

# Documenti informatici, firme elettroniche e conservazione

Avv. Andrea Lisi  
Torino - 2 febbraio 2016

Associazione Nazionale per Operatori e Responsabili  
della Conservazione Digitale

[www.anorc.it](http://www.anorc.it) mail: [segreteria@anorc.it](mailto:segreteria@anorc.it)



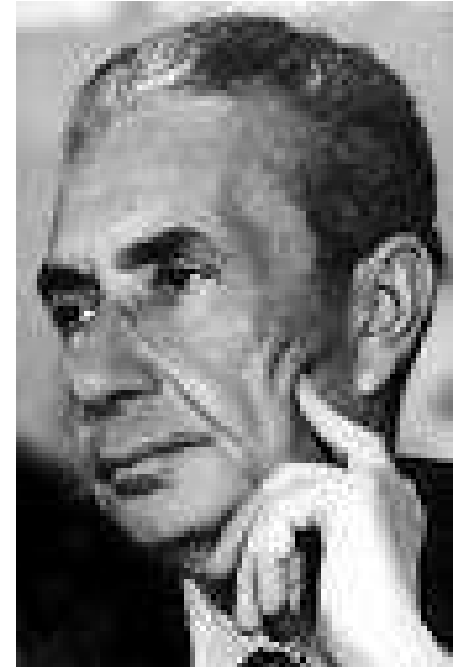
ATTENZIONE: L'utilizzo dei contenuti può causare effetti desiderati quali la fiducia nelle giovani generazioni, la collaborazione e contaminazione tra campi applicativi apparentemente distanti, la crescita di un pensiero critico.

*WARNING: The use of the content may cause desirable effects such as confidence in younger generations, collaboration and contamination between seemingly distant fields of application, growth of critical thinking.*

(di Maurizio Montalti,  
presentazione opere esposte  
presso il MAXXI di Roma – Mostra  
«tra arte e architettura»)

***Siate indipendenti. Non guardate al domani, ma al dopodomani***

(Aldo Moro)



L'Archivio di Stato di Roma ha pubblicato il volume **‘Le lettere di Aldo Moro dalla prigionia alla storia’** a cura di Michele Di Sivo, volume che propone tutte le immagini delle lettere inviate nei 55 giorni più lunghi della prima Repubblica da Aldo Moro. Tutte queste lettere sono note nel loro contenuto, ma solo ora sono state versate all'Archivio di Stato in quanto beni culturali e fonti della ricerca storica, quindi tutelate come documenti della nostra storia.

# Riflessioni visive sul domani dei nostri giorni

i intellettuali  
ecoslovacchi  
insorgono  
contro la censura

★ ★ **COME VIVREMO NEL DUEMILA** ★ ★

# Terremo in tasca l'apparecchio per comunicare con chi vorremo

Praga, 29 giugno.  
Segno di una aperta  
e con la politica del  
si sono svolte le prime  
grate del IV Congr  
scrittori cecoslovac  
monia della cultura,  
completa libertà di  
ne e l'abolizione del  
sta sono stati gli ar  
più trattati nel corso  
rosi interventi.  
e opinioni scontranti e  
sta lettura della sette  
sta dallo scrittore so  
Holzmeister al Con  
dotti scrittori sovietici  
recentemente a Mos  
che chiede fra l'altro  
ne della censura. E'  
che porta una lettera  
al Congresso da Luch  
di, il messaggero porta  
sso vivente, che, par  
la censura, ha scritto  
tempo di allontanare  
strage, non solo da  
ori ma anche dai par  
iani Kundera ha quin  
to l'autonomia della  
sistando che spesso  
diutare e con interes  
il voto del congresso  
che non può ca  
lità ha sostenuto che  
reva controlli il po  
te tutti i regimi una  
fa delle istituzioni  
per i suoi fini, e si  
di gente e di cultura



**Non sarà più grande di un pacchetto di sigarette e funzionerà insieme da teleselettore e da amplificatore -- Molti tipi di trasmissione tradizionale sono stati condannati a sparire sin dal momento in cui l'impiego dei satelliti artificiali e quello del Laser hanno rivoluzionato le telecomunicazioni -- Intervista col professor Carlo Matteini**

Soltanto dieci anni sono trascorsi dal lancio del primo satellite artificiale, lo Spasnik I, che sbarcò il mondo nell'ottobre 1957. Eppure, in così poco tempo, innumerevoli scoperte in

prendo un'idea molto certa, questa si comporta come le onde luminose, come quelle della televisione, per intenderci. Lei vede che sono necessari tanti stadi per trasmettere i programmi televisivi. Quello che trasmette Milano

minimo. Lei vede qui sul mio tavolo un amplificatore a 5 stadi a transistor della Texas Instrument, che è molto più piccolo di un normale amplificatore: si può concentrare tutto quello che si desidera, compreso la sorgente di energia,

# TIME

## Never Offline.

The Apple Watch is just the start.  
How wearable tech will change  
your life—like it or not.

BY LEV GROSSMAN  
AND MATT VELLA





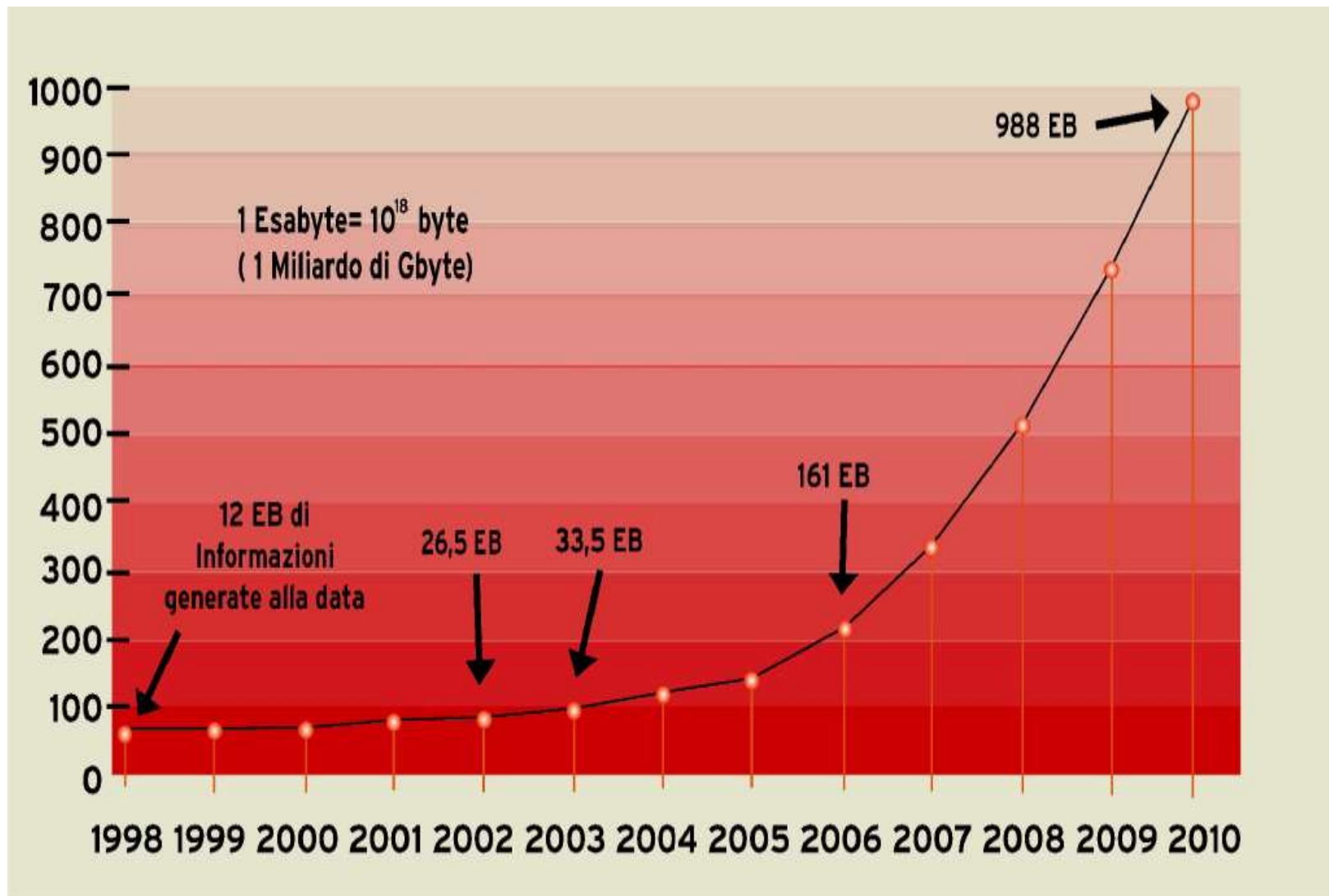
Papa Ratzinger, 19 aprile 2005



Papa Francesco, 13 marzo 2013



***Ormai tutti siamo on line e viviamo (con tranquillità)  
nelle nostre identità digitali***

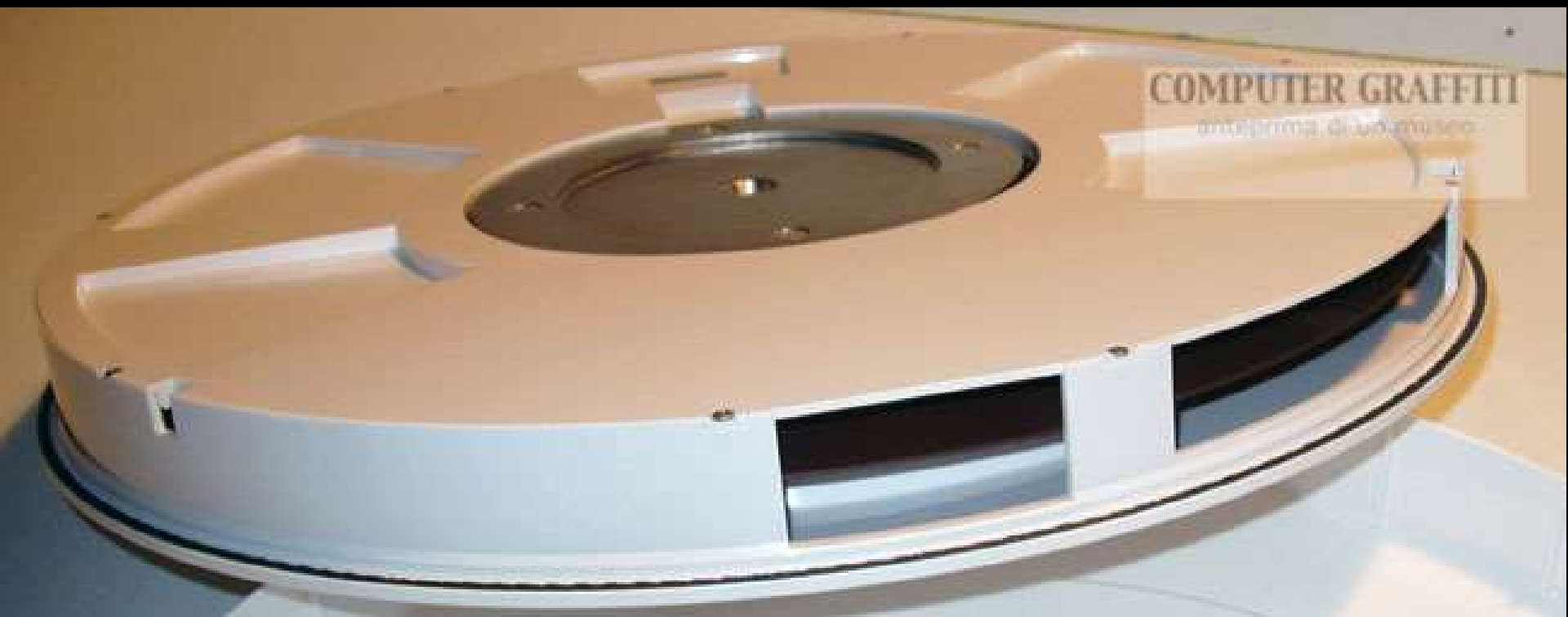


## La crescita delle informazioni

[Università di Berkeley(CA) –(2003) -IDC per EMC Corporation (2007)]

Espansione dell'universo digitale: opportunità di trasformazione

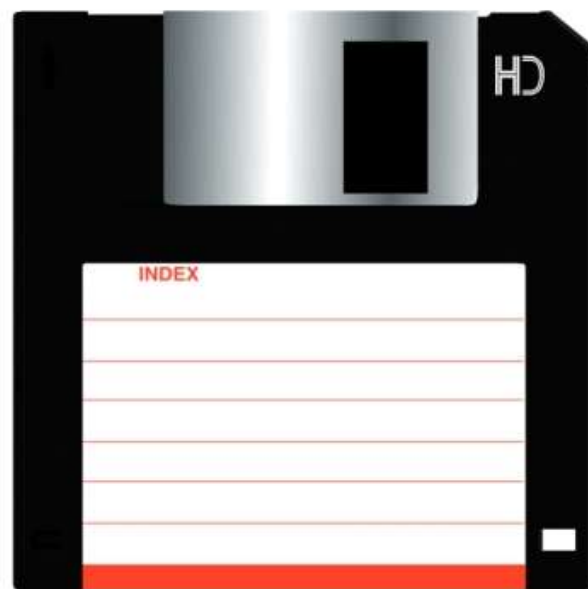
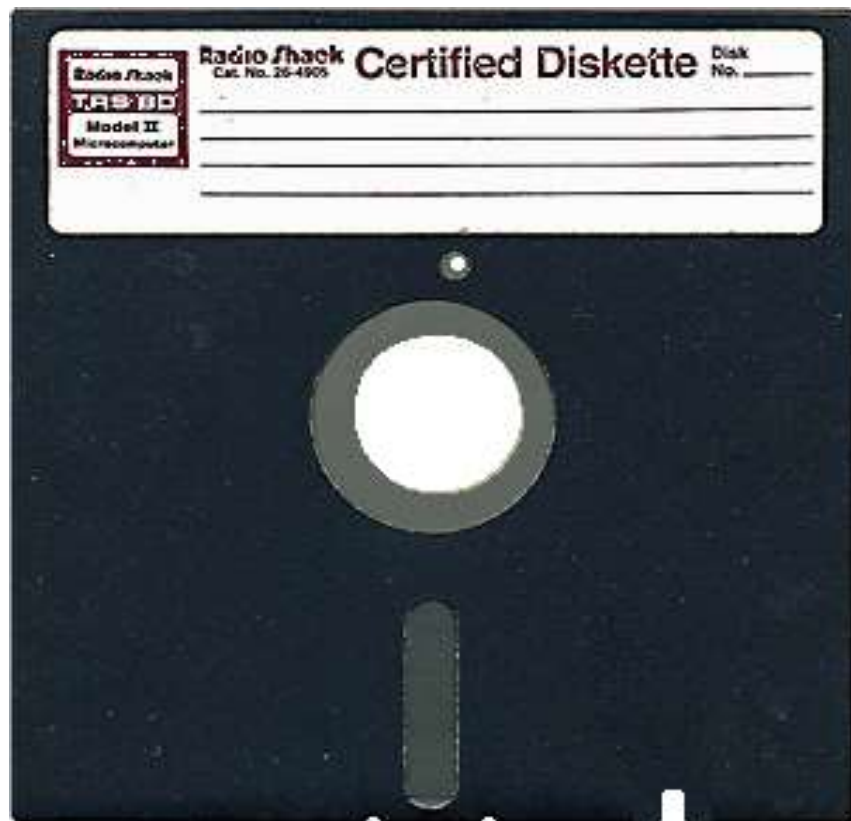
Entro il 2020 l'universo digitale raggiungerà i 44 trilioni di gigabyte (ECM 2014)



**COMPUTER GRAFFITI**

anteprima di un museo





26 aprile 2010

## Sony chiude un'era: stop alle vendite dei floppy disk dal 2011

di Gianni Rusconi

Ancora un anno, anzi meno, e poi altro pezzo di storia del personal computer andrà definitivamente in archivio. A marzo 2011, infatti, stando a quanto riportato dal Mainichi Daily Sony scriverà la parola fine all'avventura dei floppy disk anche in Giappone, interrompendone definitivamente le vendite.

Finisce quindi un'era iniziata nel lontano 1981, quando i dischetti da 3,5 pollici debuttarono sul mercato – prendendo il posto di quelli più grandi da 5,25 pollici - per diventare il supporto di memoria portatile più utilizzato da milioni di utenti informatici per oltre un ventennio. Poi vennero i Cd e i Dvd, i sistemi Zip e infine le Pen drive e le oggi popolarissime chiavette Usb. Apple fu la prima ad abbandonare i floppy con gli iMac nel 1998, negli anni a seguire la seguirono tutti gli altri produttori di pc, a cominciare da Dell per i suoi modelli da tavolo Dimension.

E per i supporti neri o colorati dotati di linguetta color acciaio e con apposito spazio per l'etichetta adesiva descrittiva è stato l'inizio della fine. Per Sony, che detiene il 70% della quota di questo ormai anemico settore, e altri produttori è stato comunque un business incredibile, con milioni di esemplari distribuiti in tutto il mondo anche in tempi recenti: proprio la casa di Tokyo ne ha venduti in terra nipponica 12 milioni di pezzi nell'esercizio 2009, rispetto ai 47 milioni del 2002. Il trentesimo compleanno del floppy coinciderà quindi con la sua annunciata morte. Nel 2007 il 98% dei computer in commercio era già privo dell'inconfondibile fessura per leggere il dischetto di memoria; oggi vedere all'opera un desktop con questo "add on" fa immediatamente pensare a un'epoca tecnologica che non esiste più. Ora ne è arrivata la conferma, da chi le diede vita.

 [FOTO / Si chiude l'era dei floppy disk](#)

26 aprile 2010

SanDisk 



MEMORY STICK PRO DUO

◀ 4.0GB MAGICGATE







## [Studio Associato Avvocati](#)

[101professionisti.it/Avvocati](http://101professionisti.it/Avvocati)

Hai bisogno di un Avvocato? Risposta in 24 ore. Contattaci Ora!

## NAPOLI, SI ROMPE IL CD CON ATTI INDAGINI, TUTTI LIBERI

Fatti

Mercoledì, 03 Aprile 2013 15:40

### [Compra CD e DVD Memorex](#)

Custodie Per Cd E Dvd Vasto assortimento di custodie

[www.AtomicShop.it](http://www.AtomicShop.it)



Scegli Tu! ➤



Un'inchiesta su un giro di tangenti per appalti pubblici aveva portato all'arresto di Raimondo Mazzearelli, sindaco di Casalduni, in provincia di Benevento, e il suo caposervizio amministrativo Cosimo D'Addona.

Ai domiciliari dal 19 marzo, oggi sono tornati in libertà per un disguido tecnico: il cd rom su cui erano contenuto i documenti dell'inchiesta si è rotto, quindi questi non sono più leggibili.

La decisione è del Tribunale del Riesame di Napoli, che hanno

accolto la richiesta degli avvocati difensori Antonio De Girolamo e Umberto Del Basso De Caro (deputato del Pd) sulla base del fatto che fosse impossibile leggere gli atti dell'indagine.

fonte: [www.leggo.it](http://www.leggo.it)

0000996

490 cp ?

Bulkpaq

DVD  
R  
4.7

UNIQUE FOR DATA, VIDEO AND GAMES  
16X DVD-R  
GENERAL PURPOSE DVD-R 4.7GB

Generation 4  
16x speed DVD-R

www.bulkpaq.co.uk

Official sponsor of speed record info - the number 1 DVD burning service





 MITSUBISHI

BD-R 2x

LTH TYPE

130min./25GB





## TECNOLOGIA



condividi



Kata Web

OKNO



## HARDWARE

## Quel cd tutto trasparente potrà contenere 100 dvd

La General Electric lavora a un disco registrabile da 500 gigabyte. Ne promette la commercializzazione entro il 2012. Il segreto? Utilizzare la memoria olografica come tecnologia per l'archiviazione di informazioni  
di RICCARDO BAGNATO



Brian Lawrence

LA FORMA è quella di un normale cd. L'unica differenza visibile è il colore, arancione, e la totale trasparenza dei materiali. La novità, però, è che potrà contenere fino a 500 gigabyte di dati. Overo 10 volte la capacità di un disco blu-ray e 100 volte quelle di un comune dvd. A prometterlo è la General Electric, che ha annunciato per il 2012 lo sbarco sul mercato di un nuovo supporto digitale per l'archiviazione dei dati, e ne ha presentato in video un prototipo.

**Fantascienza? Non proprio.** I ricercatori della società americana hanno infatti messo a punto un nuovo procedimento di registrazione e di lettura dati che permette di utilizzare non solamente la superficie del supporto,

ma - complici i materiali adottati - l'intero volume dei dischi. Il segreto? Utilizzare la memoria olografica come tecnologia per l'archiviazione di informazioni.

L'idea non è nuova. Le società InPhase Technologies e Maxell avevano promesso la stessa cosa nel 2006. Per loro, l'uscita del supporto miracoloso doveva avvenire l'anno successivo. Tanto che la stessa Nintendo, nota produttrice della di videogiochi, aveva avanzato l'ipotesi di introdurre questo tipo di tecnologia sulle proprie console.

Tuttavia...

I dati sullo smantellamento delle centrali atomiche inglesi saranno conservati su rotoli simili a quelli usati dai faraoni

## **Papiri egizi per i dati sul nucleare solo loro garantiscono l'eternità**

Le informazioni dovranno restare disponibili per decenni ma i computer e la carta tradizionale invecchiano troppo presto

**LONDRA** - Il problema si porrà in un futuro lontano, ma la soluzione arriva dal passato remoto. Così sarà l'antica sapienza egizia a venire in soccorso della moderna scienza.

A riferire dell'apparente contraddizione è un articolo del quotidiano inglese *The Guardian* che rivela come dopo diverse verifiche le autorità britanniche per l'energia nucleare abbiano deciso di ricorrere a una carta simile ai papiri dei faraoni per salvaguardare decisive informazioni sullo smaltimento delle scorie delle centrali atomiche.

Conservare i dati che potrebbero dover essere consultati anche tra centinaia di anni solo su dei computer e dei software che rischiano di diventare obsoleti nel volgere di poco tempo è infatti troppo rischioso. Così a qualcuno è venuto in mente che se conservati nella maniera giusta i rotoli egizi sono in grado di resistere migliaia di anni, a differenza della nostra carta che marcisce facilmente e rapidamente.



*Allarme planetario sulla deperibilità del materiale digitalizzato. La carta vince la sfida*

# I testi in dvd si rovinano presto

## I dati su supporti elettronici scompaiono più facilmente

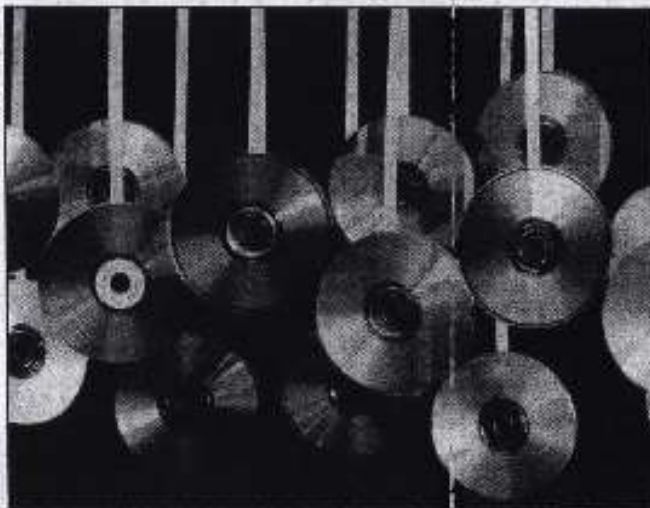
DI MASSIMO GALLI

**L**e biblioteche e gli archivi di tutto il mondo hanno scoperto quello che si sapeva fin dagli albori della diffusione di supporti digitali: i dati registrati su cd e dvd hanno una durata limitata. Gli esperti hanno sempre sostenuto che un disco poteva conservare inalterato il materiale per una ventina d'anni. E tutti a fare orecchie da mercante, avallando implicitamente le tesi estremiste dei novelli guru, che avevano profetizzato la fine dei libri tradizionali in nome della vittoria trionfale delle tecnologie informatiche. Come se gli amanuensi del Medioevo si fossero dati da fare inutilmente per salvare le opere più preziose, ricopiandole pazientemente lettera dopo lettera.

Adesso emerge non soltanto che la conservazione di testi in formato digitale non è eterna, ma anche che, passato un certo periodo di tempo, i computer e i sistemi

operativi non sono più in grado di leggere i vecchi file. A differenza degli occhi umani, che riescono sempre a decifrare il contenuto di parole e immagini stampate su carta. Dunque, il materiale è anche più costoso da preservare. Tutto quanto si legge in formato elettronico, spiegano gli studiosi, in ultima analisi non è altro che una serie di cifre (0 e 1) scritte su floppy disk, compact disc e dvd, che si rovinano più in fretta degli stampati. Anche se l'archivio di questi supporti sopravvive, l'insorribile marcia della tecnologia può significare che i vecchi strumenti e il vecchio software, che permettevano di leggere quelle informazioni, semplicemente non esistono più.

E un po' quello che succede a chi ha una cassetta registrata senza un lettore: come ascoltarla? Ci si pone, dunque, il problema di salvare tutti i dati e di come renderli accessibili col passare del tempo. A meno di non rasse-



Corsa contro il tempo per salvare gli archivi digitali

guarsi a creare una sorta di archivio provvisorio, consegnando poi il contenuto all'etere. Secondo Anne Van Camp, direttrice

dell'Istituto di archivi Smithsonian e membro di un gruppo per la tutela digitale creato negli Stati Uniti, è certamente una di

quelle questioni che tiene molta gente sveglia di notte.

Intanto è soltanto agli inizi l'opera di archiviazione degli autori che hanno affidato le loro opere all'elettronica. Per esempio, l'università americana di Emory, in Atlanta, ha aperto una mostra sulla collezione dello scrittore britannico Salman Rushdie, autore tra l'altro dei «Versetti satanici», che gli valsero la condanna a morte da parte delle autorità religiose iraniane. Non è stato facile sistemare l'intero materiale e renderlo compatibile con le tecnologie attuali, ma alla fine il gioco è valso la candela: le possibilità di approcci multimediali sono più ampie di quelle tradizionali. L'università di Stanford, dal canto suo, ha aperto un laboratorio digitale forense, il primo negli Stati Uniti. Ma servono soldi e risorse umane che non tutti possono permettersi. Nel frattempo i bit rischiano di evaporare.

di riproduzione riservata

Ieri  
CD  
e  
DVD  
Oggi  
Cloud?

