CIRPA
Centro interdipartimentale per l'Innovazione e la Ricerca nelle Pubbliche amministrazioni e nelle Organizzazioni NO Profit.

INPS Istituto Nazionale Previdenza Sociale
VALORE P.A.

La formazione dell'archivio digitale

- *La normativa di riferimento*

Patrizia Gentili, 26 Aprile 2023
pgentili60@gmail.com

Agenda

- Il TUDA
- Il CAD
- EiDAS
- Gli strumenti di cittadinanza digitale
- Il sistema sanzionatorio
- I manuali

Il Testo Unico sulla Documentazione amministrativa (TUDA)

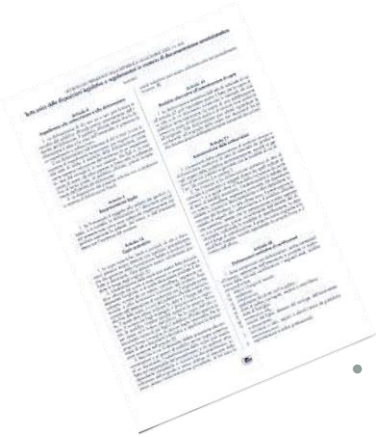
DPR 445/2000

- Il Testo unico **raccoglie e coordina**, da un lato, le norme in materia di documentazione amministrativa e, dall'altro, le norme in materia di redazione e gestione dei documenti informatici.
- **Armonizza** il loro contenuto, fortemente innovativo, con le norme riguardanti la documentazione amministrativa "tradizionale".
- Ha tentato di **non mantenere** le norme in materia di documento informatico come un **corpo a sé**, ma di collegarle strettamente ai diversi ambiti della disciplina "*tradizionale*" a cui sono legate sul piano operativo (ad esempio, le norme in materia di firma digitale sono state riunite con le norme generali in materia di sottoscrizione di documenti amministrativi e atti pubblici, ecc.).
- L'ambizione, dunque, è stata quella di riuscire a **disciplinare efficacemente** sia la fase in cui predominavano ancora gli strumenti tradizionali, sia la fase di **transizione dai documenti cartacei a quelli informatici**, sia il regime fondato in prevalenza su strumenti informatici e telematici (documento informatico, firma digitale, carta d'identità elettronica, trasmissione di dati per via telematica etc.)

Il Testo Unico sulla Documentazione amministrativa (TUDA)

DPR 445/2000

- Rappresenta, tuttora, un **punto di riferimento essenziale** nel dialogo tra privati e P.A. e uno strumento fondamentale nelle mani di tutti, privati e P.A..
- Il TUDA contiene tutte le "**definizioni utili**" per l'interpretazione e l'utilizzo di istituti largamente diffusi nell'ordinamento italiano, ossia un insieme di **definizioni fondamentali** quali ad esempio quella relativa al "documento amministrativo", al "documento informatico", alla "firma digitale" e tanti altri.
- Il D.P.R. n. 445 ha le finalità di disciplinare la formazione, il rilascio, la tenuta e la conservazione, la gestione, la trasmissione di atti e documenti da parte di organi della Pubblica Amministrazione.
- Disciplina, inoltre, la produzione di atti e documenti per gli organi della Pubblica Amministrazione nonché per i gestori di pubblici servizi nei rapporti tra loro e in quelli con l'utenza, e per i privati che vi consentono.



Principi ispiratori del TUDA

- Cittadini e operatori non devono più orientarsi in una "**giungla**" di norme e regolamenti, ma potranno finalmente trovare in unico testo normativo le disposizioni di legge e regolamentari che riguardano l'intera materia e le regole tecniche collocate in allegato.
- Il testo unico ha introdotto notevoli novità, che completano e sviluppano in modo organico le semplificazioni introdotte con le **leggi Bassanini**.
- I risultati positivi raggiunti hanno consentito di compiere un passo in avanti verso la completa eliminazione della richiesta dei certificati ai cittadini e la **decertificazione**, prevista dal piano e-government.

A chi si applica il TUDA?

Art. 2

Le disposizioni del testo unico disciplinano la formazione, il rilascio, la tenuta e la conservazione, la gestione, la trasmissione di atti e documenti da parte di organi della pubblica amministrazione; disciplinano altresì la produzione di atti e documenti e si applicano:

- ✓ **a tutte le amministrazioni pubbliche**;
- ✓ **ai gestori di servizi pubblici** nei rapporti con l'utenza. I gestori di servizi pubblici sono tenuti ad applicarle nei rapporti con l'utenza, mentre nei rapporti con il personale, con le imprese che partecipano alle gare ecc. sono equiparati ai privati, e non sono quindi tenuti ad accettare l'autocertificazione, ma possono scegliere di farlo;
- ✓ **ai privati che lo consentono**.

Le norme concernenti i documenti informatici e la firma digitale, contenute nel capo II, si applicano anche nei rapporti tra privati come previsto dall'articolo 15, comma 2 della legge 15 marzo 1997, n. 59.

Articolazione del TUDA

- Capo I - Definizioni e ambito di applicazione (Artt. 1-5)
- Capo II - Documentazione amministrativa (Artt. 6-37)
- Capo III - Semplificazione della documentazione amministrativa (Artt. 38-49)
- Capo IV - Sistema di gestione informatica dei documenti (Artt. 50-70)
- Capo V - Controlli (Artt. 71-72)
- Capo VI - Sanzioni (Artt. 73-76)
- Capo VII - Disposizioni finali (Artt. 77-78)

Sintesi delle principali disposizioni 1/4

1. **L'eliminazione della richiesta dei certificati ai cittadini**

Tutte le amministrazioni e i gestori dei servizi pubblici **non possono più chiedere ai cittadini i certificati** e sono tenuti ad **accettare le autocertificazioni** o ad acquisire d'ufficio la documentazione necessaria. La richiesta di certificati costituisce **violazione dei doveri d'ufficio**. Ad esempio non possono più essere richiesti ai cittadini i certificati anagrafici e quelli relativi alla situazione reddituale, al titolo di studio, alla qualifica posseduta, all'iscrizione in albi o elenchi della pubblica amministrazione, al non avere riportato condanne penali etc.

1. **Verso la decertificazione: scambio di dati per via telematica e controlli**

Le amministrazioni, al fine di agevolare l'acquisizione d'ufficio e i controlli da parte delle altre amministrazioni, sono tenute a garantire, senza oneri, la consultazione per via telematica dei loro archivi informatici.

La mancata risposta alle richieste di controllo entro 30 giorni (finché tutti i dati non siano integralmente disponibile on-line), costituisce **violazione dei doveri d'ufficio**.

3. **L'autentica diventa più semplice**

Tutte le domande e le dichiarazioni sostitutive dell'atto di notorietà rivolte alle amministrazioni e i gestori di servizi pubblici **non devono più essere autenticate**. Basterà firmarle davanti al dipendente addetto o inviarle con la fotocopia del documento d'identità (questa possibilità era già prevista solo per le dichiarazioni collegate alle domande). L'autentica con le modalità tradizionali rimane per le dichiarazioni rivolte ai privati e per le domande che riguardano la riscossione di benefici economici (pensioni, contributi etc.) da parte di terze persone.

Con la dichiarazione sostitutiva dell'atto di notorietà è possibile attestare la **conformità all'originale** di un documento conservato o rilasciato da una pubblica amministrazione evitando così l'autentica di copia davanti al funzionario incaricato dal sindaco o dal dipendente addetto.

Cos’è l’autocertificazione?

- Consiste nella facoltà riconosciuta ai cittadini di presentare, in sostituzione delle tradizionali certificazioni richieste, propri stati e requisiti personali, mediante **apposite dichiarazioni sottoscritte** (firmate) dall'interessato.
- La firma **non deve essere più autenticata**.
- **L'autocertificazione sostituisce i certificati** senza che ci sia necessità di presentare successivamente il certificato vero e proprio.
- La pubblica amministrazione **ha l'obbligo di accettarle**, riservandosi la possibilità di controllo e verifica in caso di sussistenza di ragionevoli dubbi sulla veridicità del loro contenuto.
- Vi sono pochi casi, nei rapporti con la Pubblica Amministrazione, in cui devono essere esibiti i tradizionali certificati:
  - ✓ pratiche per contrarre matrimonio,
  - ✓ rapporti con l'autorità giudiziaria,
  - ✓ atti da trasmettere all'estero.

Cosa non si può autocertificare

- Non possono essere sostituiti da altro documento, salvo diverse disposizioni della normativa di settore, e quindi **non si possono autocertificare**:
  - ✓ i certificati medici,
  - ✓ i certificati sanitari,
  - ✓ i certificati veterinari,
  - ✓ i certificati di origine,
  - ✓ i certificati di conformità CE,
  - ✓ i certificati di marchi o brevetti.
- Tutti i certificati medici e sanitari richiesti dalle istituzioni scolastiche ai fini della pratica non agonistica di attività sportive da parte dei propri alunni sono sostituiti con un **unico certificato di idoneità alla pratica non agonistica** di attività sportive rilasciato dal medico di base con validità per l'intero anno scolastico.

