

L'ATTUAZIONE DEL CAD DOPO LE REGOLE TECNICHE: COSA CAMBIA PER IL PROTOCOLLO E LA CONSERVAZIONE



Avv. Prof. Ernesto Belisario

SITOGRAFIA

- www.funzionepubblica.gov.it
- www.agid.gov.it
- egov.formez.it
- www.agendadigitale.eu

SOMMARIO

01
02
03
04

Il Codice dell'Amministrazione Digitale

La dematerializzazione

Il protocollo informatico

La conservazione del documento informatico

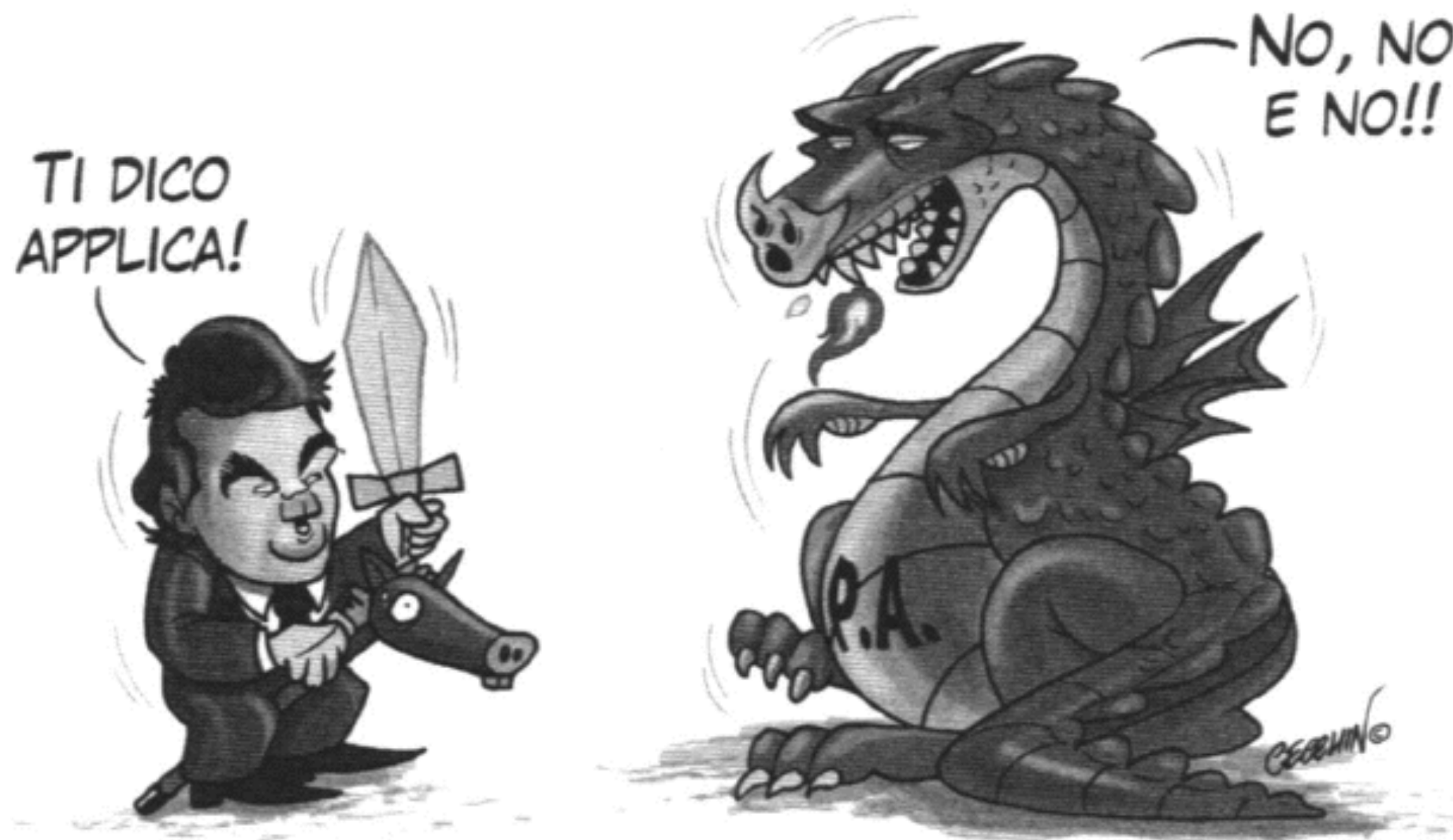
OBIETTIVI

- Conoscere le principali norme del Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005) e le finalità dell'Agenda Digitale
- Avere un quadro completo sulla dematerializzazione dei documenti
- Acquisire gli strumenti necessari per adeguare i sistemi di protocollo informatico e conservazione alle nuove regole tecniche