## Conservazione elettronica?



# Torniamo alla cara, vecchia carta?

**TREVENZUOLO.** Guasto al server del Comune: negli uffici i documenti si fanno a mano o usando i vecchi sistemi

## Computer bloccati, ritornano le macchine da scrivere

Garantita la validità delle carte d'identità e dei documenti rilasciati: la Prefettura e la Provincia avvisati del problema, che proseguirà ancora per qualche giorno

**Line Fontana**

Da oltre un mese gli impiegati comunali sono costretti, loro malgrado, a rilasciare documenti, certificati e carte d'identità scritti a mano oppure con la vecchia macchina da scrivere.

Questo avviene perché tutti i computer degli uffici comunali, quindi l'intero sistema informatico, sono fuori uso a causa di un guasto al server. In sostanza, non si possono emettere documenti o pratiche con il computer, fare ricerche d'archivio nei vari files degli uffici con la ormai consueta e apprezzata velocità che permette il mezzo informatico. Insomma, all'improvviso tutto l'apparato è tornato indietro di decenni: alla macchina da scrivere, alla penna, agli archivi cartacei da consultare estraendoli dagli armadi, magari custoditi in cartelle polverose e non più utilizzate da anni.

Il guaio è accaduto lo scorso 17 marzo quando, appunto, «il Comune di Trevenzuolo ha subito un blocco del server», spiega il sindaco Osvaldo Zoccatelli, «in quanto si sono danneggiati i dischi fissi del server, a cui sono collegati i computer degli uffici comunali».

Il primo cittadino sottolinea: «Immediatamente abbiamo provveduto a comunicare agli organi competenti - uffici provinciali, regionali, statali, prefettura eccetera - il mancato funzionamento informatico di tutti i servizi comunali, così da non incorrere in eventuali inosservanze che non sono dovute a negligenza da parte dei funzionari e degli amministratori». Quindi aggiunge: «Abbiamo subito incaricato ditte specializzate in materia di recupero dei dati e per la sostituzione del server con uno nuovo».

Il sindaco Zoccatelli aggiunge: «Abbiamo quindi deciso di attivare il servizio in-cloud (ovvero un sistema di archiviazione di tutti i dati e documenti elaborati quotidianamente in un altro server remoto ndr) di tutti i programmi in dotazione agli uffici comunali al fine di evitare, in futuro, problemi simili».

Gli uffici sono rimasti sempre operativi e continuano ad esserlo anche in questi giorni, in attesa del ripristino del server. «Sopperiamo alle mancanze informatiche», osserva ancora Zoccatelli, «con la redazione manuale dei documenti cartacei (ad esempio il rilascio delle carte d'identità)

e ovviamente non ci saranno problemi relativamente allo svolgimento delle prossime consultazioni amministrative».

Una precisazione che dovrebbe fugare i dubbi e i timori di qualche futuro candidato sindaco alle elezioni per il rinnovo del consiglio comunale, il quale teme che ci possano essere delle difficoltà nell'emissione di documenti e certificazioni relative alla tornata elettorale del 31 maggio.

Dunque se la tanto sbandierata dematerializzazione dei documenti, con lo scopo di risparmiare carta, sburocratizzare e velocizzare gli uffici pubblici, fosse andata in porto completamente e non si continuasse, come prassi tutta italiana, a lavorare ancora anche con il cartaceo, allora si che si sarebbe bloccato tutto l'apparato.

Meno male che negli uffici comunali sono ancora funzionanti le macchine da scrivere; inoltre gli stessi impiegati comunali si sono improvvisamente trovati catapultati indietro nel tempo a dover trasformarsi in tanti amanuensi, come nel medioevo. Il progresso, talvolta, riserva anche queste sorprese. ■



Macchina da scrivere e carta intestata del Comune FOTO PECORA



**Ricorreremo al cloud per avere archivi remoti. Nessun problema per le elezioni**

**OSVALDO ZOCATELLI**  
SINDACO DI TREVENZUOLO

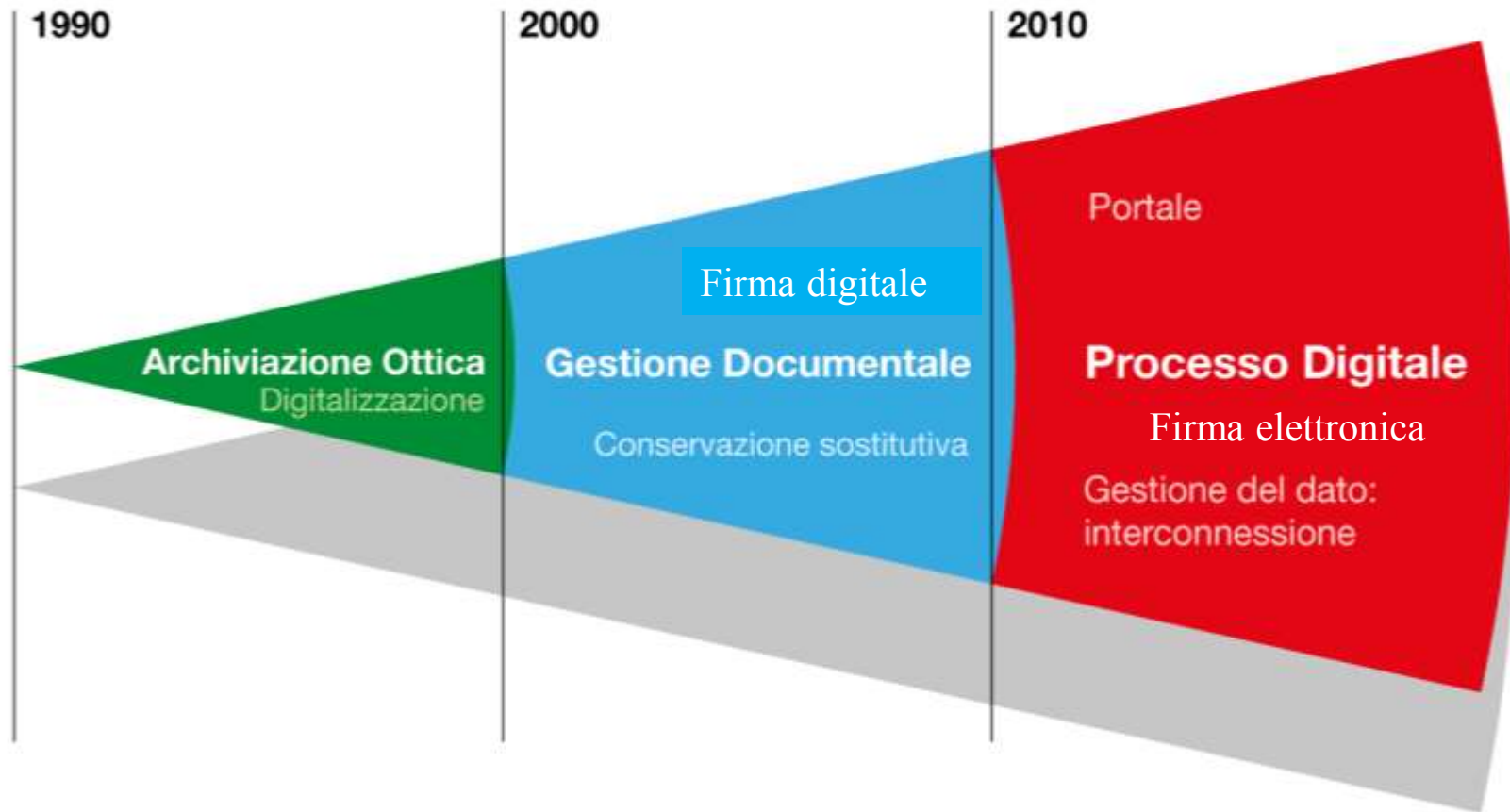
## ***Ma gli archivi cartacei sono sicuri??***





*Digitalizzare processi documentali e informativi non è semplice...*

# Document Management: stadi evolutivi



**Records management (RM)**, also known as **Records information management** or **RIM**, is the professional practice or discipline of controlling and governing what are considered to be the most important *records* of an organization throughout the records life-cycle, which includes from the time such records are conceived through to their eventual disposal. This work includes identifying, classifying, prioritizing, storing, securing, archiving, preserving, retrieving, tracking and destroying of records (def. ARMA International from "Glossary of Records and Information Management Terms, 3rd Edition").

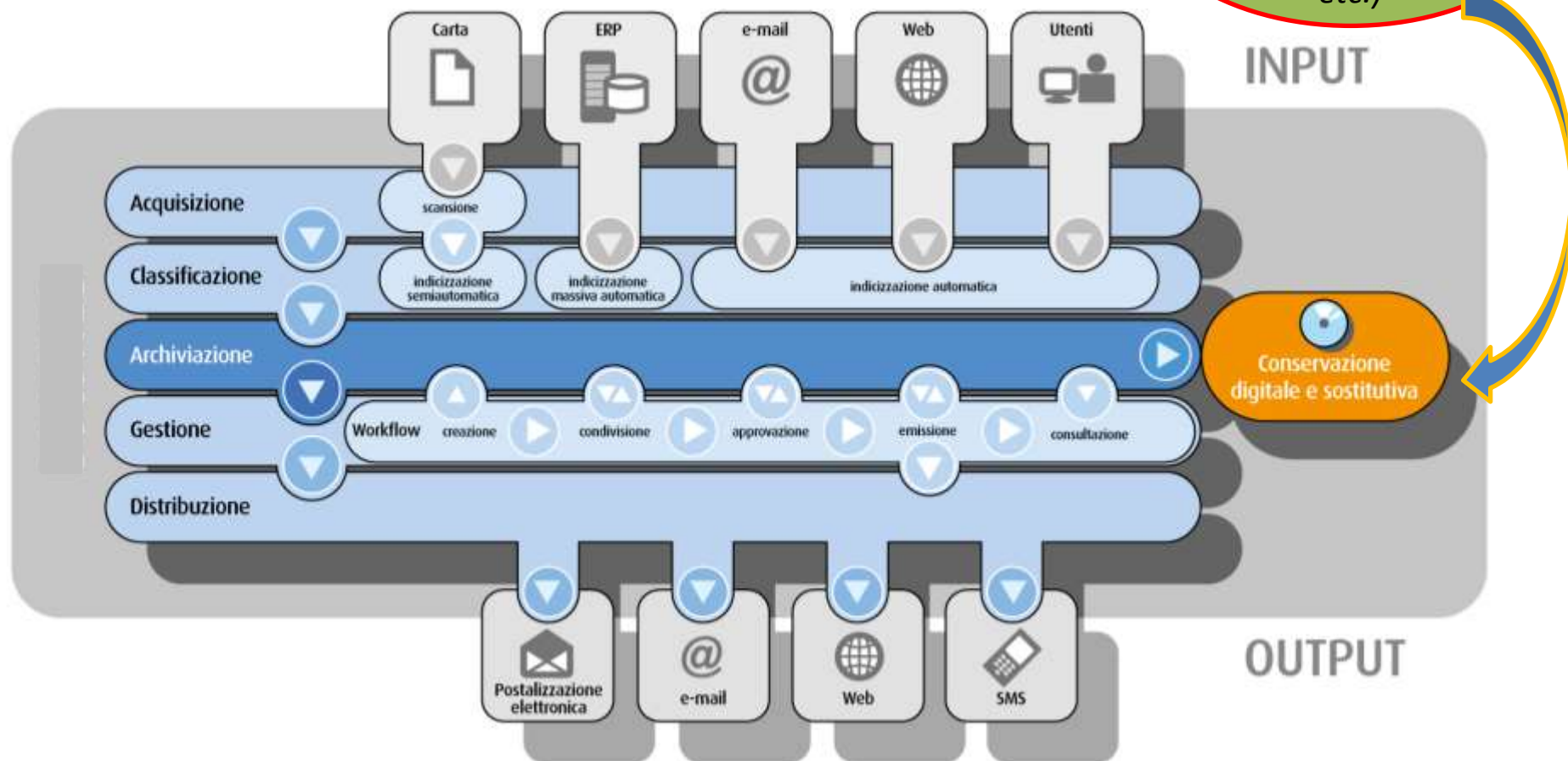
# Document Management: le tappe dello sviluppo

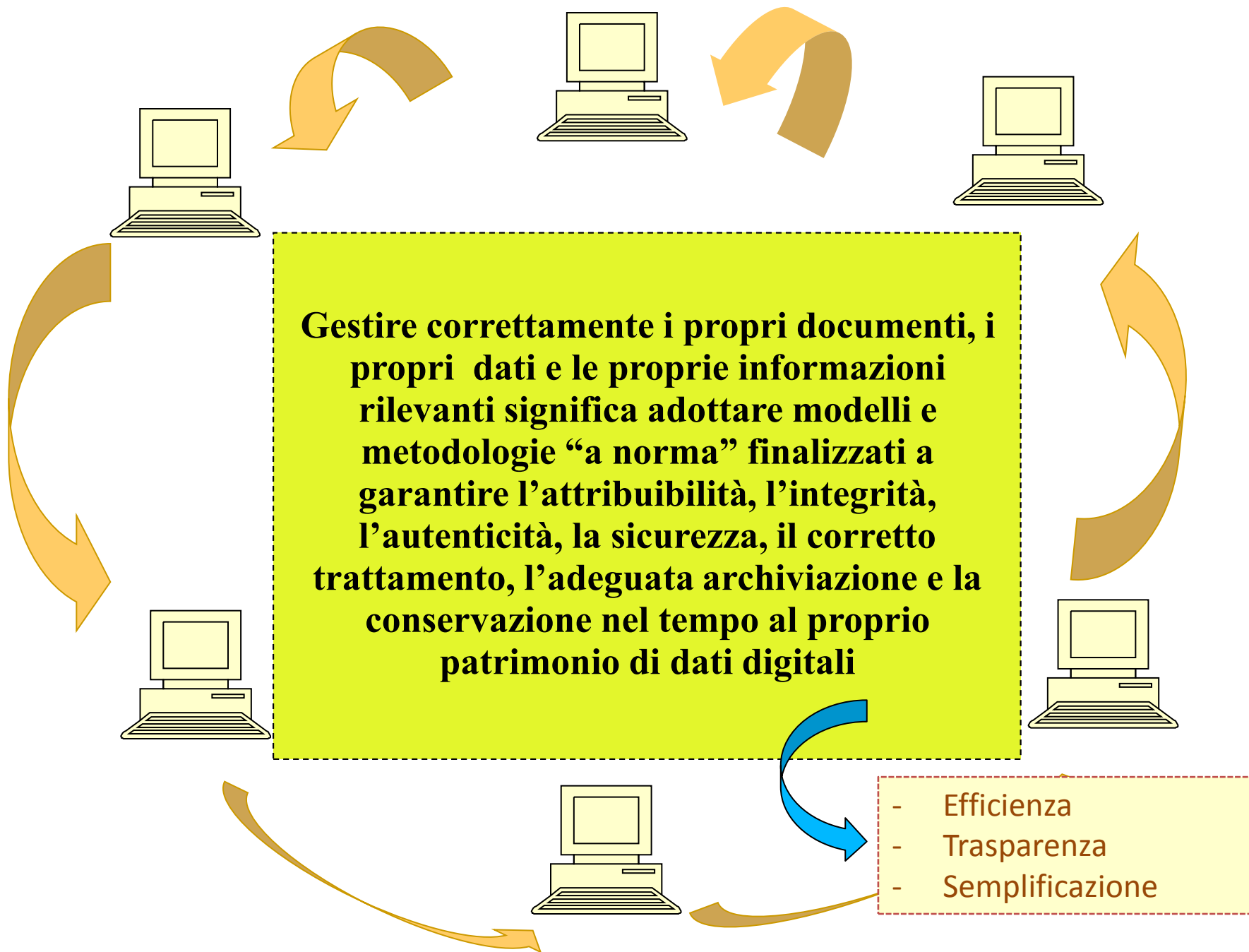


Ormai esistono e si sviluppano in tutte le realtà aziendali o amministrative piattaforme e sistemi che possono essere utilizzati da centinaia di migliaia di utenti per gestire informazioni, dati e documenti strutturati e non strutturati processati quotidianamente...

**Sistema Informativo**  
(DMS, DB, Business Intelligence, comunicazioni e informazioni etc.)

**Sistema Documentale**  
(documenti contabili, corrispondenza commerciale, contratti, etc.)





A diagram illustrating the digital document lifecycle. In the center is a light blue rectangle with a dashed border containing the text: **Carta digitale:**  
**Formazione documento e contratto informatico**  
**Firme elettroniche**  
**Verifica e Prova del consenso digitale**. Surrounding this central box are six yellow computer icons arranged in a circle. Five large, curved orange arrows connect these icons in a clockwise cycle, indicating a continuous process.

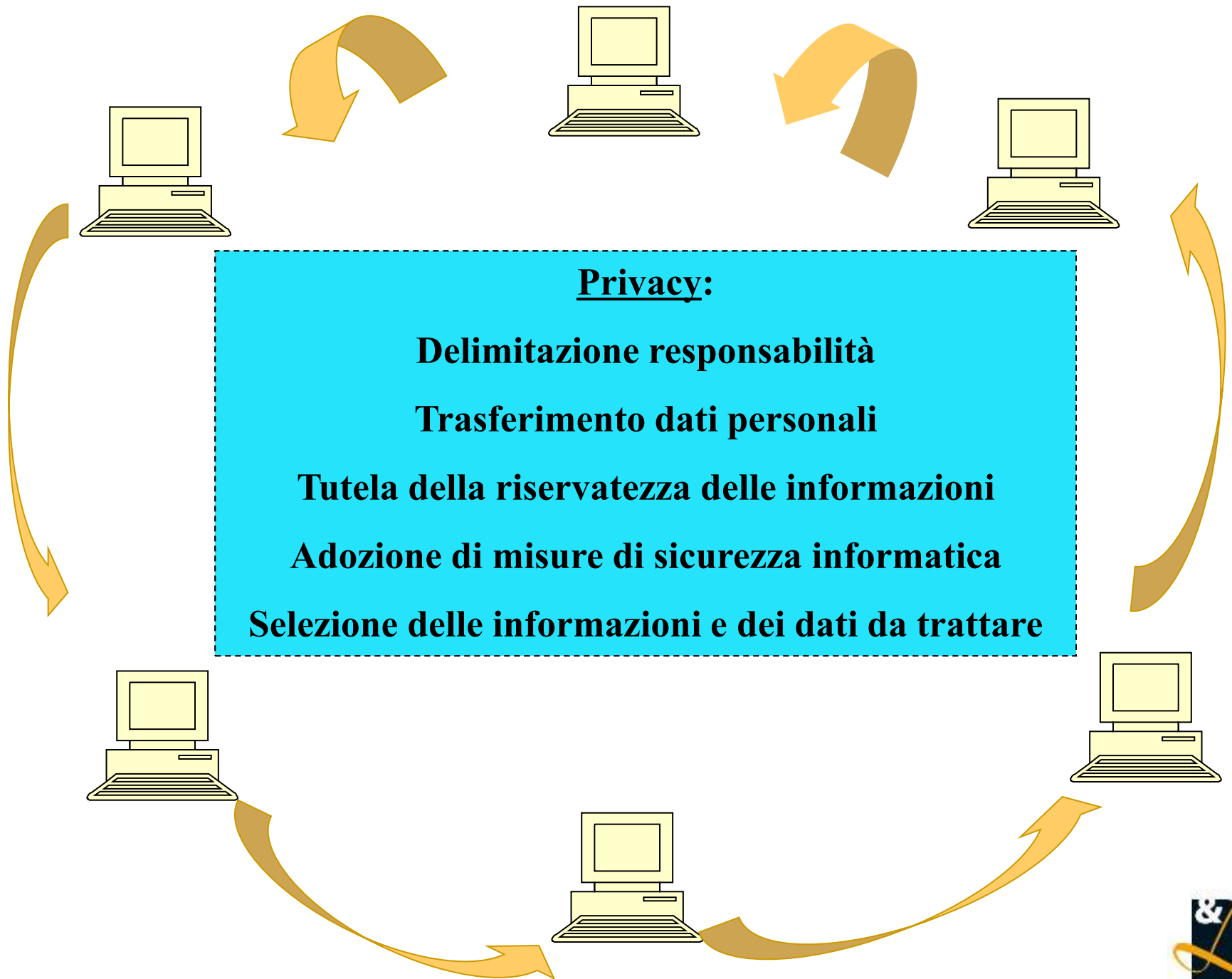
**Carta digitale:**

**Formazione documento e contratto informatico**

**Firme elettroniche**

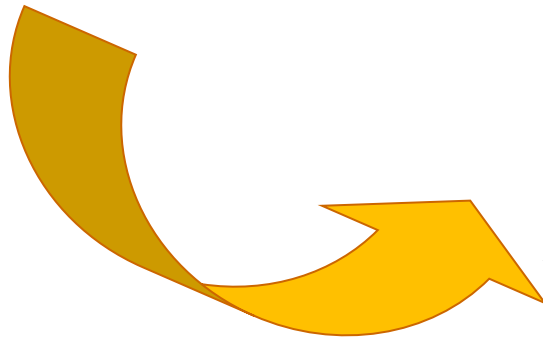
**Verifica e Prova del consenso digitale**







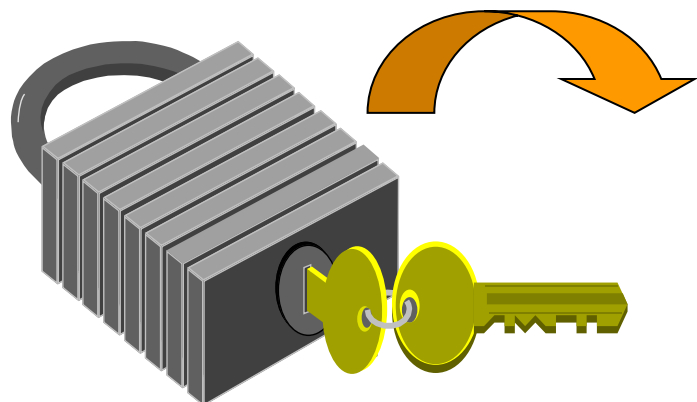
# di cosa stiamo parlando?



...del passaggio culturale, sociologico, economico e, quindi, giuridico da un documento pesante e statico ad un documento dinamico, che si condivide e che diventa “partecipativo”...

...e anche per la PA ormai il mondo digitale è sempre più multicanale:

**La rivoluzione disegnata nel  
Codice dell'Amministrazione Digitale**



**DIPENDENTI:**

- e-mail, pec, firma digitale e FEA
- protocollazione e registrazione informatica
- archiviazione e gestione documentale
- privacy e sicurezza informatica
- conservazione nel tempo della memoria

**DECERTIFICAZIONE**



**Altre Pubbliche Amministrazioni o  
imprese**



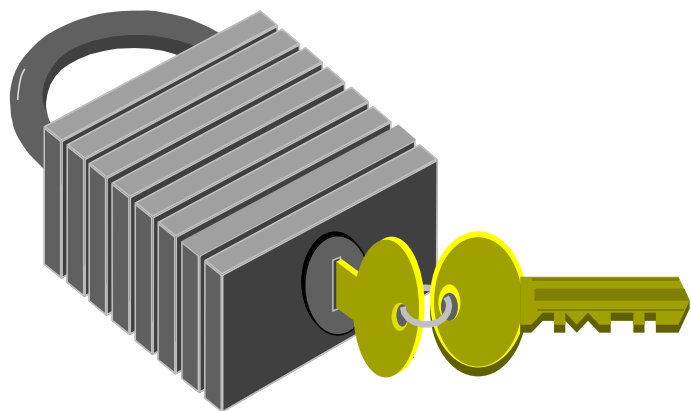
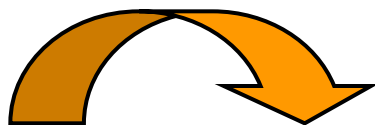
**Destinatari del servizio:**

- pubblicità legale on line
- trasparenza e accessibilità
- formulari on line
- sportelli e procedimenti on line
- contratti con firma digitale



**Connettività  
E-government  
E-procurement  
Reti di P.A.  
convenzioni digitali**

**E-GOV**



## INFORMAZIONI GENERALI:

- e-mail semplice/**CEC PAC?**
- portali informativi ad accesso libero
- chioschi telematici
- tv digitale
- sms
- call center

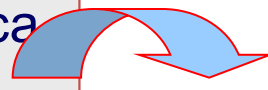


## Formulari on line

- area riservata previa registrazione

## Istanze on line e dichiarazioni:

- PEC id e autenticazione informatica
- firma digitale (e FEA)
- telefax

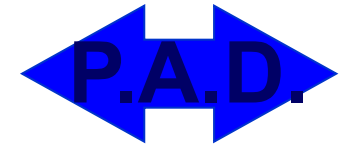


## Attivaz. procedimenti e transazioni

- autenticazione informatica (CIE/CNS...**SPID?** Italia Login??)
- posta certificata + firma digitale
- pagamenti elettronici

**ATTENZIONE:**  
**SICUREZZA INFORMATICA**

# Comunicazioni Digitali e Imprese: la chiave del successo nella Società dell'Informazione



PEC,  
FIRMA DIGITALE,  
IDENTIFICAZIONI INFORM.