Cosa fare se non viene accettata

- Il pubblico ufficiale o il funzionario dell'ufficio pubblico che non ammette l'autocertificazione o la dichiarazione sostitutiva dell'atto di notorietà, nonostante ci siano tutti i presupposti per accoglierla, incorre nelle sanzioni previste dall'art. **328 del Codice penale** e rischiano di essere puniti per **omissioni o rifiuto di atti d'ufficio**.

- Il cittadino dovrà, in primo luogo, accertare chi è il **responsabile della pratica** inoltrata, richiedendo nome, cognome e qualifica, inoltre è necessario conoscere il **numero di protocollo** della stessa e il tipo di procedimento attribuito.
- Così come la Pubblica Amministrazione sa chi è il suo interlocutore, il cittadino ha altrettanto **diritto di sapere** chi segue il procedimento che lo riguarda e come risalire agli atti relativi.

Dichiarazioni sostitutive presentate da cittadini stranieri

- Nel caso in cui le dichiarazioni sostitutive siano presentate da cittadini della Comunità Europea, **si applicano le stesse modalità** previste per i cittadini Italiani.
- I cittadini extracomunitari, residenti in Italia secondo le disposizioni del regolamento anagrafico della popolazione residente, approvato con decreto del Presidente della Repubblica il 30 Maggio 1989, n. 233, **possono utilizzare le dichiarazioni sostitutive** limitatamente ai casi in cui si tratti di comprovare stati, fatti e qualità personali **certificabili o attestabili** da parte di soggetti pubblici o privati italiani.

Sintesi delle principali disposizioni 2/4

Le istanze per via telematica

- Tutte le domande e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori e esercenti di pubblici servizi possono essere inviate anche per **fax o per via telematica**.

Il protocollo informatico

- All'art.50 si dice che «Le pubbliche amministrazioni provvedono ad introdurre nei piani di sviluppo dei sistemi informativi automatizzati progetti per la **realizzazione di sistemi di protocollo informatico** in attuazione delle disposizioni del presente testo unico»

Sintesi delle principali disposizioni 3/4

Il documento informatico

- Gli artt. 8, 9 e 10 del testo unico prevedono che il **documento informatico**, ovvero la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti, soddisfa il **requisito legale** della forma scritta ed ha efficacia di scrittura privata, purché abbia i requisiti previsti dallo stesso regolamento.
- Fra questi requisiti, in particolare, il più importante è quello della **presenza della firma digitale**.
- Quindi il Testo unico sostiene che:

*«Il documento informatico ha **l'efficacia probatoria** prevista dall'articolo 2712 del codice civile, riguardo ai fatti ed alle cose rappresentate.»*

Sintesi delle principali disposizioni 4/4

- **Le Aree Organizzative omogenee**

✓ L'art. 50 comma 4 del testo unico prevede l'individuazione da parte di ciascuna Amministrazione di Aree Organizzative Omogenee (**AOO**), ossia un insieme di risorse umane e strumentali dotate di propri organi di gestione e governo per adempiere a determinate funzioni primarie.

✓ Ogni Area Organizzativa Omogenea (AOO) deve utilizzare un **proprio protocollo unico**.

Il Protocollo informatico

Una definizione

- Il protocollo informatico è "*l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti*".
- A suffragio dell'importanza delle procedure digitali per la gestione documentale occorre considerare che "*gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici,* ***sono validi e rilevanti a tutti gli effetti di legge***" Legge 15 marzo 1997, n.59 (art.15)

Il Protocollo informatico

I compiti

- È lo **strumento tecnico** per la gestione sequenziale dei documenti nel momento della loro formazione o del loro ingresso nel perimetro dell'Ente;
- censisce la **mole documentaria** posta in essere da un ente produttore;
- poiché il progressivo di protocollo è un numero ordinale la cui numerazione è rinnovata ogni anno solare, garantisce **l'identificazione univoca** di ogni documento dell'archivio;
- avvia la corretta distribuzione dei documenti (**assegnazione**);
- realizza i **collegamenti** tra i singoli documenti e i vari fascicoli;
- assicura all'archivio una **struttura organizzata** tramite le ulteriori fasi della classificazione e fascicolazione dei documenti.

Il Protocollo informatico

Il protocollo è **strumento imprescindibile** di organizzazione e deve ispirarsi a criteri di:

La segnatura di protocollo

- La segnatura di protocollo è l'associazione all'originale del documento, in **forma permanente e non modificabile**, delle informazioni riguardanti il documento stesso; essa consente di individuare ciascun documento in modo inequivocabile.
- Le informazioni minime da apporre o associare al documento sono:
  - ✓ il **progressivo** di protocollo;
  - ✓ la **data** di protocollo;
  - ✓ **l'identificazione della struttura competente** alla gestione del documento, anche ai fini della classificazione ed archiviazione.
- L'operazione di segnatura va completata con l'apposizione al documento degli elementi necessari alla gestione archivistica dello stesso (**classificazione**).
- L'operazione di segnatura di protocollo va effettuata **contemporaneamente** all'operazione di registrazione di protocollo.

Il registro di protocollo

- Il registro giornaliero di protocollo, come **atto pubblico di fede privilegiata**, può essere considerato come una sorta di **rendicontazione**.
- In esso, infatti, devono essere riportate le registrazioni di tutti **i documenti in entrata e in uscita** da un'organizzazione nell'arco di uno stesso giorno.
- Le registrazioni devono essere:
  - ✓ **progressive** (la registrazione delle entrate e delle uscite deve seguire l'ordine temporale);
  - ✓ **univoche** (ogni movimento relativo a un documento deve poter essere individuato in maniera univoca).

Registrazione, classificazione e fascicolazione

- L’art. 53 del TUDA prevede che *«Sono oggetto di **registrazione obbligatoria** i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici.»*
- La registrazione a protocollo e la **segnatura** costituiscono un’operazione unica e vengono effettuate contemporaneamente.
- Il **titolario di classificazione** è uno strumento dell’archivio corrente che serve per organizzare la documentazione prodotta o ricevuta dall’Amministrazione in settori e categorie, schematizzando in maniera logica le sue competenze e funzioni.
- La **fascicolazione** è la creazione ordinata e funzionale di unità correlate al processo decisionale ed è strettamente correlata alla classificazione.

Effetti positivi

- **L'autocertificazione** ha rappresentato, in qualche modo, il primo segnale di una rivoluzione nei rapporti fra cittadini e amministrazione: **da sudditi a utenti** o clienti, i cittadini; da strumenti di vessazione a **servizi per la collettività**, le amministrazioni.
- I dati del monitoraggio quantitativo effettuato a suo tempo in 23 città sulla riduzione delle certificazioni anagrafiche e delle autentiche di firme rilasciate dalle anagrafi comunali e la stima del conseguente risparmio degli italiani hanno mostrato i positivi e diffusi risultati dell'attuazione delle nuove norme.
- La riduzione delle certificazioni e delle autentiche di firma ha rappresentato **un grande risparmio di tempo e di denaro** per i cittadini. Nel 1999 il progetto "**Semplifichiamo**" della Funzione Pubblica ha stimato che la spesa sostenuta dagli italiani per le certificazioni e le autentiche di firma era passata da 2.977 miliardi del 1996 a 1.107 miliardi del 1999. I risparmi rispetto al 1996 sono stati stimati rispettivamente in 1.020 miliardi per il 1998 e in 1.869 miliardi per il 1999. I dati dei primi 5 mesi del 2000, confrontati con quelli del 1996, hanno confermato il trend di decremento ed evidenziano un'ulteriore significativa riduzione sia dei certificati che delle autentiche di firma.
- Al cittadino inoltre viene chiesto di comunicare, **per una sola volta**, al sistema delle amministrazioni pubbliche i dati che lo riguardano (la nascita di un figlio, il cambio di residenza,etc.).

Principio «*ONCE ONLY*»

Il Codice dell'Amministrazione Digitale

- Il Codice dell'Amministrazione Digitale (CAD) è un Codice, ovvero un **insieme organico di disposizioni**, che presiede all'uso dell'informatica come strumento privilegiato nei rapporti tra la pubblica amministrazione e i cittadini italiani.
- Stabilisce le **regole per la digitalizzazione** della Pubblica Amministrazione e rende possibile la sua modernizzazione con la diffusione di soluzioni tecnologiche e organizzative che consentono un forte recupero di produttività.
- Ha lo scopo di assicurare e regolare la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando con le modalità più appropriate le ICT all'interno della PA, nei rapporti tra amministrazione e privati
- Emanato con decreto legislativo **n. 82 del 7 marzo 2005**, il Codice è entrato in vigore il 1 gennaio 2006. La versione vigente è la versione aggiornata con le modifiche e le integrazioni introdotte dal decreto legislativo n. 217 del 13 dicembre 2017. Ulteriori cambi sono stati inseriti con **il DL Semplificazione 2020.**

Il CAD - Finalità e principi ispiratori

Il CAD è finalizzato a promuovere e regolare l'informazione digitale sotto diversi aspetti:

Il CAD si basa su **due principi**:

Effettività

Introduzione di **misure premiali** incentivando le Amministrazioni virtuose e **misure sanzionatorie** nei confronti delle Amministrazioni inadempienti.

