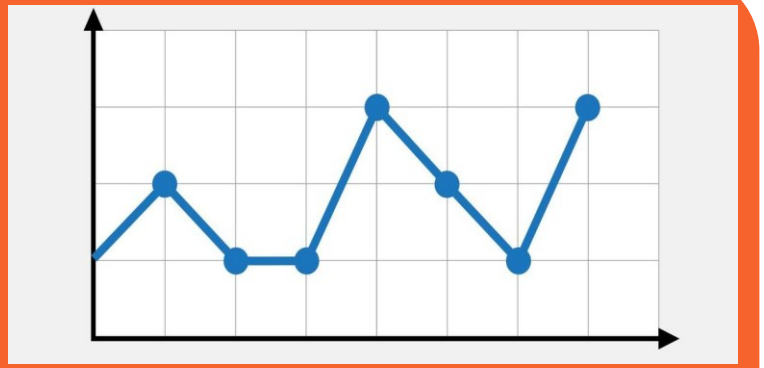
Visualizzazione dei dati: trasformare i numeri in informazioni utili



Grafici a torta: ideali per rappresentare le parti di un insieme (limitare a meno di 5 categorie).



Grafici a barre/a colonne: ideali per i confronti tra diversi gruppi o periodi di tempo.



Grafici a linee: ideali per mostrare le tendenze nel tempo.

Cofinanziato dall'Unione europea

Revisione per la qualità

Una revisione efficace comprende:

- **Grammatica** → uso corretto della lingua per garantire professionalità e credibilità
- **Chiarezza** → formulazione chiara e comprensibile, priva di ambiguità
- **Accuratezza** → fatti, dati e informazioni corretti
- **Tono** → stile appropriato al pubblico e al contesto

- Esempio:
  - *Una bozza di e-mail inviata senza revisione → messaggio poco chiaro e potenziale malinteso*
  - *Un messaggio revisionato e modificato → comunicazione chiara, precisa e professionale*

La revisione migliora sia la comprensione che l'impatto.

Scrivere è redigere — la revisione è professionalità.

Cofinanziato dall'Unione europea

Utilizzo responsabile dell'IA nello sviluppo di contenuti professionali

L'intelligenza artificiale può aiutare con:

- **Redazione** → creazione delle prime bozze dei contenuti
- **Riscrittura** → miglioramento della chiarezza, del tono o della struttura
- **Strutturazione** → organizzazione delle idee in formati logici

Principi di utilizzo etico

- **Non copiare ciecamente** → rivedere e adattare sempre i contenuti
- **Verificare l'accuratezza** → effettuare un controllo incrociato con fonti affidabili
- **Evita i pregiudizi** → valuta criticamente i contenuti generati dall'IA

Cofinanziato dall'Unione europea

Rispettare la proprietà nei contenuti digitali professionali

Il diritto d'autore garantisce una protezione giuridica automatica alle opere originali (testi, immagini, codice, musica) sin dal momento della loro creazione. Nell'Unione Europea, tutti i contenuti originali sono **protetti di diritto**.

- L'uso professionale dei contenuti richiede:
  - **Rispetto della proprietà** → riconoscere che il contenuto appartiene al suo creatore
  - **Evitare il plagio** → non copiare o presentare il lavoro altrui come proprio
  - **L'uso di materiale concesso in licenza** → assicurarsi di avere il permesso per l'uso professionale

Il mito delle immagini "pubbliche": solo perché un'immagine è su Google **non** significa che sia libera da diritti per l'uso professionale.

Esempio: *un dipendente utilizza un'immagine trovata online in una presentazione aziendale senza verificare i diritti di licenza.*

Ciò può comportare conseguenze legali e di reputazione.

Rischio

- azione legale o sanzioni pecuniarie
- violazione dei diritti di proprietà intellettuale
- danno alla reputazione dell'organizzazione
- perdita di credibilità professionale

Buona pratica

- utilizzare contenuti con licenza o esenti da diritti d'autore
- verificare sempre i diritti d'uso prima di utilizzare il materiale
- citare le fonti quando richiesto
- partire dal presupposto che i contenuti siano protetti, salvo diversa indicazione esplicita

Cofinanziato dall'Unione europea

Guida alle licenze Creative Commons (CC)

- **CC-BY (Attribuzione)** → il contenuto può essere utilizzato, ma è necessario citare l'autore
- **CC-NC (Non commerciale)** → non può essere utilizzato per attività commerciali, di marketing o a scopo di lucro
- **CC-ND (Non opere derivate)** → il contenuto può essere utilizzato, ma non può essere modificato o alterato
- **CC0 (Pubblico dominio)** → nessun diritto riservato; libero utilizzo senza restrizioni