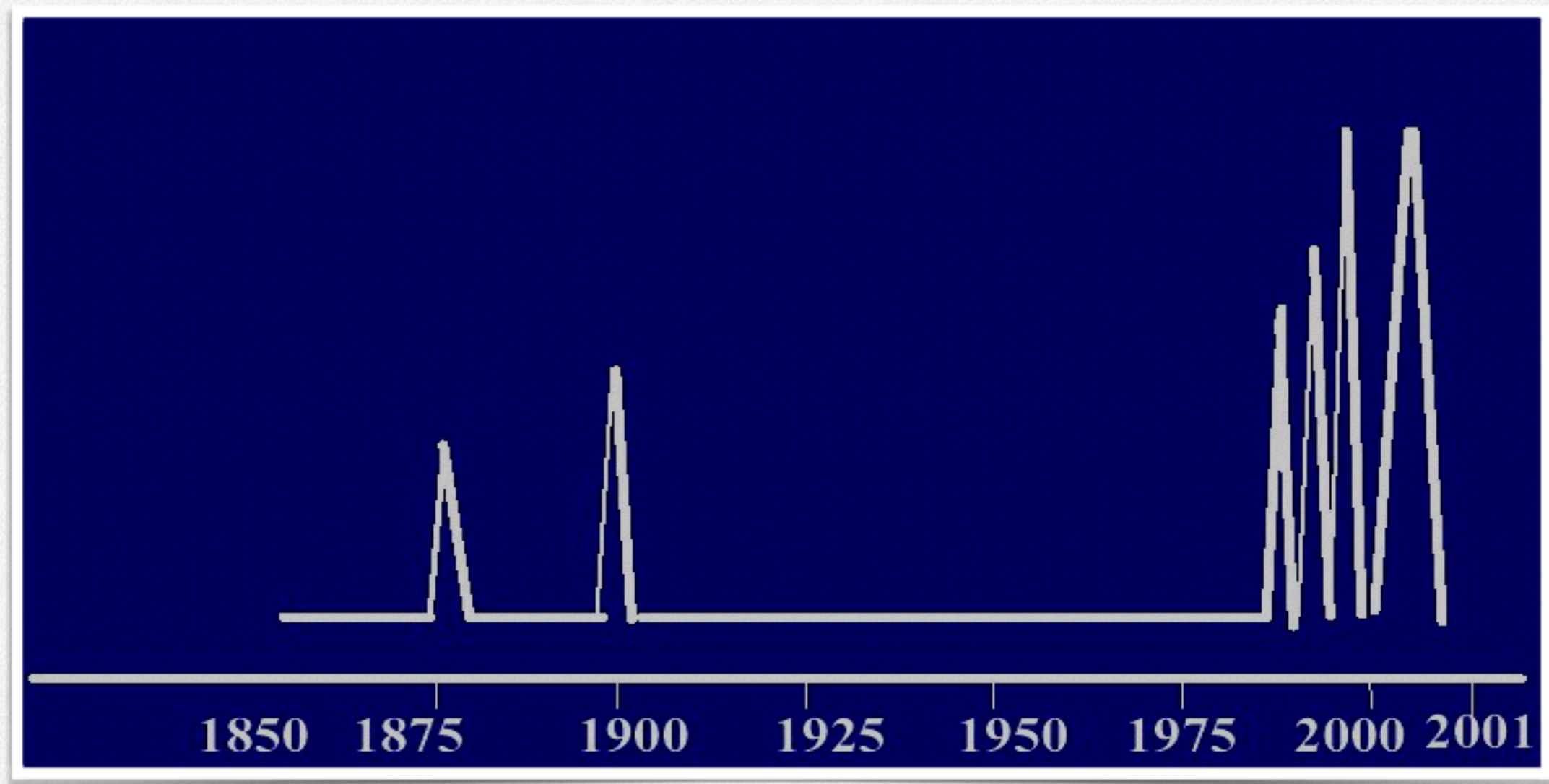
IL CODICE DELL'AMMINISTRAZIONE DIGITALE

PREMESSA

APPLICAZIONE NUOVO C.A.D.



L'ELETTROCARDIOGRAMMA NORMATIVO DELLA PA ITALIANA





COS'È IL CAD

A COSA SERVONO LE NORME

Da una PA di carta...



