GDPR & CyberSecurity

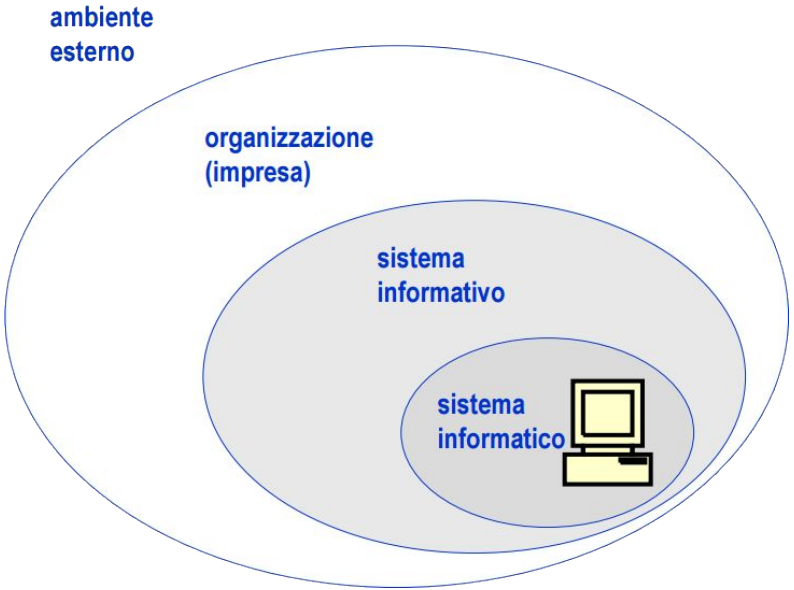
Un’introduzione ‘operativa’

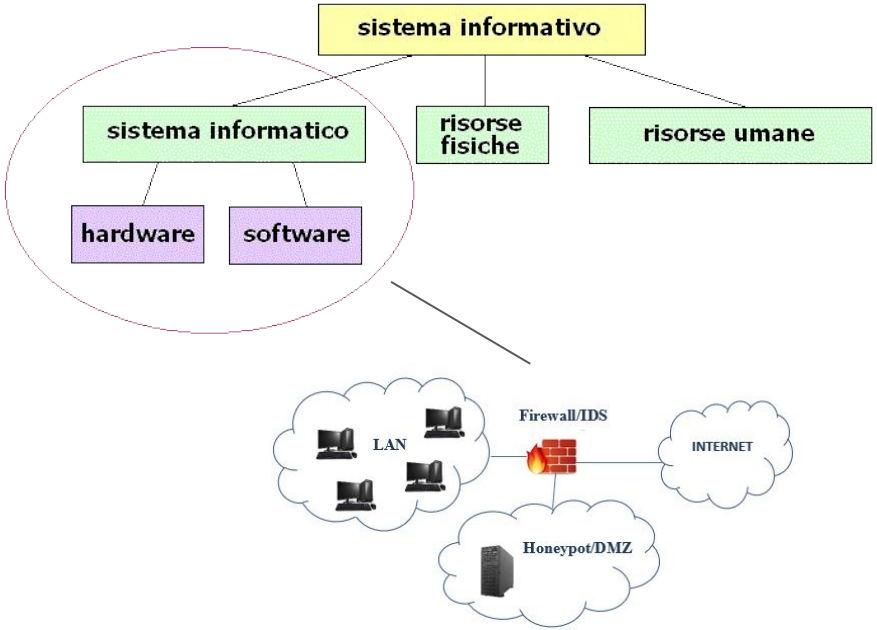
Nunzio Castaldi

Un computer sicuro è un computer spento.

(E. H. Spafford)

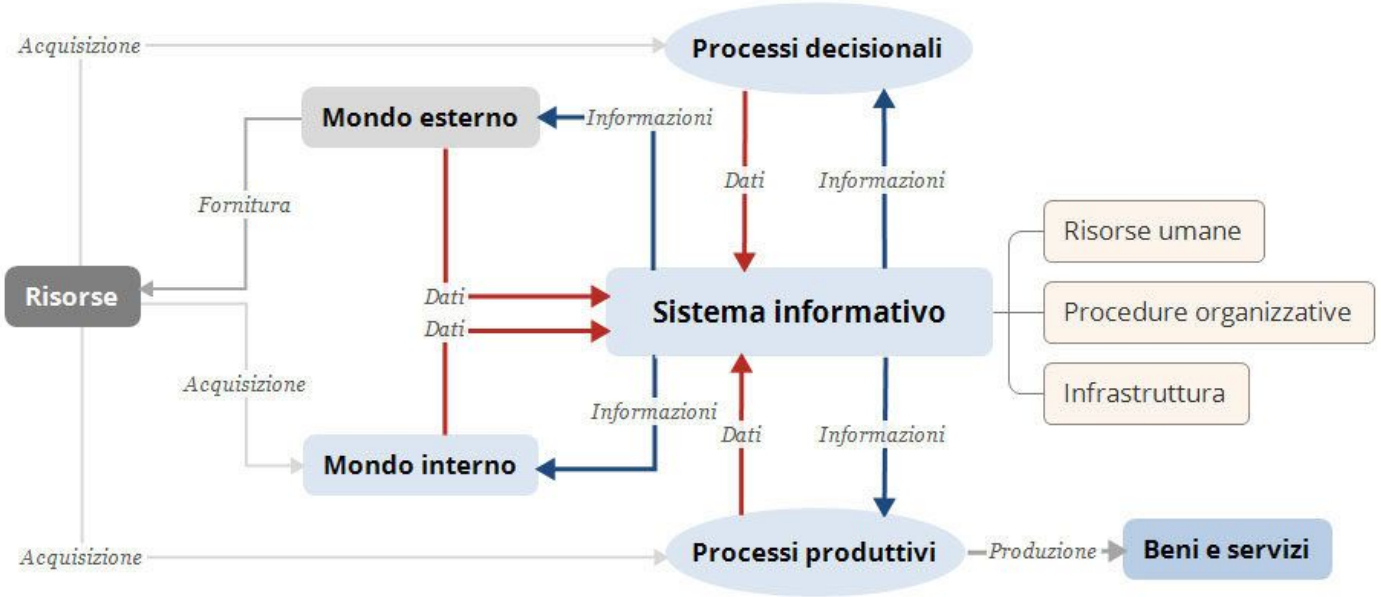
Sistema informativo e sistema informatico





sistema = connessione di elementi in un tutto organico e funzionalmente unitario
sistema informatico = la parte del sistema informativo che tratta dati e informazioni in modo automatizzato

Sistema, organizzazione, sistema informativo



sistema = insieme di elementi coordinati tra loro in una unità funzionale

organizzazione = insieme di uomini, strumenti, attività coordinato per il raggiungimento di obiettivi comuni

sistema informativo = insieme di risorse e di attività che permettono ad un'organizzazione di gestire le informazioni necessarie al posto giusto al momento giusto

Chiariamo subito…

1. la cybersecurity non è un prodotto, ma un **processo**, che si esplica soprattutto nella fase di **difesa proattiva**: occorre farsi trovare pronti anche per lo scenario peggiore

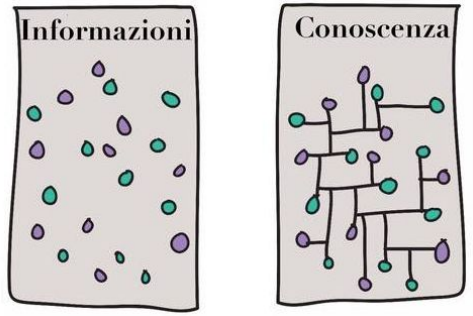
2. per le organizzazioni, la cybersecurity deve essere **investimento prioritario**