Esempio: *una PMI utilizza un'immagine con **licenza CC-NC** in una campagna di marketing. Ciò viola la licenza poiché l'uso è commerciale.*

Cofinanziato dall'Unione europea

Rapport

Guida alle licenze Creative Commons (CC)

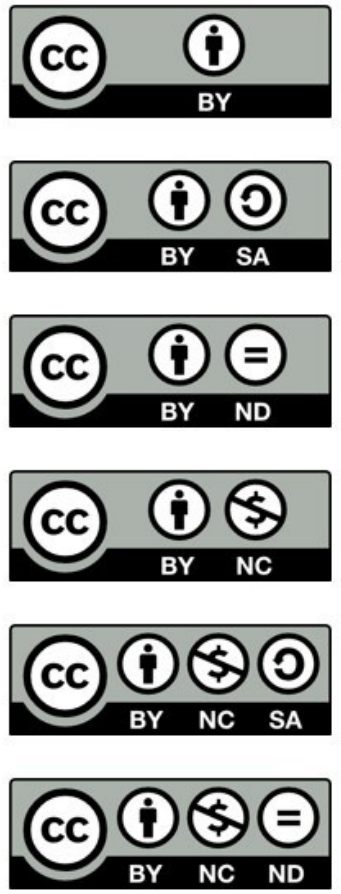
creative commons

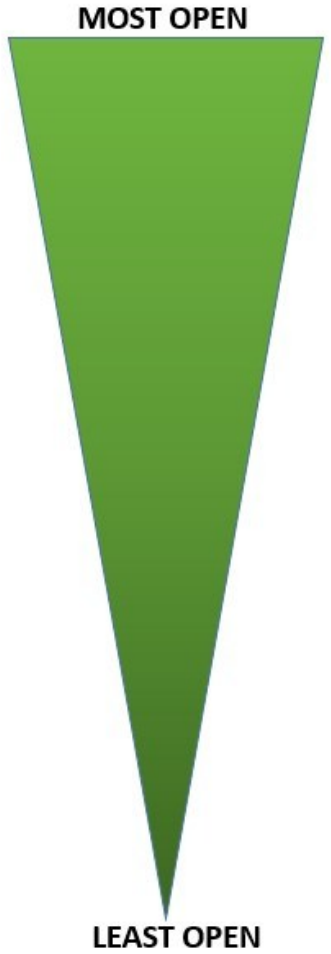
BY (attribute)

Share Alike

Non-Commercial

No Derivatives





Cofinanziato
dall'Unione europea

Approvvigionamento etico: librerie di risorse professionali

Opzioni di approvvigionamento di alta qualità:

- **Immagini:** Unsplash, Pexels, Pixabay (assicurati di controllare la licenza di ogni immagine).
- **Icone:** The Noun Project, Flaticon, Icons8 (spesso richiedono l'attribuzione).
- **Font:** Google Fonts (Open Source e sicuri per le aziende).
- **Librerie interne:** creare una cartella condivisa di risorse pre-approvate e con licenza per il proprio team per evitare incidenti.
- Esempio: un team prepara una presentazione utilizzando:
  - immagini con licenza da Unsplash
  - icone da Flaticon (con attribuzione)
  - modelli approvati dall'azienda

Ciò garantisce sia la conformità legale che la coerenza visiva professionale.

Cofinanziato dall'Unione europea

Come evitare il plagio

Il plagio consiste nel copiare testi o idee senza citarne la fonte.

- **Parafrasi professionale** → esprimere idee con parole proprie citando la fonte (ad es. *“Secondo l’ENISA (2024)…”*)
- **Citazione** → utilizzo delle parole esatte tra virgolette e con l’attribuzione (utilizzata in modo selettivo per dare enfasi)
- **Auto-plagio** → riutilizzare il proprio lavoro in contesti diversi senza indicarlo

Esempio: *un dipendente copia il contenuto di un rapporto online in un documento aziendale senza citare la fonte.*

Si tratta di plagio e può danneggiare la credibilità e la fiducia.

Cofinanziato dall'Unione europea

Verifica etica – Parafrasi vs Generazione AI

La creazione di contenuti professionali richiede trasparenza sulle modalità di produzione dei contenuti, soprattutto quando si utilizzano strumenti di intelligenza artificiale.