A COSA SERVONO LE NORME

...a una PA digitale!



LE NORME DELLA PA DIGITALE

- **LEGGE n. 59/1997 - DPR n. 513/1997** -> Documento informatico e firma digitale
- **DPR n. 445/2000** -> Gestione dei flussi documentali e protocollo informatico
- **LEGGE n. 4/2004** -> Accesso dei disabili agli strumenti informatici
- **DPR n. 68/2005** - > Posta Elettronica Certificata
- **Legge n. 69/2009** -> Albo on line
- **D.L n. 5/2012** -> Digitalizzazione di comunicazioni e servizi

IL CAD



CODICE DELL'AMMINISTRAZIONE DIGITALE

È la fonte del diritto che ha per oggetto la **regolamentazione** dell'informatizzazione della Pubblica Amministrazione.

GLI INTERVENTI DI AGGIORNAMENTO AL CAD

- D.Lgs. 4 aprile **2006**, n. **159**
- D.Lgs. 30 dicembre **2010**, n. **235**
- D.L. 18 ottobre **2012**, n. **179**

IL D.LGS N. 235/2010

Organizzazione interna:

- reingegnerizzazione dei processi e fascicolo informatico
- incentivi e sanzioni

Rapporti con cittadini e imprese:

- utilizzare le comunicazioni cartacee solo se impossibilitati all'utilizzo di quelle telematiche
- maggiore attenzione per i siti web

Sicurezza informatica:

- maggiore attenzione alla sicurezza dei dati
- continuità operativa e disaster recovery

IL D.L. N. 179/2012

**PA
DIGITALE**

**IDENTITÀ
DIGITALE**

**OPEN
DATA**

**PAGAMENTI
ELETTRONICI**

**SCUOLA
DIGITALE**

**DIVARIO
DIGITALE**

**SANITA'
DIGITALE**

**GIUSTIZIA
DIGITALE**

NON SI TORNA PIÙ ALLA CARTA



ABBIAMO RISPETTATO LE SCADENZE?

1° gennaio 2013

- accordi tra PPAA solo digitali
- contratti per lavori, servizi e forniture solo digitale
- comunicazioni tra PPAA solo telematiche
- obbligo di scrivere al domicilio telematico del cittadino

1° giugno 2013

- obbligo di consentire i pagamenti informatici

1° luglio 2013

- comunicazioni con le imprese esclusivamente telematiche

1° gennaio 2014

- tutti i servizi devono essere on line
- inefficacia comunicazioni cartacee tra PPAA

CAD

STRUTTURA E FINALITÀ

STRUTTURA DEL CODICE

Capo I - Principi generali

Capo II - Documento informatico e firme elettroniche; Trasferimenti di fondi, libri e scritture

Capo III - Formazione, gestione e conservazione dei documenti informatici

Capo IV - Trasmissione informatica dei documenti

Capo V - Dati delle pubbliche amministrazioni e servizi in rete

Capo VI - Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni

Capo VII - Regole tecniche

Capo VIII - Sistema pubblico di connettività e rete internazionale della pubblica amministrazione

Capo IX - Disposizioni transitorie finali e abrogazioni

FINALITÀ DEL CODICE

Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

(Art. 2, comma 1, D.Lgs. n. 82/2005)

AMBITO DI APPLICAZIONE

Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'**articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165** , nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione , nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.

(Art. 2, comma 2, D.Lgs. n. 82/2005)

L'IMPORTANZA DELL'ORGANIZZAZIONE

Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per la garanzia dei diritti dei cittadini e delle imprese di cui al capo I, sezione II , del presente decreto.

(Art. 12, comma 1, D.Lgs. n. 82/2005)

L'IMPORTANZA DELL'ORGANIZZAZIONE

Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell' articolo 71.

(Art. 12, comma 5, D.Lgs. n. 82/2005)

DIGITALIZZAZIONE E RIORGANIZZAZIONE

La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.

(Art. 15, comma 1, D.Lgs. n. 82/2005)

DIGITALIZZAZIONE E RIORGANIZZAZIONE

In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71 .

(Art. 15, comma 2, D.Lgs. n. 82/2005)

LE RESPONSABILITÀ

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

(Art. 12, comma 1-ter, D.Lgs. n. 82/2005)

LO STATO DI ATTUAZIONE DEL CAD

REGOLE TECNICHE

LOADING...