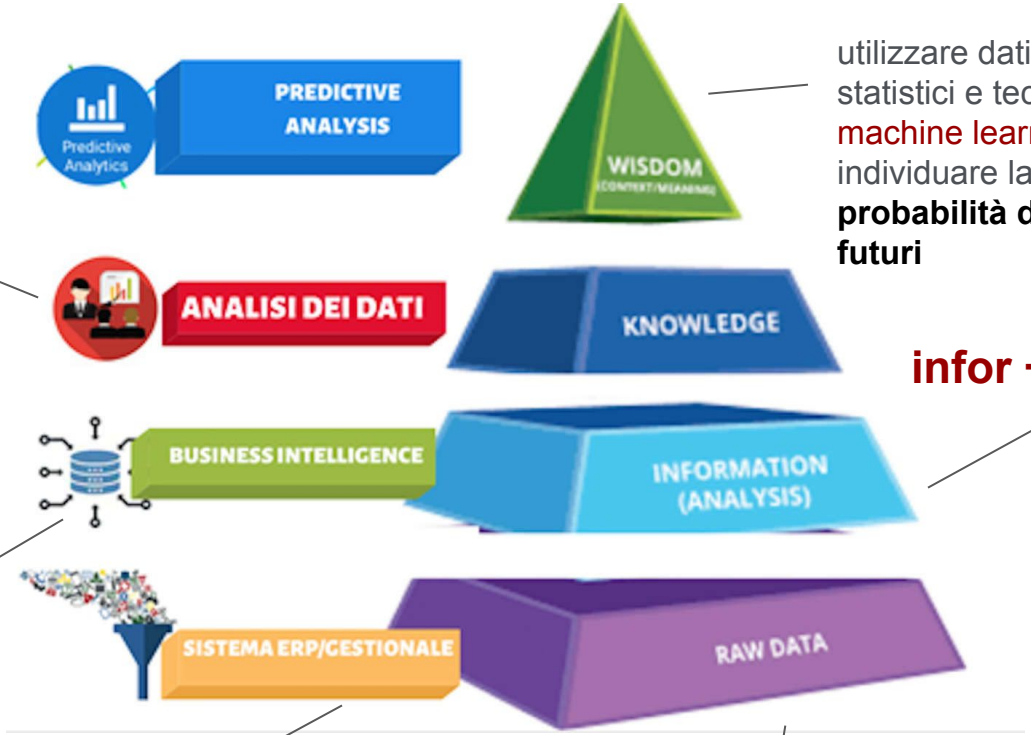
3. la cybersecurity non è un'attività che si improvvisa, ma una **disciplina con standard, framework e linee guida, da conoscere e da applicare**; in caso di attacchi, è sempre opportuno rivolgersi a **personale esperto** e alle **forze dell'ordine**

4. l'obiettivo principale della cyber security è quello di **proteggere i dati critici**

5. il **fattore umano** è centrale.

Piramide DIKW





utilizzare dati, algoritmi statistici e tecniche di machine learning per individuare la **probabilità di risultati futuri**

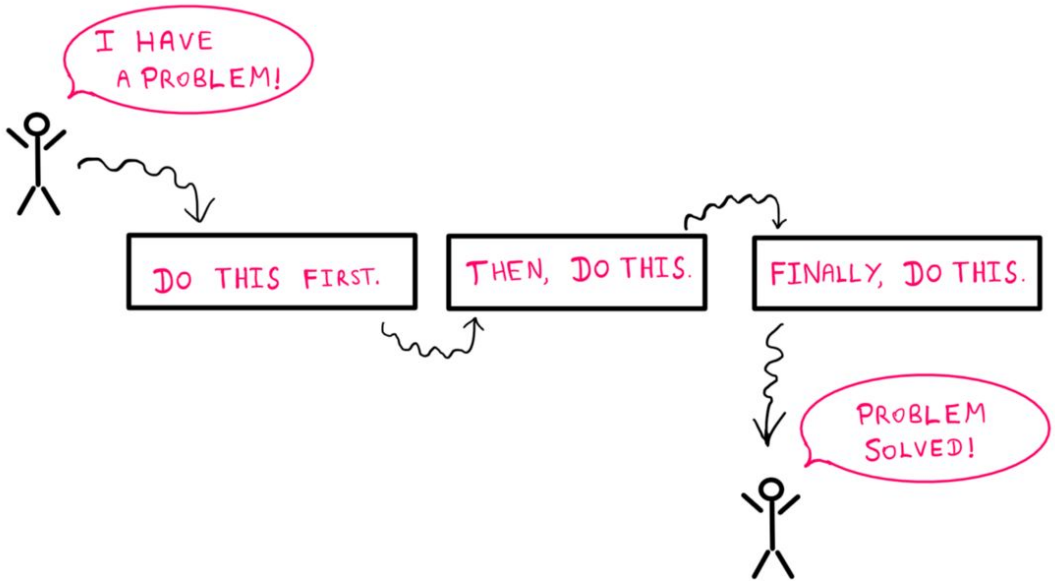
infor + matica

ERP (Enterprise Resource Planning) software che aiuta le organizzazioni ad automatizzare e gestire i processi aziendali principali

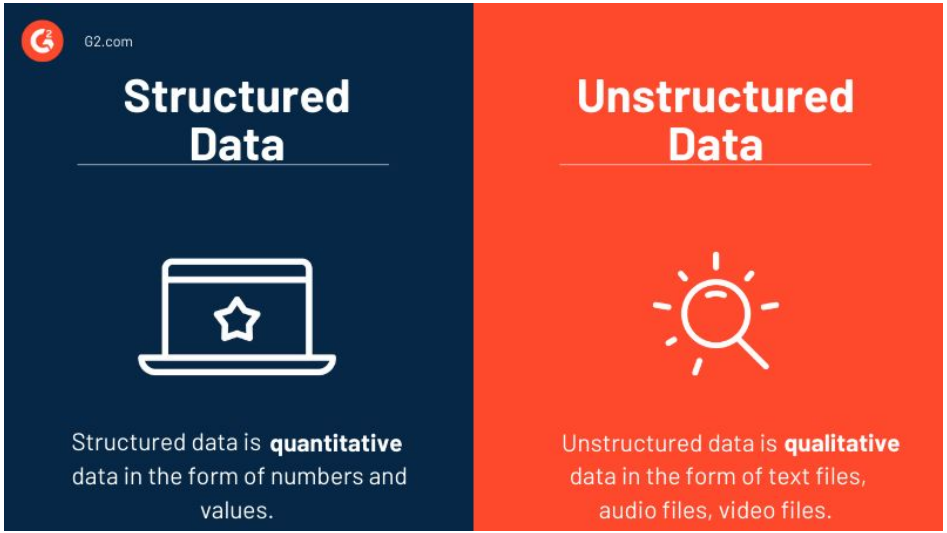
i dati grezzi (neutri) sono fondamentali e inutili

Ciclo di elaborazione dell'informazione digitale

Algoritmo = sequenza **finita**, **definita** ed **efficace** di operazioni da svolgere per giungere alla soluzione di un problema

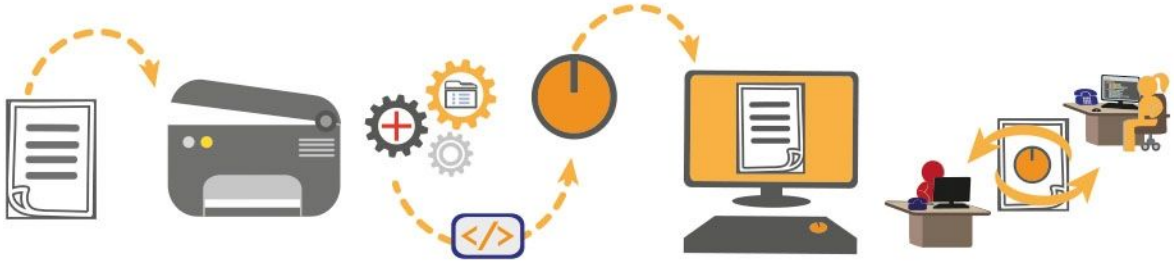


Dati strutturati e dati non strutturati / dematerializzazione



un **documento informatico** può considerarsi tale solo quando è un **documento elettronico** che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

rappresentazione informatica = i dati devono essere computabili



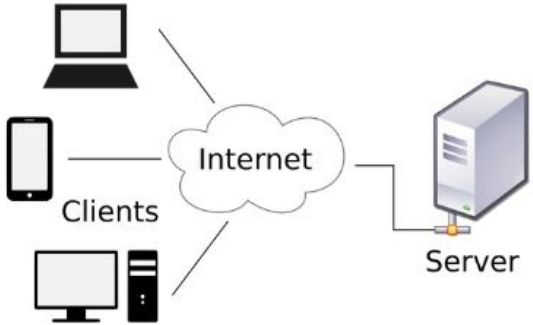
Relazione tra i dati

id	name	age
1	Jim	28
2	Pam	26
3	Michael	42

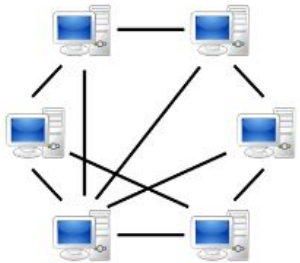
id	subject	Teacher
1	Languages	John Jones
2	Track	Wally West
3	Swimming	Arthur Curry
4	Computers	Victor Stone