Risparmi

La **razionalizzazione della organizzazione** e la informatizzazione dei procedimenti fa ottenere risparmi destinati al finanziamento di **progetti di innovazione.**

Il CAD - Obiettivi e benefici

Rendere più efficace la pubblica amministrazione
sistematizzando e accelerando il processo di digitalizzazione

Obiettivi

- Snellimento della burocrazia della PA;
- semplificazione del dialogo tra PA-imprese-cittadini;
- maggiore efficienza del sistema produttivo;
- riduzione dei tempi per la formazione delle pratiche;
- riduzione degli spazi per l'archiviazione;
- riduzione dei costi per il funzionamento della PA;
- piena esigibilità dei servizi forniti dalla PA.

Benefici

- azzeramento dei certificati (trasmissione dei documenti tra Amministrazioni e condivisione dei database);
- uso della posta elettronica (comunicazioni solo attraverso e-mail);
- digitalizzazione degli archivi (conservazione digitale);
- promozione dei servizi on line (procedimenti pubblici digitalizzati).

Perché un nuovo CAD

- Ad oltre dieci anni dall'emanazione, nel 2017, **il Parlamento ha delegato il Governo** a intervenire sul CAD al fine di promuovere e rendere effettivi i diritti di **cittadinanza digitale** di cittadini e imprese**.**

- Si è voluto accelerare l'attuazione dell'Agenda digitale europea, armonizzando il CAD con:
  - ✓ **la disciplina comunitaria del Regolamento eIDAS;**
  - ✓ **il «Piano Triennale per l'informatica nella Pubblica Amministrazione»,** la strategia del Paese per l'attuazione del digitale a livello nazionale.

Il Regolamento eIDAS

- Il Regolamento eIDAS (electronic IDentification Authentication and Signature) - **Regolamento UE n° 910/2014 sull'identità digitale** fornisce una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri ovvero servizi offerti in Rete la cui «***affidabilità***» è garantita a cittadini o imprese dalla natura stessa e dal meccanismo di erogazione del servizio.
- Fissa le condizioni per cui ciascuno Stato membro possa **notificare i sistemi di identificazione elettronica** forniti ai propri cittadini e imprese ai fini del mutuo riconoscimento.
- È stato emanato il 23 luglio 2014, è entrato in vigore direttamente in tutti gli Stati Membri il 17 settembre 2014 e ha piena efficacia dal **1 luglio 2016.**

Il Regolamento eIDAS - Obiettivi

- Instaurare la **fiducia online** per agevolare lo sviluppo economico e sociale.
- Realizzare una **base comune** per interazioni elettroniche sicure fra imprese, cittadini e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'ebusiness e del commercio elettronico, nell'Unione europea.
- Eliminare gli ostacoli **all'esercizio dei diritti** dei cittadini dell'Unione.
- Consentire ai cittadini di utilizzare la loro **identificazione elettronica** per autenticarsi in un altro Stato membro.
- Responsabilità dello **Stato membro notificante**, in merito ai sistemi di identificazione e autenticazione riconosciuti dallo stesso.
- Mutuo e pieno riconoscimento della **firma digitale.**
- Individuare formati delle **firme digitali** europei.
- Autenticazione dei **siti web.**

Il Regolamento eIDAS – Servizi fiduciari

- Nel regolamento eIDAS sono definiti **servizi fiduciari**:
  - ✓ servizi di creazione, verifica e convalida di **firme elettroniche**, **sigilli elettronici**, **validazioni temporali elettroniche**,
  - ✓ servizi elettronici di **recapito certificato**;
  - ✓ servizi di creazione, verifica e convalida dei **certificati di autenticazione di siti web;**
  - ✓ servizi di **conservazione di firme, sigilli o certificati elettronici.**
- Viene detto **servizio fiduciario qualificato** un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità
- I servizi fiduciari qualificati sono sottoposti al riconoscimento e alla vigilanza di appositi organismi governativi nazionali, in Italia l'AgID - Agenzia per l'Italia Digitale.
- I prestatori di **servizi fiduciari qualificati** sono autorizzati a caratterizzare il servizio qualificato offerto, attraverso l'uso del **marchio di fiducia UE.**

Rapporto tra eIDAS e normativa nazionale

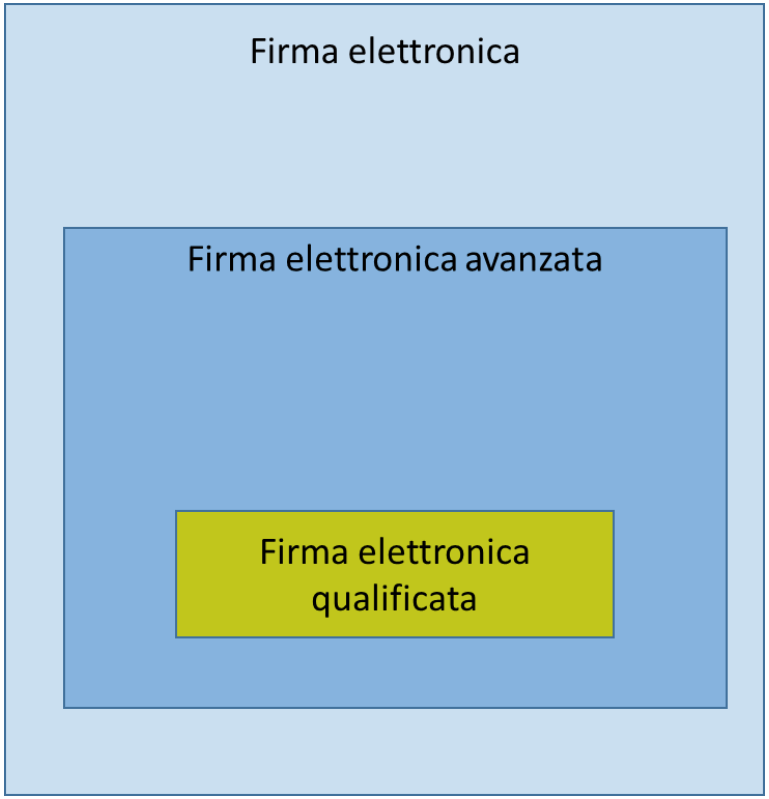
Considerando 49:

- «Il presente regolamento dovrebbe stabilire il principio secondo il quale **alla firma elettronica non dovrebbero essere negati gli effetti giuridici** per il motivo della sua forma elettronica o perché non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, **spetta al diritto nazionale** definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal presente regolamento secondo cui una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa.»

Firme elettroniche in eIDAS

Il Regolamento eIDAS riconosce 3 tipologie di firma elettronica:

- Firma elettronica semplice.
- Firma elettronica avanzata.
- Firma elettronica qualificata.



Regolamento eIDAS - Le firme

- **Firma Elettronica** - dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
- **Firma Elettronica Avanzata (FEA)** - firma elettronica che soddisfi i seguenti requisiti:
  - ✓ è connessa unicamente al firmatario;
  - ✓ è idonea a identificare il firmatario;
  - ✓ è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
  - ✓ è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
- **Firma Elettronica Qualificata (FEQ)** – che in aggiunta a quelle di una firma elettronica avanzata possiede queste caratteristiche:
  - ✓ è creata su un dispositivo qualificato per la creazione di una firma elettronica;
  - ✓ è basata su un certificato elettronico qualificato;
  - ✓ ha effetto giuridico equivalente a quello di una firma autografa.

Firma elettronica semplice

- «*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*».
- Considerata **debole.**
- Valenza probatoria **valutabile dal giudice.**

Firma elettronica semplice

Tipi di firma elettronica semplice

Esistono molti tipi di firma elettronica, descrivibili in base a:

- Metodo utilizzato.
- Finalità.
- Proprietà della firma.

Firma elettronica semplice

Tipi di firma elettronica semplice

Esistono molti tipi di firma elettronica, descrivibili in base a:

- Something You **Know.**
- Something You **Are.**
- Something You **Have.**

Firma elettronica avanzata

«firma elettronica che soddisfi i requisiti di cui all'articolo 26 del Regolamento eIDAS»

a) è connessa unicamente al firmatario;
b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Firma elettronica avanzata

Ulteriori requisiti

a) Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.
b)Individuazione del soggetto erogatore.
c) Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati.
d) Connessione univoca della firma al documento sottoscritto.

Firma elettronica avanzata

DPCM 22 febbraio 2013 Art. 60 - LIMITI D'USO DELLA FIRMA ELETTRONICA AVANZATA

«*La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche,* ***è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a).***»

Firma grafometrica

La firma grafometrica è un processo di firma che prevede **l'apposizione della firma autografa del cliente** su un **apposito tablet** con una **specifica penna**, mediante il quale è possibile collegare al documento elettronico un insieme di dati biometrici che garantiscono la connessione univoca tra documento firmato e firmatario.