FORMAZIONE DEL DOCUMENTO INFORMATICO, SISTEMA DI CONSERVAZIONE, GESTIONE DEI FLUSSI DOCUMENTALI

- 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
- Regole tecniche per il protocollo informatico
- Allegato 1 - Glossario/definizioni
- Allegato 2 – Formati
- Allegato 3 – Standard specifiche tecniche
- Allegato 4 - Specifiche tecniche del pacchetto di archiviazione
- Allegato 5 – Metadati

IDENTITÀ DIGITALI

- Regole tecniche consultazione ed estrazione indirizzi PEC
- Allegato alle regole tecniche per l'estrazione degli elenchi PEC
- Applicazione delle Regole tecniche per la consultazione e l'estrazione di caselle ed elenchi di caselle PEC da parte delle PA (PPT)

ACCESSO AI DATI DELLE P.A.

Linee guida per la stesura di convenzioni per la fruibilità di dati delle PA

CONTINUITÀ OPERATIVA E INFRASTRUTTURE CRITICHE NELLA P.A.

- Linee Guida per il *disaster recovery* nella PA
- CIRCOLARE 1° dicembre 2011 , n. 58

FIRME ELETTRONICHE

- Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

PAGAMENTI

- Linee guida per il contrassegno generato elettronicamente
- Linee guida per l'effettuazione dei pagamenti in favore delle P.P.A.A.
- Decreto interministeriale sui micropagamenti

DATI

- Agenda nazionale per la definizione dei contenuti e degli obiettivi delle politiche di valorizzazione del patrimonio informativo pubblico
- Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico
- Linee guida per la valutazione comparativa delle soluzioni software

LA DEMATERIALIZZAZIONE

IL DOCUMENTO INFORMATICO E LE FIRME ELETTRONICHE



TUTTI GLI ATTI NASCONO INFORMATICI



...ma non abbiamo ancora eliminato la carta...

PARTIAMO DALLE DEFINIZIONI

Documento amministrativo:

ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

(art. 1, comma 1, lett. A, D.P.R. 28-12-2000 n. 445)

PARTIAMO DALLE DEFINIZIONI

Documento informatico:

la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

(Art. 1, lett. p), D.Lgs. n. 82/2005)

FORMAZIONE DI DOCUMENTI INFORMATICI

1. Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.
2. (abrogato)
3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.
4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.

(Art. 40, D. Lgs. n. 82/2005)

PA E DOCUMENTI DIGITALI

Le Pubbliche amministrazioni sono obbligate a formare gli originali dei propri atti come documenti informatici (art. 40, comma 1, D.Lgs. n. 82/2005), nel rispetto delle disposizioni del CAD e delle relative regole tecniche.

Va sottolineato come formare gli originali significa non solo redigere il testo con l'ausilio degli strumenti informatici ma anche sottoscrivere gli atti in modalità elettronica.

I documenti così ottenuti saranno conservati nell'archivio digitale dell'Ente e trasmessi - ove necessario - a privati o altre PA.

Nel caso in cui gli atti debbano essere comunicati a soggetti (privati) che non abbiano un recapito elettronico, l'Amministrazione potrà estrarre copia analogica nel rispetto dell'art. 23.

ATTENZIONE A...

- SUPPORTI (ciclo di vita e profili organizzativi)
- FORMATI (per conservazione e accessibilità)

I FORMATI NELLE REGOLE TECNICHE

Le caratteristiche di cui bisogna tener conto nella scelta sono:

1. apertura
2. sicurezza
3. portabilità
4. funzionalità
5. supporto allo sviluppo
6. diffusione

FORMATI IDONEI PER LA CONSERVAZIONE

1. PDF/A
2. TIF
3. JPG
4. OOXML
5. DOC
6. ODF
7. XML
8. TXT

VALIDITÀ GIURIDICA DEL DI

- Liberamente valutabile in giudizio se sprovvisto di qualsiasi sottoscrizione o provvisto di sola firma elettronica “debole”;
- Piena prova fino a querela di falso se sottoscritto con firma elettronica avanzata, qualificata o digitale;
- Se contenente le scritture private di cui all’art. 1350 c.c. nn. 1-12 è richiesta la firma elettronica qualificata o digitale a pena di nullità;
- Se contenente le scritture private di cui all’art. 1350 c.c. n. 13 è richiesta la firma elettronica avanzata, qualificata o digitale a pena di nullità.