student_id	subject_id	grade
2	1	98
1	2	100
1	4	75
3	3	60
2	4	76
3	2	88

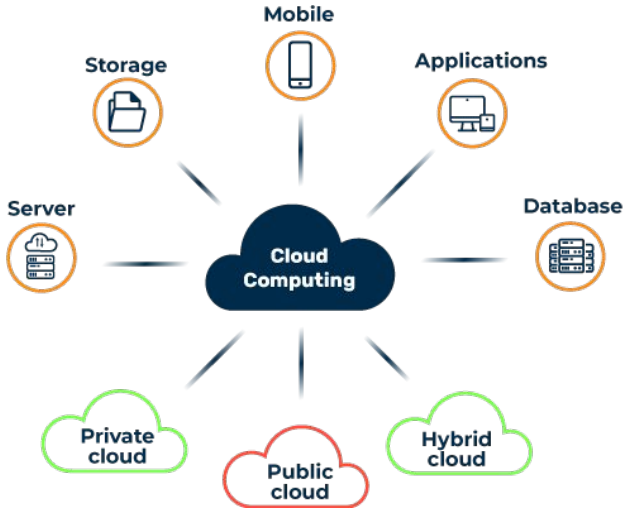
Architettura > Cloud



Client-Server

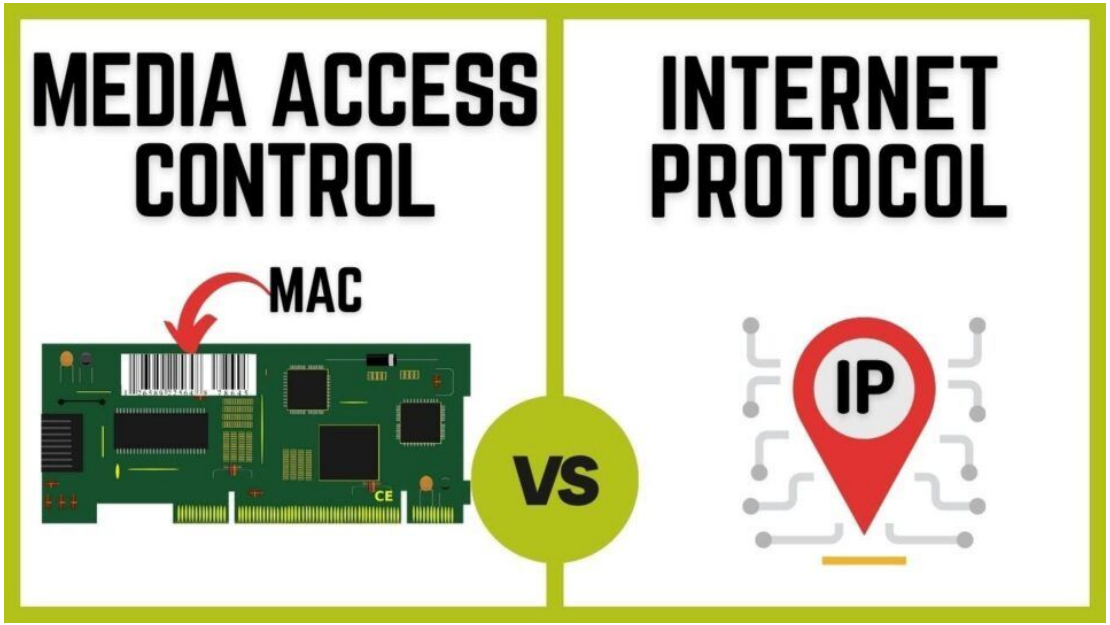


Peer-to-Peer



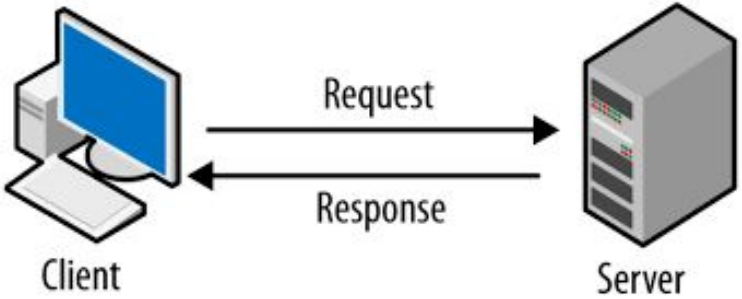
architettura informatica = organizzazione fisica e logica (= tecnologica) del sistema informatico
cloud = tecnologia che permette di elaborare e archiviare dati in rete; attraverso internet il cloud consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale.

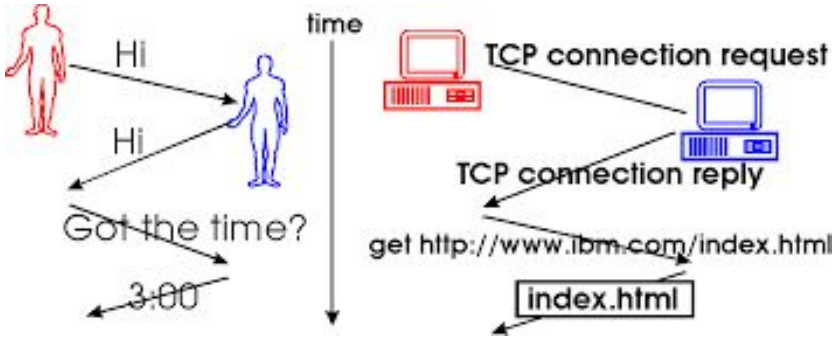
Dispositivi in Rete

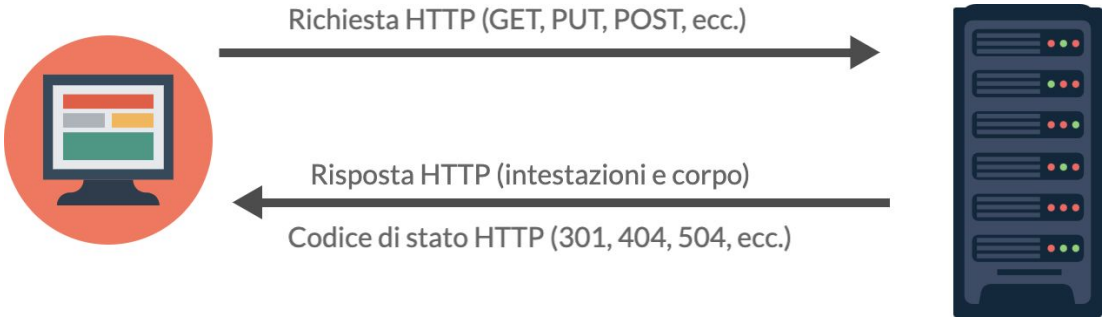


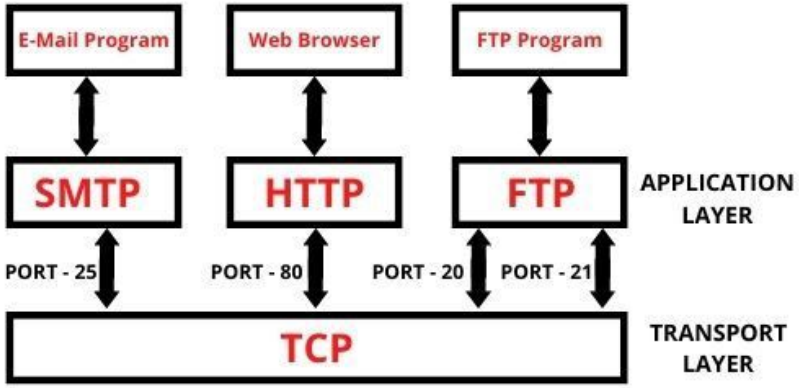
Il **MAC address** è l'identificatore fisico di un dispositivo in una rete locale, mentre l'**IP address** è l'identificatore logico che permette di comunicare su Internet.