Lo standard professionale

- **Ricerca originale** → contenuti creati dall'uomo basati su analisi e fonti citate
- **Contenuti parafrasati** → interpretazione umana di conoscenze esistenti con corretta attribuzione
- **Contenuti generati dall'IA** → output assistito da macchina che deve essere rivisto, adattato e divulgato quando significativo **La regola della trasparenza**

Se un cliente si aspetta **un giudizio esperto**, fornire contenuti interamente generati dall'IA senza indicarlo:

- fornisce una rappresentazione errata del lavoro
- potrebbe violare la fiducia professionale o i termini contrattuali

Cofinanziato dall'Unione europea

Flusso di lavoro per la creazione dei contenuti

Flusso di lavoro passo dopo passo

1. **Definire lo scopo** → Qual è l'obiettivo del contenuto? Chi è il pubblico?
2. **Bozza del contenuto** → Creare la versione iniziale concentrandosi sulle idee chiave
3. **Struttura il contenuto** → Organizza le informazioni in modo logico (titoli, sezioni, flusso)
4. **Modifica e perfeziona** → migliora la chiarezza, il tono, la grammatica e la coerenza
5. **Convalida** → verifica l'accuratezza, controlla le fonti e assicurati che sia adatto all'uso

Cofinanziato dall'Unione europea

Quiz10

Seleziona la risposta corretta.

Qual è il primo passo da compiere quando si verifica un problema tecnico?

- **4. Segnalare immediatamente il problema**
- **2. Ignorare il problema**
- **1. Provare soluzioni a caso**
- **3. Seguire una procedura strutturata di risoluzione dei problemi**

Controllo qualità e autodiagnosi

Il controllo qualità è la fase finale della creazione dei contenuti e garantisce che il risultato finale soddisfi gli standard professionali, aziendali e di comunicazione.

Prima di condividere, verifica che il tuo contenuto sia:

✓ **Chiari** → facili da comprendere, senza ambiguità
✓ **Accurati** → corretti, verificati e aggiornati
✓ **Strutturati** → organizzati in modo logico con un flusso chiaro
✓ **Adeguati al pubblico** → tono e livello corrispondono al pubblico di destinazione

Autodiagnosi (Controllo professionale)

- Utilizzo **modelli e formati strutturati** o una formattazione casuale?
- Riesco a presentare le informazioni **in modo chiaro e logico**?
- Verifico **fonti, dati e autorizzazioni** prima dell'uso?
- I miei contenuti sono **accessibili e comprensibili** agli altri?
- Seguo una **routine di revisione finale prima della condivisione**?

Cofinanziato dall'Unione europea

Scenario: Contenuti scadenti vs Contenuti professionali

Nikos lavora in una piccola azienda e gli viene chiesto di preparare una **presentazione** per **un cliente** su un nuovo servizio.

Crea la presentazione:

- copiando il testo direttamente da diverse fonti
- Utilizzando **l'intelligenza artificiale per generare diapositive senza modificarle**
- Aggiungendo troppo testo su ogni diapositiva
- Utilizzando caratteri, colori e layout non uniformi
- Includendo immagini senza verificare il copyright

La presentazione viene consegnata in tempo.

Cosa succede dopo:

- Il cliente trova la presentazione **confusa e difficile da seguire**
- Alcune informazioni sembrano **inaccurate o irrilevanti**
- Il design visivo sembra **poco professionale**
- La credibilità dell'azienda ne risente

Cofinanziato dall'Unione europea

Analisi dello scenario: cosa si sarebbe dovuto fare?

1. Mancanza di struttura

- Nessun messaggio o flusso chiaro
- Troppe informazioni per ogni diapositiva

✓ Pratica corretta: un'idea per diapositiva + sequenza logica

2. Uso improprio dell'IA

- Contenuti generati dall'IA utilizzati senza verifica
- Nessun adattamento al contesto

✓ Pratica corretta: IA = bozza → Uomo = perfezionamento + verifica

3. Design visivo scadente

- Formattazione incoerente
- Diapositive sovraccariche

✓ Pratica corretta: utilizzare modelli + gerarchia visiva

4. Questioni etiche

- Contenuti non verificati
- Possibili violazioni del copyright

✓ Pratica corretta: → Utilizzare contenuti con licenza + verificare l'accuratezza

Cofinanziato
dall'Unione europea

Rapport

Risoluzione di problemi tecnici di base

Unità 6

Cofinanziato
dall'Unione europea

Il costo dei problemi tecnici

I problemi tecnici incidono direttamente sulla produttività, sul flusso di lavoro e sulle prestazioni organizzative.