VALIDITÀ GIURIDICA DEL DI

Inversione dell'onere della prova - valida fino a querela di falso

Soddisfa il requisito della forma scritta ex art. 1350 n. 13

Liberamente valutabile

FIRMA ELETTRONICA

FIRMA ELETTRONICA
AVANZATA

Soddisfa il requisito della forma
scritta ex art. 1350 nn. 1-12

FIRMA ELETTRONICA
QUALIFICATA

FIRMA DIGITALE

LE TIPOLOGIE DI FIRMA ELETTRONICA

QUALCHE DOMANDA

- Il certificato di firma digitale in uso al mio ufficio è scaduto. Cosa devo fare?
- Devo utilizzare la marca temporale per tutti gli atti e i contratti?
- Quali tipologie di firme elettroniche hanno l'efficacia della forma scritta?
- È valida l'apposizione di una firma digitale con certificato scaduto?

SOTTOSCRIZIONI ELETTRONICHE

Nel mondo informatico il problema della sottoscrizione viene affrontato e risolto in modo sostanzialmente differente dal “mondo della carta” attraverso le firme elettroniche.

Firma autografa Vs firma elettronica

- la firma autografa è un "segno" che una persona appone in calce alle proprie dichiarazioni con lo scopo di attestare, attraverso la riconoscibilità della grafia, la personale provenienza della dichiarazione stessa;
- la firma elettronica, invece, è un metodo di attribuzione della paternità e di garanzia della riservatezza di un documento informatico che si basa su un procedimento tecnico fondato sui principi individuati dalla crittografia moderna.
- la firma elettronica, invece, è un metodo di attribuzione della paternità e di garanzia della riservatezza di un documento informatico che si basa su un procedimento tecnico fondato sui principi individuati dalla crittografia moderna.

FIRME ELETTRONICHE

D.P.R. 513/1997

- Firma digitale

D.P.R. 51 Dir. 1999/93/CE

- Firma elettronica
- Firma elettronica avanzata

D.Lgs. 10/2002

- Firma elettronica
- Firma elettronica avanzata

D.P.R. 137/2003

- Firma elettronica
- Firma elettronica avanzata
- Firma elettronica qualificata
- Firma digitale

D.Lgs. 82/2005

- Firma elettronica
- Firma elettronica qualificata
- Firma digitale

D.Lgs. 235/2010

- Firma elettronica
- Firma elettronica avanzata
- Firma elettronica qualificata
- Firma digitale

TIPOLOGIE DI FIRME ELETTRONICHE

È possibile distinguere tra **due macro-tipologie** di firme elettroniche:

- le “**firme deboli**” (firma elettronica): consentono di ricondurre in qualsiasi forma dei dati elettronici, ad esempio una firma a stampa, ad un soggetto, ma non assicurano l'integrità del documento stesso. Il documento è liberamente valutabile in giudizio, tenendo conto delle sue caratteristiche oggettive di qualità e sicurezza;
- le “**firme forti**” (firma elettronica avanzata, firma elettronica qualificata e firma digitale) sono quelle per cui il firmatario non può disconoscere semplicemente la sottoscrizione se non a querela di falso. Garantiscono l'identità dell'autore e l'integrità del documento firmato.

FIRMA ELETTRONICA

La **firma elettronica** che viene definita dal legislatore come “l’insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica” (art. 1, comma 1, lett. q).

La firma elettronica può essere ricondotta all’inserimento o alla digitazione di un semplice codice di identificazione (pin) oppure di una parola chiave (password), che in qualche modo possono avere una “connessione logica” con il titolare.

FIRMA ELETTRONICA AVANZATA

La firma elettronica avanzata risponde all'obiettivo di mettere a disposizione dell'utente strumenti più semplici con i quali sottoscrivere documenti informatici con piena validità legale.

La firma elettronica avanzata (definita dall'art. 1, comma 1, lett. q-bis) deve sempre garantire:

- l'identificazione del firmatario del documento
- la connessione univoca della firma al firmatario
- il controllo esclusivo del firmatario del sistema di generazione della firma
- la possibilità di verificare che il documento non abbia subito modifiche dopo l'apposizione della firma
- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto
- l'individuazione del soggetto che eroga le soluzioni di firma elettronica avanzata

FIRMA ELETTRONICA QUALIFICATA

La firma elettronica qualificata è 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 (art. 1, comma 1, lett. r).

Questo tipo di firma deve essere accompagnata da un certificato digitale, rilasciato da apposito soggetto (definito, appunto, Certificatore) munito di numero di serie o altro codice di identificazione.

FIRMA DIGITALE

La **firma digitale** è una 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.

La firma digitale (secondo la definizione data all'art. 1, comma 1, lett. s, CAD) è il risultato di una complessa procedura informatica di validazione di un documento elettronico per mezzo del quale, attraverso l'utilizzo di una doppia chiave di cifratura (una pubblica ed accessibile, l'altra rigorosamente privata e segreta).