Client - Server



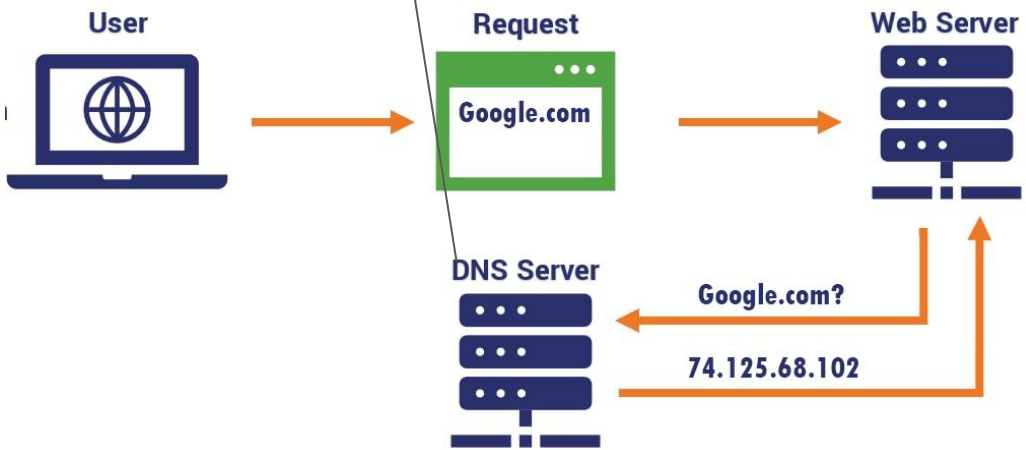






Simple **M**ail **T**ransfer **P**rotocol
File **T**ransfer **P**rotocol
Hyper**T**ext **T**ransfer **P**rotocol

Domain **N**ame **S**erver



HTTP Status Codes

HTTP STATUS CODES

2xx Success

200	Success / OK

3xx Redirection

301	Permanent Redirect
302	Temporary Redirect
304	Not Modified

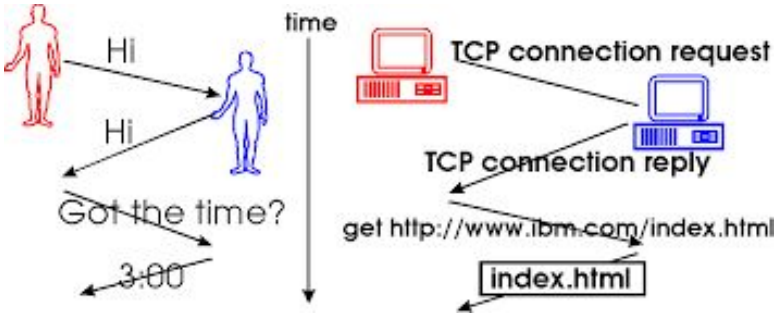
4xx Client Error

401	Unauthorized Error
403	Forbidden
404	Not Found
405	Method Not Allowed

5xx Server Error

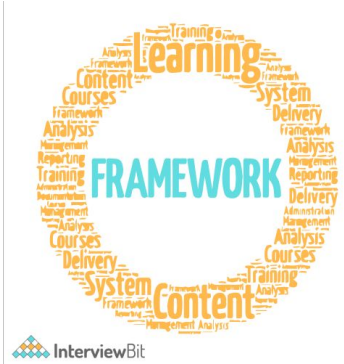
501	Not Implemented
502	Bad Gateway
503	Service Unavailable
504	Gateway Timeout

Comunicare i dati: protocolli framework standard linee guida



protocollo = sistema di regole che permette a due o più dispositivi di comunicare

standard = formalizzazione di un protocollo condiviso

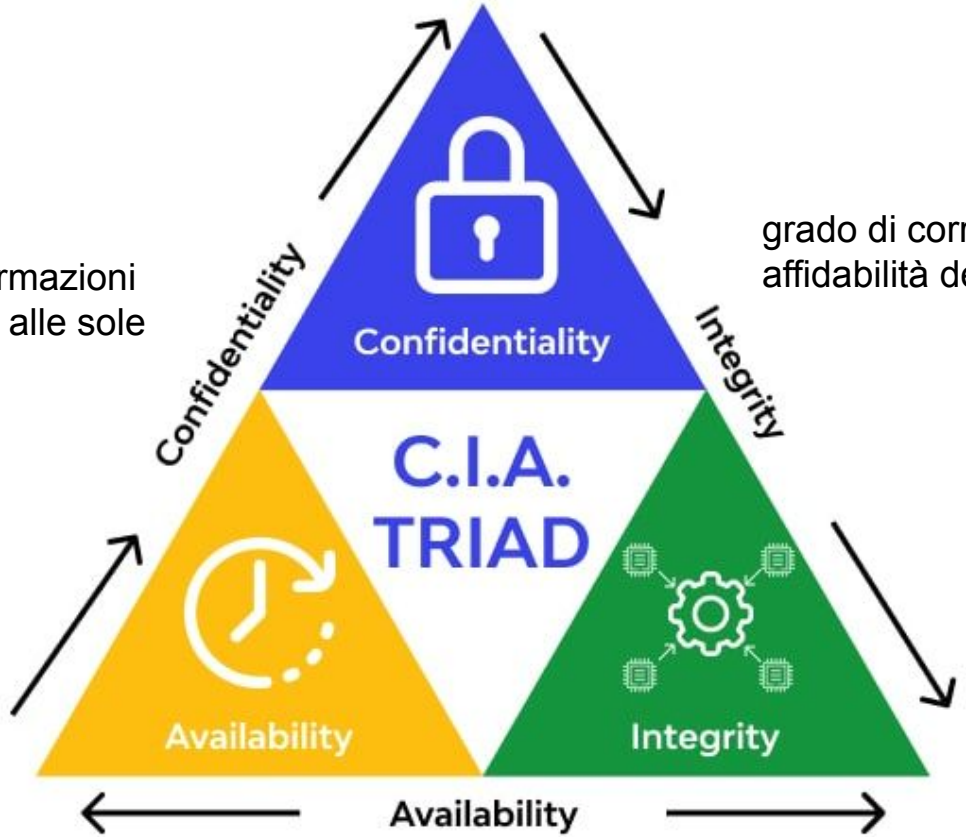


framework = documento che traduce lo standard in funzioni di indirizzo

linee guida = documenti che traducono i framework in procedure operative

C.I.A. Triad

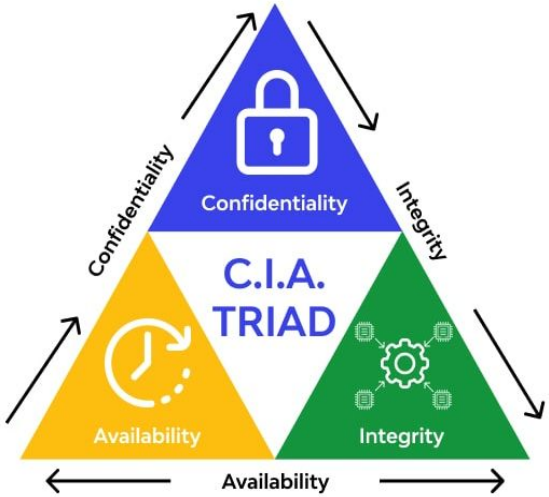
limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate

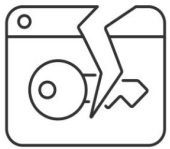


grado di correttezza, coerenza e affidabilità delle informazioni

informazioni e risorse accessibili agli utenti che ne hanno diritto, nel momento in cui servono

Compromettere la C.I.A. Triad

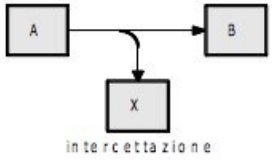
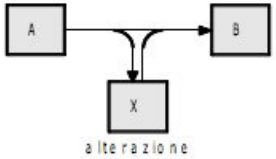
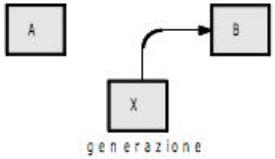
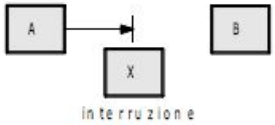