Il loro impatto negativo:

- Perdita di produttività
- Mancato rispetto delle scadenze
- Frustrazione e stress
- Impatto sulla reputazione

Esempio:

File non sincronizzato → invio di una versione errata al cliente, con ripercussioni sia sull'accuratezza che sulla fiducia

Piccoli problemi tecnici possono avere gravi conseguenze per l'azienda

Cofinanziato dall'Unione europea

Tipi di problemi tecnici comuni

La maggior parte dei problemi tecnici sul posto di lavoro rientra in un numero limitato di categorie che possono essere individuate e risolte in modo sistematico.

Categorie comuni

- **Problemi di connettività** → problemi con Internet, Wi-Fi o accesso VPN
- **Problemi di accesso** → errori di login, restrizioni di autorizzazione, problemi con l'account
- **Errori software** → arresti anomali delle applicazioni, bug o problemi di prestazioni
- **Problemi relativi ai dati** → file mancanti, problemi di sincronizzazione, conflitti di versione

Esempio:

Un utente non riesce ad accedere a un documento condiviso → il problema potrebbe riguardare le autorizzazioni, la sincronizzazione o la connettività

Se riesci a classificare il problema, puoi risolverlo più rapidamente.

Cofinanziato dall'Unione europea

La mentalità della risoluzione dei problemi

Una risoluzione efficace dei problemi richiede un pensiero logico e un approccio strutturato alla risoluzione dei problemi.

Principi fondamentali

- pensiero sereno
- logica passo dopo passo
- evitare supposizioni

Approccio sbagliato

- clic casuali
- tentativi e errori

Approccio corretto

- diagnosi strutturata
- test controllati

Esempio: *cliccare su più impostazioni a caso → il problema peggiora*

Indovinare aumenta i problemi — la logica li risolve.

Cofinanziato dall'Unione europea

La logica di base della risoluzione dei problemi

Procedura dettagliata

1. Identificare chiaramente il problema
2. Verificare le cause di base (connessione, accesso, sistema)
3. Verificare le soluzioni passo dopo passo
4. Verificare la risoluzione

<u>Esempio:</u>

Impossibile aprire il file → verificare l'accesso → provare un'alternativa → confermare la risoluzione

Inizia sempre con soluzioni semplici prima di passare a quelle complesse

Cofinanziato dall'Unione europea

La regola RRU (Riavvia–Riconnetti–Aggiorna)

Molti problemi tecnici possono essere risolti con semplici operazioni di sistema.

Azioni principali

- **Riavvia** → risolve i problemi di memoria temporanea
- **Riconnettere** → ripristina l'accesso alla rete
- **Aggiorna** → risolve bug e problemi di compatibilità

Esempio:

Applicazione non risponde → riavvia → problema risolto

Soluzioni semplici risolvono la maggior parte dei problemi

Cofinanziato dall'Unione europea

Diagnosticare prima di agire - Chiedere prima di intervenire

Domande chiave

- Cosa è cambiato?
- Quando è iniziato il problema?
- È un problema solo mio o riguarda tutto il sistema?

Esempio:

Se è interessato un solo utente → probabilmente si tratta di un problema locale

Se sono coinvolti più utenti → problema di sistema

Cofinanziato dall'Unione europea

Hardware vs Software vs Rete

Distinzione

- **Hardware** (la parte fisica) → Si tratta dei componenti tangibili che puoi toccare: cavi, dispositivi, monitor e periferiche come mouse o tastiere
- **Software** (il digitale) → Si tratta delle applicazioni, dei sistemi operativi e dei programmi che girano sul vostro hardware
- **Rete** (l'invisibile) → È il ponte che collega i dispositivi al sistema interno dell'azienda o alla rete Internet più ampia

Esempio:

Il mouse non funziona → controllare prima il cavo o la batteria

Il segreto per una risoluzione dei problemi professionale è l'isolamento. Testando un livello alla volta, è possibile individuare la causa esatta del guasto.

Cofinanziato dall'Unione europea

Risoluzione dei problemi di connettività

Controlli da effettuare

- Connessione Internet → Inizia dalla fonte. L'intero edificio è offline o è solo il tuo dispositivo? Verifica se altri siti web si caricano o se i tuoi colleghi stanno riscontrando lo stesso problema
- Stato del Wi-Fi → Assicurati che il Wi-Fi sia effettivamente attivato. A volte, basta semplicemente spegnere e riaccendere il Wi-Fi per costringere il dispositivo a cercare nuovamente il segnale più forte
- Stato del router → Se lavori da casa o in un piccolo ufficio, controlla l'hardware. Le spie sono verdi? Una spia rossa o lampeggiante di solito indica un problema del provider di servizi o la necessità di un riavvio fisico
- Impostazioni VPN → Per molti professionisti, la VPN è l'ultimo baluardo. Se Internet funziona ma gli strumenti aziendali no, la tua VPN potrebbe aver "superato il timeout" o non essere riuscita ad autenticarsi. Disconnettiti e accedi nuovamente alla VPN per aggiornare il tunnel sicuro