DIPENDENTI (INTRANET)

Fornitori/imprenditori  
(extranet - B2B)

CLIENTI/UTENTI (B2C)

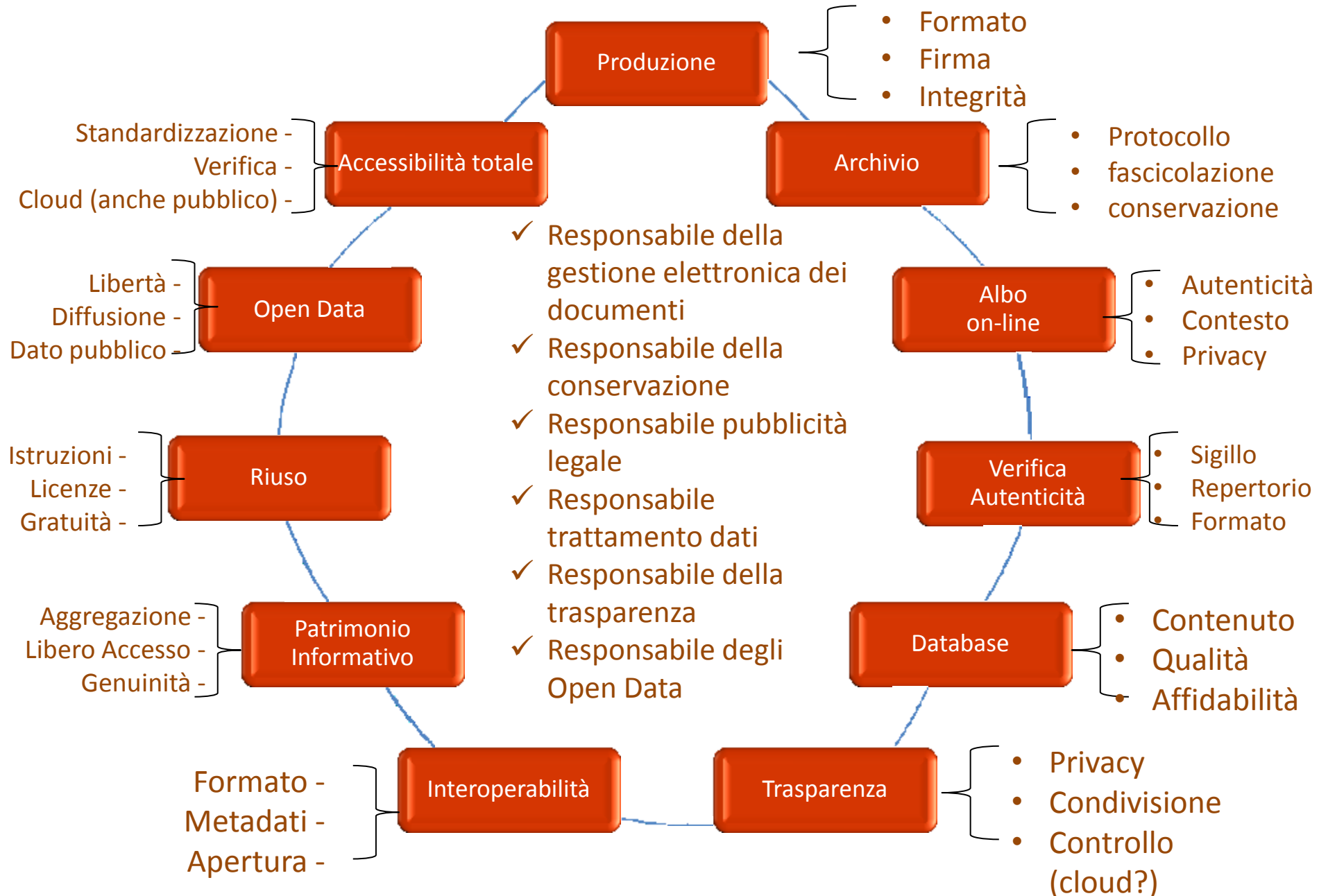
Distretti industriali  
Filiera  
Consorzi  
Gruppi di imprese

**servizi on line di comunicazione**  
(email, sms, mms, siti web, blog, social etc.)

E-marketplaces



# Le fasi del documento informatico amministrativo



# Professionista della digitalizzazione documentale

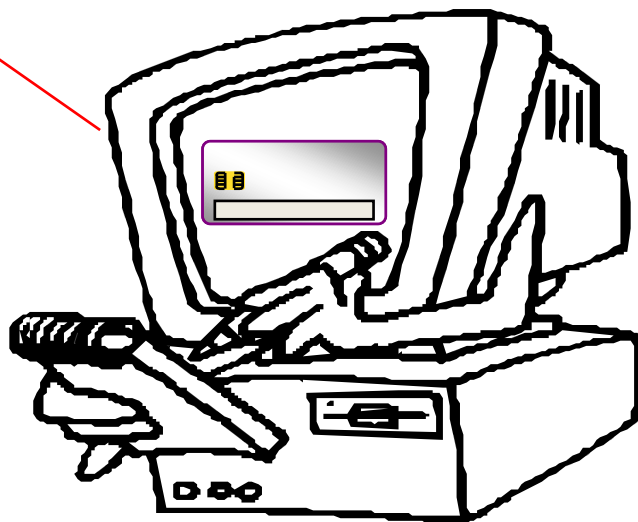


### **Autenticazione:**

- PEC
- VPN e SPC
- EDI
- Aree Riservate

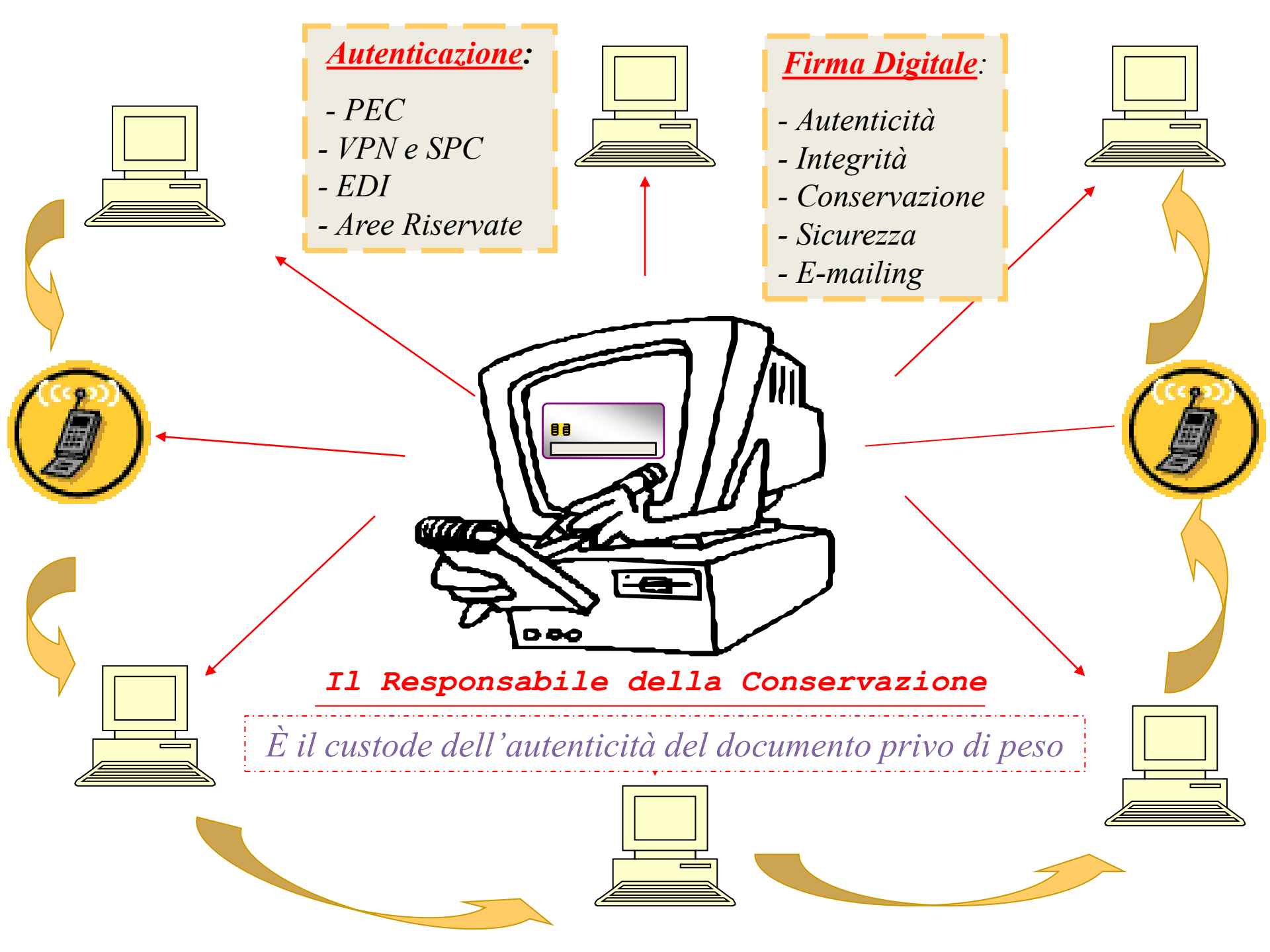
### **Firma Digitale:**

- Autenticità
- Integrità
- Conservazione
- Sicurezza
- E-mailing



### **Il Responsabile della Conservazione**

*È il custode dell'autenticità del documento privo di peso*

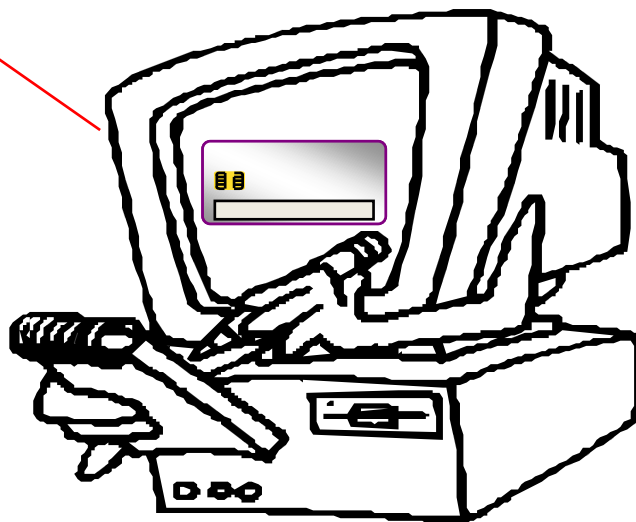


### **Identificazione:**

- PEC
- VPN e SPC
- EDI
- Aree Riservate

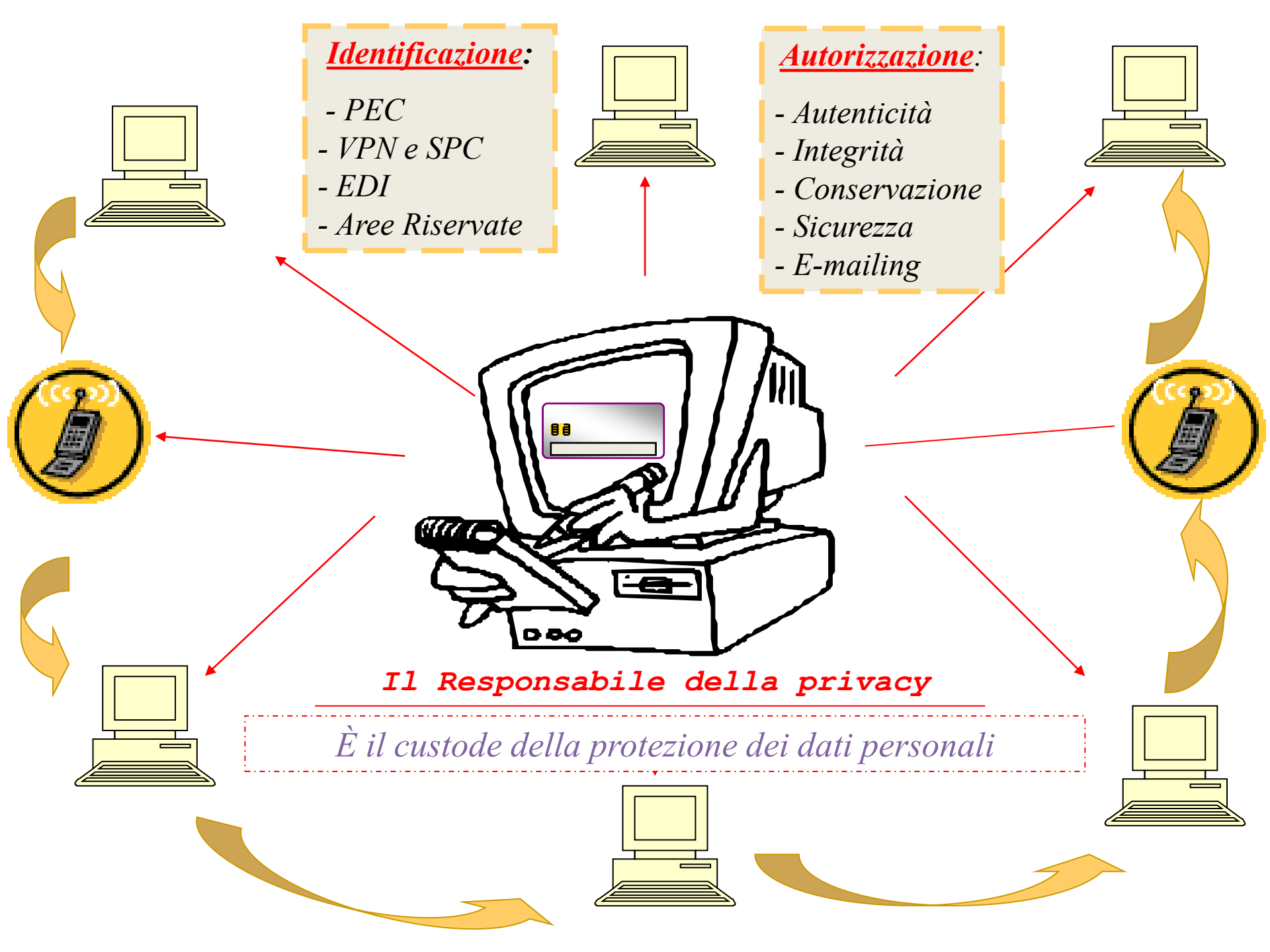
### **Autorizzazione:**

- Autenticità
- Integrità
- Conservazione
- Sicurezza
- E-mailing



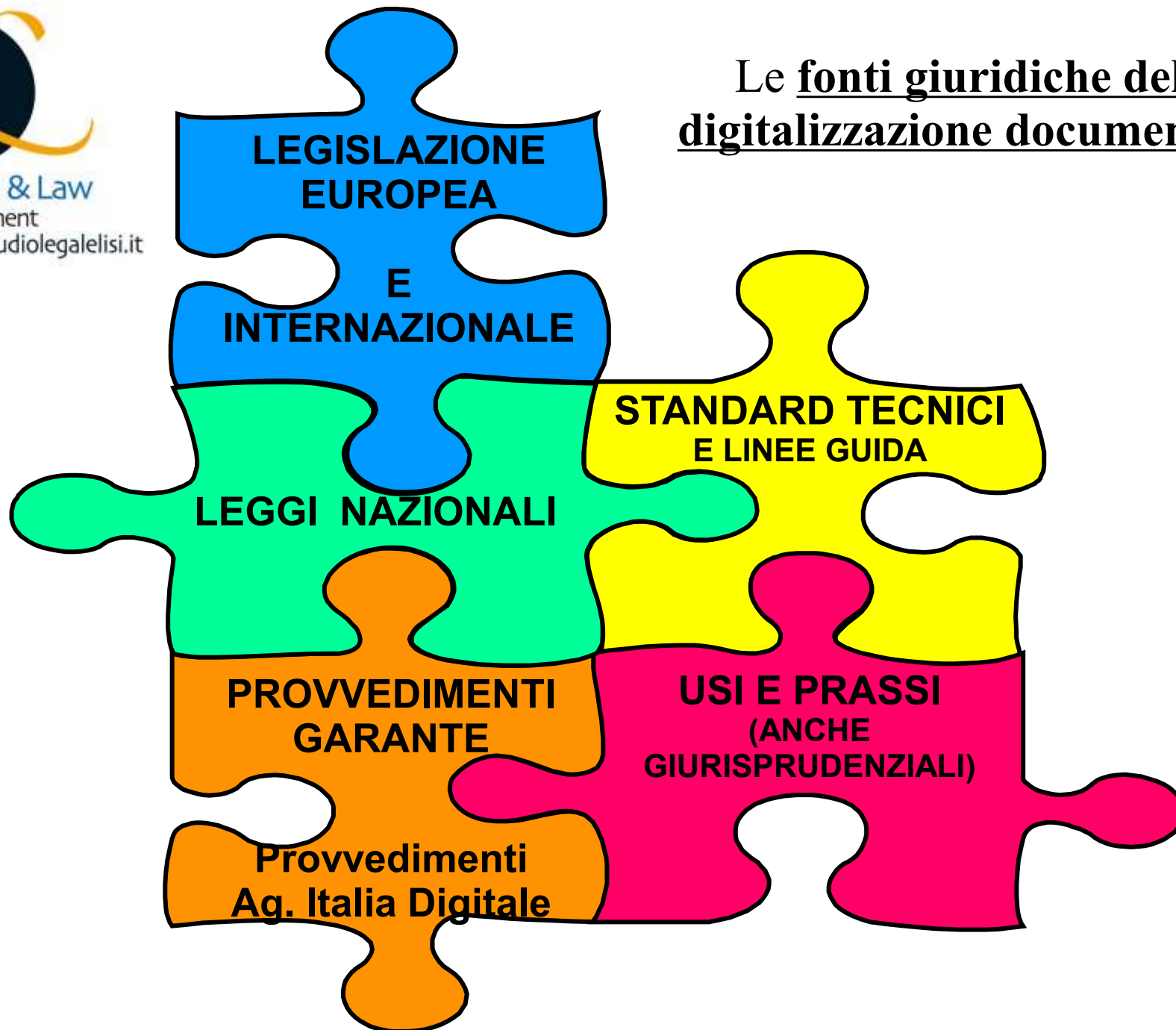
**Il Responsabile della privacy**

*È il custode della protezione dei dati personali*



Le norme  
ci sono?

## Le fonti giuridiche della digitalizzazione documentale:



*Le norme in Italia ci sono e sono anche troppe!!!*

## **CI SONO le norme sul Documento Informatico, sulla Firma digitale e sulla Conservazione digitale:**

- **Codice della Amministrazione Digitale** (D. Lgs. 82/2005)
- **Codice della Privacy** (Allegato B del D. Lgs. 196/2003)
- **DPCM 13 novembre 2014** (Regole tecniche documento informatico)
- **Deliberazione CNIPA del 19 febbraio 2004 n. 11** (regole conservazione) – **DPCM 3 dicembre 2013**
- **DPCM del 30 marzo 2009 – DPCM 22 febbraio 2013** (Regole tecniche firma digitale)
- DPR 11 febbraio 2005 n. 68 (Posta Elettronica Certificata)

## **Fatturazione Elettronica e Conservazione Documenti Fiscali:**

- DMEF 23 gennaio 2004 (conservazione digitale documenti fiscali) (oggi **DMEF 17 giugno 2014**)
- D. Lgs. 20 febbraio 2004 n. 52 (fattura elettronica)
- Circolare Agenzia delle Entrate n. 45/E (del 19/10/2005)
- Circolare Agenzia delle Entrate n. 36/E (del 06/12/2006)
- Direttiva 45/2010/UE del 13 luglio 2010 (Legge n. 228/2012)
- Circolare AE 12/E del 3 maggio 2013

# Le regole tecniche

## Libro Unico del Lavoro:

**Legge 133/2008 (conv. D.L. 112/2008) – artt. 39-40**

**Decreto Ministero Lavoro 9 luglio 2008**

**Circolare n. 20/2008 Ministero Lavoro 21/08/2008 + Note Inail  
26/08/2008 e 10/09/2008**



## - Registri e contratti assicurativi:

**Regolamento ISVAP n. 27 del 14 ottobre 2008 (*in vigore dal 1 °luglio 2009*)**

**Regolamento ISVAP n. 34 del 19 marzo 2010 (*in vigore dal 15 luglio 2010*)**

**Regolamento IVASS n. 8 del 3 marzo 2015** in materia di semplificazione delle procedure e degli adempimenti burocratici nei rapporti tra imprese, intermediari e clientela

## - Documenti bancari:

**«Assegno elettronico» (DL 70/2011 + DMEF 03.10.2014 n° 205 + Regole Tecniche Banca d'Italia)**

**Trasparenza operazioni e servizi finanziari – Provv. Banca d'Italia del  
15/07/2015 (in vigore dal 1/10/2015)**

**Finanziaria 2005:** comma 197 – e-cedolino

**Finanziaria 2006:** comma 51 – dematerializzazione corrispondenza

**Finanziaria 2007 :** trasparenza retribuzioni

**Finanziaria 2008:** commi 209-214 – obbligo di fatturazione elettronica alla PA – **New Decreto “Salva Italia”** (DL 201/2011 - conv in L. 214/2011)

commi 589-593 – obbligo di PEC e telefonia VOIP

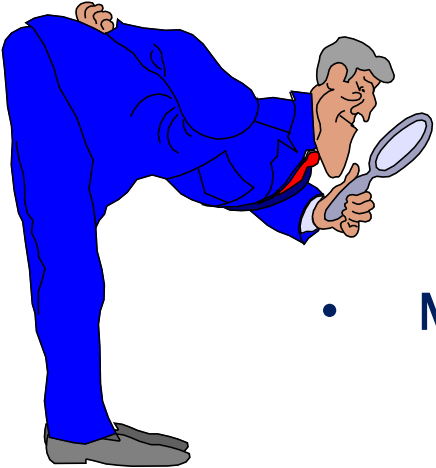
**Manovra Fine Estate** (DL 112/2008): artt. 39-40 – digitalizzazione LUL

**Legge 18 giugno 2009 n. 69** – “taglia carta, revisione CAD, Voip, AOL”

**DL anticrisi 78/2009** – convertito in Legge 3 agosto 2009, n. 102

■ **D.L. 185/08 (L. 28 gennaio 2009 n. 2) – PEC obbligatoria per tutti e Documenti originali unici “smaterializzabili” senza notaio!**

■ **D.L. 70/2011 – decreto Sviluppo (legge di conversione 12 luglio 2011, n. 106) – dematerializzazione assegni!**



## Le ultime novità

- DECRETO LEGISLATIVO 30 dicembre 2010, n. 235
- Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

### Nuove Regole Tecniche

**Decertificazione:** art. 15 L. 183/2011+Direttiva Pres. Consiglio Ministri 14/2011

**Decreto semplificazioni:** DL 9 febbraio 2012 n. 5 convertito in Legge 4 aprile 2012 n. 35 (Agenda Digitale)

**Misure urgenti crescita Paese:** DL 22 giugno 2012 n. 83 convertito in Legge 7 agosto 2012 n. 134 (Agenzia per l'Italia Digitale)

**Decreto crescita:** 179/2012 conv. in Legge 221/2012

**Decreto Trasparenza:** D.Lgs. n. 33/2013

**Decreto Pubblica Amministrazione:** DL 90/2014 conv. L. 114/2014

**Regolamento eIDAS:** Regolamento N. 910/2014 del PARLAMENTO

**EUROPEO e del CONSIGLIO del 23 luglio 2014** in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

# Le (altre) ultimissime novità

- DPCM 24 ottobre 2014 – Definizione delle caratteristiche del Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese, nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese
- DPCM 10 novembre 2014, n. 194 - Regolamento recante modalità di attuazione e di funzionamento dell'Anagrafe nazionale della popolazione residente (ANPR) e di definizione del piano per il graduale subentro dell'ANPR alle anagrafi della popolazione residente
- Secondo e ultimo decreto sulla fatturazione elettronica per le PA in Italia (Decreto 3 aprile 2013, n. 55 Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244 - GU n. 118 del 22.5.2013)
- Circolare AGID n. 62/2013 concernente le Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD
- D.P.C.M. del 21 marzo 2013 - Il Decreto indica le particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la necessità di autenticare la loro conformità all'originale ad opera di un notaio o di un altro pubblico ufficiale a ciò autorizzato, con dichiarazione da questi firmata digitalmente ed allegata al documento informatico ai sensi dell'art. 22, comma 5, del CAD
- Decreto «FARE» (D. L. n. 69/2013 conv. L. 98/2013) - Agid sotto Pres. del Consiglio dei Ministri – domicilio digitale unico e PEC per tutti – razionalizzazione CED – FSE per le Regioni – wi-fi per tutti – eliminazione del valore giuridico del fax

# Il Codice dell'Amministrazione Digitale

**15/02/2015**

Piano di  
informatizzazione  
D.L. 90/2014 art.  
24 comma 3 bis

**31/03/2015**

Obiettivi  
accessibilità  
Circolare  
61/2013 Agid

**11/10/2015**

Protocollo  
Informatico  
**Dpcm**  
**3/12/2013**

**Agosto 2016**

Nuove Regole  
Tecniche  
Documento  
Informatico  
**Dpcm**  
**13/11/2014**

**11 Aprile 2017**

Manuale di  
Conservazione  
**Dpcm**  
**3/12/2013**

# Documento Informatico & Firme elettroniche

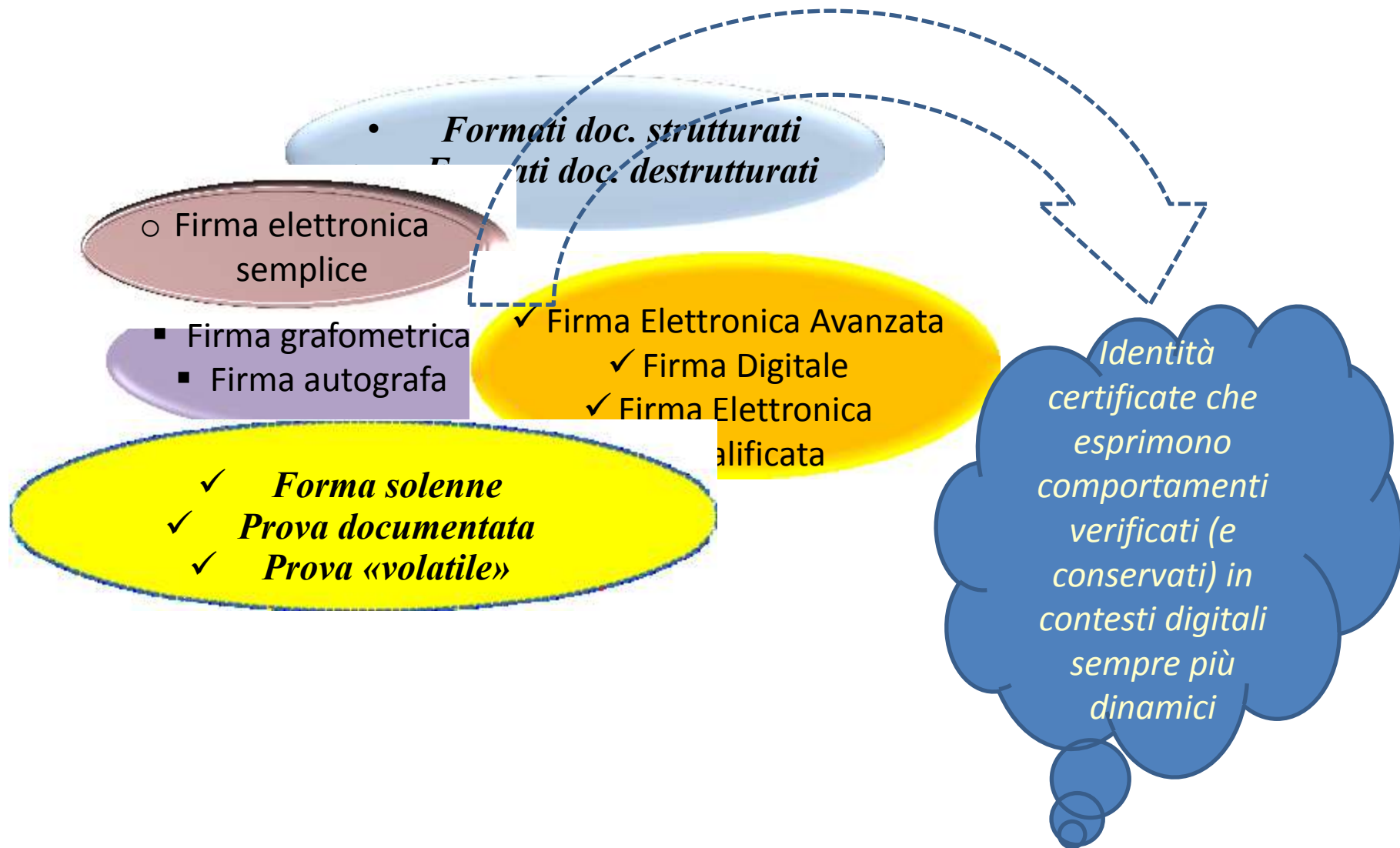
L'informazione digitale rilevante per sua natura ormai è sempre più dinamica, spesso strutturata e rappresentata da flussi di dati trasmessi in modalità multicanale:

- *è quindi sempre più spesso modificabile*
  - *non è facilmente attribuibile*
- *viaggia su canali tendenzialmente insicuri*
- *è continuamente sottoposta al cambiamento tecnologico*
  - *non è facilmente conservabile nel tempo*

...ma l'informazione è  
un documento??

va, quindi, inevitabilmente  
ridisegnato il concetto di  
forma scritta digitale

Nel nostro attuale ordinamento giuridico abbiamo diverse tipologie di formati documentali, quindi più forme e più firme in merito al documento informatico :

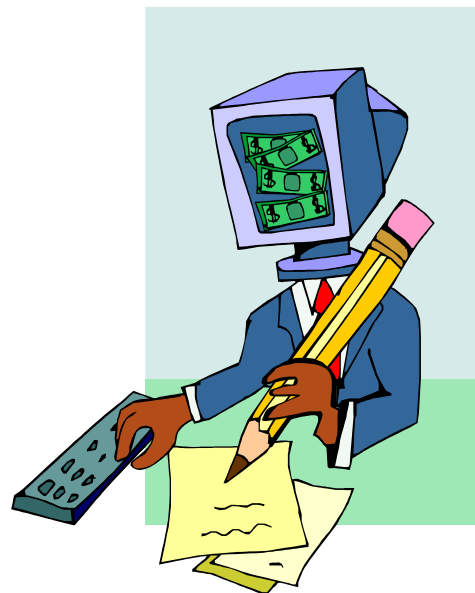




# La scommessa del futuro digitale è:

## Garantire:

- La (ragionevolmente) certa paternità
- La corretta trasmissibilità e gestione
- La adeguata fascicolazione e archiviazione
- Il trattamento a norma
- La necessaria sopravvivenza nel tempo a tutti i **dati** digitali che siano strategici per l'impresa o la PA e/o che abbiano un rilievo giuridico attraverso avanzate tecniche di sicurezza informatica



# Cosa è un dato?

**Dato** (dal latino *datum* che significa letteralmente fatto) ciò che è conosciuto o accertato, specialmente in quanto può servire di base per successivi calcoli o ragionamenti (i dati di un problema; dati statistici). In informatica ogni informazione che possa essere trattata da un computer: elaborazione elettronica dei dati (Dizionario Garzanti).

**Dati di identificazione personale**: un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica o un'unica persona fisica che rappresenta una persona giuridica (Reg. EIDAS)

**Dato personale**: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (Codice privacy)

**Dato identificativo**: i dati personali che permettono l'identificazione diretta dell'interessato (Codice privacy)

**Dato delle pubbliche amministrazioni**: il dato formato, o comunque trattato da una pubblica amministrazione (Codice Amministrazione Digitale).

*In realtà, facciamo riferimento a un «**dato informativo**», perché a voler essere precisi il dato è la più piccola unità significativa dell'informazione non ancora elaborata, mentre l'**informazione** è un insieme di dati aggregati a scopo di comunicazione attraverso lo spazio o il tempo .*

# Cosa è un documento?

**Documento** (deriva dal latino *Docere*, cioè insegnare - *documentum* : rappresentare, dare prova): in senso generico si considera l'informazione affissa in un supporto. In senso più proprio esso è lo scritto che convalida o certifica la realtà di un fatto, di una condizione, di una situazione, specialmente in ambito burocratico, amministrativo o giuridico (Dizionario Garzanti)

**Documento** (in ambito diplomatistico): Testimonianza scritta di un fatto di natura giuridica, compilata con l'osservanza di determinate forme, le quali sono destinate a procurarle fede e a darle forza di prova (Cesare Paoli, *Diplomatica*, Firenze, Le Lettere, 1987, p.18).

**Documento** (in ambito archivistico) «Tutti i libri, le carte, le mappe, le fotografie o gli altri materiali documentari, indipendentemente dalla forma o dalle loro caratteristiche, prodotti o ricevuti da ogni pubblica o privata istituzione, nello svolgimento delle sue funzioni istituzionali o in connessione con la conduzione dei suoi affari particolari, e conservati, o degni di essere conservati, dalla stessa istituzione o dal suo successore, come testimonianza delle sue funzioni, della sua politica, delle decisioni, procedure, operazioni, o altre attività, o a causa del valore informativo dei dati ivi contenuti» (Th.R.Schellenberg, *Modern Archives:Principles and Techniques*, Chicago, Illinois, Midway, 1975).

# Il documento informatico non è “carta informatica”:

«**documento digitale**»: testi, immagini, dati strutturati, disegni, programmi, filmati formati tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica, di cui sia identificabile l'origine (art. 1 lett. d) DMEF 23 gennaio 2004 - Modalita' di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto e art. 1 lett. d) deliberazione ALPA 13 dicembre 2011)

“**documento informatico**: rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti” (C.A.D., art. 1, comma 1° , lett.p)

«**documento elettronico**»: qualsiasi contenuto **conservato** in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (Regolamento eIDAS - REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

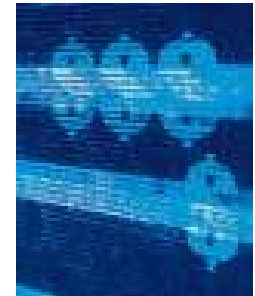
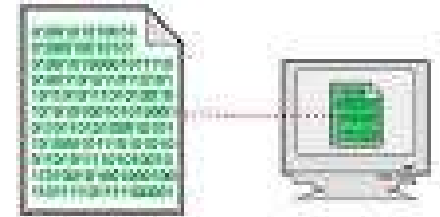
## IL DOCUMENTO ANALOGICO

è un oggetto materiale



## IL DOCUMENTO INFORMATICO

è un oggetto immateriale



# I dati e i documenti informatici amministrativi nel CAD...

**Art. 23 ter** : “Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i **dati** e i **documenti informatici** detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge”.

**Art. 51 comma 2 bis** le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri **archivi**, non appena vengano a conoscenza dell'inesattezza degli stessi

Ai sensi dell'art. 40 del CAD comma 1, le PA formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni del codice e delle regole tecniche in vigore.

## *Lo scopo della Normativa*

*Garantire al Documento Informatico Amministrativo, Contabile e Fiscale:*

- **La paternità (Firma Digitale o altri sistemi di identificazione)**
- **L'integrità (Firma Digitale/Firma Elettronica Qualificata e FEA)**
- **La trasmissibilità informatica (e-mail, PEC o SPC o EDI...)**
- **la corretta gestione (archiviazione elettronica)**
- **La “memorizzazione digitale” nel tempo (Firma Digitale, Marca Temporale e Procedure di Sicurezza)**

*attraverso una complessa procedura di conservazione*

Massima attenzione ai  
formati documentali

**N.B.:** *Duplica  
funzione della  
firma digitale*

## Forma scritta (digitale) ad substantiam

è un documento informatico con firma digitale, con firma elettronica qualificata o con firma elettronica avanzata



*La firma garantisce  
l'integrità e la solennità  
formale*



## Forma scritta (digitale) ad probationem

è il dato informativo e identificativo registrato durevolmente in un sistema di conservazione



*documenti informatici a  
formazione progressiva*



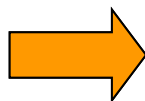
*Documentazione scritta digitale: registrazione statica e immutabile di informazioni digitali  
giuridicamente rilevanti*

## ... la fase di formazione del documento informatico, quindi, si modifica

*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle PA*

Secondo il comma 1 dell'art. 3 del **DPCM 13 novembre 2014** il documento informatico è formato mediante una delle seguenti principali modalità:

- a) redazione tramite l'utilizzo di appositi strumenti software;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.



*Integrità e immutabilità?*



*Commi 2 e 3 dell'art. 3 delle Regole tecniche sulla formazione del documento informatico:*



«Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

Il documento informatico, identificato in modo univoco e persistente, è memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.».

*Commi 4 e 5 dell'art. 3 delle Regole tecniche sulla formazione del documento informatico:*



«Nel caso di documento informatico formato ai sensi del comma 1, lettera a) , le caratteristiche di immutabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
- b) l'apposizione di una validazione temporale;
- c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
- d) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
- e) il versamento ad un sistema di conservazione.

Nel caso di documento informatico formato ai sensi del comma 1, lettera b) , le caratteristiche di immutabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione».



*Commi 6 e 7 dell'art. 3 delle Regole tecniche sulla formazione del documento informatico:*



«nel caso di documento informatico formato ai sensi del comma 1, lettere c) e d), le caratteristiche di immodificabilità e di integrità sono determinate dall'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, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione. Laddove non sia presente, al documento informatico immodificabile è associato un riferimento temporale».



## *Comma 9 delle Regole tecniche sulla formazione del documento informatico:*



«9. Al documento informatico imm modificabile vengono associati i metadati che sono stati generati durante la sua formazione. L'insieme minimo dei metadati, come definiti nell'allegato 5 al presente decreto, è costituito da:

- a) l'identificativo univoco e persistente;
- b) il riferimento temporale di cui al comma 7;
- c) l'oggetto;
- d) il soggetto che ha formato il documento;
- e) l'eventuale destinatario;
- f) l'impronta del documento informatico.

Eventuali ulteriori metadati sono definiti in funzione del contesto e delle necessità gestionali e conservative.»



## La più bella definizione, non tecnica, di archivio

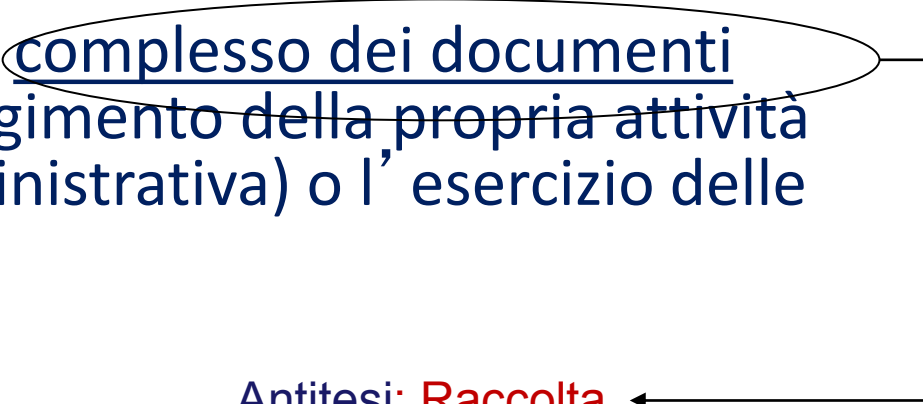
L'archivio è una **istituzione di pubblica fede da cui dipende la nostra democrazia**. Permette alla gente di ispezionare la documentazione di ciò che il governo ha fatto. Mette i funzionari e le istituzioni in grado di rivedere le proprie azioni e aiuta i cittadini ad assegnare le responsabilità a coloro a cui esse appartengono.

<http://www.archives.gov>

# DEFINIZIONE DI ARCHIVIO

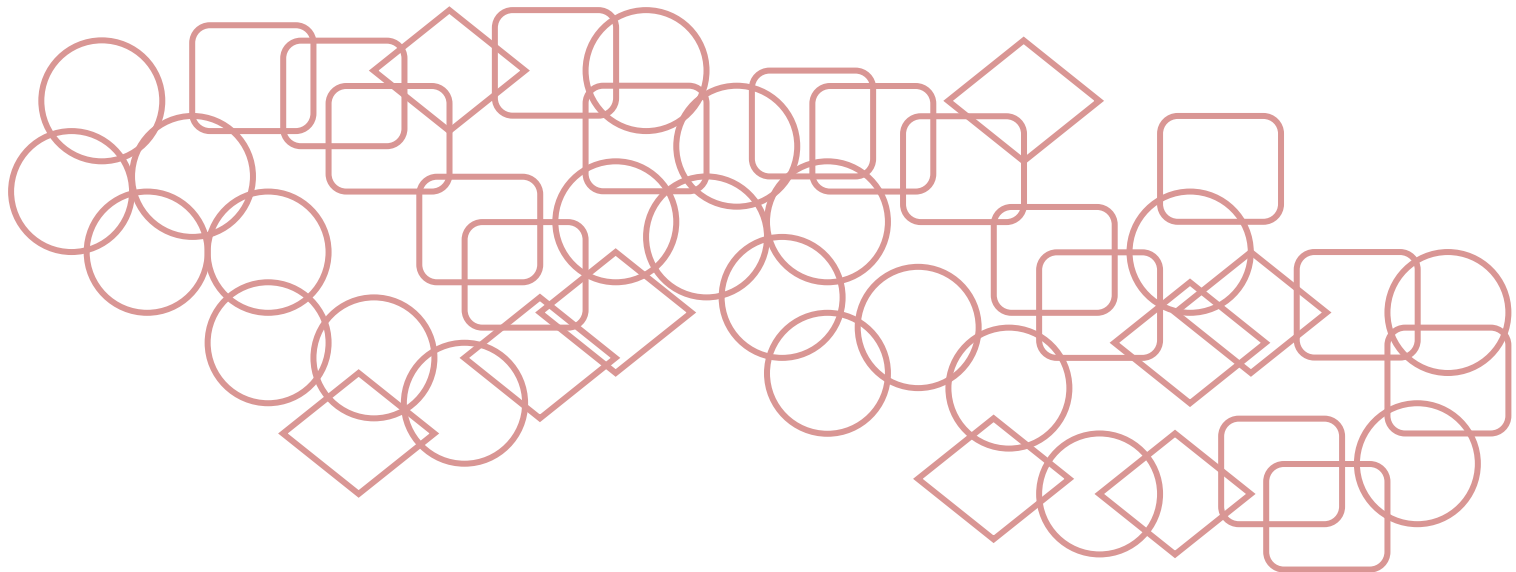
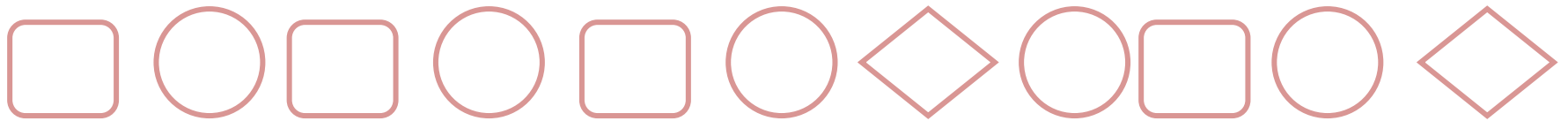
Per archivio si intende il complesso dei documenti prodotti durante lo svolgimento della propria attività (pratica, giuridica, amministrativa) o l'esercizio delle proprie funzioni.

Antitesi: Raccolta



# MEMORIZZAZIONE PIATTA

## MEMORIZZAZIONE ARCHIVISTICA



# La registrazione e la segnatura di protocollo

Il registro di protocollo è un registro nel quale si annotano in ordine cronologico la ricezione o la spedizione di atti (provenienti da privati o da altre pubbliche amministrazioni).

I registri di protocollo della pubblica amministrazione costituiscono una fonte di prova privilegiata che fa fede fino a querela di falso per la posizione e la responsabilità di cui sono investiti gli addetti alla relativa tenuta (Consiglio di Stato sez. VI, 26 maggio 1999, n. 693).

**È, quindi, un atto pubblico di fede privilegiata!**

# Il nuovo DPCM 3 dicembre 2013 - Regole tecniche per il protocollo informatico

## Requisiti minimi di sicurezza

Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Le registrazioni delle attività rilevanti e delle modifiche devono essere protette da modifiche non autorizzate.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immodificabilità del contenuto.

## Le novità contenute nel DPCM 13 novembre 2014 per i documenti amministrativi informatici

**Art. 9** - Il documento amministrativo informatico, di cui all'art 23 -ter del Codice, formato mediante una delle modalità di cui all'art. 3, comma 1, del presente decreto, è identificato e trattato nel sistema di gestione informatica dei documenti di cui al Capo IV del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, comprensivo del registro di protocollo e degli altri registri di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, dei repertori e degli archivi, nonché degli albi, degli elenchi, e di ogni raccolta di dati concernente stati, qualità personali e fatti già realizzati dalle amministrazioni su supporto informatico, in luogo dei registri cartacei, di cui all'art. 40, comma 4, del Codice, con le modalità descritte nel manuale di gestione.

**4.** Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis , 40 -bis e 65 del Codice sono identificate e trattate come i documenti amministrativi informatici nel sistema di gestione informatica dei documenti di cui al comma 3 ovvero, se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto, memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione.

**5.** Il documento amministrativo informatico assume le caratteristiche di immutabilità e di integrità, oltre che con le modalità di cui all'art. 3, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti di cui al comma 3.

## Le novità contenute nel DPCM 13 novembre 2014 per i documenti amministrativi informatici

### **Art. 11. Trasferimento nel sistema di conservazione**

1. Il responsabile della gestione documentale, ovvero, ove nominato, il coordinatore della gestione documentale:

- a) provvede a generare, per uno o più documenti informatici, un pacchetto di versamento nelle modalità e con i formati concordati con il responsabile della conservazione e previsti dal manuale di conservazione;
- b) stabilisce, per le diverse tipologie di documenti, in conformità con le norme vigenti in materia, con il sistema di classificazione e con il piano di conservazione, i tempi entro cui i documenti debbono essere versati in conservazione;
- c) verifica il buon esito dell'operazione di versamento tramite il rapporto di versamento prodotto dal sistema di conservazione.

### **Art. 12. Misure di sicurezza**

1. Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale predispone, in accordo con il responsabile della sicurezza e il responsabile del sistema di conservazione, il piano della sicurezza del sistema di gestione informatica dei documenti, nell'ambito del piano generale della sicurezza ed in coerenza con quanto previsto in materia dagli articoli 50 -bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. Le suddette misure sono indicate nel manuale di gestione.

## **Le novità contenute nel DPCM 13 novembre 2014 per i documenti amministrativi informatici**

### **I FASCICOLI INFORMATICI, I REGISTRI E I REPERTORI INFORMATICI DELLA PUBBLICA AMMINISTRAZIONE SI FORMANO COME DOCUMENTI INFORMATICI E VANNO VERSATI IN CONSERVAZIONE**

#### **Art. 15. Trasferimento in conservazione**

1. Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale provvede a generare, per uno o più fascicoli o aggregazioni documentali informatiche o registri o repertori informatici di cui all'art. 14, un pacchetto di versamento che contiene i riferimenti che identificano univocamente i documenti informatici appartenenti al fascicolo o all'aggregazione documentale informatica.
2. Ai fascicoli informatici, alle aggregazioni documentali informatiche, ai registri o repertori informatici si applica quanto previsto per il documento informatico all'art. 11, comma 1, lettere b) e c) .

Ma l'identità è una firma?

E la PEC firma?



*"On the Internet, nobody knows you're a dog."*

## Il documento cartaceo - La firma analogica

**Funzioni della sottoscrizione** tese a garantire la **sicurezza ed autenticità** del documento:

- indicativa;
- dichiarativa;
- probatoria.

**Caratteristiche della sottoscrizione:**

- autografia;
- nominatività;
- leggibilità;
- non riproducibilità.

**Art. 2699 c.c.:** “L’atto pubblico è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l’atto è formato”.

**Art. 2702 c.c.:** “La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta”.

**Art. 2712 c.c.:** “Le riproduzioni fotografiche o cinematografiche (*oggi anche informatiche*), le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime”.

**Art. 2719 c.c.:** “Le copie fotografiche di scritture hanno la stessa efficacia delle autentiche, se la loro conformità con l'originale è attestata da pubblico ufficiale competente ovvero non è espressamente disconosciuta”.

Ma c'è sempre bisogno  
della forma scritta e sottoscritta  
per stipulare i contratti on line?

**Art. 1321. (Nozione).**

Il contratto è l'accordo di due o più parti per costituire, regolare o estinguere tra loro un rapporto giuridico patrimoniale.

**Art. 1322. (Autonomia contrattuale).**

Le parti possono liberamente determinare il contenuto del contratto nei limiti imposti dalla legge e dalle norme corporative.

Le parti possono anche concludere contratti che non appartengano ai tipi aventi una disciplina particolare, purchè siano diretti a realizzare interessi meritevoli di tutela secondo l'ordinamento giuridico.

**Art. 1325. (Indicazione dei requisiti).**

I requisiti del contratto sono:

- 1) l'accordo delle parti;
- 2) la causa;
- 3) l'oggetto;
- 4) la forma, quando risulta che è prescritta dalla legge sotto pena di nullità.

## La legge attualmente in vigore e le sue definizioni

**Firma elettronica** (lett. q) - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

**Firma elettronica avanzata** (lett. q-bis) - Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

**Firma elettronica qualificata** (lett. r) - Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

**Firma digitale** (lett. s) - Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario 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

→ L'imputabilità giuridica

Le distinzioni:

- la sottoscrizione

- la firma

→ ...la forma scritta digitale non sempre coincide con la sottoscrizione del documento ...

## Il Codice della amministrazione digitale (artt. 20, 21)

1-bis. L'idoneità del documento informatico a soddisfare il requisito della **forma scritta** e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

1. Il documento informatico, cui è apposta una **firma elettronica**, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con **firma elettronica avanzata, qualificata o digitale**, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria 2-bis). Salvo quanto previsto dall'articolo 25, le **scritture private di cui all'articolo 1350**, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. [...]

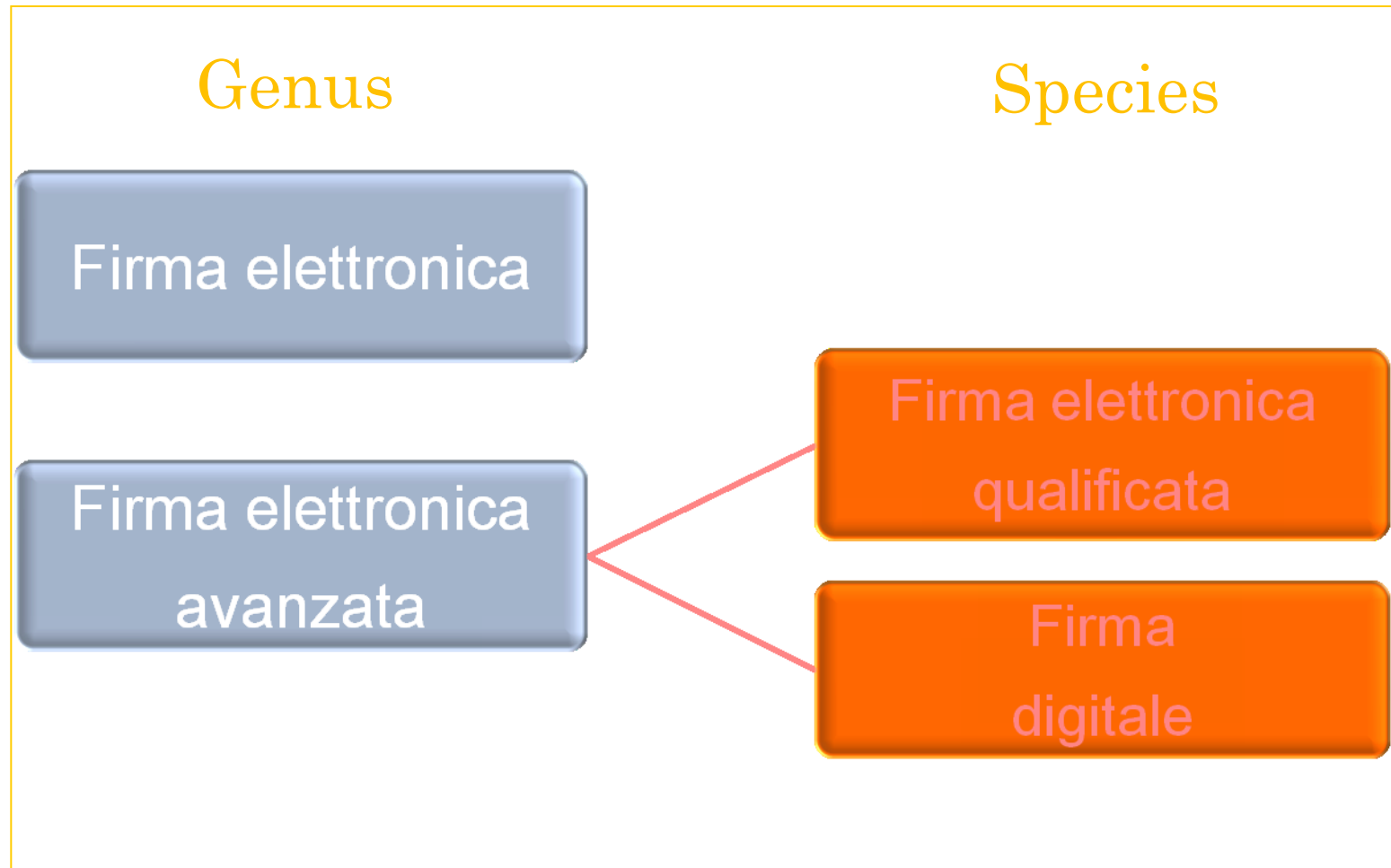
I formati documentali

La forma digitale sottoscritta:

- firma digitale
- **FEA**
- firma «grafometrica»

... differenziare documenti e contratti...