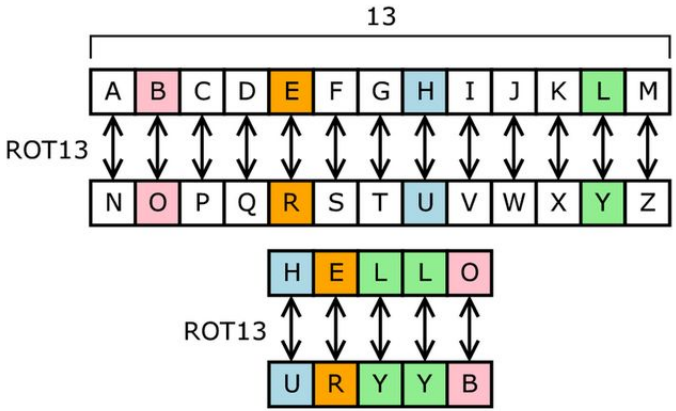
data breach

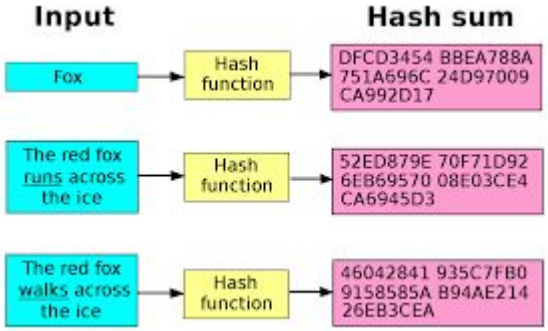
data leak

data loss

Attacco	*Schema*	*Esempi del mondo reale*
Flusso normale dell'informazione		Invio di un pacchetto IP Invio di email Accesso a una pagina web Lettura di dati da un database
Intercettazione		Sniffing di pacchetti di rete Furto di informazione mediante crittoanalisi Furto di informazione mediante analisi del traffico Furto di informazione mediante covert channel
Alterazione		Modifiche non autorizzate a file o programmi Attacchi "man in the middle" Azioni di disturbo del canale di comunicazione
Generazione		Masquerading Spoofing Intrusioni
Interruzione		Denial of service Flooding, resource starvation, mail storm Crashing di applicazioni Sabotaggio linee di comunicazione Danneggiamenti fisici

CRITTOGRAFIA



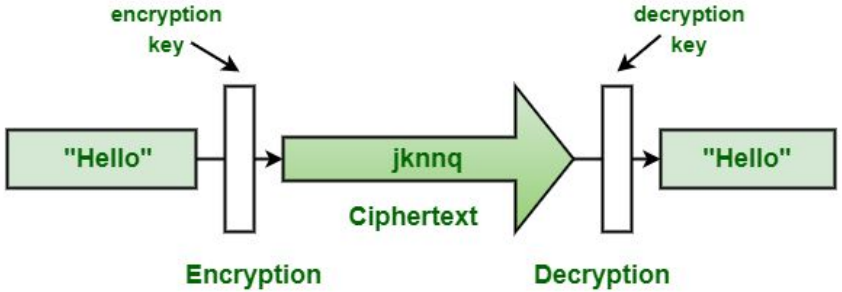


HTTPS

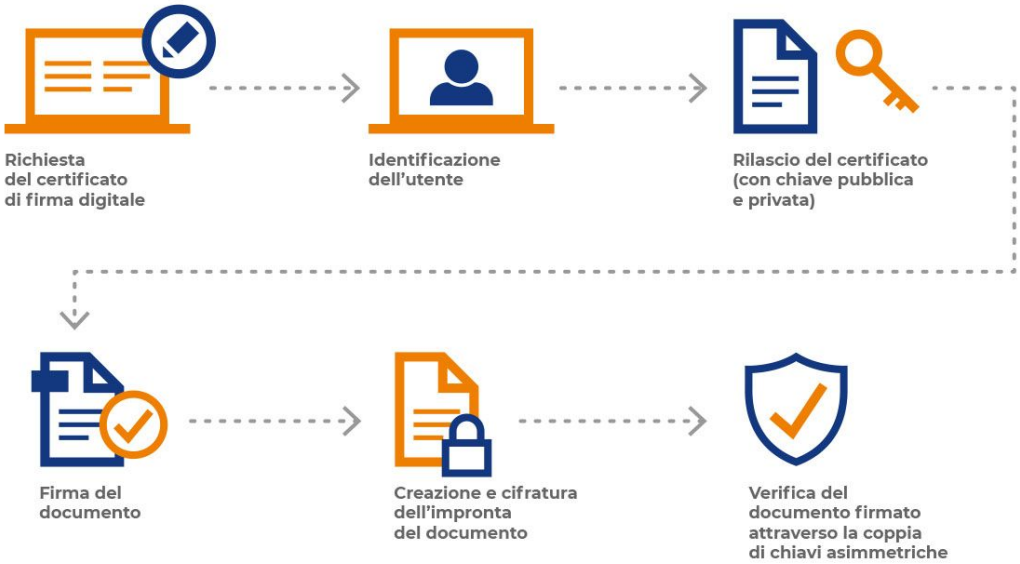

http://www.example.com
password: abc123
Helen
HTTP
Without password encryption
Hacker see "abc123"


https://www.example.com
password: abc123
Carol
HTTPS
With password encryption
Hacker see "xyaerXzabc"


HTTPS://
HTTP + SSL = HTTPS
Hypertext Transfer Protocol
Secure Socket Layer
Hypertext Transfer Protocol Secure


encryption key
decryption key
"Hello"
jknnq
Ciphertext
"Hello"
Encryption
Decryption

Firma digitale

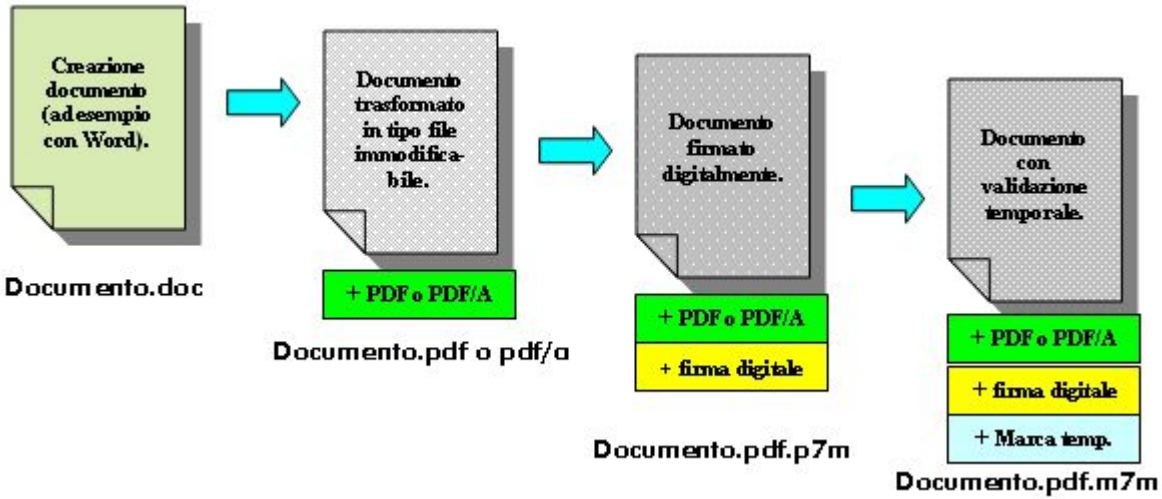


La **firma elettronica qualificata** (FEQ) - o digitale - è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici.

Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni. È possibile rivolgersi ai prestatori di servizi (provider) fiduciari qualificati autorizzati da AgID che garantiscono l'identità dei soggetti che utilizzano la firma digitale.

sito di riferimento: pec.it

Marca temporale



La **marca temporale** è un servizio offerto da un Certificatore accreditato, che consente di associare data e ora, certe e legalmente valide, a un documento informatico, permettendo una validazione temporale del documento opponibile a terzi.

firma CAdES (Cryptographic Message Syntax Advanced Electronic Signature): il documento viene 'imbustato' insieme con il file di firma digitale (estensione .p7m)

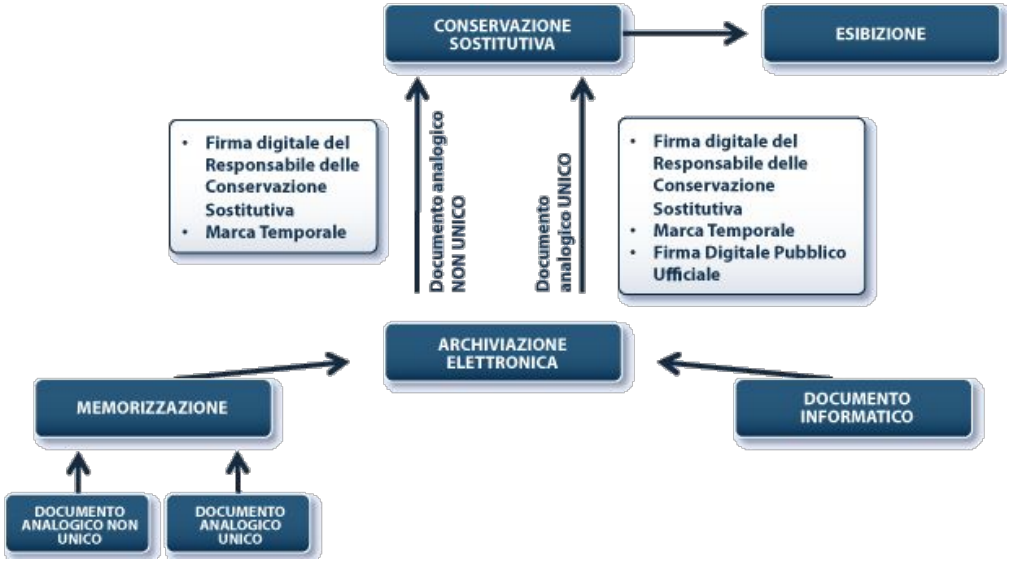
firma PAdES (PDF Advanced Electronic Signature):la firma difitale viene integrata nel documento .pdf