<u>Esempio:</u>

Provi ad aprire un report basato su cloud e riceve un errore "Nessuna connessione Internet". Invece di chiamare immediatamente l'IT, controlla il router, vede che lampeggia e ricollega la rete spegnendo e riaccendendo il dispositivo. Entro due minuti, è di nuovo online senza alcun aiuto esterno.

Cofinanziato dall'Unione europea

Sfide della connettività remota

Problemi

- **Wi-Fi domestico debole:** la distanza dal router, gli ostacoli fisici o l'elevato traffico di rete proveniente da altri dispositivi domestici possono causare "lag" durante videochiamate importanti o rallentare il caricamento dei file
- **Instabilità della VPN:** le VPN aziendali sono essenziali per la sicurezza, ma possono essere instabili. Le frequenti disconnessioni spesso indicano un conflitto tra il tuo ISP locale e il tunnel crittografato
- **Rischi delle reti pubbliche:** utilizzare il Wi-Fi in un bar o in aeroporto può essere comodo, ma queste reti sono spesso non crittografate, rendendole una "miniera d'oro" per il furto di dati e gli attacchi informatici

Buone pratiche

- **Utilizza reti sicure:** dai sempre la priorità alla tua rete domestica protetta da password. Assicurati che il tuo router abbia l'ultimo firmware e sia posizionato in un punto centrale.
- **Evita il Wi-Fi pubblico per attività sensibili:** non accedere mai a database aziendali, documenti finanziari o dati privati dei clienti tramite una connessione pubblica. Se devi lavorare in pubblico, usa sempre la tua VPN.
- **Utilizza un hotspot mobile come backup:** se la tua connessione Internet domestica non funziona, un hotspot mobile è il tuo "Piano B" professionale. È molto più sicuro di una rete pubblica e ti garantisce di rimanere online per le scadenze importanti.

Connettività = affidabilità professionale

Cofinanziato dall'Unione europea

Risoluzione dei problemi di accesso - Autorizzazioni e autenticazione

I problemi di accesso si verificano quando gli utenti non riescono a raggiungere sistemi, file o piattaforme a causa di problemi di autenticazione o di autorizzazione.

I problemi di accesso sono solitamente legati a:

- autorizzazioni errate → questa è la causa più frequente. Potresti avere il link a un file, ma al tuo profilo utente non sono stati concessi i diritti specifici di "visualizzazione" o "modifica" richiesti
- accesso scaduto → per motivi di sicurezza, la maggior parte dei sistemi professionali richiede di effettuare periodicamente una nuova autenticazione. Se hai lasciato una scheda aperta per tre giorni, la tua "sessione" è probabilmente scaduta, anche se sembra che tu sia ancora connesso.
- account errato → molti di noi gestiscono più identità digitali: un account Gmail personale, un account aziendale e forse un login specifico per un cliente. Se provi ad aprire un documento aziendale mentre sei connesso al tuo profilo browser personale, il sistema ti bloccherà.

<u>Esempio:</u>

L'utente non può aprire il file condiviso → il file esiste ma i diritti di accesso non sono concessi

La maggior parte dei problemi di accesso è legata alle autorizzazioni, non a errori tecnici

Cofinanziato dall'Unione europea

Gestione dei problemi relativi al cloud e alla sincronizzazione

I sistemi cloud si basano sulla sincronizzazione continua tra i dispositivi locali e l'archiviazione online.

Problemi comuni

- file non aggiornati
- conflitti di versione (versioni duplicate)
- dati mancanti

Pratica corretta

- verificare lo stato della sincronizzazione
- utilizzare versioni condivise
- evitare i file duplicati

"Salvato" non significa sempre "sincronizzato"

Cofinanziato dall'Unione europea

Comprensione approfondita della sincronizzazione cloud - Riconoscere gli indicatori dello stato di sincronizzazione

I sistemi cloud utilizzano indicatori visivi per mostrare lo stato dei file.