# *Genus e species di firma elettronica in Italia*



## La “sottoscrizione” nel documento informatico: la firma digitale

La **crittografia** è la scienza che studia la tecnica che consente la trasformazione di un messaggio universalmente leggibile in uno leggibile soltanto a coloro che dispongono della chiave di decifrazione.

### Funzione:

- integrità;
- paternità;
- riservatezza;
- non ripudio.



Per assicurare ciò è fondamentale l'uso di algoritmi matematici applicando i quali si garantisce:

la **segretezza** del contenuto dell'informazione;

l'**autenticità**, individuando univocamente la sorgente;

l'**integrità**, verificando che il messaggio non abbia subito alterazioni;

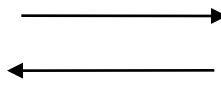
la **non ripudiabilità**, assicurando che l'autore del messaggio non possa negare di aver generato il messaggio stesso.

# Le Chiavi asimmetriche

CERTIFICATORE QUALIFICATO

Generazione della coppia di chiavi

Chiave  
privata



Chiave  
pubblica  
Certificata

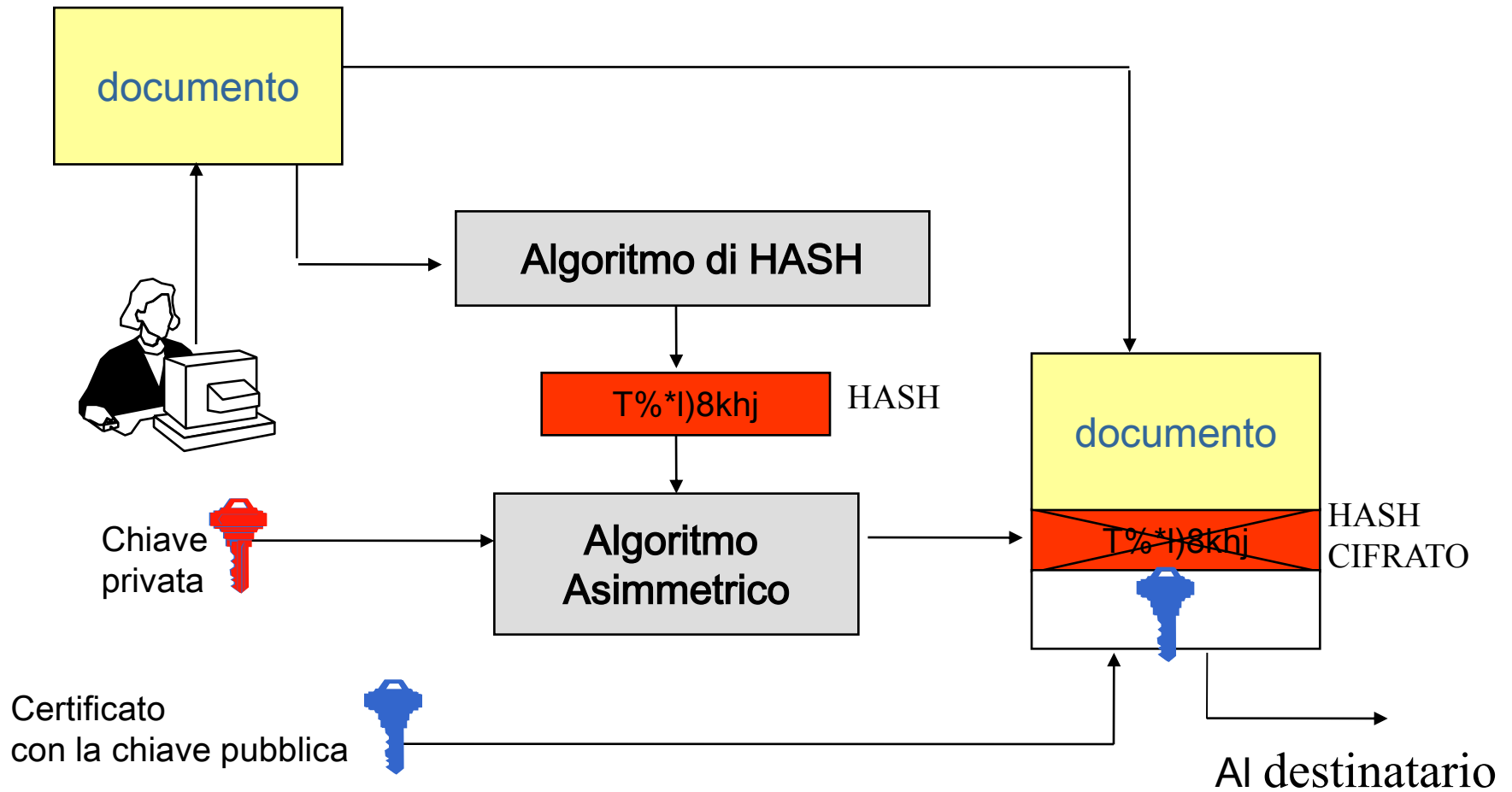


Può solo  
chiudere

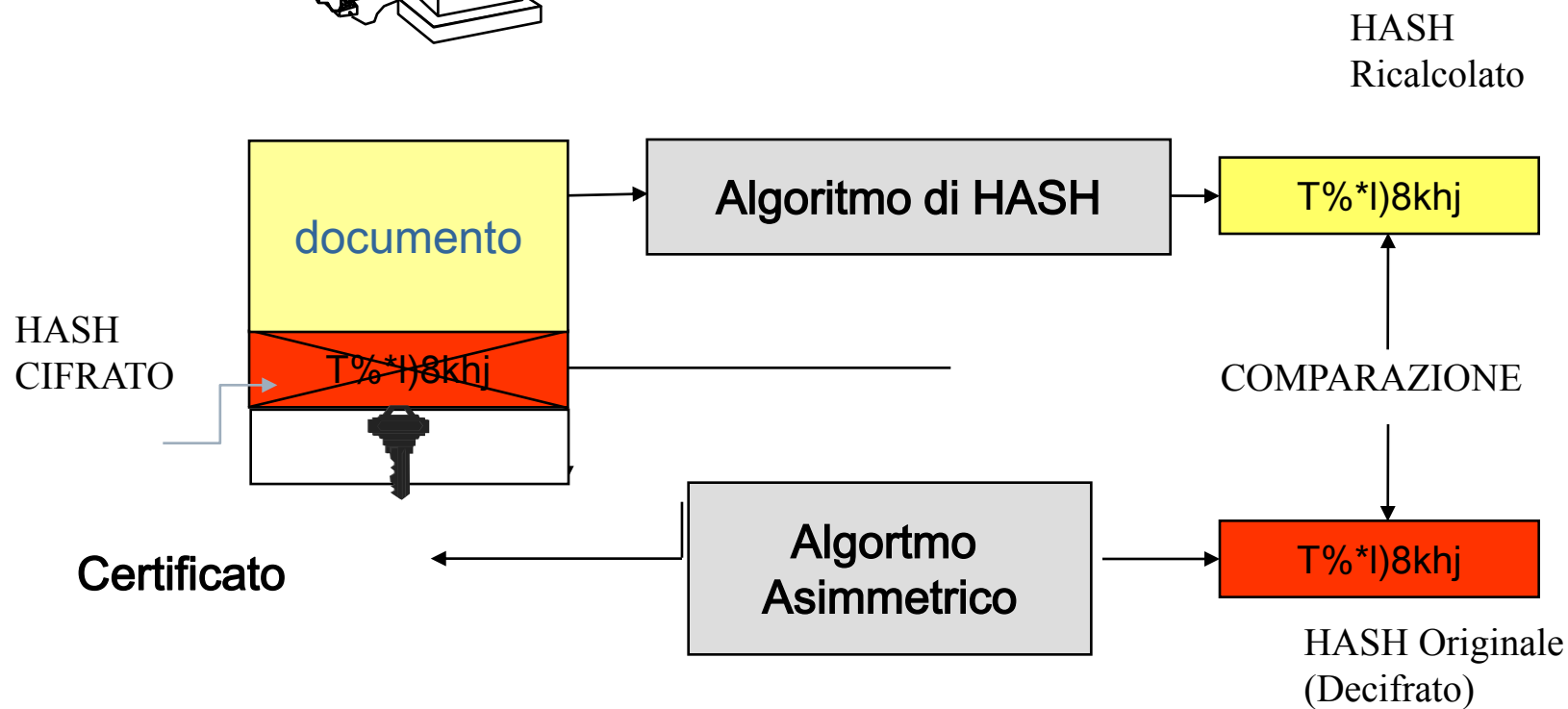
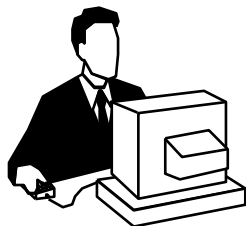


Può solo  
aprire e leggere

# Processo di firma digitale



# Verifica della firma digitale



## FIRMA DIGITALE

valore formale e probatorio  
predefinito per legge

difficilmente disconoscibile

equivale alla sottoscrizione  
cartacea

associata alla marca temporale  
conferisce al documento  
certezza giuridica

**E la firma  
elettronica  
avanzata?**



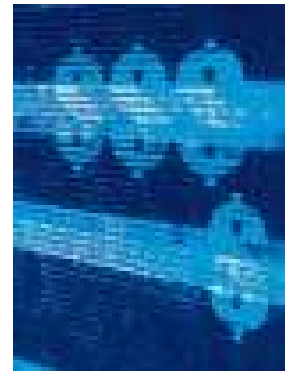
## FIRMA ELETTRONICA

è genus indefinito

La sua valenza formale  
e probatoria è relativa

può essere facilmente  
disconoscibile

garantisce la paternità,  
non sempre l'autenticità





# Valore giuridico della Firma Digitale

## Comma 3 dell'art. 21 del CAD

L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

## ART. 62 DPCM 22 febbraio 2013 - Valore della firma digitale nel tempo

La firma digitale, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma digitale in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato.



# Valore giuridico della Firma Digitale

## **ART. 4 comma 3 DPCM 22 febbraio 2013**

Il documento informatico sottoscritto con firma elettronica qualificata o firma digitale non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21 comma 2 del Codice se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.



# Valore giuridico della Firma Digitale

*Limiti d'uso al certificato di firma?*

*(artt. 28 e 30 CAD)*

Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato (art. 30, comma 3).

## **ART. 24 (Firma digitale)**

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. **L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.**
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71 , la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

## **Art. 35. Dispositivi sicuri e procedure per la generazione della firma**

**1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:**

- a) sia riservata;**
- b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;**
- c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.**

**2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.**

**3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima. (si vedano anche artt. 3 e 5 DPCM 22 febbraio 2013)**

# La firma elettronica avanzata

## Le nuove regole Tecniche

La Firma Elettronica Avanzata, non è un determinato software, né una determinata tecnologia, ma è un sistema neutro, sicuro e affidabile che garantisca l'appartenenza di un documento informatico reso imm modificabile ad un soggetto

### Art. 56 Caratteristiche delle soluzioni di firma elettronica avanzata

1. Le soluzioni di firma elettronica avanzata devono garantire:
- a) l'identificazione del firmatario del documento;
  - b) la connessione univoca della firma al firmatario;
  - c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
  - d) la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
  - e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
  - f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
  - g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati
  - h) la connessione univoca della firma al documento sottoscritto

*La sua valenza formale e probatoria dipende dal sistema che si sviluppa*

*E ricordiamoci sempre:*

**Articolo 1352 c.c.** Se le parti hanno convenuto per iscritto di adottare una determinata forma per la futura conclusione di un contratto, si presume che la forma sia stata voluta per la validità di questo

**Esempio di firma elettronica avanzata:** strong authentication + sistema sicuro di transazione + sistema di conservazione dei log

## La firma elettronica avanzata - Le nuove regole Tecniche

### Art. 57 - Obblighi per i soggetti che erogano per proprio conto soluzioni di firma elettronica avanzata

1. I soggetti di cui all'art. 55, comma 2, lettera a) devono:

a) **identificare in modo certo l'utente tramite un valido documento di riconoscimento**, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una **dichiarazione di accettazione delle condizioni del servizio da parte dell'utente**;

b) conservare per almeno venti anni la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'art. 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;

c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;

d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;

e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1;

f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;

g) pubblicare le caratteristiche di cui alle lettere e) e f) sul proprio sito internet; anche sul proprio sito internet;

**f) consentire l'uso della firma elettronica qualificata e della firma digitale, ove applicabile, in alternativa alla firma elettronica avanzata per i procedimenti per i quali è previsto l'uso della firma elettronica avanzata;**

g) assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della firma elettronica avanzata e un servizio di assistenza.

+ copertura danni sino a € 600.000 (copertura assicurativa) e pubblicazione su sito web del sistema di copertura

***Limiti d'uso:** 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) (art. 60 Regole*

***Non è prevista alcuna autorizzazione preventiva***

#### **Le domande:**

-so quello che firmo?  
-come associo la firma al documento?  
-cosa conservo? e chi conserva?  
-rilascio ricevute certe su ciò che si è firmato? *Etc.*

## La firma elettronica avanzata - Le nuove regole Tecniche

### **Art. 58 - Obblighi per i soggetti che realizzano per terzi soluzioni di firma elettronica avanzata**

Certificazione obbligatorie per soluzione di firma elettronica avanzata realizzate per le amministrazioni pubbliche:

- ISO/IEC 27001
- ISO 9001

Non sono richieste per le persone giuridiche pubbliche e per le persone giuridiche private possedute o controllate dall'amministrazione pubblica che realizzino soluzioni di firma elettronica avanzata per altre amministrazioni pubbliche.

**Art. 60 Limiti d'uso:** 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 che dispone l'utilizzo della firma elettronica avanzata

# La firma elettronica avanzata - Le nuove regole Tecniche

## Art. 61 Soluzioni di firma elettronica avanzata

1. L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del Codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005 recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata» sostituisce, nei confronti della pubblica

amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche.

2. L'utilizzo della Carta d'Identita' Elettronica, della Carta Nazionale dei Servizi, del documento d'identita' dei pubblici dipendenti (Mod. ATe), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del codice.

3. I formati della firma di cui al comma 2 sono gli stessi previsti ai sensi dell'art. 4, comma 2.

4. Le applicazioni di verifica della firma generata ai sensi del comma 2 devono accertare che il certificato digitale utilizzato nel processo di verifica corrisponda ad uno degli strumenti di cui al medesimo comma.

5. I certificatori accreditati che emettono certificati per gli strumenti di cui al comma 2 rendono disponibili strumenti di verifica della firma.

6. Fermo restando quanto disposto dall'art. 55, comma 1, al fine di favorire la realizzazione di soluzioni di firma elettronica avanzata, l'Agenzia elabora Linee guida sulla base delle quali realizzare soluzioni di firma elettronica avanzata conformi alle presenti regole tecniche.

## Firma elettronica avanzata - Considerazioni

La firma elettronica avanzata non è un oggetto ma è un processo complesso che tende al raggiungimento di un risultato al quale le norme riconoscono un determinato valore giuridico.

Tutto il processo dev'essere orientato alla sicurezza delle informazioni trattate; si deve garantire l'integrità e la leggibilità dei dati oltre ad impedire ogni possibile accesso abusivo ai dati stessi (soprattutto quando i dati trattati siano di tipo biometrico). Si consiglia il rispetto di standard relativi alla sicurezza delle informazioni trattate (ISO 27001)

E' molto importante che tutto il processo sia correttamente registrato e i relativi *log file* siano conservati insieme al documento e a tutte le altre informazioni relative al processo di firma elettronica.

Un idoneo sistema di conservazione garantirà l'integrità e l'esibizione dei documenti e delle relative informazioni associate (tali informazioni, legate al documento, costituiscono la FEA).

# **Le tecniche biometriche**

Impronte digitali

Riconoscimento della geometria della mano

Riconoscimento dell'iride

Sistemi per il riconoscimento del volto

Sistemi per il riconoscimento della voce

Riconoscimento della retina

**Sistemi per il riconoscimento della firma**

## La firma biometrica

**Il termine “riconoscimento biometrico” fa riferimento all’identificazione o alla verifica automatica dell’identità attraverso strumenti di valutazione di caratteristiche fisiche o comportamentali (Linee Guida CNIPA 2004)**

Acquisizione sul documento dell’immagine della sottoscrizione di un soggetto



Se non è verificabile il comportamento di chi firma, non è biometria e non crea problemi tecnici e di privacy, ma ha scarso valore giuridico

Acquisizione evoluta sul documento di vari dati comportamentali di chi firma



È la versione elettronica della sottoscrizione cartacea. Può essere di volta in volta verificabile la sua autenticità e non c’è centralizzazione di dati biometrici

(può richiedere la necessità di interpello ai sensi dell’art. 17 Codice privacy e la sua valenza probatoria può essere robusta)

Acquisizione biometrica come credenziale forte di autenticazione



Può servire a garantire un accesso riservato di transazione, ma anche come modello di sottoscrizione digitale e, quindi, garantire un accesso in remoto al proprio certificato di firma custodito da un HSM

(può richiedere la necessità di interpello ai sensi dell’art. 17 Codice privacy e può servire per “sbloccare” in remoto certificati di firma digitale)

## **25. Firma autenticata.**

**1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.**

**2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste**

**nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.**

**3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.**

**4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.**

...ma tanto i giudici  
di queste cose non si occupano  
..... no?

## *La Giurisprudenza:*

- **il TAR Puglia - Bari, Sez. I, con la sentenza n. 1019 del 24 maggio 2012** dichiara l'obbligatorietà della sottoscrizione dell'offerta con firma digitale in caso di gare telematiche

- una recente sentenza del **TAR Milano** (T.A.R. Lombardia Milano Sez. IV, Sent., 11-07-2012, n. 1942) ha annullato un provvedimento di esclusione dalla procedura di gara indetta da LOMBARDIA INFORMATICA SPA. Lombardia Informatica S.p.A. aveva provveduto all'esclusione dalla gara per la fornitura di soluzioni infusionali la Baxter S.p.A., società ricorrente, in quanto all'atto della presentazione dell'offerta in via elettronica, avrebbe sottoscritto ed immesso nel sistema un documento vuoto, file di dimensioni pari a 0 kb nonchè privo dei contenuti richiesti, in luogo della dichiarazione di offerta economica. La procedura di gara pubblica era gestita in via informatica per il tramite di piattaforma "SinTel". E' stato accertato che il sistema SinTel utilizzato non garantiva il tracciamento di ogni operazione compiuta sulla piattaforma, e l'inalterabilità delle registrazioni (log) di sistema, quali rappresentazioni informatiche degli atti e delle operazioni compiute, valide e rilevanti ai sensi di legge.

## Firma digitale e e-mail...

**Cons. Stato Sez. VI, 20/09/2013, n. 4676**

Ai sensi dell'art. 1, comma 1, lettera s) del Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82) la **firma digitale** si distingue dall'ordinaria **firma elettronica** per il particolare grado di certezza ed attendibilità che la caratterizza (Parziale riforma della sentenza del T.a.r. Lombardia - Milano, sez. III, n. 842/2013).

**Cons. Giust. Amm. Sic., 31/05/2011, n. 404**

Nell'ipotesi di **polizza generata in via informativa**, ma prodotta in forma cartacea, il requisito dell'autenticità deve essere asseverato da un pubblico ufficiale ai sensi del ripetuto art. 23, comma 2-bis del D.Lgs. n. 82 del 2005 (codice dell'amministrazione digitale), a mente del quale "le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte, se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato".

## Valore della PEC e della email...

### Giudice di pace Palermo Sez. III, 21/07/2012

In ossequio a quanto stabilito dagli artt. 20, 21 e 45 del Codice dell'Amministrazione Digitale (D.Lgs. n. 82 del 2005), la **posta elettronica non certificata** e, quindi, priva di sottoscrizione digitale, è considerata alla stregua del telegramma, avente efficacia probatoria della scrittura privata ex art. 2705 c.c. e, ad ogni modo, liberamente apprezzabile dal Giudice

### Trib. Prato, 15/04/2011

#### Ditta Naturaasi c. Soc. R.F. & Sanilab

Posto che **l'e-mail non certificata** è qualificabile come documento informatico dotato di firma elettronica c.d. semplice, la stessa, sul piano probatorio, è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità (nella specie, l'e-mail tradizionale era volta a provare l'avvenuta tempestiva denuncia dei vizi della merce acquistata).

Dello stesso avviso **Tribunale Termini Imerese, ordinanza**

**22.02.2015** «i documenti informatici inviati via email non certificata, devono essere considerati documenti sottoscritti con firma elettronica “leggera”».

## originale informatico vs. copia cartacea



La Suprema Corte accogliendo il ricorso dell'Agenzia delle Entrate specifica come **i dati dichiarativi presentati dal contribuente sono quelli contenuti nella traccia telematica**, “mentre la copia cartacea sottoscritta dal contribuente è strumento utile ai soli controlli, eventuali e successivi. Non vi è perciò ragione per ritenere che in ipotesi di contraddizione tra i dati risultanti nella dichiarazione presentata in via telematica e la copia conservata con modalità cartacea il giudicante possa attribuire preferenza a questi ultimi e perciò ritenere che la predetta copia cartacea sia opponibile all'Amministrazione a preferenza di quella trasmessale per via telematica”. (**ordinanza Cassazione n. 20047 del 30 agosto 2013**)

## Valore probatorio dei log



Il tribunale di Napoli esamina il caso di un licenziamento di un dipendente per accesso abusivo alle mail aziendali e approfondisce il profilo dell'efficacia probatoria dei file di log (**Tribunale Napoli, Ordinanza 29/04/2014**). La relazione del CTU ha evidenziato come i sopra citati dati non siano attendibili né affidabili. L'azienda **non ha adottato adeguate misure per attestare e preconstituirsì l'immodificabilità e attendibilità dei file di log**. Nel momento in cui è stata effettuata la copia dei log che ricollegano al pc del ricorrente l'indirizzo Ip utilizzato – il contenuto del file non è stato sottoposto a nessun controllo di integrità al fine di sancire l'identità assoluta con il dato nel suo contenuto originale, così come prodotto dal sistema. Secondo il CTU, **in assenza di tali garanzie, il dato dei file di log è alterabile**. I log sono stati infatti esportati su file di testo, consultabili e alterabili con un normale strumento di edizione. **L'azienda avrebbe dovuto adottare specifiche policy di conservazione della prova digitale attraverso la produzione di log firmati digitalmente e marcati temporalmente**, al fine di stabilire, in questo caso, l'esatta identità con il dato originale. In mancanza del sopra citato accorgimento, il CTU sottolinea la reale possibilità di alterazione del contenuto del file in considerazione del fatto che il file copiato è in semplice formato testo: **secondo il giudice, alla luce delle risultanze del CTI, viene così a mancare la prova inconfutabile del contenuto del file di log**.

## Utilità di Policy di utilizzo e Privacy policy e Validità dei log

### Garantire prove digitali giuridicamente rilevanti

«Per quanto concerne l'attestazione di tutte le operazioni effettuate dal Pannello il Cliente prende atto ed accetta, per se e per i terzi cui ha consentito, a qualsiasi titolo, di utilizzare il Servizio, che faranno fede esclusivamente i LOG del Fornitore conservati a norma di legge, come indicato nella Policy Privacy Aruba» (fonte **contratto Cloud Aruba**).

# E allora il cinguettio è un dato o un documento?



Il Consiglio di Stato (sentenza n. 769 del 12 febbraio 2015) ha avuto modo di precisare che “**gli atti dell’autorità politica, limitati all’indirizzo, controllo e nomina ai sensi del decreto legislativo n.165 del 2001, debbono pur sempre concretarsi nella dovuta forma tipica dell’attività della pubblica amministrazione [...], anche, e a maggior ragione, nell’attuale epoca di comunicazioni di massa, messaggi, cinguettii, seguiti ed altro, dovuti alle nuove tecnologie e alle nuove e dilaganti modalità di comunicare l’attività politica**”. Già nella sentenza del Consiglio di Stato n. 5444/2003, richiamata nella pronuncia n. 769/2015, i Giudici di Palazzo Spada avevano evidenziato che **le forme tipiche degli atti e dei provvedimenti amministrativi rappresentano uno “strumento di garanzia del regolare svolgimento dell’attività amministrativa, sia nell’interesse del cittadino, costituendo remora ad arbitri, sia nell’interesse della stessa p.a., agevolando detta forma l’espletamento della funzione di controllo, ed è, quindi, espressione dei principi di buon andamento ed imparzialità dell’amministrazione**”. Anche la Cassazione Civile, nella sentenza n.1970/2002 (anche questa richiamata nel recente arresto del Consiglio di Stato) aveva precisato che la **volontà di obbligarsi della p.a. non può desumersi per implicito da fatti o atti, dovendo essere manifestata nelle forme, necessariamente rigide, richieste dalla legge.**

# Comunicazioni rilevanti nella Società dell'Informazione



**La premessa:  
per comunicare  
nella Società dell'informazione  
è davvero necessario  
trasmettere i documenti?**

## **ART. 34 (Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati)**

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29 ; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto **ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri**; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

2. Per la **formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna** ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui **all'articolo 71**.  
[...]

5. **Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali** secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

## Art. 47 CAD

### (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

**1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.**

2. Ai fini della **verifica della provenienza** le comunicazioni sono valide se:

- a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
- c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. **È in ogni caso esclusa la trasmissione di documenti a mezzo fax (\*) ;**
- d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

3. Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. Le pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

*(\*) punto aggiunto dal c.d. Decreto del Fare (Decreto legge n. 69/2013), in seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto 2013.*

## **Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni**

1. La **carta d'identità elettronica** e la **carta nazionale dei servizi** costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (**SPID**).