sito di riferimento: pec.it

PEC (Posta elettronica certificata)

sito di riferimento: pec.it

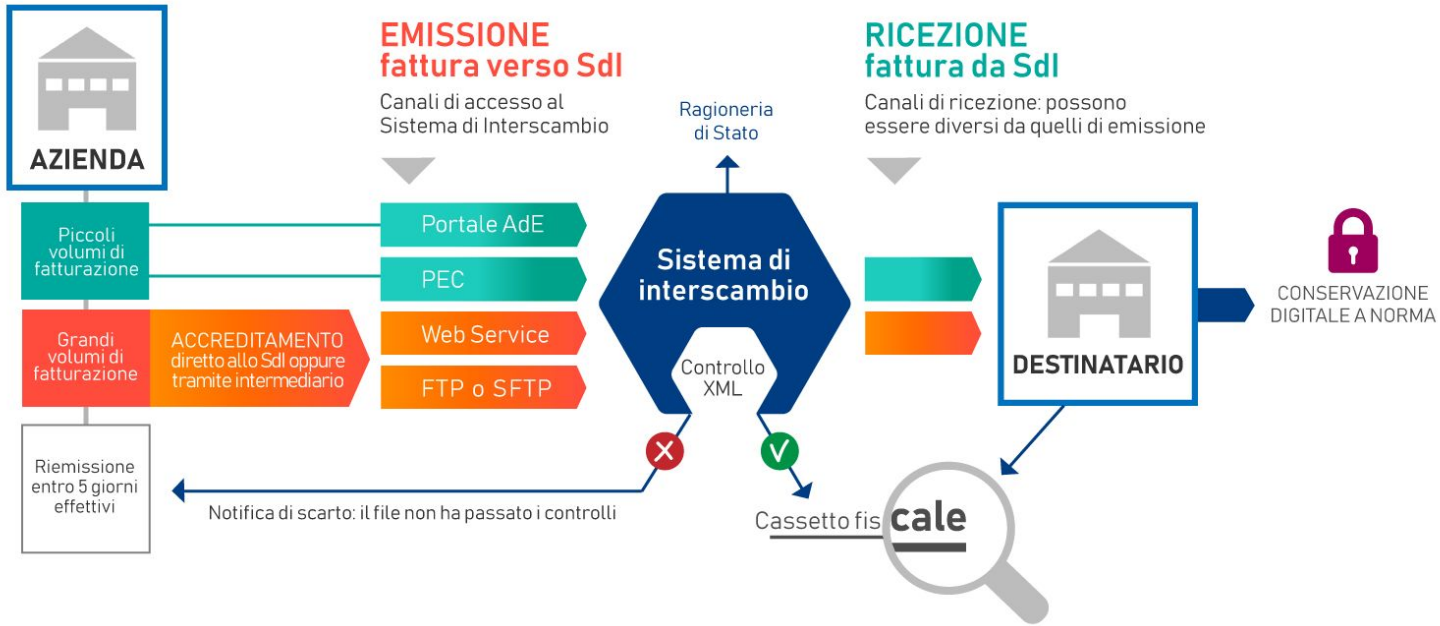
Conservazione digitale (= valenza legale nel tempo)



La principale differenza tra **conservazione sostitutiva** e **conservazione digitale** è che la prima sostituisce il documento cartaceo con una copia digitale certificata, mentre la seconda conserva il documento digitale nato tale

sito di riferimento: pec.it

Fatturazione elettronica (Sistema di Interscambio)



sito di riferimento: pec.it

SPID (Servizio Pubblico di Identità Digitale)

Il **Sistema Pubblico di Identità Digitale** (SPID) è un'identità digitale composta da una coppia di credenziali (username e password), strettamente personali, con le quali è possibile accedere ai servizi online della pubblica amministrazione e dei privati aderenti.

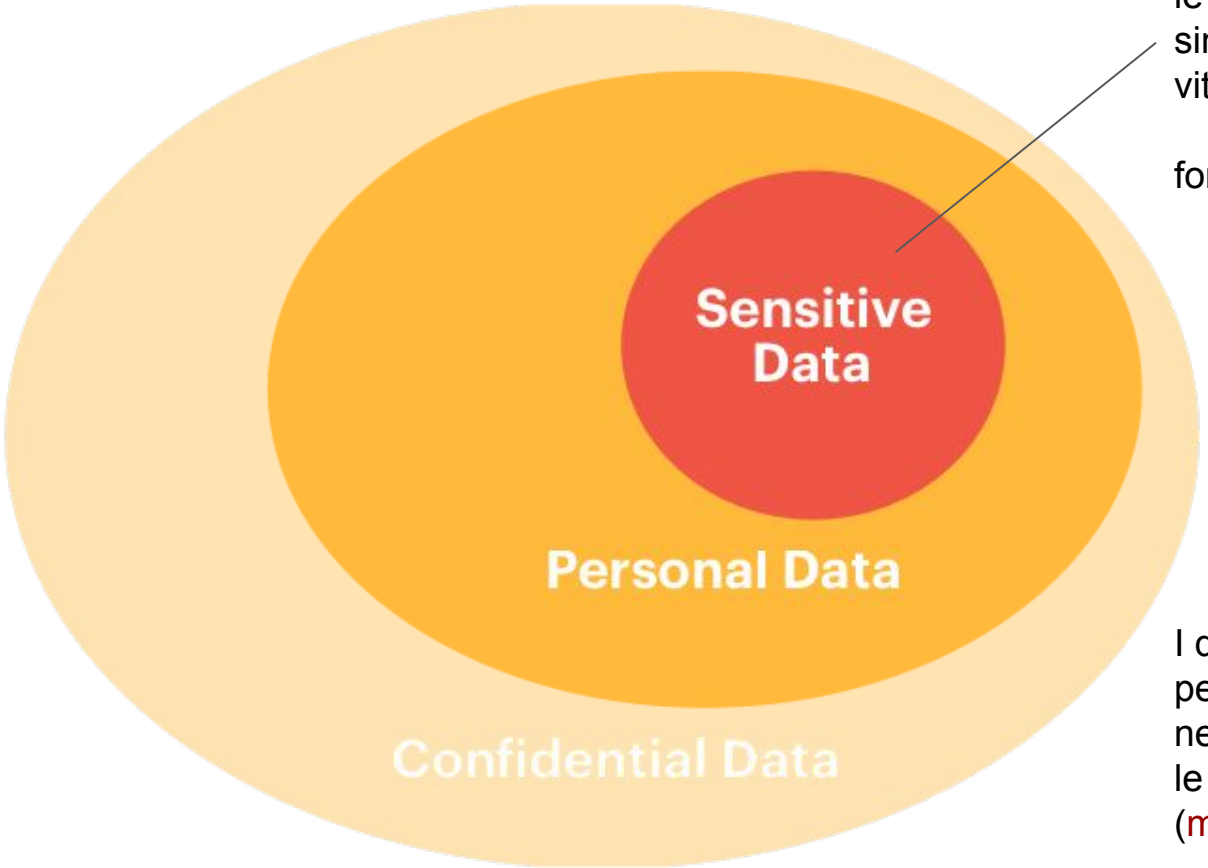
sito di riferimento: spid.gov.it

GDPR - Dati personali

Sono **dati personali** le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

fonte: https://www.garanteprivacy.it/

GDPR - Dati sensibili



rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale

fonte: https://www.garanteprivacy.it/

I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati) [GDPR]

È un **Regolamento**, quindi si applica direttamente in tutta l'UE senza bisogno di una legge nazionale di recepimento.

È **Generale**, quindi si applica a tutti i settori (scuole, aziende, enti pubblici, sanità, ecc.), a differenza delle direttive e regolamenti specifici (es. e-Privacy per le telecomunicazioni).

Data protection?

Regolamento Generale sulla Protezione dei Dati (RGPD)
(in vigore dal 24 maggio 2016, applicato dal 25 maggio 2018)

Privacy = Data protection?