FIRMA GRAFOMETRICA

Una delle applicazioni più importanti



COME FUNZIONA

- Nessuna necessità di smartcard o certificati;
- Sottoscrizione autografa su una tavoletta grafica che acquisisce a sistema dati quali: tempo, posizione, pressione di ogni singolo punto del tratto di penna;
- Questi dati (c.d. biometrici) dopo l'acquisizione sono codificati nel documento, creando così un'associazione forte tra quest'ultimo e la sottoscrizione.

DATI BIOMETRICI

- Pressione, velocità, angolazione del tratto, tempo, posizione...
- Le caratteristiche dinamiche della sottoscrizione autografa vengono registrate all'atto dell'apposizione della firma (di norma tramite una penna elettronica su un tablet apposito)
- La raccolta di tali dati consente, in caso di contestazione, la verifica da parte di un grafologo al pari di quanto avviene con i documenti cartacei.

FIRMA ELETTRONICA AVANZATA GRAFOMETRICA

Non tutte le soluzioni di firma grafometrica rientrano tra le firme elettroniche avanzate

È necessario che sia garantita:

- la cifratura dei dati;
- l'immediata associazione dei dati al documento (associazione di dati biometrici e hash del documento)
- generazione di una chiave pubblica e di una privata (che servirà eventualmente per verificare l'indissolubilità tra dati biometrici ed il documento)

VERIFICA PRELIMINARE

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

(Art. 17, D.Lgs. n. 196/2003)



FIRMA DIGITALE REMOTA

La firma digitale remota permette di apporre tale tipologia di firma senza la dotazione hardware indispensabile per la firma digitale tradizionale.

La generazione e la conservazione delle chiavi di firma è centralizzata e consente di apporre la firma digitale da remoto (attraverso un qualsiasi PC, tablet o smartphone con accesso alla rete) mediante:

- OTP
- PIN
- Riconoscimento grafometrico della firma autografa

LA POSIZIONE DEL GARANTE PRIVACY

Parere (anche se in relazione ad un caso specifico) favorevole al trattamento dei dati biometrici mediante l'utilizzo di tale tipologia di firma, a condizione che:

– la società adotti presidi tecnici e organizzativi di sicurezza a protezione dei dati biometrici degli interessati e, segnatamente:

- idonee misure volte a ridurre i rischi di installazione abusiva di software o di modificazione della configurazione dei dispositivi in dotazione ai promotori, adottando altresì ogni accorgimento utile a contrastare l'azione di eventuali agenti malevoli (malware);

- un sistema di gestione dei dispositivi impiegati nei trattamenti grafometrici basato su certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro. In particolare, dovranno risultare disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi;

- adeguate policy per la gestione degli incidenti di sicurezza nell'ambito delle diverse fasi del processo biometrico/grafometrico;

– la società si faccia rilasciare e conservi l'attestato di conformità di cui alla regola 25 dell'Allegato "B" al Codice Privacy;

COPIE E DUPLICATI

DEFINIZIONE

copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.

VALIDITÀ

- Con attestazione di conformità da parte di notaio o altro pubblico ufficiale, stessa efficacia probatoria degli originali;
- Senza attestazione di conformità, stessa efficacia probatoria degli originali se non espressamente disconosciuta;
- Nel caso di documenti della PA è sempre richiesta l'attestazione di conformità da parte del pubblico ufficiale.

DOCUMENTI AMMINISTRATIVI INFORMATICI

3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

(Art. 23-bis, D. Lgs. n. 82/2005)

DEFINIZIONE

copia analogica di documento informatico: il documento su carta avente contenuto identico a quello del documento informatico da cui è tratto.

VALIDITÀ

- Con attestazione di conformità da parte di notaio o altro pubblico ufficiale, stessa efficacia probatoria degli originali;
- Senza attestazione di conformità, stessa efficacia probatoria degli originali se non espressamente disconosciuta;
- La stampa di documenti della PA deve contenere un contrassegno che garantisce la conformità all'originale