2-ter Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.

## **Art. 64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni**

2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'*articolo 17 del decreto legislativo 9 aprile 2003, n. 70*.

2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

- a) al modello architetturale e organizzativo del sistema;
- b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;
- c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;
- d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;
- e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;
- f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

## **Art. 65 CAD (Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica)**

1. Le istanze e le dichiarazioni presentate **per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici** ai sensi **dell'articolo 38, commi 1 e 3**, del decreto del presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

- a) se sottoscritte mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato;
- b) ovvero, **quando l'autore è identificato** dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente,
- c) ovvero quando l'autore **è identificato dal sistema informatico con i diversi strumenti di cui all'articolo, 64, comma 2**, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente nonché quando le istanze e le dichiarazioni sono inviate con modalità le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000 n. 445;
- c-bis) ovvero se trasmesse dall'autore mediante la propria **casella di posta elettronica certificata** purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale.

1-ter. Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate ai sensi e con le modalità di cui al comma 1, lettere a), c) e c-bis), comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso.

2. Le istanze e le dichiarazioni inviate o compilate sul sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.

3. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:

«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82».

## Art. 38 TUDA - Modalità di invio e sottoscrizione delle istanze

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

2. Le istanze e le dichiarazioni inviate per via telematica, vi comprese le domande per la partecipazione a selezioni e concorsi per l'assunzione, a qualsiasi titolo, in tutte le pubbliche amministrazioni, o per l'iscrizione in albi, registri o elenchi tenuti presso le pubbliche amministrazioni, sono valide se effettuate secondo quanto previsto dall'*articolo 65 del decreto legislativo 7 marzo 2005, n. 82*.

3. Le istanze e le dichiarazioni sostitutive di atto di notorietà da produrre agli organi della amministrazione pubblica o ai gestori o esercenti di pubblici servizi sono sottoscritte dall'interessato in presenza del dipendente addetto ovvero sottoscritte e presentate unitamente a copia fotostatica non autenticata di un documento di identità del sottoscrittore. La copia fotostatica del documento è inserita nel fascicolo. Le istanze e la copia fotostatica del documento di identità possono essere inviate **per via telematica**; nei procedimenti di aggiudicazione di contratti pubblici, detta facoltà è consentita nei limiti stabiliti dal regolamento di cui all'articolo 15, comma 2 della legge 15 marzo 1997, n. 59.

## **Art. 45. CAD Valore giuridico della trasmissione**

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

## **Sentenza della Corte di Cassazione sulla validità della trasmissione via PEC**

Secondo la sentenza n. 9892/2015 della Suprema Corte, la notifica mediante posta elettronica certificata è valida ed efficace, trattandosi di uno strumento di comunicazione di atti ed avvisi a soggetti diversi dall'imputato previsto direttamente dalla legge, per cui il destinatario dell'atto non può eccepire di non aver letto il messaggio o di non averlo ricevuto per difficoltà tecniche o malfunzionamenti della rete telefonica o telematica presso lo studio professionale.

#### **46. Dati particolari contenuti nei documenti trasmessi. (CAD)**

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

**La conservazione a norma  
dei documenti informatici  
(firmati e trasmessi)  
è un'eventualità o un obbligo?**



**In verità non è solo questione di adeguamento a leggi:  
è in gioco il futuro delle nostre informazioni rilevanti e, per rendere  
sicuro questo futuro, l'unico scenario possibile è garantire nell'ente  
pubblico e nell'impresa la possibilità di sviluppare una nuova forma  
di organizzazione e di gestione dei flussi documentali digitalizzati in  
modo certo e incontrovertibile!**



**E solo un sistema di conservazione digitale a norma può consentire un futuro  
giuridicamente rilevante ai nostri documenti informatici!**



## ART. 43 CAD (Riproduzione e conservazione dei documenti)

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui e' prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformita' dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.

La conservazione digitale non è una scelta eventuale, ma un dovere!

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71.





Quindi, **chi fattura elettronicamente, chi invia e riceve PEC, chi utilizza la firma digitale** (o altre forme di firma) per sottoscrivere documenti informatici, chi pubblica online documenti, **deve conservare tali oggetti informatici predisponendo un idoneo sistema di conservazione allineato alle nuove regole tecniche, altrimenti mette a rischio la validità di tutti i documenti informatici prodotti o ricevuti dal proprio ente di appartenenza.**

**si deve conservare la PEC?**



**Dal Codice Civile:**

**Articolo 2220.** Le scritture devono essere conservate per dieci anni dalla data dell'ultima registrazione (2312).

Per lo stesso periodo devono conservarsi le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti.

**Le scritture e documenti di cui al presente articolo possono essere conservati sotto forma di registrazioni su supporti di immagini**, sempre che le registrazioni corrispondano ai documenti e possano in ogni momento essere rese leggibili con mezzi messi a disposizione dal soggetto che utilizza detti supporti (Comma aggiunto dall'Articolo 7 bis, Decr.Legge 10 giugno 1994, n. 357, convertito con modificazioni dalla Legge 8 agosto 1994, n. 489 )



La PEC non è forse corrispondenza?



## Art. 2214.

### Libri obbligatori e altre scritture contabili.

L'imprenditore che esercita un'attività commerciale deve tenere il libro giornale e il libro degli inventari.

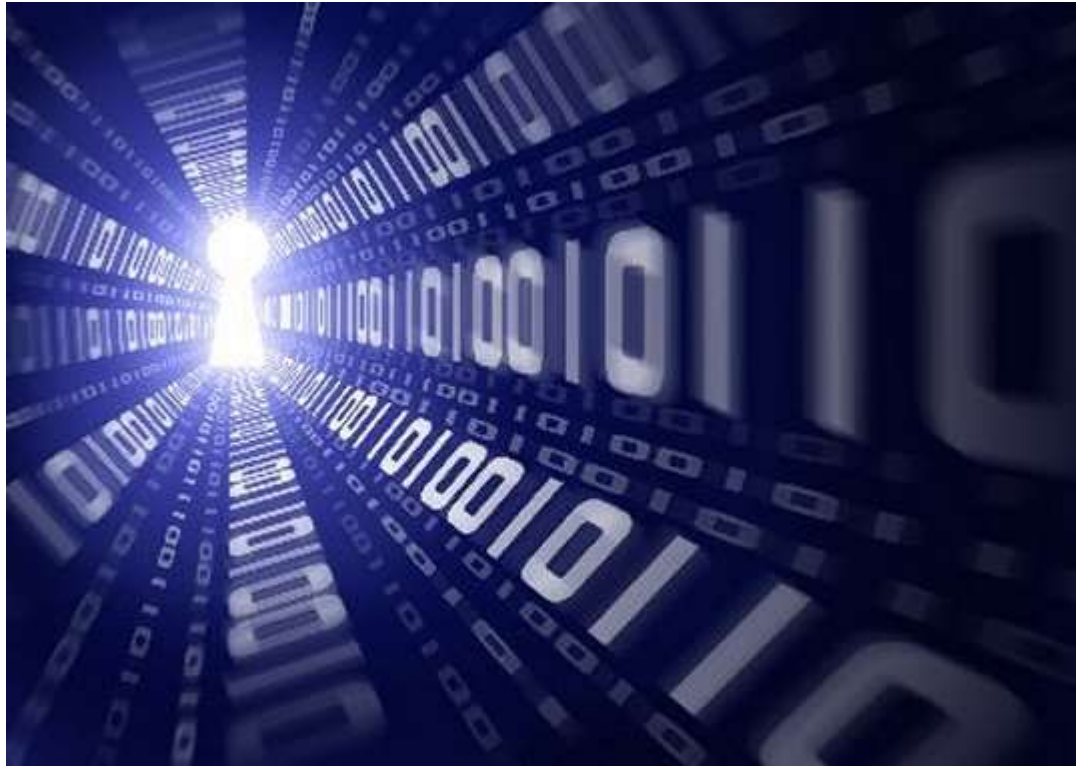
Deve altresì tenere le altre scritture che siano richieste dalla natura e dalle dimensioni dell'impresa e conservare ordinatamente per ciascun affare gli **originali** delle lettere, dei telegrammi e delle fatture ricevute, nonché le copie delle lettere, dei telegrammi e delle fatture spedite.

### Cosa conservo?

**Messaggio di posta elettronica certificata:** un documento informatico composto dal **testo del messaggio**, dai **dati di certificazione** e dagli eventuali **documenti informatici allegati** (art. 1, lett. g - f del DPR 68/2005)

- *Testo del messaggio (solitamente formato eml)*
- *dati di certificazione: ricevute (formato xml e p7s)*
- *eventuali allegati (documenti informatici sottoscritti e non..)*

# La casistica per il protocollo e la PEC



# Il DPCM 31 ottobre 2000 vige ancora??

## art. 15, commi 2 e 3

### *Modalità di trasmissione e registrazione dei documenti informatici*

3. Ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti. L'indirizzo di tale casella è riportato nell'indice delle amministrazioni pubbliche.

**DPR 445/2000 Art. 53 comma 5** Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione.

## **40-bis. Protocollo informatico. (CAD)**

**1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71.**

**Art. 17 DPCM 3 dicembre 2013 contenente le nuove Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis , 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005**

**2. Ciascuna amministrazione istituisce, per ogni area organizzativa omogenea, almeno una casella di posta elettronica certificata direttamente associata al registro di protocollo da utilizzare per la protocollazione dei messaggi ricevuti e spediti, ai sensi dell'art. 40 -bis del Codice. L'indirizzo di tali caselle è riportato nell'indice delle amministrazioni e nel manuale di gestione di cui all'art. 5, nonché pubblicato sul sito dell'amministrazione.**

# La casistica: cosa si protocolla?

Messaggio o documento?

(DPR 445/2000, art. 53.5)

**PEC**  
e documento informatico



**PEC**



**PEC**  
e documento scansionato  
(pdf, tiff, gif, jpeg, etc.)



**PEC**

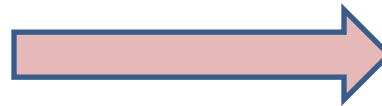


N.B. Distinguere sempre vettore da autore  
e la spedizione a nome di terzi

# La casistica: cosa si protocolla?

Messaggio o documento?  
(DPR 445/2000, art. 53.5)

**PEC**  
e documento scansiono  
(pdf, tiff, gif, jpeg, etc.)



**PEC**



In questo caso la PEC è equiparabile  
alla copertina telefax, anche priva di messaggio



Documentazione  
Cognome, Nome e Indirizzo del Privato  
Cognome  
Cognome  
Cognome

**[Non è società]**

**Fax**

Al: \_\_\_\_\_ Da: \_\_\_\_\_  
Per: \_\_\_\_\_ Per: \_\_\_\_\_  
Indirizzo: \_\_\_\_\_ Indirizzo: \_\_\_\_\_  
Città: \_\_\_\_\_ Città: \_\_\_\_\_

☐ In risposta ☒ Per la consegna ☐ Per la consegna ☐ Per la consegna

☐ In risposta

Il documento non deve essere più grande di 10.000 byte e deve essere in formato pdf, tiff, gif, jpeg, ecc. Per  
cognome e cognome di nascita per l'indirizzo deve essere in italiano, cognome italiano con nome nel vostro  
fax. Almeno un numero di telefono fisso o cellulare. Il documento, il cognome, il telefono, il fax,  
cognome e cognome. Almeno un numero di telefono fisso o cellulare.

# La casistica: cosa si protocolla?

## Messaggio o documento? (DPR 445/2000, art. 53.5)

**PEC**

**e documento scansito  
(pdf, tiff, gif, jpeg, etc.)  
con documento di identità**



PEC



In questo caso la PEC è equiparabile all'istanza via telefax

[illegible]

# La casistica: cosa si protocolla?

Messaggio o documento?  
(DPR 445/2000, art. 53.5)

**PEC**

**e documento testuale**  
**(Word, Excel, Open office, etc.)**



**PEC**



# La casistica: cosa si protocolla?

Messaggio o documento?  
(DPR 445/2000, art. 53.5)

**em@il**  
e documento informatico



**PEC**  
(se aperta)



**em@il**  
e documento scansionato  
(pdf, tiff, gif, jpeg, etc.)  
con documento identità



**PEC**  
(se aperta)



# La casistica: cosa si protocolla?

Messaggio o documento?  
(DPR 445/2000, art. 53.5)

**em@il**

e documento scansito  
(pdf, tiff, gif, jpeg, etc.)



**PEC**  
(se aperta)



**em@il**

e documento testuale  
(Word, Excel, Open office, etc.)



**PEC**  
(se aperta)



# La casistica: cosa si protocolla?

(DPR 445/2000, art. 53.5)

PEC



em@il

**Possiamo equiparare la trasmissione  
a una raccomandata semplice?**

E se la PEC trasmette allegati?

**È necessario almeno stabilire  
e dichiarare i formati accettati!**

Quali documenti  
sono digitalizzabili?



*Ci facciamo ancora questa domanda?*



## DOCUMENTI RILEVANTI AI FINI TRIBUTARI SMATERIALIZZABILI AI SENSI DEL DM 23 GENNAIO 2004

- Fatture, bollette, lettere, telegrammi ricevuti
- Distinte meccanografiche e registri (corrispettivi e registri fatture emesse)
- Il libro giornale e il libro degli inventari
- Le scritture ausiliarie nelle quali devono essere registrati gli elementi patrimoniali e reddituali
- Le scritture ausiliarie di magazzino
- Il registro dei beni ammortizzabili
- Il bilancio d'esercizio, composto da stato patrimoniale, conto economico e nota integrativa
- I registri prescritti ai fini IVA, quali ad esempio il registro degli acquisti, il registro dei corrispettivi, il registro delle fatture emesse
- Dichiarazioni fiscali, modulistica relativa ai pagamenti (ad esempio i modelli F23 ed F24), alle fatture e documenti simili
- I libri sociali
- Il libro delle adunanze e delle deliberazioni delle assemblee
- Il libro delle adunanze e delle deliberazioni del collegio sindacale
- Il libro delle adunanze e delle deliberazioni del comitato esecutivo
- Il libro delle adunanze e delle deliberazioni delle assemblee degli obbligazionisti
- Le disposizioni contenute nel DMEF 23 gennaio 2004, infine, si applicano alla relazione sulla gestione (art.2428 c.c.) e alla relazione dei sindaci (art. 2429 c.c.) e dei revisori contabili , che per legge devono essere allegate al bilancio d'esercizio.



Oggi comunque tutti i documenti possono nascere informatici o comunque sono digitalizzabili ex lege

### **Altre tipologie documentali:**

- Documenti amministrativi
- Documenti privacy
- Contratti e atti di trasferimento quote societarie (DL 112/2008)
- Documenti sanitari e amministrativi
- Nota spese dipendenti e schede carburante
- Libro Unico del lavoro (DL 112/2008 conv. L. 133/2008 + Circ. Min. Lavoro n. 20/2008)
- Registri assicurativi
- la corrispondenza telematica, la PEC
- ...contratti web, «registrazioni informatiche», tracciati strutturati etc.

**Documenti analogici?**

**Documenti informatici?**



**Copie e Duplicati**  
**Documenti analogici originali unici:**

**DPCM 21 marzo 2013**  
**DMEF 17 giugno 2014)**  
**DPCM 13 novembre 2014**

## Il Codice della amministrazione digitale (art. 1)

i-bis) **copia informatica di documento analogico**: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-ter) **copia per immagine su supporto informatico di documento analogico**: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) **copia informatica di documento informatico**: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinquies) **uplicato informatico**: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

### Da leggere:

**Art. 22.** Copie informatiche di documenti analogici;

**Art. 23.** Copie analogiche di documenti informatici;

**Art. 23-bis.-** Duplicati e copie informatiche di documenti informatici;

**Art. 23-ter.** Documenti amministrativi informatici

**Art. 35** – Firma automatica e firma remota



Le copie e i duplicati

**Il caos nelle PA:**

-Chi fa cosa?

**Articolo 4 - Conservazione sostitutiva di documenti analogici**

1. Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o piu' impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta cosi' il corretto svolgimento del processo.
2. Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformita' di quanto memorizzato al documento d'origine.
3. La distruzione di documenti analogici, di cui e' obbligatoria la conservazione, e' consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo quanto previsto al comma 4 dell'art. 6 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
4. Il processo di riversamento sostitutivo di documenti analogici conservati avviene mediante memorizzazione su altro supporto ottico. Il responsabile della conservazione, al termine del riversamento, ne attesta il corretto svolgimento con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti o su una evidenza informatica contenente una o piu' impronte dei documenti o di insiemi di essi. Qualora il processo riguardi documenti originali unici di cui al comma 2, e' richiesta l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformita' di quanto riversato al documento d'origine.

## **CAD - Art. 22. Copie informatiche di documenti analogici**

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.
2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.
3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.
4. Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.
5. **Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.**
6. **Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.**

## **DPCM 21 marzo 2013 - Art. 1**

1. Il presente decreto individua, ai sensi dell'art. 22, comma 5, del decreto legislativo 7 marzo 2005, n. 82, le tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale cartaceo oppure, in caso di conservazione sostitutiva, la loro conformita' all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a cio' autorizzato con dichiarazione da questi apposta e firmata digitalmente nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71, del decreto legislativo n. 82 del 2005.
2. I documenti di cui al comma 1 sono indicati nell'allegata Tabella A che forma parte integrante del presente decreto.
3. Resta ferma la facolta' per le pubbliche amministrazioni di conservare in originale analogico unico documenti diversi da quelli oggetto del presente decreto.
4. Dalla data di pubblicazione del presente decreto sulla Gazzetta Ufficiale della Repubblica italiana, viene meno per le pubbliche amministrazioni l'obbligo previsto dall'art. 22, comma 6 del decreto legislativo n. 82 del 2005 della conservazione dei documenti originali analogici unici diversi da quelli oggetto del presente decreto oppure, in caso di conservazione sostitutiva degli stessi, dell'attestazione della loro conformita' all'originale con dichiarazione autentica di un notaio o di altro pubblico ufficiale a cio' autorizzato, firmata digitalmente ed allegata al documento informatico.

• Con l'entrata in vigore del DPCM 21 marzo 2013, l'obbligo generale di conservazione cartacea o di autenticazione della copia digitalizzata in caso di conservazione sostitutiva dei documenti analogici originali unici è dunque venuto meno, in quanto sono state individuate le particolari tipologie di documenti analogici originali unici interessati da questo obbligo ai sensi dell'art. 22 comma 5 del Codice dell'Amministrazione Digitale, elencate nella tabella A dell'allegato al decreto, ossia:

- i documenti che è possibile **dematerializzare e conservare digitalmente**, garantendo la conformità all'originale attraverso **l'autenticazione da parte di un notaio o di un altro pubblico ufficiale** (ad esempio: decreti del Presidente del Consiglio dei Ministri, decreti ministeriali, interministeriali o ancora i titoli del debito pubblico; documenti inerenti alla tutela dello Stato, dell'ordine e della sicurezza pubblica; atti soggetti alla classificazione di segretezza e al segreto di Stato);
- documenti per i quali permane, invece, **l'obbligo della conservazione dell'originale cartaceo** (tra questi ultimi troviamo, a titolo di esempio, gli atti giudiziari, processuali o di polizia giudiziaria e gli atti notarili).

*Ciò implica che...*

Il DPCM 21 marzo 2013 implicitamente individua un'ulteriore categoria di documenti analogici unici, che non sono stati espressamente ricompresi negli elenchi di cui all'allegato:

per tali documenti è possibile mettere in atto un processo di conservazione digitale SENZA che la loro conformità all'originale debba essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con apposita dichiarazione firmata digitalmente ed allegata al documento informatico.

**Ma sulla disciplina relativa alla  
conservazione di questi documenti...**

*Qual è la posizione del  
Ministero dei beni culturali?*

## Art. 43, comma 4, del CAD

*“Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.*



Viene meno l'automaticità dell'applicazione delle procedure di digitalizzazione, così come descritte nel CAD, e la conseguente distruzione dei documenti analogici amministrativi, che rimane comunque sempre subordinata all'autorizzazione del Ministero dei beni culturali

Da ultimo il **DMEF 17 giugno 2014** - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto – articolo 21, comma 5, del decreto legislativo n. 82/2005 (in GU 26 giugno 2013 n. 146)



Art. 4. Obblighi da osservare per la dematerializzazione di documenti e scritture analogici rilevanti ai fini tributari

1. Ai fini tributari il procedimento di generazione delle copie informatiche e delle copie per immagine su supporto informatico di documenti e scritture analogici avviene ai sensi dell'art. 22, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e termina con l'apposizione della firma elettronica qualificata, della firma digitale ovvero della firma elettronica basata sui certificati rilasciati dalla Agenzie fiscali. La conservazione avviene secondo le modalità di cui all'art. 3 del presente decreto.

2. Ai fini fiscali, la conformità all'originale delle copie informatiche e delle copie per immagine su supporto informatico di documenti analogici originali unici, è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le modalità di cui all'art. 22, comma 2, del decreto legislativo 7 marzo 2005, n. 82, e delle relative regole tecniche.

Grandi novità si respirano in materia di copie per immagine su supporto informatico di documenti analogici (art. 4), di duplicati informatici di documenti informatici (art. 5) e di copie ed estratti informatici di documenti informatici (art. 6). Il legislatore tecnico, infatti, non si è limitato a puntualizzare i concetti già espressi nel CAD (artt. 22 e segg.), ma di fatto ha deciso di **autorizzare forme certificate di acquisizione automatica di estratti e copie di documenti originariamente analogici o nativamente informatici**. Tali processi di acquisizione dovranno ovviamente assicurare che le copie prodotte abbiano forma e contenuto identici a quelli dei documenti da cui sono tratte, ma non più attraverso il solo raffronto dei documenti, ma anche attraverso la certificazione di processo nei casi in cui siano si sia deciso di adottare tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia. Questa importante novità si attendeva da tempo nel mercato della digitalizzazione documentale e sarà salutata con grande attenzione e probabile soddisfazione da chi da tempo si occupa di queste materie.

**come si conservano  
i documenti informatici?**



# Attraverso lo sviluppo di un Sistema di Conservazione Digitale dei documenti



**Non è solo questione di adeguamento a leggi:  
è in gioco il futuro delle nostre informazioni rilevanti e, per rendere  
sicuro questo futuro, l'unico scenario possibile è garantire nell'ente  
pubblico e nell'impresa la possibilità di sviluppare una nuova forma  
di organizzazione e di gestione dei flussi documentali digitalizzati in  
modo certo e incontrovertibile!**



**E solo un sistema di conservazione digitale a norma può consentire un futuro  
giuridicamente rilevante ai nostri documenti informatici!**



## Art. 44 CAD (Requisiti per la conservazione dei documenti informatici)

1. Il sistema di conservazione dei documenti informatici assicura:

- a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
- b) l'integrità del documento;
- c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originali;
- d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

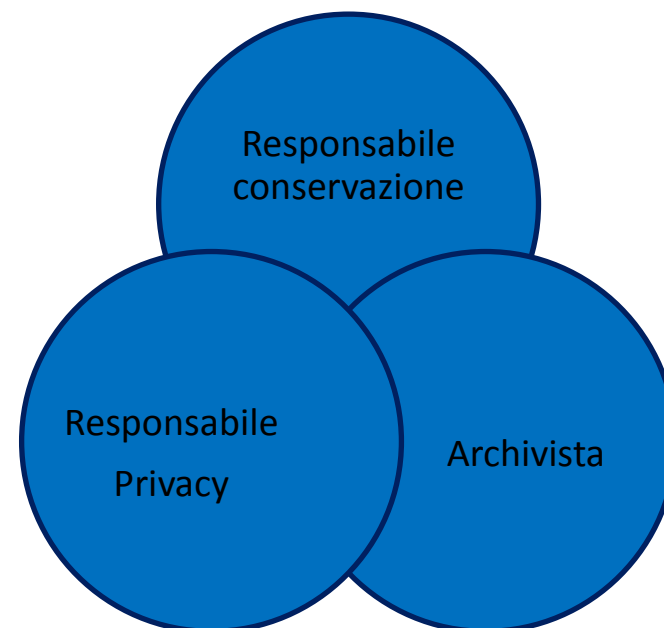


Chiave interpretativa per la normativa sulla conservazione dei documenti informatici e sulla fatturazione elettronica

## Art. 44, comma 1 bis CAD (Requisiti per la conservazione dei documenti informatici) - NEW

Il sistema di conservazione è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

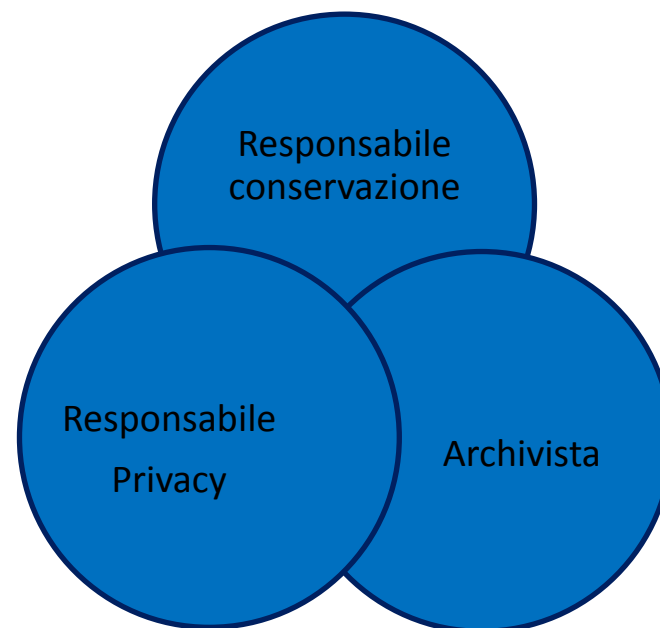
**La  
conservazione  
digitale si fa in  
tre!**



## Art. 7 Nuove Regole Tecniche in materia di conservazione contenute nel DPCM 3 dicembre 2013 (Responsabile della conservazione) - **NEW**