Dichiarazione universale dei diritti dell'uomo (1948) delle Nazioni Unite (ONU)
Articolo 12

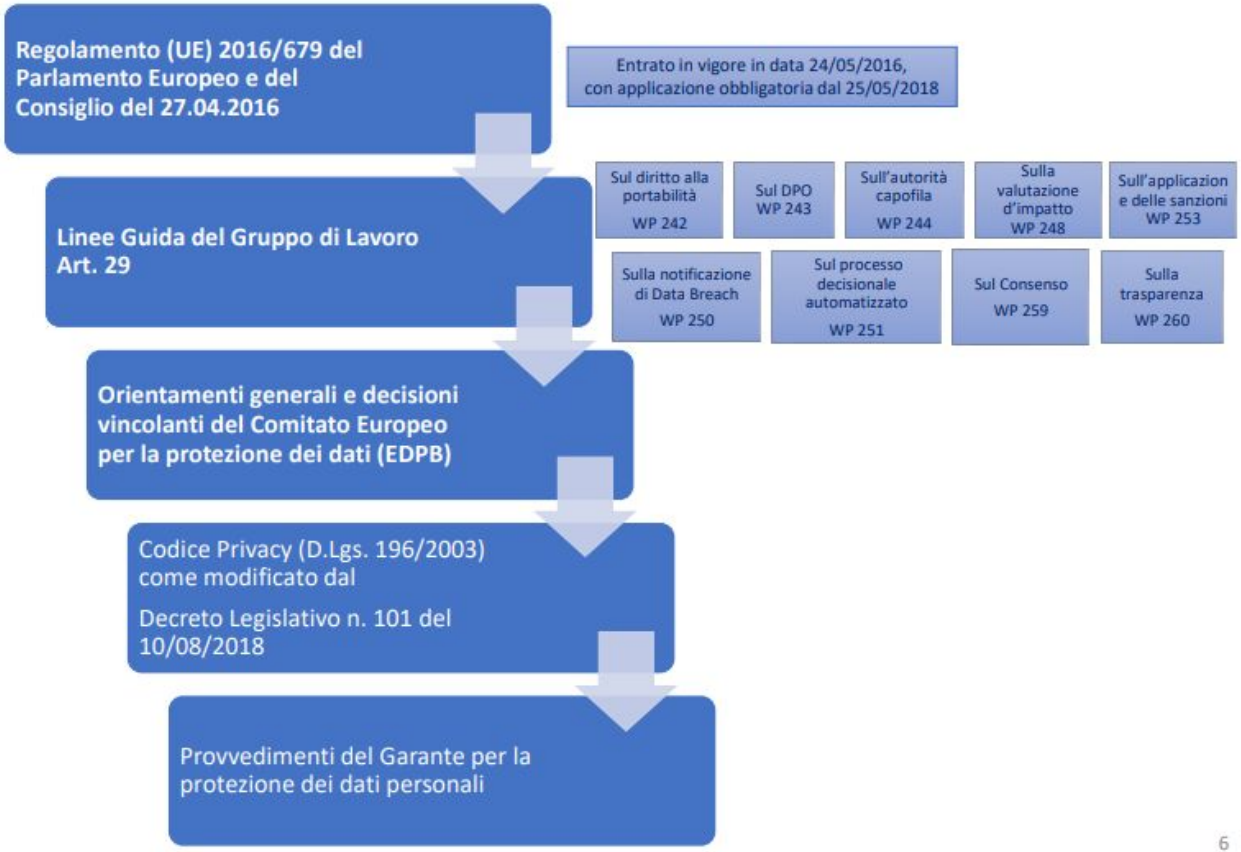
Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni.

Carta dei diritti dell'Unione europea (Carta di Nizza, 2000)
[originariamente documento politico, diventa giuridicamente vincolante nel 2007 con la firma del Trattato di Lisbona (entrato in vigore nel 2009)].

Articolo 7
[Rispetto della vita privata e della vita familiare (privacy)]
Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Articolo 8
[Protezione dei dati di carattere personale (data protection)]
1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Riferimenti normativi



Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce **norme** relative alla **protezione** delle **persone fisiche** con riguardo al **trattamento** dei **dati personali**, nonché norme relative alla **libera circolazione** di tali dati.

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Si definisce **persona fisica** qualunque essere umano, nato e vivente, senza alcuna distinzione di razza, sesso, condizioni economiche-sociali.

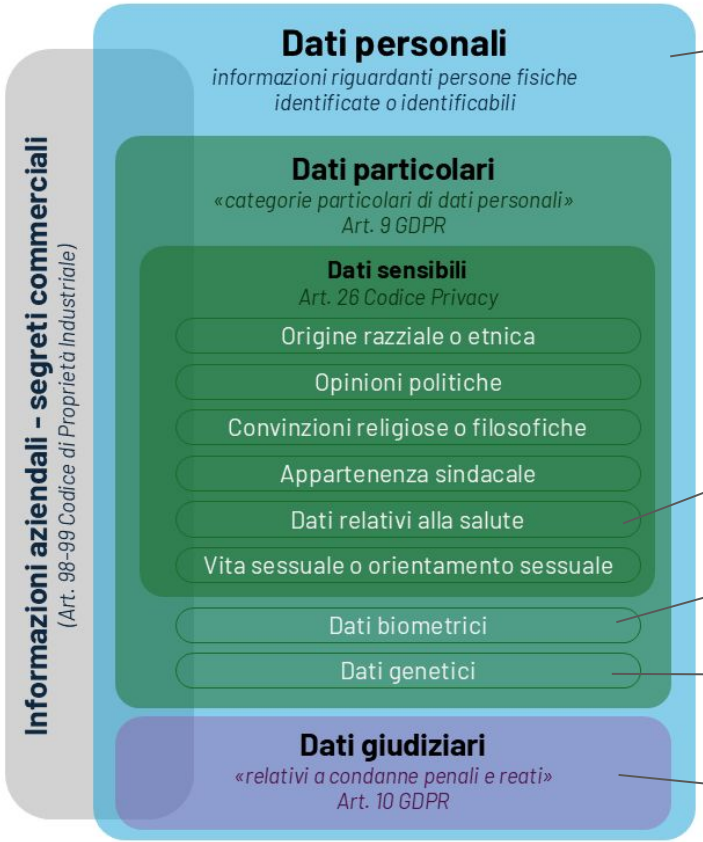
Si definisce **persona giuridica** un insieme strutturato di persone e mezzi, finalizzato a obiettivi sociali e riconosciuto dall'ordinamento giuridico come soggetto del diritto.

Con l'art. 21 della Legge n.59/1997 (**Riforma Bassanini)** è stata attribuita alle Istituzioni scolastiche l'**autonomia funzionale** e la **personalità giuridica**.

3. La libera circolazione dei dati personali nell'Unione **non può essere limitata né vietata** per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 1
Oggetto e finalità

Dati nel GDPR



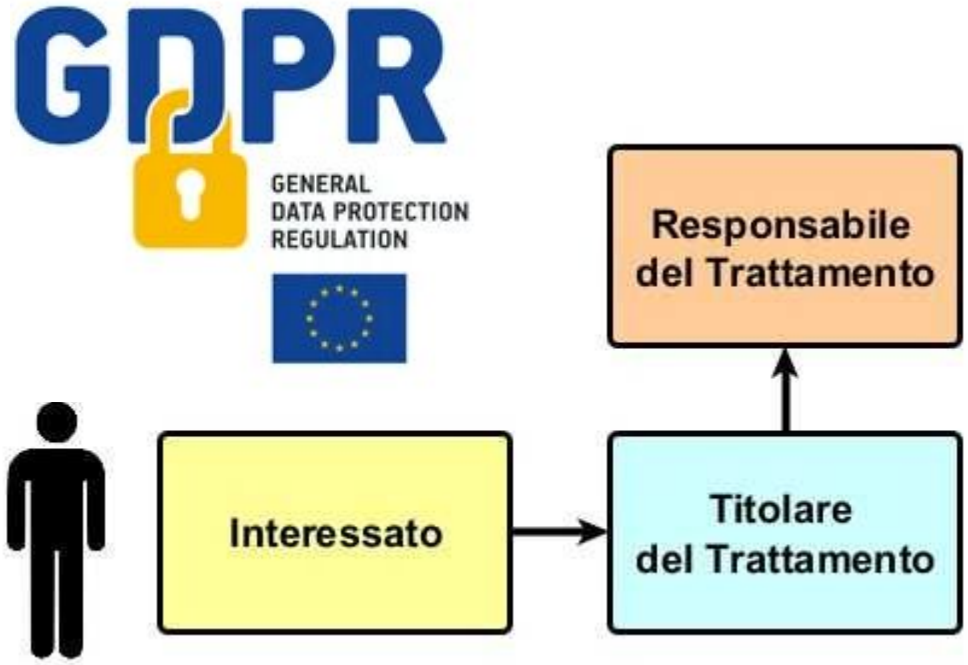
art. 4

art. 15

art. 14

art. 13

artt. 9 e 10



Interessato è la persona fisica alla quale si riferiscono i dati personali.