Firma elettronica qualificata

eIDAS art. 3 c.1 n.12

«una firma elettronica avanzata

1. *creata da un **dispositivo** per la creazione di una firma elettronica qualificata*
2. *basata su un **certificato qualificato** per firme elettroniche»*

Certificato elettronico

«un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona»

Firma elettronica qualificata

eIDAS – formati di firma

Decisione di esecuzione (UE) 2015/1506

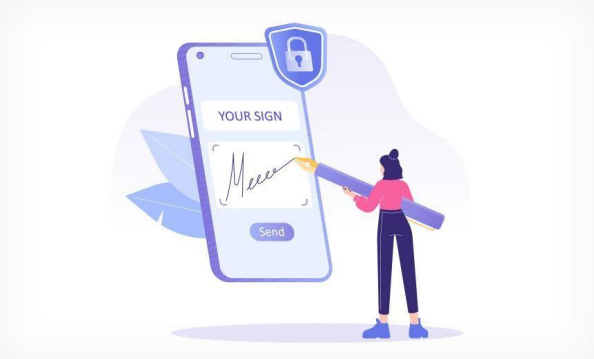
- CAdES (*.p7m)
- PAdES (*.pdf)
- XAdES (xml)

Firme elettroniche italiane

Firma remota – DPCM 22 febbraio 2013

«particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse»

HSM - *Hardware Security Module - è un dispositivo fisico attraverso il quale è possibile produrre e gestire chiavi digitali per la «strong authentication».*

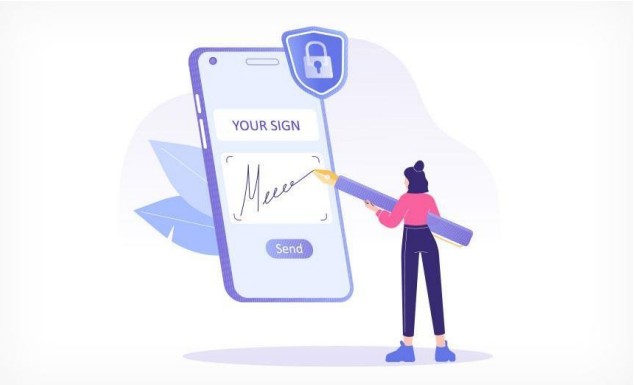


Firme elettroniche italiane

Firma remota – DPCM 22 febbraio 2013

Occorrente

- Connessione internet.
- Software di firma.
- Una OTP.



Firme elettroniche italiane

Firma remota – DPCM 22 febbraio 2013

Vantaggi

- Nessun vincolo di utilizzo di un **Hardware dedicato** né tantomeno di un **sistema operativo predefinito**.

Firme elettroniche italiane

Firma automatica – DPCM 22 febbraio 2013

«particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita ***previa autorizzazione del sottoscrittore*** *che mantiene il controllo esclusivo delle proprie chiavi di firma,* ***in assenza di presidio puntuale e continuo da parte di questo****»*

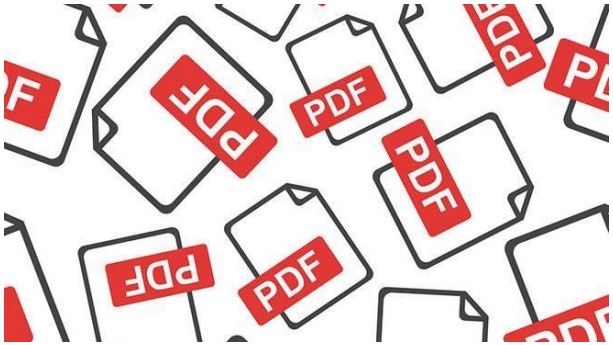


Tabella riassuntiva tipologie di firme elettroniche

Tipologie di Firme	Caratteristiche	Valore giuridico	Valore probatorio
Firma elettronica "semplice" (FE)	Sicurezza, integrità e immodificabilità.	Forma scritta.	Liberamente valutabile in giudizio dal giudice.
Firma elettronica avanzata (FEA)	FE + Art. 26 del Regolamento eIDAS e Titolo V del DPCM 22 febbraio 2013.	Forma scritta ex art. 2702 c.c. in ambito chiuso. Non può essere utilizzata per gli atti di cui ai punti da 1 a 12 dell'art. 1350 c.c..	Firma autografa riconducibile al titolare se la parte che vuole avvalersene ne dimostra la conformità con quanto prescritto al Titolo V del suddetto DPCM.
Firma elettronica qualificata (FEQ) e Firma digitale	FEA + dispositivo sicuro di firma + certificato qualificato.	Forma scritta ex art. 2702 c.c.	Firma autografa legalmente riconosciuta. Presunzione firma autografa ex art. 25 del Regolamento eIDAS. Presunzione sull'utilizzo del dispositivo sicuro di firma ex art. 20, comma 1 ter, del CAD da parte del titolare.

Il Sigillo Elettronico Qualificato

- Il sigillo elettronico qualificato è stato introdotto nel nostro ordinamento con l'emanazione del Regolamento eIDAS.
- Sostanzialmente **è equivalente a una firma elettronica qualificata**, con la differenza che **non afferisce a una persona fisica**, bensì a una persona giuridica.
- In altri termini, mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice fiscale ecc., **da un sigillo possiamo risalire con certezza ad una persona giuridica** attraverso la sua denominazione, partita IVA o codice fiscale, ma non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.

Linee portanti del nuovo CAD

- L'attenzione del legislatore si è spostata **dal processo di digitalizzazione ai diritti digitali di cittadini e imprese.**
- Le **linee portanti** del nuovo intervento legislativo sono:
  - ✓ la deregolamentazione, attribuendo ad **AgID competenza all'emanazione di linee guida**, strumento di regolazione flessibile, contenenti **regole tecniche** spesso soggette a cambiamenti legati all'evoluzione tecnologica;
  - ✓ la **natura di «Carta di cittadinanza digitale» dei cittadini e delle imprese** per:
    - accelerare il **diritto alla fruizione di servizi on line** semplici e mobile-oriented;
    - partecipare effettivamente al **procedimento amministrativo** per via elettronica;
    - promuovere la completa adozione degli strumenti di identità digitale SPID e di pagamento elettronico PagoPa;
  - ✓ la promozione dei processi di **interoperabilità tra i servizi** erogati dalle diverse amministrazioni;
  - ✓ l'utilizzo più efficace dei dati pubblici attraverso la realizzazione di piattaforme tecnologiche e **soluzioni di data analysis** per un accesso unitario e semplificato.

CAD – La struttura

- **Capo I** - PRINCIPI GENERALI (1 – 19)
- **Capo II** - DOCUMENTO INFORMATICO, FIRME ELETTRONICHE, SERVIZI FIDUCIARI E TRASFERIMENTI DI FONDI (20 – 39)
- **Capo III** – GESTIONE, CONSERVAZIONE E ACCESSIBILITA' DEI DOCUMENTI E FASCICOLI INFORMATICI (40 – 44 bis)
- **Capo IV** - TRASMISSIONE INFORMATICA DEI DOCUMENTI (45 – 49)
- **Capo V** - DATI DELLE PUBBLICHE AMMINISTRAZIONI, IDENTITA' DIGITALI, ISTANZE E SERVIZI ON-LINE (50 – 66)
- **Capo VI** - SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI (67 – 70)
- **Capo VII** - REGOLE TECNICHE (71)
- **Capo VIII** - SISTEMA PUBBLICO DI CONNETTIVITA‘ (72 – 87)
- **Capo IX** - DISPOSIZIONI TRANSITORIE FINALI E ABROGAZIONI (88 – 92)

Le novità – art. 1

- Sono state **soppresse le diverse definizioni di firma elettronica**, che sono invece contenute nel Regolamento eIDAS e resta solo la definizione di **firma digitale**, che è una tipologia tutta italiana – *particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;*
- la definizione di **documento informatico** racchiude anche quella di documento elettronico del Regolamento eIDAS . Infatti:
  - documento elettronico - *qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;*
  - documento informatico - *il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;*
- la definizione di **domicilio digitale** diventa: *un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale.*

Le novità – art. 2

- L'ambito di applicazione, oltre che alle PA e alle società a controllo pubblico non quotate, viene **ampliato ai gestori di servizi pubblici in relazione ai servizi di pubblico interesse.**
- Inoltre, si applica a:
  - ✓ **Privati**: relativamente a comunicazioni elettroniche, documenti informatici, firme elettroniche, servizi fiduciari, conservazione dei documenti informatici, domicilio digitale, identità digitale e servizi in rete;
  - ✓ **Organismi di diritto pubblico**: relativamente all'accesso ai documenti informatici e alla fruibilità delle informazioni digitali.

- E' **applicabile a tutte le tipologie di processi telematici** (civile, penale, amministrativo, contabile e tributario) salvo che non vi siano disposizioni diverse in materia;
- è **applicabile agli atti di liquidazione, rettifica, accertamento e irrogazione delle sanzioni di natura tributaria**, previo DPCM su modalità e termini.