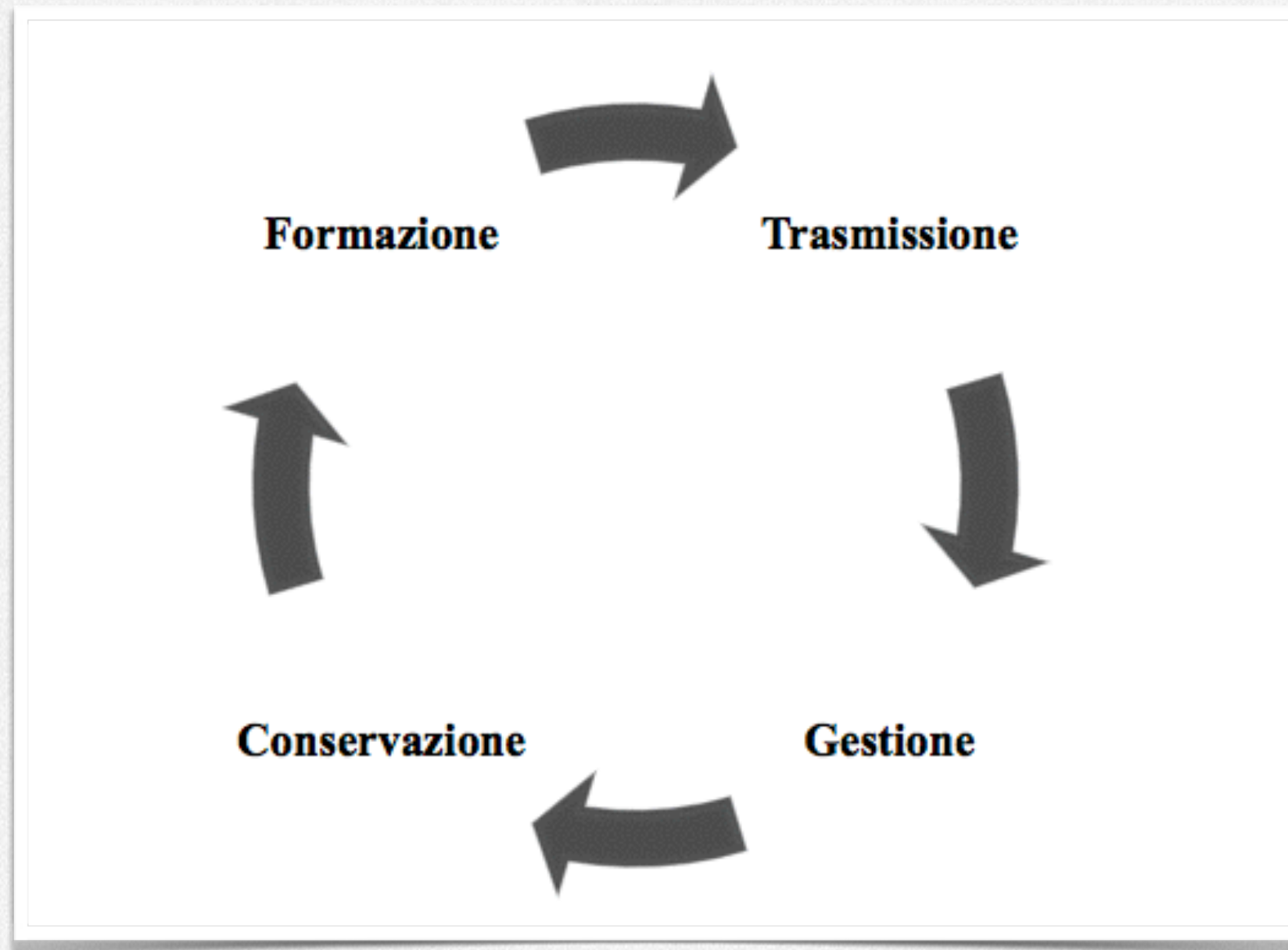
COPIA INFORMATICA DI DOCUMENTO INFORMATICO

- Trasformazione che comporta la **modifica** dell'*hash* del *file*;
- **Necessaria** l'attestazione di conformità;
- Esempio tipico: **conversione** da Word a PDF.

DUPLICATO DI DOCUMENTO INFORMATICO

- **Nessuna modifica** dell'*hash* del *file*;
- **Non necessaria** l'attestazione di conformità;
- Esempio tipico: **copia/incolla**.

CICLO DI VITA DEL DOCUMENTO INFORMATICO



IL FASCICOLO INFORMATICO

NUOVI STRUMENTI, STESSE CATEGORIE

Da un esame sistematico delle norme è opportuno ricavare come il legislatore non abbia introdotto nuovi procedimenti nel nostro ordinamento, limitandosi - invece - a consentire una diversa modalità di attuazione di quelli già esistenti.

Nel digitalizzare il procedimento, il legislatore ha utilizzato le categorie tradizionali, disciplinandole nella loro versione informatica.