Indicatori

- icona blu → sincronizzazione in corso
- segno di spunta verde → sincronizzazione completata
- errore rosso → problema di sincronizzazione

Esempio: chiusura del portatile prima del completamento della sincronizzazione → file non aggiornato

Rischio

- perdita di dati
- versioni non aggiornate
- file mancanti

Corretta pratica

- verificare il completamento della sincronizzazione prima di chiudere il lavoro
- monitorare gli errori di sincronizzazione

Cofinanziato dall'Unione europea

Comprendere gli errori del software

Gli errori software si verificano a causa dei limiti del sistema o di ambienti non aggiornati.

Cause comuni

- software obsoleto
- sovraccarico del sistema
- problemi di compatibilità

Esempio: *l'applicazione si blocca → versione non compatibile con il sistema*

I problemi software sono spesso prevedibili

Rischio

- interruzione del lavoro
- perdita di dati
- riduzione della produttività

Buona pratica

- aggiornare regolarmente il software
- chiudere le applicazioni non necessarie
- riavviare i sistemi quando necessario

I problemi software sono spesso prevedibili e prevenibili

Cofinanziato dall'Unione europea

Risoluzione dei problemi delle periferiche - Problemi relativi a dispositivi e hardware

Molti problemi tecnici hanno origine dai dispositivi fisici.

Controllare

- cavi collegati correttamente
- dispositivo acceso
- driver installati/aggiornati

Esempio:

Si invia un documento alla stampante, ma non succede nulla. Invece di approfondire le impostazioni del documento, si riavvia il dispositivo e si ricollegano i cavi. Spesso, questo "reset fisico" risolve un blocco di comunicazione e la stampante riprende immediatamente a funzionare. Stampante non funzionante → riavviare il dispositivo → ricollegare

Molti problemi sono di natura fisica, non digitale.

Cofinanziato dall'Unione europea

Manutenzione preventiva: evitare i problemi prima che si verifichino

Azioni

- **aggiornare regolarmente i sistemi** → gli aggiornamenti software non riguardano solo nuove funzionalità; contengono patch di sicurezza fondamentali e correzioni per migliorare le prestazioni. Ritardare un aggiornamento equivale essenzialmente a lasciare una porta aperta nel proprio ufficio digitale.
- **organizza i file** → Un desktop disordinato e una struttura di cartelle caotica non solo rallentano te, ma rallentano anche il tuo computer. L'indicizzazione di migliaia di file sparsi mette a dura prova le risorse del tuo sistema operativo.
- **pulire lo spazio di archiviazione** → Un desktop disordinato e una struttura di cartelle caotica non rallentano solo te, ma anche il tuo computer. L'indicizzazione di migliaia di file sparsi mette a dura prova le risorse del sistema operativo.

Esempio: *prendiamo in considerazione due dipendenti. Uno ha un desktop ricoperto da 500 icone sparse a caso; l'altro utilizza un sistema di cartelle strutturato. I file organizzati consentono un accesso più rapido, il che si traduce in un minor numero di errori e in una minore fatica mentale. File organizzati → accesso più rapido → meno errori*

Prevenire è più efficiente che riparare

Cofinanziato dall'Unione europea

Igiene digitale

Per "igiene digitale" si intende la manutenzione dei sistemi al fine di garantirne prestazioni ottimali.

Pratiche

- **Rimuovere i file non necessari:** controllate regolarmente le cartelle "Download" e "Desktop". Eliminate i file temporanei, i vecchi programmi di installazione e i documenti che non vi servono più. Se non aprite un file da un anno, è un candidato per l'archiviazione o il cestino.
- **Gestisci lo spazio di archiviazione:** il tuo sistema operativo ha bisogno di spazio libero per "respirare" e scambiare dati temporanei. Se il tuo disco è quasi pieno, il tuo computer farà fatica a svolgere anche le attività di base. Cerca di mantenere libero almeno il 15% dello spazio di archiviazione.
- **Disattiva le app di avvio inutilizzate:** molti programmi si impostano per aprirsi automaticamente non appena accendi il computer. Questo consuma preziosa memoria (RAM) prima ancora che tu abbia iniziato a lavorare.

Esempio:

Troppe app di avvio → sistema lento

I sistemi puliti funzionano meglio

Cofinanziato dall'Unione europea

Backup e protezione dei dati

I backup garantiscono il recupero dei dati in caso di guasto.