Le novità – art. 3bis, 6, 6bis, 6ter, 6quater

- **il domicilio digitale nasce per assegnare a imprese e cittadini un recapito su cui ricevere tutte le comunicazioni in** formato elettronico, inviate da PA, gestori di servizi pubblici e da privati, aventi valore legale;
- è un indirizzo online di PEC o di servizio di recapito certificato qualificato **destinazione di ogni comunicazione avente valore di notifica;**

  - gli indirizzi di **PA e gestori di servizi pubblici** sono inseriti nell'**indice IPA** gestito da AgID;
  - gli indirizzi di **imprese e professionisti iscritti in albi ed elenchi** sono inseriti nell'**indice INI-PEC;**
  - gli indirizzi di cittadini e enti non presenti nei precedenti indici sono inseriti nell'**indice delle persone fisiche e altri enti di diritto privato (INAD).**

- **i cittadini potranno**, non obbligatoriamente, scegliere di eleggere un **domicilio digitale;**
- **con DPCM verrà stabilita la data a decorrere dalla quale verranno inviate comunicazioni solo telematiche.**

Il CAD - Diritti dei cittadini e delle imprese esigibili nei rapporti con la PA (1/2)

Le Pubbliche Amministrazioni, attraverso l'adozione delle tecnologie informatiche, sono chiamate ad una vera e propria **riorganizzazione strutturale e gestionale interna** in vista del raggiungimento degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.

All'interno di questo scenario **il CAD ha attribuito a cittadini e imprese diritti** esigibili nei rapporti con la PA. In particolare:

Art. 3 - Diritto all'uso delle tecnologie

I cittadini e le imprese hanno il diritto a richiedere e ottenere **l'uso delle moderne tecnologie informatiche** nelle comunicazioni con le Amministrazioni dello Stato. Ogni cittadino può indicare alla Pubblica Amministrazione un proprio indirizzo di posta elettronica certificata quale suo **domicilio digitale**.

Art. 5 – Effettuazione di pagamenti con modalità informatiche

I cittadini e le imprese hanno il diritto di effettuare ogni tipo di pagamento verso la Pubblica Amministrazione attraverso le tecnologie informatiche e telematiche: **piattaforma pagoPA**

Il CAD - Diritti dei cittadini e delle imprese esigibili nei rapporti con la PA (2/2)

Art. 7 - Qualità dei servizi resi e soddisfazione dell'utenza

I cittadini e le imprese hanno diritto a **servizi pubblici di qualità**, sulla base di una preventiva analisi delle loro reali esigenze. Le Pubbliche Amministrazioni, a tal fine, sviluppano l'uso delle tecnologie dell'informazione e della comunicazione e organizzano i servizi in modo da controllarne periodicamente **la qualità e la soddisfazione dell'utenza.**

Art. 8 - Alfabetizzazione informatica dei cittadini

Lo Stato promuove iniziative volte a favorire **l'alfabetizzazione informatica** dei cittadini, con particolare riguardo alle categorie a rischio di esclusione.

Art. 9 - Partecipazione democratica elettronica

I cittadini hanno diritto di partecipare al **processo democratico** e di esercitare i diritti politici e civili, sia individuali che collettivi, usufruendo delle possibilità offerte dalle nuove tecnologie.

Introduzione del principio "innanzitutto digitale" (c.d. digital first) per il procedimento amministrativo

- ***Art 3, comma 1-quater***. «La gestione dei procedimenti amministrativi è attuata dai soggetti di cui all'articolo 2, comma 2, in modo da consentire, mediante strumenti informatici, la possibilità per il cittadino di verificare anche con mezzi telematici i termini previsti ed effettivi per lo specifico procedimento e il relativo stato di avanzamento, nonché di individuare l'ufficio e il funzionario responsabile del procedimento.»
- La P.A. deve consentire a tutti gli interessati, anche da remoto e attraverso le tecnologie ICT, di verificare per ogni specifico procedimento amministrativo :
  - ✓ **i tempi di risposta previsti ed effettivi;**
  - ✓ **lo stato di avanzamento;**
  - ✓ **l'ufficio e il responsabile del procedimento.**

Le novità – art. 17

- **Ogni PA individua il Responsabile della transizione digitale** tra i dirigenti generali o le figure apicali;
- è previsto che tale responsabile possa esercitare **anche in forma associata;**

- essendo stata disattesa l'istituzione dell'ufficio del difensore civico digitale presso ogni PA, il nuovo CAD prevede l'**istituzione di un unico ufficio del Difensore Civico Digitale presso AgID** per raccogliere le segnalazioni dei cittadini e garantire il rispetto dei diritti di Cittadinanza digitale;
- al difensore civico, in possesso di requisiti di terzietà, autonomia ed imparzialità, non sono attribuiti poteri coercitivi, ma unicamente di "***moral suasion***" rispetto alle PA inadempienti.

Le novità – art. 20 –23ter

- Il **documento informatico soddisfa il requisito della forma scritta e ha l'efficacia probatoria quando**:
  - ✓ vi è apposta una firma digitale;
  - ✓ vi è apposta una firma elettronica qualificata;
  - ✓ vi è apposta una firma elettronica avanzata;
  - ✓ è formato da un autore che è stato identificato digitalmente, attraverso un processo, definito nelle Linee guida AgID, tale da garantire qualità, sicurezza, integrità, immodificabilità e riconducibilità al suo autore (firma elettronica avanzata integrata con SPID). Questa modalità può essere utilizzata anche per la presentazione di istanze e dichiarazioni telematiche (art. 65).
- **Per la copia per immagine su supporto informatico di un documento analogico** (scansione) **sono possibili forme certificate di acquisizione automatica**.
- **Possono essere prodotte mediante processi e strumenti** che dovranno assicurare che le copie abbiano forma e contenuto identici a quelli dei documenti da cui sono tratte, **non solo attraverso il raffronto dei documenti, ma anche attraverso la certificazione di processo** nei casi in cui si sia deciso di adottare tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Le novità – art. 29 – 37

- Sono recepite le indicazioni del regolamento eIDAS per la **qualificazione dei servizi fiduciari**:
  - ✓ firma digitale e validazione temporale;
  - ✓ certificati di autenticazione di siti web;
  - ✓ identità digitale (SPID per l'Italia);
  - ✓ servizio di recapito.
- le **qualifiche** sono convergenti con le regole comunitarie ma i dettagli operativi, quali **capitale sociale, certificazioni e altri requisiti richiesti, sono rimandati a un DPCM;**
- i procedimenti di qualifica non saranno più gratuiti;
- sono introdotte le sanzioni per i prestatori di servizi fiduciari qualificati.

Le novità – art. 45-48

- La **Posta Elettronica Certificata (PEC)** diventa lo strumento per realizzare il domicilio digitale;
- il **servizio elettronico di recapito certificato qualificato eIDAS** rispetto alla nostra PEC richiede la garanzia dell'identificazione del destinatario prima della trasmissione dei dati e anche un elevato livello di sicurezza per l'identificazione del mittente;
- la PEC è in corso di adeguamento alla normativa Europea.

Le novità – Le regole tecniche

Ai sensi dell'art.71 del CAD «L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del CAD.»

- **Linee guida del Modello di interoperabilità**
- **Linee guida acquisizione e riuso dei software per la P.A.**
- **Linee Guida dei Criteri di Qualificazione dei Cloud Service Provider**
- **Linee Guida dei Criteri di Qualificazione Servizi SaaS per il Cloud della PA**
- **Linee Guida sulla formazione del documento informatico –** emanate il 9 settembre 2020
- **Linee Guida sull' Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel Registro Imprese**
- **Linee guida di design per i siti internet e i servizi digitali della PA**
- **….**

Le novità sulla conservazione ex Decreto Semplificazione (D.L. 76/2020)

- **Per <u>la gestione e la conservazione dei documenti informatici</u> viene modificato l'articolato normativo**. In particolare:
  - ✓ la conservazione dei documenti informatici da parte di soggetti esterni all'amministrazione interessata deve uniformarsi - nel rispetto della disciplina europea - alle **Linee guida** contenenti le regole tecniche e di indirizzo per l'attuazione del CAD nonché ad un **regolamento**, le une come l'altro adottati dall'Agenzia per l'Italia digitale (AgID).
  - ✓ Il regolamento determina i **criteri** per la fornitura dei servizi di conservazione dei documenti informatici, affinché sia assicurata la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.
  - ✓ Le Linee guida determinano i **requisiti di qualità**, di **sicurezza e organizzazione**, che i soggetti conservatori debbono possedere.
  - ✓ Si pone l'accento cioè sul possesso di requisiti e su criteri di fornitura, non già ad un meccanismo di accreditamento in senso stretto **.**
  - ✓ Fino all'adozione del regolamento e delle Linee guida, in materia di conservazione dei documenti informatici si applicano le disposizioni vigenti al momento dell'entrata in vigore del decreto-legge.

Il CAD - L'innovazione nella PA

- L'innovazione è intesa come **riorganizzazione delle funzioni**, **delle strutture e degli strumenti** per il raggiungimento di obiettivi di miglioramento dei servizi al cittadino.
- Innovare non comporta legiferare/regolamentare per **introdurre la tecnologia** nei procedimenti amministrativi tradizionali.
- In pratica non si deve **progettare il futuro con i limiti e i difetti del presente** e si finisce per pianificare interventi minimali per la gestione dei sistemi funzionali all'amministrazione amministrativa.

È necessario un cambiamento organizzativo della PA attraverso
la reingegnerizzazione dei processi e dei flussi di lavoro

Le pubbliche amministrazioni devono quindi…

- **utilizzare la posta certificata** per tutte le comunicazioni che necessitano di una ricevuta di invio e di una di consegna verso cittadini, professionisti, imprese che hanno preventivamente comunicato il proprio indirizzo di PEC;
- **istituire almeno una casella di posta elettronica certificata** collegata al registro di protocollo;
- **pubblicare i propri indirizzi di posta elettronica certificata** nell'Indice delle Pubbliche amministrazioni, che costituisce la rubrica degli indirizzi delle amministrazioni, accessibile e consultabile da tutti;
- **pubblicare i propri indirizzi di posta elettronica certificata sul proprio sito** istituzionale al fine di consentire al cittadino l'inoltro di richieste in modalità telematica.