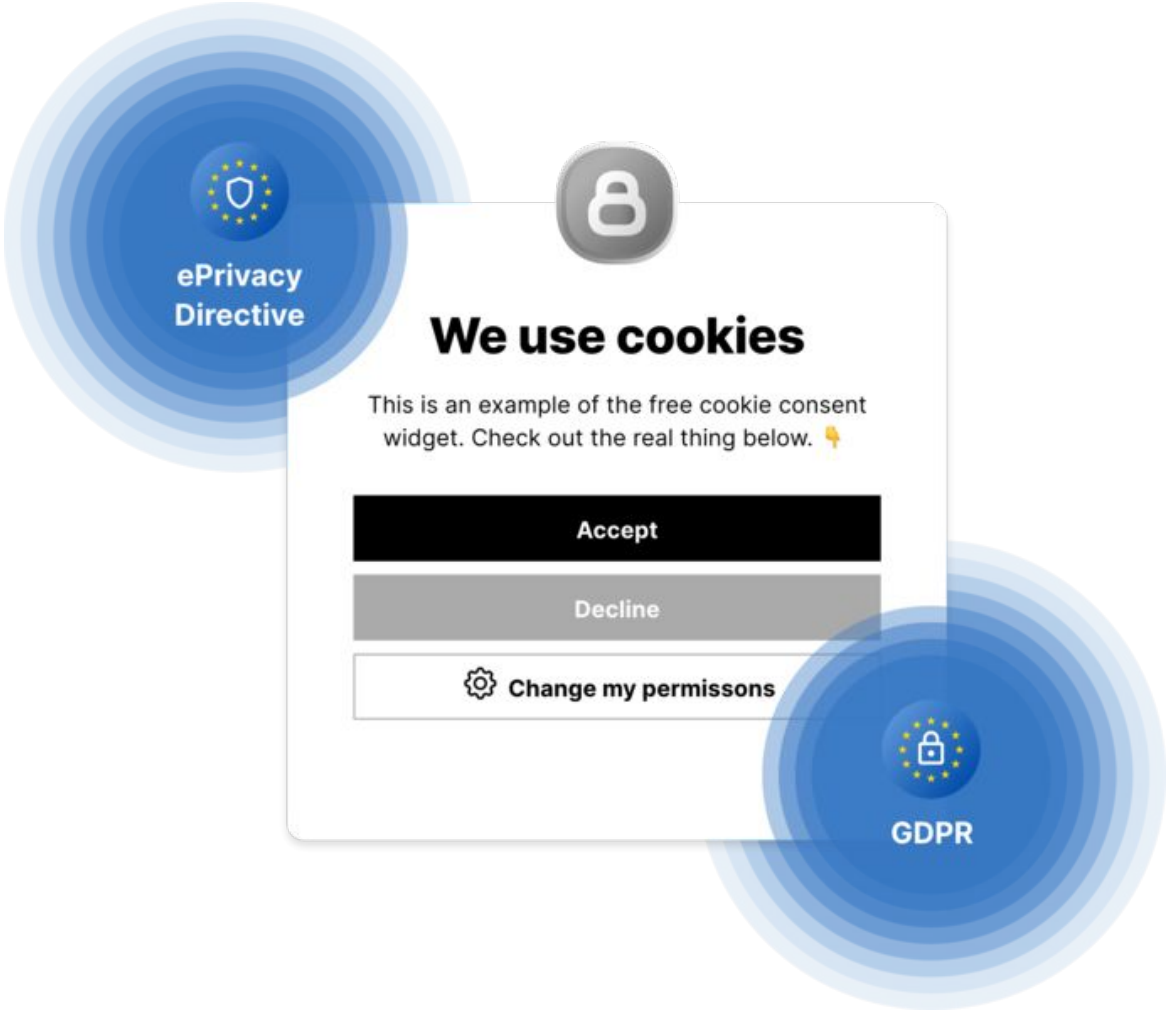
Responsabile è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo per suo conto del trattamento dei dati.

Trattamento è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali.

Titolare è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento.

GDPR

GENERAL
DATA PROTECTION
REGULATION



Italia digitale

AGID
Agenzia per l'Italia Digitale

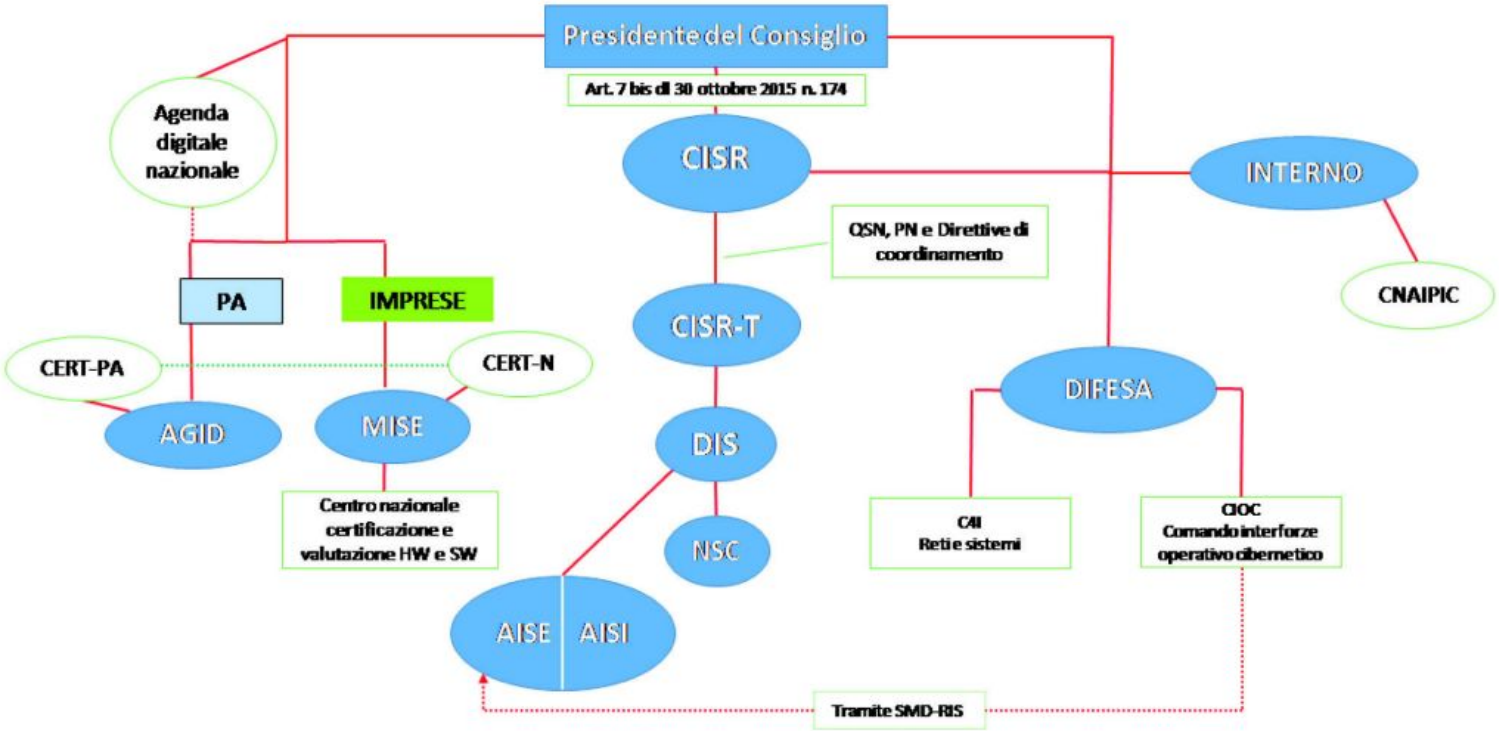
Il **Codice dell'Amministrazione Digitale** (CAD) è un testo unico che riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese.

PagoPA è il portale nazionale dei pagamenti a favore della Pubblica Amministrazione.

Id2026
Italiadigitale2026

Italia digitale 2026 è il piano strategico per la transizione digitale e la connettività promosso dal Dipartimento per la trasformazione digitale.

Architettura nazionale di cybersecurity



Grazie per l’attenzione :)

Nunzio **Castaldi**

weben.fad@gmail.com
weben.it