Pratiche

- **Salvate regolarmente:** non affidatevi esclusivamente al "salvataggio automatico". Prendete l'abitudine di salvare manualmente il vostro lavoro durante le pause naturali nel vostro processo di pensiero. Questo garantisce che anche un'improvvisa interruzione di corrente vi costi solo pochi minuti di lavoro, non ore.
- **Utilizza il backup su cloud:** piattaforme come OneDrive, Google Drive o Dropbox forniscono una rete di sicurezza continua. Lavorando all'interno di queste cartelle, i tuoi file vengono automaticamente replicati su server remoti sicuri, proteggendoli da guasti hardware locali.
- **Conserva copie locali**: per i progetti critici, segui la "regola del 3-2-1": conserva tre copie dei tuoi dati, su due diversi tipi di supporto, con una copia fuori sede (il cloud). Avere una copia locale su un'unità esterna ti garantisce di poter continuare a lavorare anche se perdi l'accesso a Internet.

Esempio

Immagina che il tuo computer subisca un grave crash di sistema un'ora prima di una scadenza importante. Poiché hai mantenuto un backup costante, ti basta accedere a un altro dispositivo e ripristinare il tuo lavoro. Quello che avrebbe potuto essere un disastro diventa un ritardo minore di 10 minuti.

Dobbiamo trattare la protezione dei dati con la serietà che merita: la perdita di dati equivale a una perdita di affari. Che si tratti di ore fatturabili perse, scadenze non rispettate o fiducia del cliente compromessa, il costo della perdita di dati è sempre superiore allo sforzo necessario per eseguirne il backup.

Nella creazione di contenuti moderna, il backup non è facoltativo: è essenziale.

Cofinanziato
dall'Unione europea

Strategia di backup (regola 3-2-1)

Per garantire la totale sicurezza dei dati, la vostra strategia deve prevedere:

- **3 copie dei tuoi dati:** questo include la versione principale su cui stai lavorando attualmente e almeno due backup aggiuntivi.
- **2 tipi diversi di archiviazione:** non conservare tutti i backup sullo stesso dispositivo. Utilizza due supporti diversi, ad esempio il disco rigido interno del tuo computer e un'unità esterna. In questo modo sarai protetto in caso di guasto di un componente hardware.
- **1 copia fuori sede:** almeno un backup deve trovarsi in una sede fisica diversa. Al giorno d'oggi, solitamente si tratta del cloud. In questo modo, anche in caso di incendio, furto o allagamento nel tuo ufficio, i tuoi dati rimarranno al sicuro e accessibili.

Esempio

Conserva il file di lavoro sul PC locale, una copia secondaria su un SSD esterno e una terza copia sincronizzata sul cloud (come OneDrive o Dropbox).

- I guasti sono inevitabili: la preparazione previene il disastro

Cofinanziato dall'Unione europea

Il fattore umano nei problemi tecnici

Il comportamento umano è spesso la causa principale dei problemi tecnici.

Cause

La maggior parte degli "errori dell'utente" può essere ricondotta a tre stati psicologici:

- **Fretta:** cercare di rispettare una scadenza spesso porta a saltare passaggi essenziali, come controllare lo stato di sincronizzazione o verificare la destinazione di un file.
- **Distrazione:** il multitasking o il lavoro in un ambiente disordinato aumenta la probabilità di cliccare sul pulsante sbagliato o di cancellare la cartella sbagliata.
- **Incomprensione:** l'utilizzo di uno strumento senza leggere le istruzioni di base o comprenderne la logica porta a errori prevedibili.

Esempio

- Clic su file sbagliato → dati sovrascritti
- Spesso sono gli esseri umani a creare problemi tecnici
- La tecnologia fallisce, ma spesso è il comportamento umano a provocarlo

Cofinanziato dall'Unione europea

Comunicazione dei problemi tecnici

Una comunicazione chiara riduce i tempi di risoluzione dei problemi.

Cosa includere

- **Descrizione del problema:** sii specifico. Invece di dire "Non riesco ad accedere", scrivi "Ricevo l'errore '404' quando provo ad accedere al Portale Clienti". Descrivi esattamente ciò che vedi sullo schermo.
- **Azioni già intraprese:** elenca ciò che hai già provato. Indica se hai applicato la regola RRU (Riavvia, Riconnetti, Aggiorna). Ciò evita che il team di assistenza suggerisca passaggi che hai già completato, facendo risparmiare tempo a tutti.
- **Screenshot o prove:** un'immagine vale più di mille parole nella risoluzione dei problemi. Cattura il messaggio di errore o il problema visivo. Questo fornisce la "prova" di cui il team tecnico ha bisogno per diagnosticare la causa principale.

Esempio

- "Impossibile accedere al file – ho controllato la connessione e le autorizzazioni"

Segnalazioni chiare = soluzioni più rapide

Cofinanziato dall'Unione europea

Protocolli di escalation

L'escalation fa parte del processo professionale di risoluzione dei problemi.