Gli strumenti per la cittadinanza digitale: SPID, ANPR, PagoPA

SPID: Cos'è

Il nuovo sistema di login che permette a cittadini e imprese di accedere con un'UNICA IDENTITÀ DIGITALE ai servizi online pubblici e privati in maniera semplice, sicura e veloce

UN UNICO ACCESSO PER TUTTI I SERVIZI.

Da pc, smartphone e tablet

A decorrere dal 10 settembre 2019 l'identità digitale SPID può essere usata per l'accesso ai servizi in rete **di tutte le pubbliche amministrazioni dell'Unione**.

SPID: Modello di funzionamento e caratteristiche

Il funzionamento

Come è fatto

- L'**identità SPID** è costituita da credenziali di accesso (userid, password) che hanno caratteristiche diverse in base ai **3 livelli di sicurezza** esistenti

Livelli di sicurezza

- PA e privati definiscono il **livello di sicurezza** necessario per accedere ai propri servizi
- Le identità di livello superiore comprendono quelle di livello inferiore

Chi la eroga

- I **Gestori di Identità Digiale**, soggetti privati accreditati da AgID **rilasciano Identità Digitali** ai cittadini e alle imprese che le richiedono

La scelta

- **Ogni cittadino potrà scegliere il Gestore** che preferisce
- Un cittadino potrà avere **più di un ID** anche **con più Gestori**
- Tutti i gestori garantiscono di rispettare le **regole emanate da AgID**

Livelli di sicurezza

L'identità **SPID** di **primo livello** permette l'autenticazione tramite un fattore di sicurezza (es. **ID e password** scelta dall'utente)

L'identità **SPID** di **secondo livello** permette l'autenticazione tramite due fattori di sicurezza (es. **ID e password** + generazione di una **One Time Password** inviata all'utente)

L'identità **SPID** di **terzo livello** permette l'autenticazione tramite due fattori di sicurezza attraverso **strumenti certificati** (es. **ID e password** + **dispositivo di accesso** (es. smart card)

SPID oggi

SPID Sistema pubblico di identità digitale	
Identità SPID erogate	34.691.233
Gestori di identità digitale attivi	10
Amministrazioni attive	14.048
Fornitori di Servizi privati attivi	155

L’ecosistema SPID

- Il Sistema Pubblico di Identità Digitale si compone di **diversi attori:**
  - ✓ **i gestori dell’identità digitale** (identity provider o IdP), soggetti privati accreditati da AgID per la creazione e la gestione delle identità digitali degli utenti;
  - ✓ **i fornitori di servizi** (service provider o SP), organizzazioni pubbliche o private che, abilitando l’accesso ai propri servizi online tramite l’identità digitale, consentono una fruizione veloce, sicura e protetta ai servizi;
  - ✓ **gli utenti (cittadini e imprese)** che dispongono della propria identità digitale, certificata da uno o più gestori, per accedere ai servizi online della Pubblica Amministrazione e dei privati aderenti.

SPID e l’Europa

- Tutte le pubbliche amministrazioni che rendono accessibili i propri servizi online con credenziali SPID di livello 2 o 3 (come anche attraverso la carta di identità elettronica), hanno **l’obbligo di rendere accessibili detti servizi** anche con gli strumenti di autenticazione notificati dagli altri Stati membri.
- Non rispettare tale obbligo, implica esporsi a una **procedura di infrazione** per violazione dell’articolo 6 del regolamento eIDAS.

Firma SPID 1/2

- Nel tipico scenario d'uso un Service Provider (SP) propone all'utente, che si è già autenticato presso il SP mediante la propria identità digitale SPID, di **sottoscrivere un documento** (ad esempio, un contratto con il SP stesso).
- Se l'utente accetta, il SP predispone un modello di documento, apponendovi un **"invisibile" strumento fiduciario** chiamato **sigillo elettronico qualificato** ("QSeal") e lo invia all'Identity Provider (IdP) prescelto dall'utente.
- Per il momento, **il PDF/A-2** su cui sono apposti sigilli elettronici PAdES è l'unico formato di file previsto per la firma con SPID.

Firma SPID 2/2

- L’IdP autentica nuovamente l’utente (tramite credenziali di livello minimo 2), consentendo all’utente di **visionare l’intero documento** presso la propria piattaforma online.
- L’IdP richiede all’utente di **acconsentire esplicitamente alla sottoscrizione dello stesso** (eventualmente in più punti).
- Terminata l’acquisizione del consenso (ovvero dei consensi, nel caso di firme multiple), **l’IdP sigilla** ulteriormente il documento apponendovi il proprio invisibile Qseal.
- L’IdP consente all’utente di **visualizzare e scaricare il file PDF** così risigillato, che costituisce il **documento firmato con SPID**.

SPID e i minori – Linee guida

Con l'identità digitale dei minori si mira a garantire il raggiungimento dei seguenti obiettivi:

1. rilasciare SPID ai minori **previa richiesta da parte di chi esercita la responsabilità genitoriale;**

2. consentire al minore di **utilizzare la propria identità digitale SPID autonomamente** ferma restando la possibilità di controllo da parte dei genitori;

3. impedire ai minori di **accedere ai servizi in rete non destinati a loro**;

4. consentire **la selezione dei fruitori dei servizi in rete in base all'età**;

5. garantire che i dati personali del minore siano trattabili solo in presenza dello specifico consenso al trattamento da parte del titolare della responsabilità genitoriale o, qualora, ultraquattordicenne, del minore stesso.

SPID e i minori – Linee guida

1. Garantire che l'identità digitale sia rilasciata al minore **esclusivamente previa richiesta del genitore.**

2. Consentire al genitore di **avere evidenza delle identità digitali rilasciate** ai propri figli minori.

3. Consentire al genitore di gestire le identità digitali rilasciate ai propri figli minori con la **possibilità di revocare le singole autorizzazioni all'accesso ai servizi** della società dell'informazione o la stessa identità digitale del minore.

4. Garantire che **nessun dato del minore sia fornito ai SP in assenza del consenso del genitore** e del minore che ha compiuto almeno quattordici anni.

5. **Informare il genitore in merito al rilascio dell'identità digitale** al figlio minore.

Anagrafe Nazionale della Popolazione Residente (ANPR)

Un'unica banca dati anagrafica che subentra alle oltre 8.000 Anagrafi comunali e alla Anagrafe degli Italiani Residenti all'Estero. Permette di:

- eliminare gli adempimenti a carico dei cittadini in caso di variazione dei dati anagrafici;
- integrare altri servizi e basi dati nazionali (INPS, …);
- fornire il censimento permanente della popolazione;
- allineare gli indirizzi con l'Anagrafe nazionale dei numeri civici e delle strade urbane (ANNCSU).

Soggetti coinvolti: Ministero dell'interno, AgID, Istat, Anci in rappresentanza dei Comuni, Cisis per le Regioni, Sogei in qualità di fornitore

ANPR oggi

ANPR
Anagrafe Nazionale Popolazione Residente

ANPR

Anagrafe nazionale della popolazione residente

Popolazione presente in ANPR	59.674.978
Comuni subentrati	7.904
Comuni in pre-subentro	0