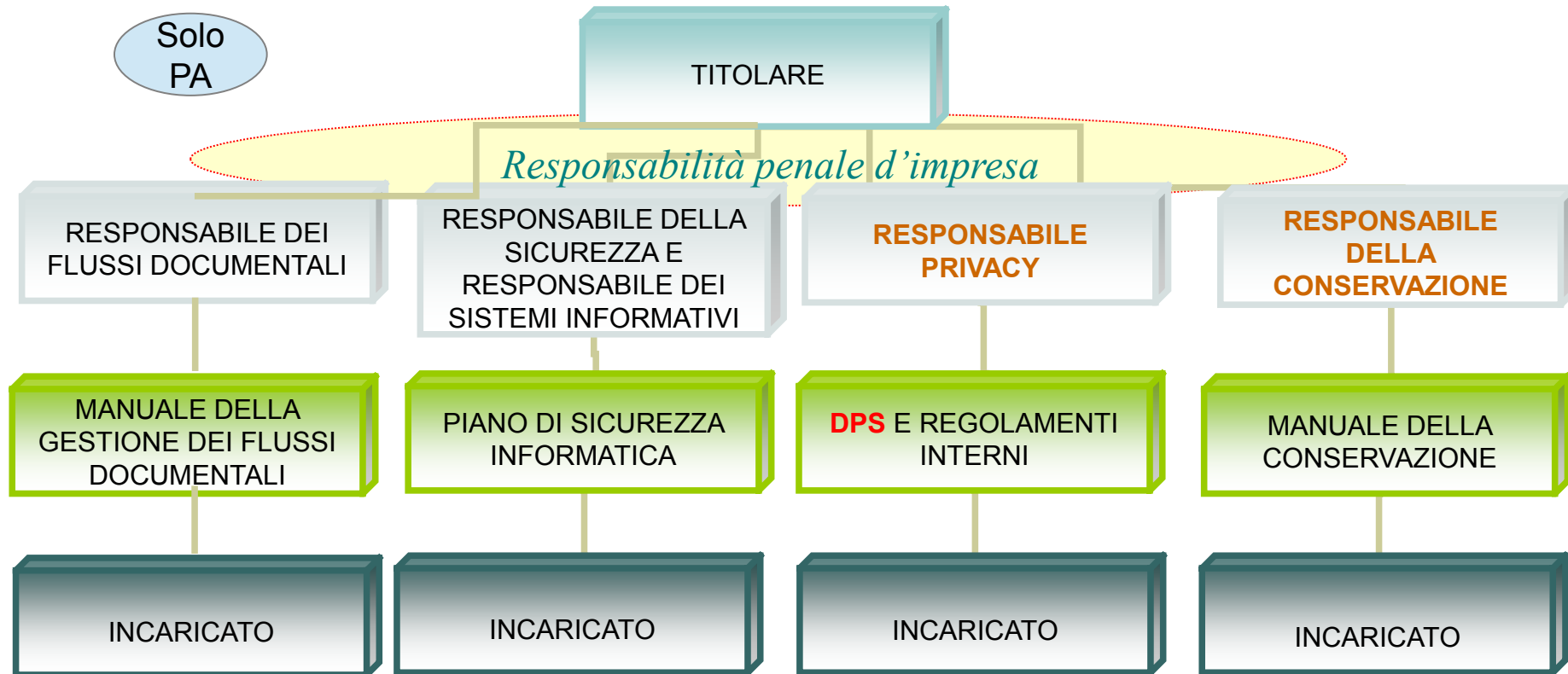
“Il responsabile della conservazione opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi che, nel caso delle pubbliche amministrazioni centrali, coincide con il responsabile dell'ufficio di cui all'art. 17 del Codice, oltre che con il responsabile della gestione documentale ovvero con il coordinatore della gestione documentale ove nominato, per quanto attiene alle pubbliche amministrazioni

***(almeno)* TRE figure professionali obbligatorie per chi gestisce documenti informatici**



# L'organizzazione

In strutture complesse gerarchia di responsabili a più livelli



*La Governance del patrimonio informativo di una società o una PA:  
Compliance normativa nella Società dell'Informazione*

# outsourcing?



Dal “nuovo” Codice della Amministrazione Digitale:

## Art. 44, comma 1 ter (Requisiti per la conservazione dei documenti informatici) - NEW

Il **responsabile della conservazione** può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.



Possibilità per i Responsabili della conservazione di aziende e P.A. di affidare in outsourcing i processi di conservazione digitale e ottenere la “certificazione di conformità” dei relativi processi!



Dalle Regole Tecniche (art. 6 Ruoli e Responsabilità):

6. Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare le specifiche funzioni e competenze affidate al delegato.

7. La conservazione può essere affidata ad un soggetto esterno, secondo i modelli organizzativi di cui all'art. 5, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.



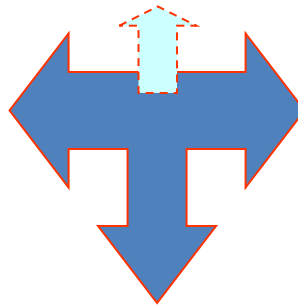
Possibilità per i Responsabili della conservazione di aziende e P.A. di affidare internamente o esternamente ruoli e responsabilità

## Un possibile schema di esternalizzazione dei servizi di conservazione

**Titolare** dei Documenti e dei Dati

(nomina Responsabile interno del procedimento conservazione  
che predispone il Manuale)

**Responsabile** del  
sistema di conservazione  
- **CONSERVATORE**  
(con suo referente  
interno)



**Delegato** al alcuni processi  
(back up, disaster recovery,  
verifiche, restore, procedure  
operative etc.)

**Organismo di Vigilanza e  
Certificazione**

Dal “nuovo” Codice della Amministrazione Digitale:

## **Art. 44 bis (Conservatori accreditati) - NEW**

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.
2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.
3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.



Vi è ora la possibilità di far accreditare presso **DigitPA (AGID)** i propri processi di conservazione sotto il profilo della sicurezza e della qualità (nel rispetto, quindi, di una serie di misure di sicurezza che variano a seconda della tipologia del dato trattato e degli strumenti utilizzati).  
(Circolare DigitPA 29 dicembre 2011 n. 59)

**Circolare AgID n. 65 del 10 aprile 2014**

Dalle Regole Tecniche (art. 5 Modelli organizzativi della conservazione):

1. Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente.

2. Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta:

a) all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare;

b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

3. Le pubbliche amministrazioni realizzano i processi di conservazione all'interno della propria struttura organizzativa o affidandoli a conservatori accreditati, pubblici o privati, di cui all'art. 44 -bis , comma 1, del Codice, fatte salve le competenze del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.



Tutto chiaro??

# **RESPONSABILITA' CONTRATTUALE DEL FORNITORE**

**Il Titolare deve nominare  
la società fornitrice esterna Responsabile del  
trattamento "in outsourcing" (art. 29 d.lgs.  
196/2003 e art. 6 comma 8 delle Regole  
Tecniche) del processo di conservazione o del  
trattamento dei dati**



Responsabilità ex art. 1218 c.c.  
(responsabilità contrattuale  
del debitore)



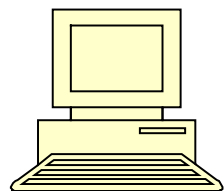
Responsabilità ex art. 1710 c.c.  
(rapporto di mandato, per  
violazione obbligo di diligenza)

### Criteri di scelta di un buon conservatore:

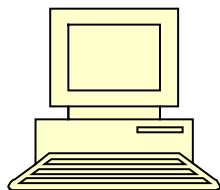
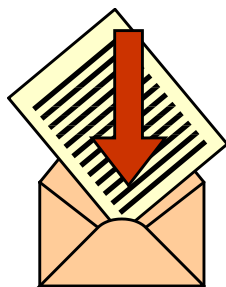
- la capacità di fornire una **prestazione altamente qualificata e specifica**;
- l'**esperienza** del fornitore nella conservazione sostitutiva in generale e, in particolare, per la specifica tipologia di documenti da conservare (nel caso, ad esempio, si tratti di documenti sanitari da conservare, sarà opportuno verificare la particolare esperienza del fornitore nella conservazione sostitutiva di tali documenti);
- la **conoscenza ed il rispetto della normativa privacy**, anche in considerazione della nuova formulazione dell'art. 44 del Codice dell'Amministrazione digitale;
- l'ampiezza dei servizi offerti, tra i quali merita di essere attentamente valutata anche l'offerta di applicazione dei **modelli organizzativi nell'azienda di cui al D. Lgs. 231/01**;
- il possesso di eventuali **certificazioni sui servizi proposti**;
- il **prezzo** del servizio;
- le **referenze**;

- le garanzie tecnologiche e di sistema offerte dal fornitore in relazione agli **standard di sicurezza informatica**, per esempio, in riferimento alla protezione dei dati personali e delle informazioni scambiate. Per quanto concerne la sicurezza informatica della globalità del sistema di conservazione, le norme ISO/IEC 27001:2013 e la specifica ETSI TS 101 533 (2011) (“Linee Guida per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni”); Standard UNI SInCRO 11386: 2010 (interoperabilità dell’indice) ; UNI ISO 15489-1-2:2006/2007 (Record Management); ISO 14721:2002 (OAIS – Open Archival Information System) etc.
- il livello di **professionalità del personale**;
- **polizze assicurative** a copertura dei rischi di custodia
- le **dimensioni ed il grado di umidità dei locali** in cui saranno conservati gli eventuali documenti analogici non distrutti in seguito al processo di conservazione, verificando preventivamente che siano stati rispettati gli standard richiesti dalla normativa europea;
- l’eventuale **accreditamento del fornitore ex art. 44-bis del CAD**, così come modificato dal D.lgs. 235/2010.

*i servizi in  
outsourcing*



Cliente



Outsourcer

*Fatturazione*

*Servizi di conservazione  
con nomina  
CONSERVATORE*

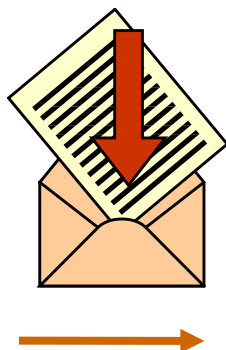
*Mi conviene esternalizzare?  
Cosa esternalizzo?*

**Responsabile del  
procedimento di  
conservazione**

**deleghe**

- Verifica
- Firma
- Gestione e Controllo
- **Studio e progettazione**
- Sicurezza e privacy
- Esibizione
- etc.

*i servizi in  
outsourcing*



*Fatturazione conto  
terzi*

*Chi  
firma?*

*Chi  
controlla?*

*Chi è  
responsabile?*

Cliente

Outsourcer

*L'“esternalizzazione” di alcuni  
processi aziendali fortemente  
specializzati e complessi, i quali  
devono essere realizzati in  
assoluto adeguamento a  
normative specifiche!*

*Servizi di conservazione  
con nomina quale  
CONSERVATORE*

*(che è anche  
responsabile esterno del  
trattamento dei dati  
personali)*



## Outsourcing... a cosa prestare attenzione?

- Formati da utilizzare (art. 68 CAD)
- Supporti idonei
- Certificazione di processi
- Modelli di disaster recovery
- Modelli di business continuity
- La copia della copia della copia...chi la effettua?
- Lock-in
- *Etc.*

## I documenti del Buon Responsabile della Conservazione in outsourcing

- **Contratto di Outsourcing** per l'affidamento del servizio
- **Allegato A** – Offerta Economica
- **Allegato B** – Descrizione procedure operative e aspetti tecnici
- **Allegato C** – Nomina del Conservatore
- **Allegato D** – Nomina a Responsabile Esterno per il trattamento dei dati personali
- **Allegato E** – **Manuale della conservazione dei documenti**
- **Allegato F** – **Documento Programmatico sulla Sicurezza** (o suo estratto) e Piano della Sicurezza del sistema di conservazione
- **Allegato G** – Delega interna per il coordinamento delle funzioni nel procedimento di conservazione
- **Allegato H** – Deleghe operative interne

**Quale modello organizzativo  
e quali regole seguire  
per il proprio sistema di conservazione  
?**



Riferimento  
temporale/marca  
temporale

**Dematerializzazione e  
conservazione  
sostitutiva  
(C.A.D. e Del. CNIPA n.  
11/2004)**

Attribuibilità e  
immodificabilità  
del documento



Formazione del documento o  
sua “riproduzione sostitutiva”

Conservazione  
documento

Sicurezza della  
conservazione

**Firme Elettroniche/  
Digitali e Riferimenti  
Temporali su singoli  
documenti**

Archiviazione Elettronica

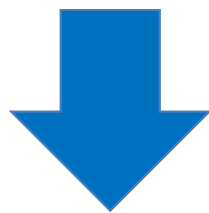
**Firma digitale +  
Marca Temporale sul  
lotto di documenti**

**Misure di sicurezza:  
back up, disaster  
recovery e restore**

Outsourcing  
(art. 5 Del. CNIPA)

**ART. 12 5-bis CAD. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.**

Le nuove Regole tecniche in materia di sistema di CONSERVAZIONE ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44 –bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005.



**DPCM 3 DICEMBRE 2013**

# LE NUOVE REGOLE TECNICHE

***Regole tecniche in materia di formazione , trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni e di gestione del fascicolo informatico***

***Regole tecniche in materia di sistema di conservazione ai sensi degli artt. 44 e 44bis del CAD***

**ALLEGATI:**

- 1) Glossario/Definizioni***
- 2) Formati***
- 3) Misure, Standard, Specifiche tecniche***
- 4) Specifiche tecniche del pacchetto di archiviazione***
- 5) Metadati***

## Definizioni (art 1)

1. Ai fini del presente decreto si applicano le definizioni del **glossario** di cui all'allegato 1 che ne costituisce parte integrante.

2. Le specifiche tecniche relative alle regole tecniche di cui al presente decreto sono indicate nell'allegato n. 2 relativo ai **formati**, nell'allegato n. 3 relativo agli **standard tecnici** di riferimento per la formazione, la gestione e la conservazione dei documenti informatici, nell'allegato n. 4 relativo alle **specifiche tecniche del pacchetto di archiviazione** e nell'allegato n. 5 relativo ai **metadati**.

Le specifiche tecniche di cui al presente comma sono aggiornate con delibera dell'Agenzia per l'Italia digitale, previo parere del Garante per la protezione dei dati personali, e pubblicate sul proprio sito istituzionale.

## Ambito di applicazione (art 2)

1. Il presente decreto, adottato ai sensi dell'art. 71 del Codice, stabilisce le regole tecniche previste dall'art. 20, commi 3 e 5 -bis , dall'art. 23 -ter , comma 4, dall'art. 43, commi 1 e 3, dall'art. 44 e dall'art. 44 -bis del Codice.
2. Le disposizioni del presente decreto **si applicano ai soggetti di cui all'art. 2, commi 2 e 3, del Codice**, nonché ai soggetti esterni a cui è eventualmente affidata la gestione o la conservazione dei documenti informatici.
3. Ai sensi dell'art. 2, comma 5, del Codice, le presenti regole tecniche si applicano **nel rispetto della disciplina rilevante in materia di tutela dei dati personali** e, in particolare, del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196

## Il sistema di conservazione (art 3 commi 1-3)

1. In attuazione di quanto previsto dall'art. 44, comma 1, del Codice, il sistema di conservazione assicura, dalla presa in carico dal produttore di cui all'art. 6 fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:
  - a) i **documenti informatici** e i **documenti amministrativi informatici** con i metadati ad essi associati di cui all'allegato 5 al presente decreto;
  - b) i **fascicoli informatici** ovvero le aggregazioni documentali informatiche con i metadati ad essi associati di cui all'allegato 5 al presente decreto, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.
2. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.
3. Il sistema di conservazione **garantisce l'accesso all'oggetto conservato**, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

**METADATI:** insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto.

## Il sistema di conservazione (art 3, comma 4)

Gli elenchi degli **standard**, delle **specifiche tecniche** e dei **formati** utilizzabili quali riferimento per il sistema di conservazione sono riportati negli allegati 2 e 3 al presente decreto.

### **Allegato 3 STANDARD E SPECIFICHE TECNICHE**

#### Conservazione di documenti informatici

**ISO 14721:2002** *OAIS* (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

**ISO/IEC 27001:2005**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).

**ETSI TS 101 533-1 V1.1.1 (2011-05)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

**ETSI TR 101 533-2 V1.1.1 (2011-05)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

**UNI 11386:2010** Standard SInCRO - Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

**ISO 15836:2003** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

# **Formati degli oggetti di conservazione (allegato 2)**

PDF -PDF/A

TIFF

JPG

Office Open XML (OOXML)

Open Document Format

XML

TXT

Formati messaggi di posta elettronica (RFC 2822/MIME )

# Gli oggetti della conservazione sono organizzati in PACCHETTI INFORMATIVI

## Oggetti della conservazione (art. 4)

Pacchetto di versamento : il pacchetto informativo inviato dal Produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

Pacchetto di archiviazione : il pacchetto informativo conservato in un sistema di conservazione. È derivato dalla trasformazione di uno o più Pacchetti di versamento a scopo di conservazione.

Pacchetto di distribuzione: il pacchetto inviato ad un Utente dal sistema di conservazione in risposta ad una sua specifica richiesta.

2. Ai fini dell'interoperabilità tra i sistemi di conservazione, i soggetti che svolgono attività di conservazione dei documenti informatici adottano le specifiche della struttura dati contenute nell'allegato 4, almeno per la gestione dei pacchetti di archiviazione.

# Indice del Pacchetto di Archiviazione - IPDA (Allegato 4)

## - informazioni generali relative all'indice del pacchetto di archiviazione:

- un identificatore dell'IPdA
- il riferimento all'applicazione che l'ha creato
- eventuali riferimenti ad altri IPdA da cui deriva il presente
- eventuale elemento "ExtraInfo" per l'inserimento di metadati soggettivi

## - informazioni inerenti il Pacchetto di Archiviazione:

- un identificatore del PdA
- eventuali riferimenti ad altri PdA da cui deriva il presente
- informazioni relative a una eventuale tipologia/aggregazione cui il PdA appartiene
- eventuale elemento "ExtraInfo" per l'inserimento di metadati soggettivi
- **indicazione di uno o più raggruppamenti di uno o più file che sono contenuti nel PdA.**
- **informazioni relative al processo di produzione del PdA:**
  - l'indicazione del nome e del ruolo dei soggetti che intervengono nel processo di produzione

del PdA (es. responsabile della conservazione, delegato, pubblico ufficiale ecc.),

- il riferimento temporale adottato (generico riferimento temporale o marca temporale)
- l'indicazione delle norme tecniche e giuridiche applicate per l'implementazione del processo

di produzione del PdA

- eventuale elemento "ExtraInfo" per l'inserimento di metadati soggettivi

## Rapporto di versamento

Documento Informatico che viene rilasciato dal sistema di conservazione, anche in automatico, successivamente alla presa in carico e alla verifica del pacchetto di versamento inviato dal produttore.

Viene univocamente identificato e conservato dal sistema di conservazione.

Contiene un riferimento temporale e una o più impronte del pacchetto di versamento.

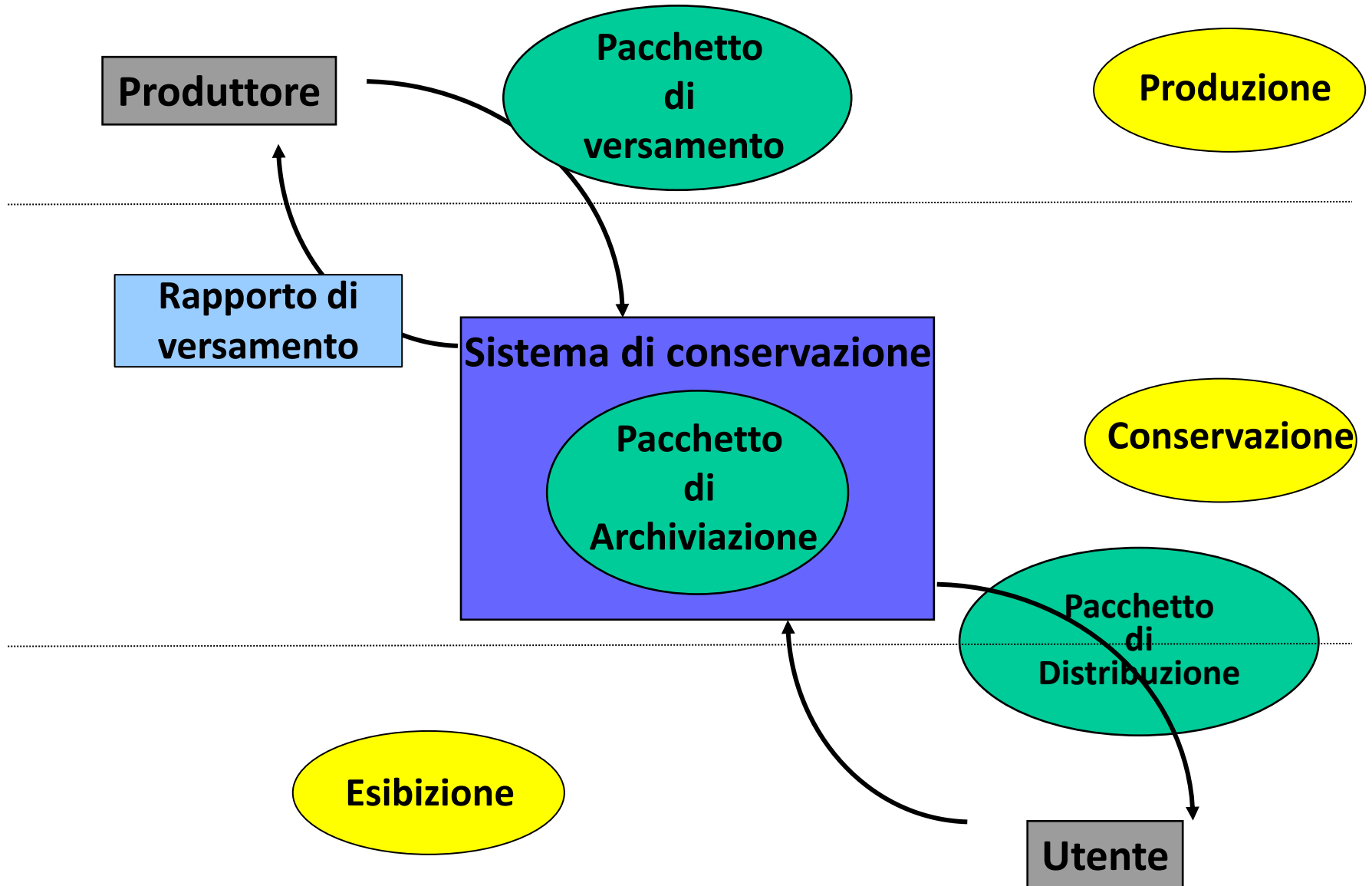
Può essere firmato digitalmente dal responsabile della conservazione  
(*soluzione consigliabile ove venga rilasciato da un conservatore*)

## Ruoli e responsabilità

- ❑ **Produttore:** persona fisica o giuridica che dispone dei documenti da conservare e che, quindi, produce il pacchetto di versamento. Nelle PA solitamente si identifica con il Responsabile della gestione documentale.
- ❑ **Responsabile della Conservazione:** definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia
- ❑ **Utente:** persona fisica o giuridica che richiede accesso ai documenti presenti nel sistema di conservazione al fine di acquisire informazioni di interesse



# Ruoli e responsabilità



## Compiti del responsabile della conservazione (art. 7)

- a. definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- b. gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c. genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d. genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f. assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

## Compiti del responsabile della conservazione

g. al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h. provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;

i. adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

## Compiti del responsabile della conservazione

- j. assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k. assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l. provvede, nel caso di amministrazioni statali, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- m. predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

## **Il responsabile della conservazione e i «certificatori» (art. 7, 2° comma)**

Ai sensi dell'art. 44, comma 1 -ter , del Codice, il responsabile della conservazione può chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati che offrano idonee garanzie organizzative e tecnologiche, ovvero a soggetti a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44 -bis, comma 1, del Codice, distinti dai conservatori o dai conservatori accreditati. Le pubbliche amministrazioni possono chiedere di certificare la conformità del processo di conservazione a soggetti, pubblici o privati, a cui è stato riconosciuto il possesso dei requisiti di cui all'art. 44 -bis , comma 1, del Codice, distinti dai conservatori accreditati

## Il Manuale della conservazione

### Art. 8

Il manuale di conservazione illustra dettagliatamente l'**organizzazione**, i **soggetti coinvolti** e i **ruoli** svolti dagli stessi, il **modello di funzionamento**, la **descrizione del processo**, la descrizione 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.

**È un documento informatico e diviene obbligatoria la sua redazione**

# Il Manuale della conservazione

## Contenuto minimo obbligatorio

- a. i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- b. la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- c. la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell' indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni;
- d. la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- e. la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;

## Manuale della Conservazione – contenuto minimo obbligatorio

- f. la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g. 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;
- h. la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- i. la descrizione delle procedure per la produzione di duplicati o copie;
- l. i tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione;
- m. le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- n. le normative in vigore nei luoghi dove sono conservati i documenti.