Quando segnalare il problema

- non è possibile risolvere il problema
- il problema riguarda più utenti
- coinvolge dati sensibili

Regola

Regola dei 30 minuti: se non riesci a risolvere un problema tecnico entro 30 minuti di lavoro concentrato, smetti. Continuare oltre questo punto porta a rendimenti decrescenti e a ore fatturabili sprecate.

Sapere quando smettere è una competenza professionale

Cofinanziato dall'Unione europea

Comunicare con l’IT – Scrivere un rapporto sull’incidente chiaro

Includi

- sistema/ambiente
- azione tentata
- messaggio di errore
- passaggi effettuati

Esempio

“Windows 11 – impossibile caricare il file – errore 404 – ho provato a riavviare”

Segnalazioni chiare = soluzioni più rapide. Trasforma un blocco tecnico frustrante in un'attività amministrativa semplificata.

Cofinanziato dall'Unione europea

Scenario – Guasto del sistema

Scenario

- L'utente non può accedere ai file condivisi prima della scadenza

La reazione a catena

- **Panico:** l'utente va in "panico digitale", perdendo la capacità di pensare con lucidità o di diagnosticare il problema.
- **Azioni casuali:** senza un piano, inizia a modificare impostazioni a caso, a cliccare nei menu e a scollegare cavi.
- **Cancellazione dei file:** nel tentativo maldestro di "liberare spazio" o "resettare" la cartella, inizia a cancellare i file, sperando che ciò risolva il problema di connessione.

Le conseguenze di queste azioni vanno ben oltre un semplice problema di accesso:

- **Perdita di dati:** le cancellazioni casuali comportano la perdita definitiva del lavoro.
- **Ritardi significativi:** il tempo speso in azioni casuali è tempo che avrebbe potuto essere utilizzato per una corretta risoluzione dei problemi o per l'escalation.
- **Interruzione del lavoro del team:** i colleghi devono ora interrompere il proprio lavoro per aiutare a recuperare ciò che è andato perso, compromettendo le prestazioni dell'intero reparto.

Le decisioni sbagliate prese sotto pressione aumentano il danno

Cofinanziato
dall'Unione europea

Analisi dello scenario

Passaggi

✓ controllare la connessione
✓ verificare l'accesso
✓ controllare la sincronizzazione
✓ evitare azioni dannose

Pratica corretta

- agire in modo logico
- evitare azioni irreversibili
- Una logica serena previene l'escalation

Cofinanziato
dall'Unione europea

Lista di controllo per la risoluzione dei problemi

Controllo finale in 5 passaggi

✓ riavviare

✓ controllare la connessione
✓ verificare l'accesso
✓ controllare gli aggiornamenti
✓ provare semplici soluzioni

La resilienza digitale è una competenza professionale fondamentale

Cofinanziato
dall'Unione europea

Punti chiave

1. **Sicurezza digitale**
    1. Protegge i dati, i sistemi e la fiducia.
    2. Rischi principali: phishing, malware, ingegneria sociale, autenticazione debole.
2. **GDPR e trattamento dei dati**
    1. Il rispetto del GDPR è fondamentale per la protezione dei dati personali e la conformità legale.
    2. Sono necessarie pratiche di gestione e archiviazione sicure.
3. **Autenticazione e protezione dei dispositivi**
    1. L'autenticazione a più fattori (MFA) e la sicurezza dei dispositivi sono fondamentali per impedire accessi non autorizzati.
    2. Aggiornamenti regolari e crittografia sono essenziali per la protezione dei dispositivi.
4. **Gestione dei file**
    1. Organizza i file con strutture chiare per prevenire la perdita o l'accesso non autorizzato.
    2. Utilizza misure di condivisione controllata dei file e di protezione dei dati.
5. **Responsabilità nell'uso dell'IA**
    1. Utilizza gli strumenti di IA in modo responsabile, garantendo la conformità al GDPR e la protezione dei dati.
    2. Convalidare i risultati dell'IA per evitare errori e risultati fuorvianti.
6. **Lavoro da remoto e benessere**
    1. Utilizza reti e dispositivi sicuri per il lavoro da remoto.
    2. Dare priorità al benessere digitale per prevenire sovraccarichi e stress.
7. **Risoluzione dei problemi tecnici**
    1. Seguire la logica "Riavvia – Riconnetti – Aggiorna" per la risoluzione dei problemi.
    2. Una comunicazione chiara con i team IT è fondamentale per una rapida risoluzione dei problemi.

Cofinanziato dall'Unione europea



Cofinanziato dall'Unione europea

Finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.