pagoPA: sistema dei pagamenti a favore della PA

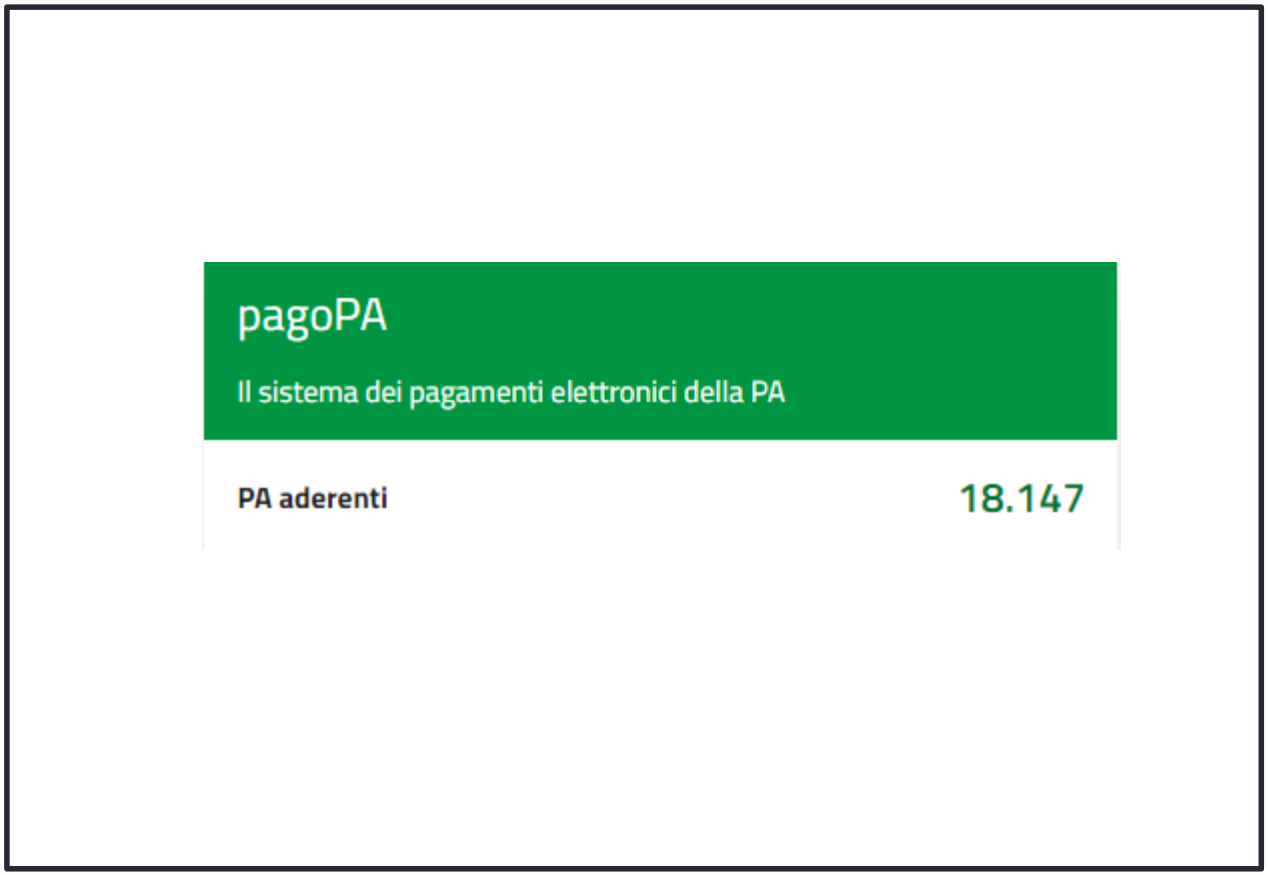
Tutte le Pa sono tenute ad accettare pagamenti elettronici.
Il sistema di integrazione tra banche e PA - Nodo dei pagamenti - realizzato da AGID e Banca d'Italia, è attivo ed è gratuitamente disponibile per tutte le PA

Permette di:

- effettuare qualsiasi pagamento in modalità elettronica verso le PA, con la stessa interfaccia utilizzata nei siti di e-commerce;
- velocizzare la riscossione degli incassi ed effettuare la relativa riconciliazione in modo certo e automatico, con conseguente riduzione di contestazioni, reclami e contenziosi, lato PA.

Soggetti coinvolti: Società di servizi PagoPA (prima AgID), tutte le PA, Banca d'Italia, Prestatori di servizi di pagamento

pagoPA oggi


pagoPA
Il sistema dei pagamenti elettronici della PA
PA aderenti
18.147

Esistono sanzioni per il mancato rispetto del CAD?

CAD, Art. 12 comma 1 ter:

- I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le **eventuali responsabilità penali, civili e contabili** previste dalle norme vigenti.
- L'attuazione delle disposizioni del presente decreto è comunque **rilevante** ai fini della misurazione e valutazione della **performance organizzativa ed individuale dei dirigenti.**

CAD art. 17 comma 1 quater – Il difensore civico

- Il Difensore civico per il digitale, come detto, è una figura prevista dal Codice dell'amministrazione digitale a **garanzia dei diritti digitali** di cittadini e imprese.
- I diritti di cittadinanza digitali, a livello giuridico, si concretizzano principalmente nella possibilità per il cittadino e le imprese di utilizzare l'identità digitale, il domicilio digitale, i pagamenti con le modalità informatiche e la comunicazione mediante le tecnologie dell'informazione.

- A livello etico e formativo, la cittadinanza digitale, inoltre, si può definire come **l'unione tra l'educazione civica e l'educazione digitale**, quindi da un lato la formazione ai propri diritti e doveri come cittadini e dall'altro la consapevolezza che le azioni che si effettuano **on-line e off-line** hanno un impatto nel presente e nel futuro per sé stessi e per gli altri.

Il difensore civico – I compiti

Il Difensore civico ha **una duplice funzione**:

- **Funzione A -** raccoglie le segnalazioni relative alle presunte violazioni del Codice dell'Amministrazione Digitale (CAD) o di ogni altra norma in materia di digitalizzazione ed innovazione, (art.17, comma 1 quater del CAD).
- **Funzione B -** in caso di contestazione sulla dichiarazione di accessibilità o di esito insoddisfacente del monitoraggio decide in merito alla **corretta attuazione della legge sulla accessibilità** agli strumenti informatici per le persone con disabilità. In caso di reclami di utenti relativi a dichiarazioni di accessibilità dispone eventuali misure correttive. (art.3-quinquies della legge n.4/2004).

Decreto Semplificazioni 2021

- Il decreto attribuisce nuovi poteri di vigilanza all'AgID "*al fine di assicurare l'attuazione dell'Agenda digitale italiana ed europea, la digitalizzazione dei cittadini, delle pubbliche amministrazioni e delle imprese, con specifico riferimento alla realizzazione degli obiettivi fissati dal Piano nazionale di ripresa o di resilienza*";
- Per raggiungere l'obiettivo l'Agid viene anche dotata di un **potere sanzionatorio**:
  - ✓ le amministrazioni che non ottemperano alla "richiesta di dati, documenti o informazioni" o violano "gli obblighi di transizione digitale" rischiano **multe da 10mila a 100mila euro.**

D.L. 77/2021 CAD, Art. 18 BIS
Violazione degli obblighi di transizione digitale

- L'AgID esercita poteri di **vigilanza, verifica, controllo e monitoraggio** sul rispetto delle disposizioni del Codice e di ogni altra norma in materia di innovazione tecnologica e digitalizzazione della pubblica amministrazione, ivi comprese quelle contenute nelle Linee guida e nel Piano triennale per l'informatica nella pubblica amministrazione, e procede, **d'ufficio ovvero su segnalazione del difensore civico digitale**, all'accertamento delle relative violazioni.
- Nell'esercizio dei poteri di vigilanza, verifica, controllo e monitoraggio, l'AgID richiede e acquisisce presso i soggetti di cui all'articolo 2, comma 2, **dati, documenti e ogni altra informazione strumentale e necessaria**. La mancata ottemperanza alla richiesta di dati, documenti o informazioni di cui al secondo periodo ovvero la trasmissione di informazioni o dati parziali o non veritieri è punita ai sensi del comma 5, con applicazione della sanzione ivi prevista ridotta della metà.

D.L. 77/2021 CAD, Art. 18 BIS
Violazione degli obblighi di transizione digitale

- L'AgID, quando dagli elementi acquisiti risulta che sono state commesse una o più violazioni delle disposizioni di cui al comma 1, procede alla **contestazione nei confronti del trasgressore**, assegnandogli un **termine perentorio** per inviare scritti difensivi e documentazione e per chiedere di essere sentito.
- Il termine perentorio è **proporzionato** rispetto al tipo e alla gravità della violazione, per conformare la condotta agli obblighi previsti dalla normativa vigente, **segnalando le violazioni all'ufficio competente per i procedimenti disciplinari di ciascuna amministrazione**, nonché ai competenti organismi indipendenti di valutazione.
- L'AgID pubblica le predette segnalazioni su apposita area del proprio sito internet istituzionale.
- La disciplina per la vigilanza e per l’esercizio del potere sanzionatorio previsto dall’articolo 18-bis è oggetto di **apposito Regolamento** adottato dall'Agenzia.

D.L. 77/2021 CAD, Art. 18 BIS
Violazione degli obblighi di transizione digitale

- Le violazioni accertate dall'AgID **rilevano ai fini della misurazione e della valutazione della performance individuale dei dirigenti responsabili** e comportano responsabilità dirigenziale e disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165.
- Contestualmente all'irrogazione della sanzione nei casi di violazione delle norme specificamente indicate al comma 5, nonché di violazione degli obblighi di cui all'articolo 13-bis, comma 4, l'AgID **segnala la violazione alla struttura della Presidenza del Consiglio dei ministri** competente per l'innovazione tecnologica e la transizione digitale, la quale, ricevuta la segnalazione, **diffida ulteriormente il soggetto** responsabile a conformare la propria condotta agli obblighi previsti dalla disciplina vigente entro un congruo termine perentorio, proporzionato al tipo e alla gravità della violazione, avvisandolo che, in caso di inottemperanza, potranno essere esercitati i poteri sostitutivi del Presidente del Consiglio dei ministri o del Ministro delegato.
- Decorso inutilmente il termine, il Presidente del Consiglio dei ministri o il Ministro delegato per l'innovazione tecnologica e la transizione digitale, valutata la gravità della violazione, può nominare un **commissario ad acta** incaricato di provvedere in sostituzione.