## Processo di conservazione (art. 9)

1. Il processo di conservazione prevede:

a) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;

b) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato all'art. 11 (formati degli oggetti destinati alla conservazione – *rinvio all. 2*);

c) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie;

d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;

## Processo di conservazione (art. 9)

e) l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove prevista nel manuale di conservazione;

f) la preparazione, la sottoscrizione con firma digitale o firma elettronica qualificata del responsabile della conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 e secondo le modalità riportate nel manuale della conservazione;

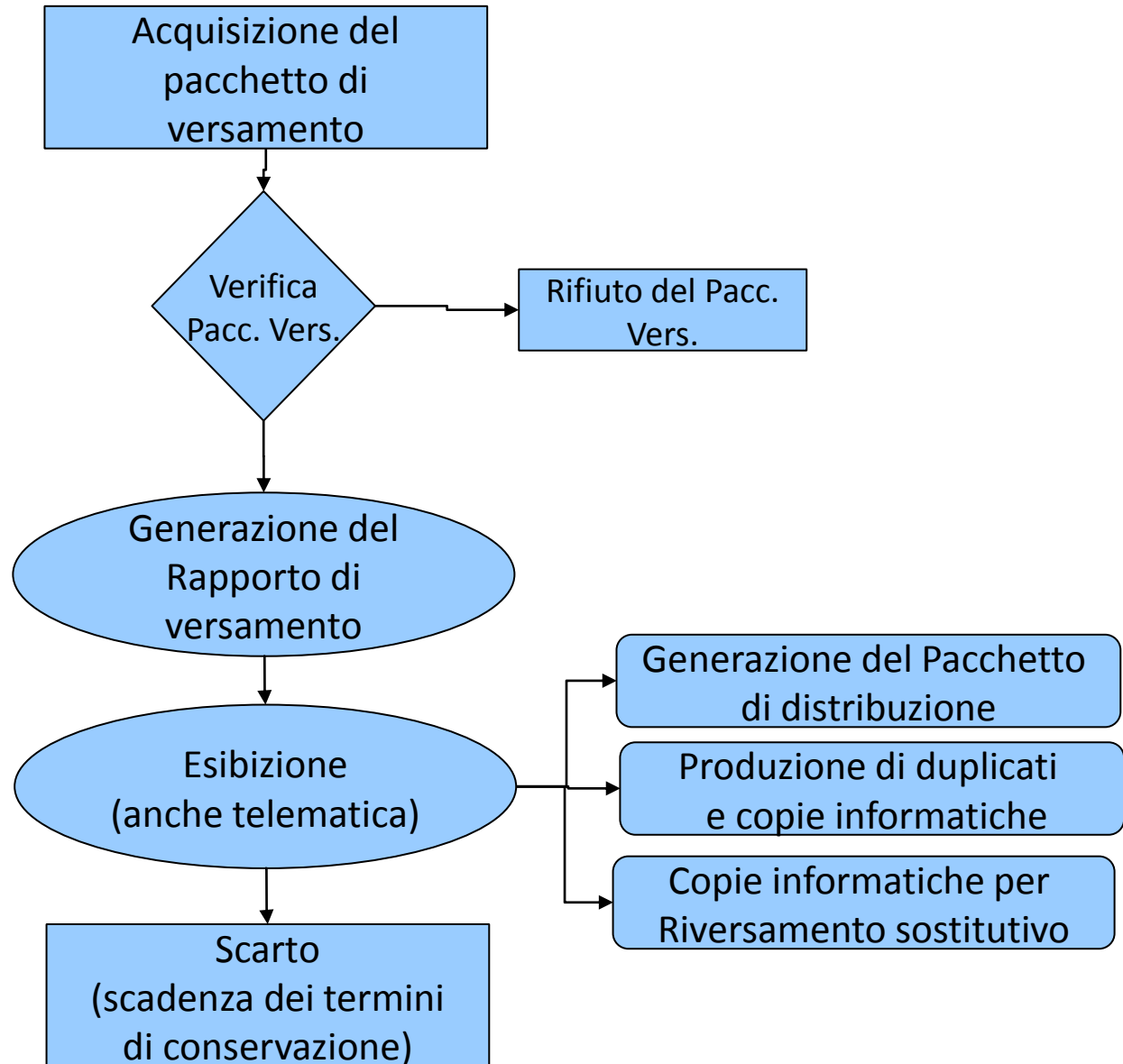
(il DMEF 17 giugno 2014 all'art. 3 comma 2 prevede che «il processo di conservazione dei documenti informatici termina con l'apposizione di un riferimento temporale opponibile a terzi sul pacchetto di archiviazione»; inoltre si ricorda che l'art. 41 del DPCM 22 febbraio 2013 prevede all'art. 41 che costituisce validazione temporale «il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione»)

g) la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata, ove prevista nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione richiesta dall'utente;

## Processo di conservazione (art. 9)

- h) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione;
- i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto **dalle regole tecniche in materia di formazione del documento informatico**;
- j) la produzione delle copie informatiche al fine di adeguare il formato di cui all'art. 11, in conformità a quanto previsto dalle **regole tecniche in materia di formazione del documento informatico**;
- k) lo scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al produttore;
- l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, lo scarto del pacchetto di archiviazione avviene previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo rilasciata al produttore secondo quanto previsto dalla normativa vigente in materia.

## Schema del Processo di conservazione (art. 9)



## Processo di conservazione e luogo di conservazione (art. 9 comma 2)

Fatto salvo quanto previsto dal decreto legislativo 22 gennaio 2004, n. 42, in ordine alla tutela, da parte del Ministero dei beni e delle attività culturali e del turismo, sugli archivi e sui singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico, i sistemi di conservazione delle pubbliche amministrazioni e i sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte dell'Agenzia per l'Italia digitale su questi ultimi, prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle stabilite dal presente decreto.

...e il Cloud???



## Modalità di esibizione (art. 10)

1. Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettiva secondo le modalità descritte nel manuale di conservazione.

L'art. 5 del **DMEF 17 giugno 2014** prevede che il documento conservato può essere esibito per via telematica secondo le modalità stabilite con provvedimenti dei direttori delle competenti Agenzie delle Entrate (*che si attendono dal 2004!*)



**C'È UN TEMPO PER OGNI COSA**

Tempi Certi per Tutelare la Salute dei Cittadini

## Sicurezza del sistema di conservazione (art. 12)

1. Nelle **pubbliche amministrazioni**, il responsabile della conservazione, di concerto con il responsabile della sicurezza e, nel caso delle pubbliche amministrazioni centrali, anche con il responsabile dell'ufficio di cui all'art. 17 del Codice, provvede a predisporre, nell'ambito del piano generale della sicurezza, il piano della sicurezza del sistema di conservazione, nel rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del medesimo decreto, nonché in coerenza con quanto previsto dagli articoli 50 -bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. Le suddette misure sono descritte nel manuale di conservazione di cui all'art. 8.

2. I **soggetti privati** appartenenti ad organizzazioni che già adottano particolari regole di settore per la sicurezza dei sistemi informativi adeguano il sistema di conservazione a tali regole. Gli altri soggetti possono adottare quale modello di riferimento le regole di sicurezza indicate dagli articoli 50 -bis e 51 del Codice e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. I sistemi di conservazione rispettano le misure di sicurezza previste dagli articoli da 31 a 36 e dal disciplinare tecnico di cui all'allegato B del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196

# GLI STANDARD DELLA CONSERVAZIONE

## Allegato 3

### STANDARD E SPECIFICHE TECNICHE

#### Conservazione di documenti informatici

**ISO 14721:2002** *OAIS* (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

**ISO/IEC 27001:2005**, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System).

**ETSI TS 101 533-1 V1.1.1 (2011-05)** Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

**ETSI TR 101 533-2 V1.1.1 (2011-05)** Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

**UNI 11386:2010** S-Recupero degli Oggetti digitali.

**ISO 15836:2003** Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

## **Standard ETSI TS 101 533-1 (v.1.2.1)**

Lo standard rielabora quanto già contenuto nelle norme **ISO/IEC 27001 e 27002** e nelle specifiche tecniche **ETSI TS 102 573** (Policy requirements for trust service providers signing and/or storing data for digital accounting)

**Scopo: Individuare i requisiti di sicurezza e affidabilità di un sistema di conservazione documentale a cui dovranno conformarsi i Fornitori di servizi di conservazione al fine di offrire servizi affidabili e attendibili**

Lo standard non si occupa di aspetti più prettamente archivistici relativi a formazione, gestione e conservazione dei documenti, per i quali viene fatto rinvio ad altre norme tecniche (ISO 14721, ISO 15489, ISO 23081)

## **Standard ETSI TS 101 533-2 (v.1.2.1)**

Lo scopo dello standard è quello di fornire delle linee guida per i valutatori che verificheranno e valuteranno il grado di adeguamento ai requisiti previsti per i sistemi di conservazione dal documento ETSI TS 101 533-1.

## **Standard ETSI TS 101 533-1 (v.1.2.1)**

### **Obblighi derivanti dallo standard ETSI TS 102 573 per i fornitori di servizi di conservazione (IPSP)**

- Valutazione del rischio finanziario
- rispetto dei requisiti indicati anche da parte di eventuali subappaltatori (attraverso la predisposizione di opportune clausole contrattuali)
- indicazione della/e legislazione/i a cui il sistema di conservazione è conforme
- predisposizione di strumenti di esibizione o consegna solo ai soggetti autorizzati (autorità competenti, proprietario dei documenti, titolare del trattamento)

# Standard ETSI TS 101 533-1 (v.1.2.1)

## Requisiti contrattuali

- Adozione di procedure che assicurino le informazioni sull'identità e sul ruolo del contraente
- Indicazione sul diritto/dovere di estrazione di dati e metadati dai documenti da conservare e relative modalità
- indicazione dei soggetti che hanno titolo per accedere ai documenti conservati e dei tempi per effettuare l'esibizione
- adozione di procedure per la restituzione degli archivi di conservazione (ed eventualmente dei relativi metadati) nei tempi e con i formati concordati
- predisporre idonee procedure di cancellazione dei documenti conservati
- indicazione di uno o più soggetti incaricati della trasmissione e della ricezione dei documenti da conservare
- indicazione dei supporti di memorizzazione ed esibizione dei documenti conservati
- obbligo di fornire ai proprietari dei documenti conservati tutti gli strumenti che ne assicurano l'integrità e l'autenticità

## **Standard ETSI TS 101 533-1 (v.1.2.1)**

### **Ulteriori requisiti per gli IPSP**

- predisporre procedure per registrare e conservare in modo sicuro e affidabile la prova della ricezione delle informazioni
- fornire una ricevuta che contenga informazioni dettagliate atte a comprovare l'inoltro ai fini della conservazione. (log trail)
- Indipendenza dell'organizzazione (da CA e TSA fornitrici e fornitori di riferimenti temporali UTC a meno di poter dimostrare che le decisioni riguardanti la conservazione non vengano in alcun modo influenzate)
- rendere disponibili le informazioni riguardanti l'organizzazione dei servizi di conservazione (Es. presenza e identità di eventuali subfornitori)

# Standard OAIS ISO 14721/2002

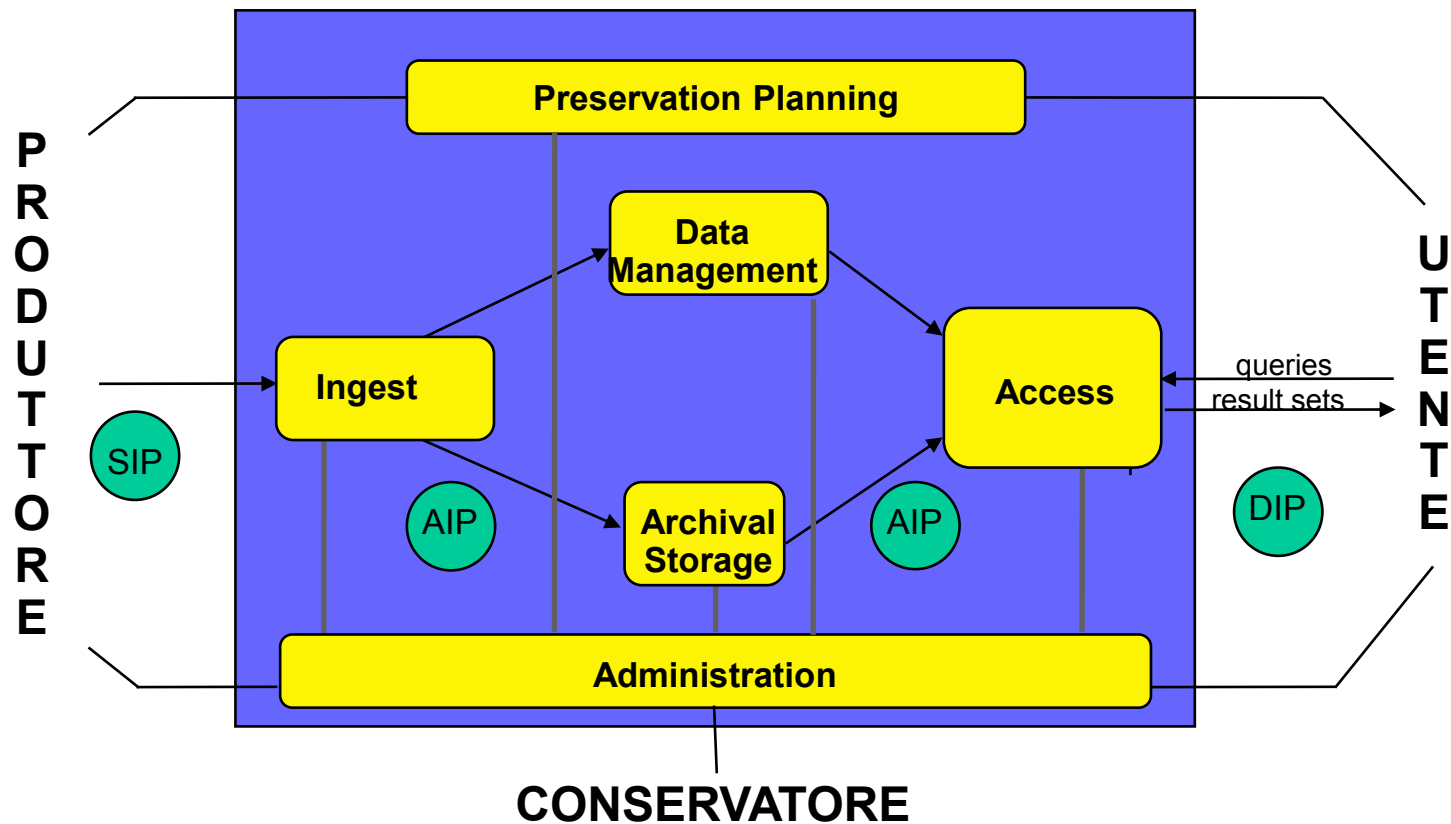
**OAIS:** Open Archival Information System

Standard sviluppato dal CCSDS (Consultive Committee for data space system) nel 2002 per definire concetti, modelli e funzionalità inerenti agli archivi digitali.

Il Modello OAIS descrive un archivio come un'organizzazione all'interno della quale uomini e sistemi operano insieme nell'intento di conservare determinate informazioni per metterle a disposizione di una cerchia definita di utenti. Il modello descrive dettagliatamente come l'informazione elettronica creata dal produttore deve giungere in un sistema d'archivio, quali fasi di trattamento sono necessarie per l'archiviazione a lungo termine e come si può accedere alle informazioni stoccate nell'archivio.

E' un modello strettamente logico che non dipende dunque da nessuna implementazione.

## Modello OAIS: Entità funzionali



## **Descrizione delle entità funzionali 1**

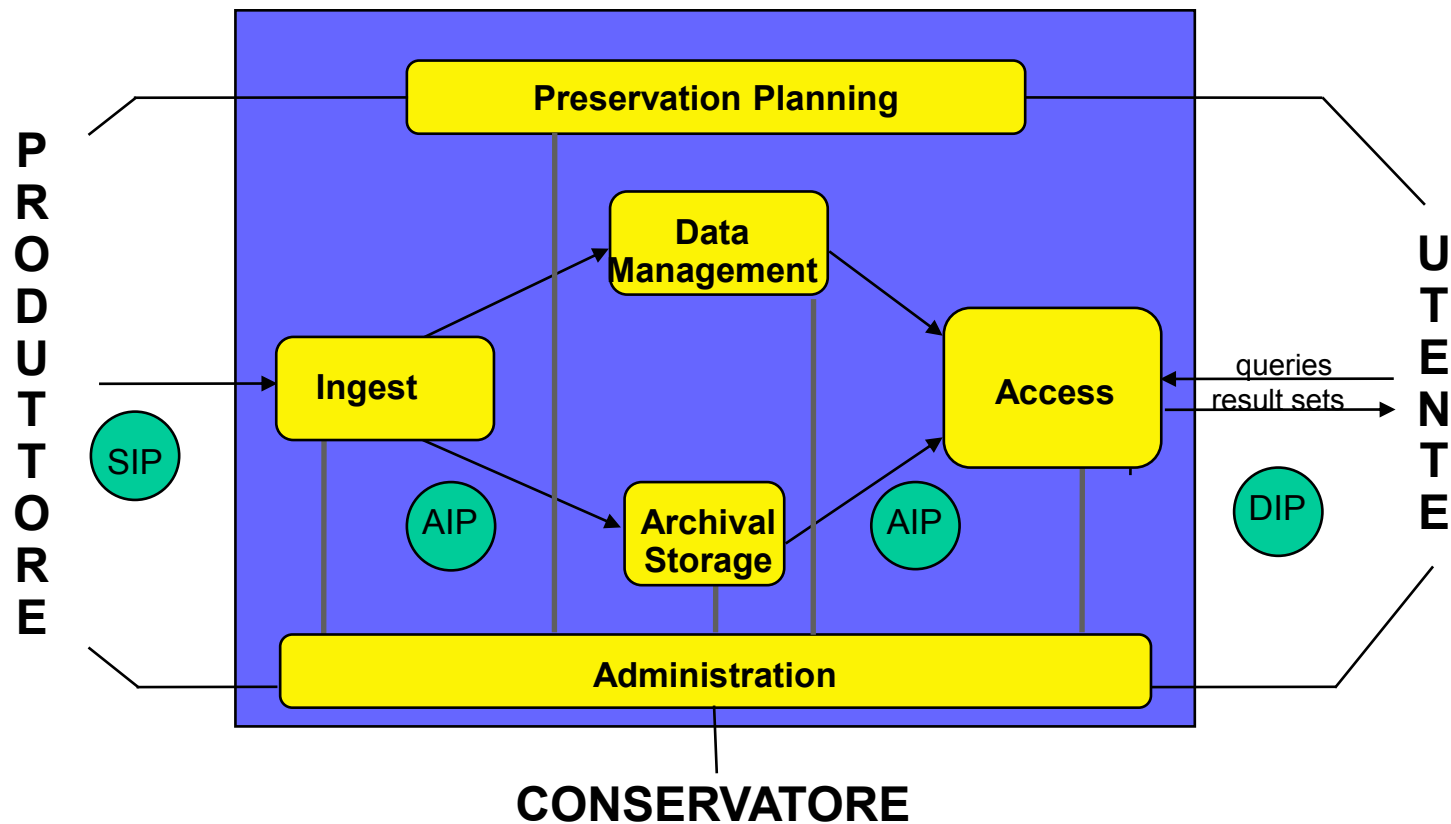
### **Preservation Planning (pianificazione dell'archiviazione)**

- formulazione di raccomandazioni in relazione agli standard ed alla politica d'archiviazione e seguito degli sviluppi tecnologici
- sorveglianza degli sforzi fatti in materia d'archiviazione
- formulazione di raccomandazioni per il mantenimento della leggibilità dell'informazione stoccata
- pianificazione delle migrazioni e dei processi di copiatura

### **Ingest (presa in carico dei dati)**

- presa a carico dei SIP (Submission Information Package) creati dal produttore
- controllo dell'integrità e dell'integrità
- trasformazione dei SIP in AIP (Archival Information Package)
- estrazione dell'informazione descrittiva per la base dati di ricerca
- trasmissione degli AIP alla memoria d'archivio
- comunicazione al Data Management

## Modello OAIS: Entità funzionali



## Descrizione delle entità funzionali 2

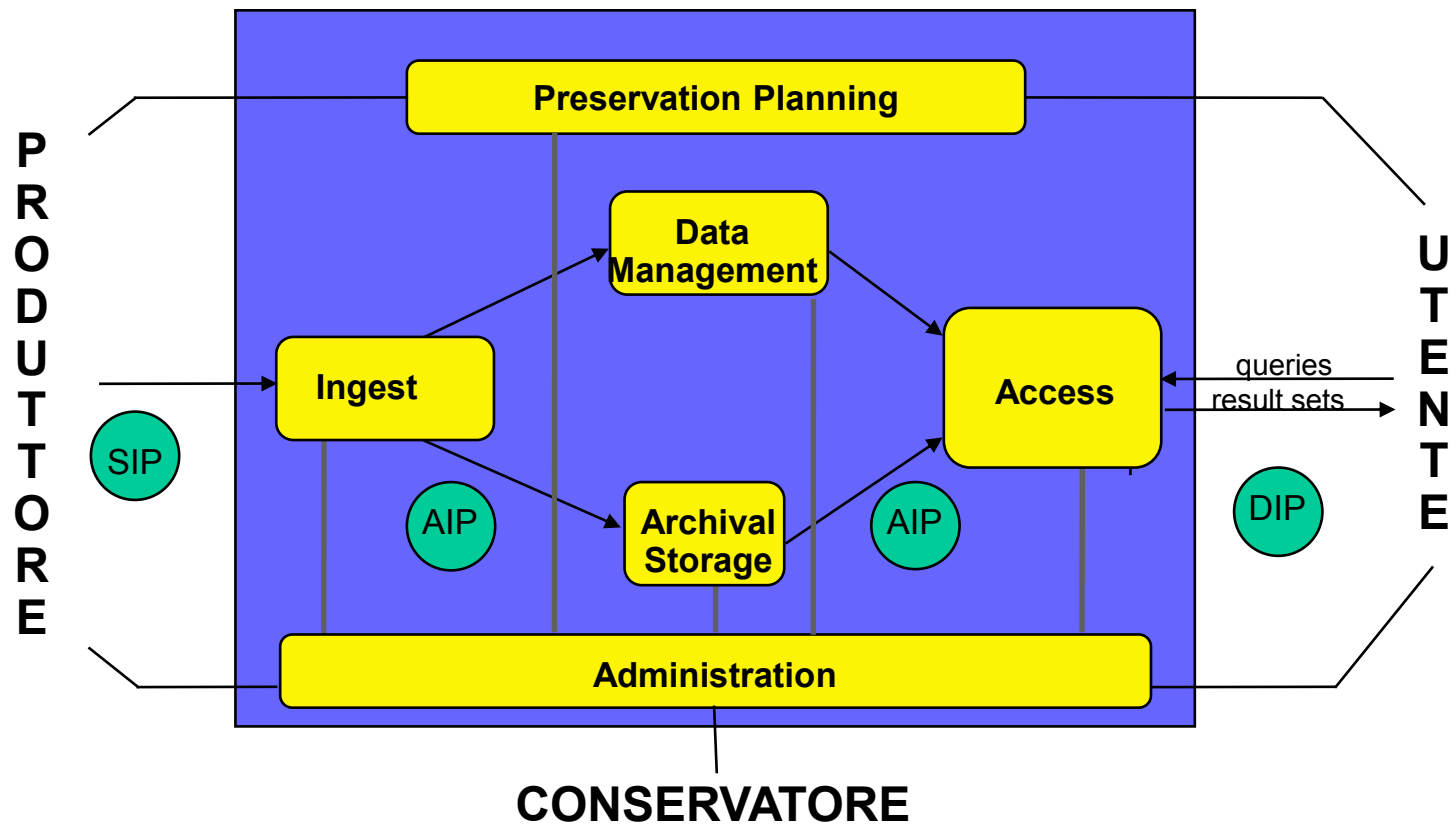
### **Data Management (gestione dei dati)**

- gestione delle informazioni descrittive (base dati) che identificano i fondi d'archivio ed i documenti nonché di altri dati necessari per l'utilizzazione dei materiali d'archivio
- ricezione e trattamento delle richieste (query) provenienti dall'utenza

### **Archival Storage (memoria d'archivio)**

- conservazione e manutenzione degli AIP
- realizzazione di backup
- controllo regolare dell'integrità dei dati
- meccanismi di ripristino (restore) in caso d'urgenza
- trasmissione degli AIP ad Access per l'utilizzazione

## Modello OAIS: Entità funzionali



## **Descrizione delle entità funzionali 3**

### **Access (esibizione)**

- interfaccia utente
- permettere la ricerca e generare delle risposte contenenti la descrizione degli AIP e le informazioni sulla loro disponibilità
- ricezione e trattamento delle richieste di dati (request), trasformazione degli AIP in DIP (Dissemination Information Package) e fornitura dei DIP agli utenti
- garanzia del rispetto dei diritto d'accesso

### **Administration (amministrazione)**

- controllo dei processi globali in OASIS e delle sue relazioni esterne
- configurazione di hardware e software
- attribuzione dei diritti d'accesso.

# The Dublin Core metadata element set ISO 15836/2003

E' nato in ambito OCLC (On line Computer Library Center), la comunità del Dublin Core metadata che unisce produttori, autori e detentori dei diritti sulla documentazione in rete, al fine di fornire strumenti per l'accesso alle risorse digitali. Il consorzio di utilizzatori che si è costituito ha incominciato ad implementare una architettura per i metadati che venga incontro alle necessità dei venditori e dei produttori di informazioni.

## Metadati minimi del documento informatico (Nuove regole tecniche - allegato 5)

Identificativo

Data di chiusura

Oggetto

Soggetto produttore

*nome; cognome; codice fiscale*

Destinatario

*nome; cognome; codice fiscale*

## Standard Uni SinCRO

### ISO 11386/2010 – Recupero degli oggetti digitali

**Scopo:** Definire la struttura-dati necessaria per sostenere il processo di conservazione sostitutiva attraverso la definizione dell'Indice di Conservazione (il cosiddetto *file di chiusura*)

**Risultato:** Creazione di uno Schema XML da seguire per la creazione dell'indice di conservazione

Ad ogni pacchetto di archiviazione (Volume di conservazione) viene associata un'evidenza informatica contenente un insieme di informazioni relative ai documenti e al processo di conservazione

L'indice di conservazione sarà corredato da un riferimento temporale e la firma digitale dei soggetti intitolati a effettuare il processo di conservazione

***Grazie per l'attenzione***



**Avv. Andrea Lisi**

**email:**

**andrealisi@studiolegalelisi.it**

**D&L Department s.r.l.**

**telefax +39 0832 25 60 65**

**Studio Legale Lisi è anche su:**



<https://www.facebook.com/pages/Studio-Legale-Lisi/206384912798924>

<https://twitter.com/LisiDigitalLaw>

Per maggiori informazioni e richiedere le modalità di adesione ad ANORC ecco i nostri contatti:

c/o D&L Department srl  
via Mario Stampacchia, 21  
73100 Lecce

Tel e Fax: 0832 25.60.65  
Cell: 3277027035

Ufficio di Presidenza: [ufficio.presidenza@anorc.it](mailto:ufficio.presidenza@anorc.it)  
Segreteria: [segreteria@anorc.it](mailto:segreteria@anorc.it)  
Direzione: [direzione@anorc.it](mailto:direzione@anorc.it)  
Comunicazione: [comunicazione@anorc.it](mailto:comunicazione@anorc.it)  
Pec: [anorc@pec.it](mailto:anorc@pec.it)