Il manuale di gestione 1/5

- Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici prevedono che il Responsabile della gestione documentale per quanto riguarda tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, CAD adotti il manuale di gestione.
- Il manuale di gestione descrive il sistema di gestione documentale dei documenti informatici , anche ai fini della conservazione, a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna…
- ….fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
- Obiettivo del Manuale di gestione è anche descrivere le funzionalità disponibili per gli addetti al servizio e per i soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il manuale di gestione 2/5


COMUNE DI GAETA

MANUALE

- Il manuale di gestione documentale dunque nel nostro ordinamento è lo strumento cui è demandata:
  - ✓ la descrizione dei sistemi di gestione e conservazione dei documenti;
  - ✓ la regolamentazione per il funzionamento del servizio per la tenuta del protocollo informatico;
  - ✓ la regolamentazione per la gestione dei flussi documentali e degli archivi, all'interno di ogni aerea organizzativa omogenea (AOO).
- Nel tempo sono stati prodotti vari modelli di Manuali di gestione utili per le amministrazioni che non hanno le necessarie risorse per redigerli in autonomia.
- In un contesto caratterizzato da incessante trasformazione, il manuale di gestione documentale deve essere sottoposto a **continuo aggiornamento**, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati.

Il manuale di gestione 3/5


COMUNE DI GAETA

MANUALE

- L’adozione del manuale di gestione documentale e del manuale di conservazione non risponde solo ad esigenze pratico-operative, ma **rappresenta un preciso obbligo**;
- la PA ha l’ulteriore obbligo della sua pubblicazione sul sito istituzionale dell’ente in una parte chiaramente identificabile dell’area “Amministrazione trasparente” prevista dall’art. 9 del d.lgs. 33/2013;
- la PA nel Manuale di gestione descrive inoltre specifiche politiche e procedure adottate dall’ente al fine di garantire la disponibilità e la riservatezza delle informazioni contenute nel documento informatico, in conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali.

Il manuale di gestione 4/5


COMUNE DI GAETA

MANUALE

Sempre dalle Linee guida:

- La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis11, 40 -bis12 e 6513 del CAD.
- Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.
- Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici.
- Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il manuale di gestione 5/5


COMUNE DI GAETA

MANUALE

Sempre dalle Linee guida:

- Il manuale conterrà inoltre, come parte integrante dello stesso, il **piano per la sicurezza informatica**, per la quota parte di competenza, nel rispetto delle:
  - ✓ **misure di sicurezza** predisposte dagli organismi preposti;
  - ✓ **disposizioni in materia di protezione dei dati personali** in linea con l'analisi del rischio fatta;
  - ✓ indicazioni in **materia di continuità operativa** dei sistemi informatici.
- Il manuale conterrà inoltre, relativamente alle azioni di classificazione e selezione:
  - ✓ **il piano di classificazione** adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle **procedure di scarto**.

Il Manuale di conservazione

- Le Pubbliche Amministrazioni sono tenute a:
  - ✓ redigere,
  - ✓ adottare con provvedimento formale,
  - ✓ pubblicare sul proprio sito istituzionale il Manuale di conservazione.
- La pubblicazione deve avvenire in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

A chi è rivolto

- Il Manuale della conservazione è un **documento obbligatorio anche per i privati** che conservano i propri documenti in modalità informatica.
- L'obbligatorietà per le pubbliche amministrazioni e i privati riguarda l'individuazione delle tipologie documentali trattate e dei relativi metadati da associare, le modalità e i tempi di trasmissione dei pacchetti di versamento e le tempistiche di selezione e scarto dei propri documenti informatici.

- Dobbiamo immaginare il manuale come un **contenitore** che **racchiude tutto il processo** che riguarda la conservazione dei documenti informatici di un'organizzazione.
- Pertanto, al suo interno sarà necessario descrivere le attività del personale coinvolto in questo processo, le tipologie documentali trattate dall'organizzazione (fatture, documenti di trasporto, mail, PEC e altre ancora) e con quali modalità queste vengono prodotte e conservate per far sì che si garantiscano **i criteri di autenticità, integrità, affidabilità, leggibilità e reperibilità.**

Chi scrive il Manuale: la figura del Responsabile della Conservazione

- Per redigere il Manuale della Conservazione si devono possedere adeguate competenze archivistiche, informatiche e gestionali.
- All'interno di ogni PA deve essere identificata una figura che le possiede tutte: il **Responsabile della Conservazione**.
- All'interno delle Pubbliche Amministrazioni il Responsabile della Conservazione dev'essere obbligatoriamente nominato internamente.
- Per le aziende private, invece, questa figura può anche essere demandata esternamente. Attenzione, però: se ci si avvale di un servizio di conservazione in outsourcing → **il Responsabile della Conservazione non può essere il conservatore**.
- Il Manuale della Conservazione, quindi, **deve essere redatto dal Responsabile della Conservazione.**

Il Manuale di conservazione

- Nel **manuale di conservazione** sono formalizzati i requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione.
- Illustra dettagliatamente:
  - ✓ l'organizzazione,
  - ✓ i soggetti coinvolti e i ruoli svolti dagli stessi,
  - ✓ il modello di funzionamento,
  - ✓ la descrizione del processo, delle architetture e delle infrastrutture utilizzate,
  - ✓ le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Le scelte di carattere prettamente archivistico sono di competenza delle istituzioni archivistiche.

Manuale di conservazione – contenuti 1/2

- I dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema;
- la struttura organizzativa;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione;
- la descrizione delle modalità di presa in carico dei pacchetti di versamento e generazione del rapporto di versamento;
- la descrizione del processo di conservazione dei pacchetti di archiviazione;
- la modalità di produzione del pacchetto di distribuzione;

Manuale di conservazione – contenuti 2/2

- la descrizione del **sistema di conservazione**, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime;
- la descrizione delle **procedure di monitoraggio** della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi;
- la descrizione delle **procedure per la produzione di duplicati o copie**;
- i tempi entro i quali le diverse tipologie di documenti devono essere **scartate** o trasferite in conservazione qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel **piano di conservazione** allegato al manuale di gestione documentale;
- le modalità con cui viene richiesta la presenza di un **pubblico ufficiale**.

Il sistema di gestione documentale

Il sistema documentario ha un ruolo essenziale di supporto

- è il **fulcro** di tutte le attività dell'Ente;
- garantisce **trasparenza** e controllo;
- soprintende il "**Ciclo di Vita del documento**" dall a sua formazione

Regole tecniche per la formazione del documento informatico

E’ importante stabilire tutte le modalità con le quali produrre:

- un documento informatico che abbia **pieno valore legale**;
- un **duplicato o una copia** di documenti analogici e di documenti i nformatici;
- un **fascicolo** informatico.

Il documento informatico

- Secondo e-IDAS il **documento elettronico** è **qualsiasi contenuto** conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva.
- Secondo il CAD **il documento informatico** è il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
- Dal punto di vista informatico è un **insieme di valori binari** la cui materialità è data dal sistema e dal supporto informatico in cui è memorizzato.
- Può essere **modificato o riprodotto infinite volte**, ottenendo copie assolutamente identiche all'originale.
- Il suo contenuto è **svincolato** dal supporto.

Regole - Documento informatico

Documento informatico “**nativo**”

Documento informatico da documento analogico

Registrazione informatica, generazione o raggruppamento di insiemi di dati da basi di dati (viste)

Regole - Documento informatico

Modalità per rendere un documento informatico immodificabile

Documento informatico “nativo”

- sottoscrizione con firma digitale ovvero con firma elettronica qualificata
- apposizione di una validazione temporale
- trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa
- memorizzazione su sistemi di gestione documentale che adottino politiche di sicurezza
- riversamento ad un sistema di conservazione
- per le PA con la registrazione nel registro di protocollo, repertori o albi

Regole - Documento informatico

Modalità per rendere un documento informatico immodificabile

Documento informatico da documento analogico

memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione

Regole - Documento informatico

Modalità per rendere un documento informatico immodificabile

Registrazione informatica, generazione o raggruppamento di insiemi di dati da basi di dati (viste)

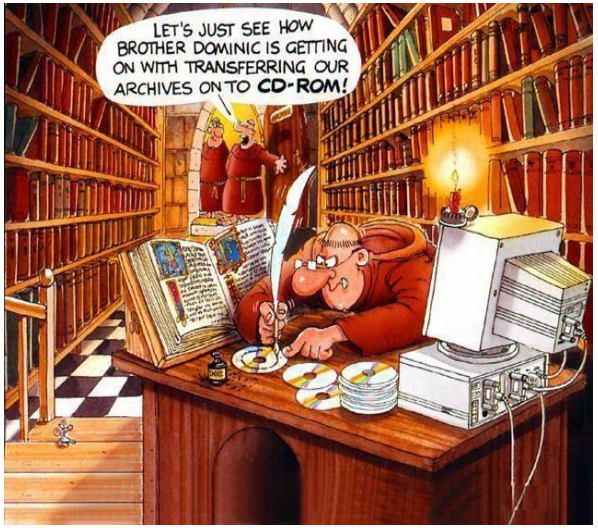
operazione di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema

produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione

In conclusione la digitalizzazione richiede innovazione e gradualità …

“Non si manda via un’abitudine buttandola dalla finestra, ma occorre farle scendere le scale, un gradino dopo l’altro”.

Mark Twain



… e molta cooperazione…

If you want to go fast, go alone.
If you want to go far, go together

Grazie dell’attenzione

Dr.ssa Patrizia Gentili
pgentili60@gmail.com