DAL FASCICOLO CARTACEO AL FASCICOLO INFORMATICO

In base all'art. 41, comma 2, CAD, ogni Amministrazione deve raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; la creazione di un fascicolo informatico per ogni procedimento comporta per gli Enti la necessità di utilizzare i sistemi di gestione informatica dei flussi documentali, oltre che di protocollo informatico (cui pure erano già tenuti a partire dal 1° gennaio 2004).

Tale obbligo è ulteriormente sottolineato dalla disposizione contenuta all'art. 40-bis CAD che sancisce espressamente che gli Enti devono sottoporre a registrazione di protocollo le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica (anche certificata) istituzionali.

IL FASCICOLO INFORMATICO

Il fascicolo informatico (inteso come insieme dei documenti informatici relativi al procedimento) deve comunque recare l'indicazione:

- a) dell'Amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- b) delle altre Amministrazioni partecipanti;
- c) del responsabile del procedimento;
- d) dell'oggetto del procedimento;
- e) dell'elenco dei documenti contenuti;
- g) e-bis) dell'identificativo del fascicolo medesimo.

PROCEDIMENTO E FASCICOLO INFORMATICO

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.

1-bis. La gestione dei procedimenti amministrativi e' attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all'articolo 54, commi 2-ter e 2-quater.

2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.

2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell'articolo 71, di concerto con il Ministro della funzione pubblica.

PROCEDIMENTO E FASCICOLO INFORMATICO

2-ter. Il fascicolo informatico reca l'indicazione:

- a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- b) delle altre amministrazioni partecipanti;
- c) del responsabile del procedimento;
- d) dell'oggetto del procedimento;
- e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater.

e-bis) dell'identificativo del fascicolo medesimo.

2-quater. Il fascicolo informatico **può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati**; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990.

3. Ai sensi degli articoli da 14 a 14-quinquies della legge 7 agosto 1990, n. 241, previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

(Art. 41, D.Lgs. n. 82/2005)

IL PROTOCOLLO INFORMATICO

COS'È IL PROTOCOLLO

Il protocollo è un servizio **obbligatorio** negli Enti pubblici che ha la funzione di gestire, sia in entrata che in uscita dall'organizzazione, tutte le scritture e documenti.

È uno strumento dal duplice valore, giuridico-probatorio e gestionale.

Sotto il primo profilo, sul registro di protocollo vengono trascritti progressivamente i documenti e gli atti in entrata e in uscita di un ufficio pubblico, attribuendo certezza ai momenti di arrivo/spedizione degli stessi; il valore gestionale, invece, è determinato dall'attività di classificazione del documento che consente il suo inserimento nel contesto del procedimento e quindi in relazione con i documenti correlati.

A COSA SERVE?

Attraverso il protocollo i documenti amministrativi, ricevuti o adottati, ricevono un'**esatta e univoca identificazione**. In questo modo, anche il cittadino ottiene la certezza che i documenti da lui prodotti siano stati acquisiti e registrati.

Questo servizio ha inoltre il compito di **organizzare** la memoria dell'Ente, mediante la **classificazione** degli atti protocollati secondo un **ordinamento logico** basato sulle funzioni e sulle attività dell'amministrazione.

FUNZIONE CERTIFICATIVA

Il protocollo delle p.a. è un atto pubblico di fede privilegiata avente ad oggetto, tra l'altro, la data di ricezione dei singoli atti, sicché, in mancanza di querela di falso nei confronti delle risultanze del protocollo, è priva di fondamento la pretesa di far accertare dal giudice amministrativo una situazione contrastante con le risultanze di un atto pubblico fidefaciente.

Consiglio di Stato, Ad. Plen. n. 10/1993

FUNZIONE CERTIFICATIVA

CARTACEO

- inchiostro indelebile
- registri vidimati e numerati progressivamente
- divieto cancellature ed abrasioni

SISTEMA INFORMATICO

- registrazione in un'unica soluzione con informazioni assegnate direttamente dal sistema
- archiviazione su supporto imm modificabile
- produzione registro giornaliero di protocollo
- operazioni di annullamento e modifica delle informazioni inserite nella fase di registrazione devono avvenire in modo che ne rimanga traccia
- vietate modifiche non autorizzate
- rispetto misure di sicurezza e predisposizione manuale sulla sicurezza
- il fornitore del sistema di protocollo è tenuto a rilasciare dichiarazione di conformità dello stesso ai requisiti minimi di sicurezza normativamente richiesti.

L'EVOLUZIONE DEL PROTOCOLLO INFORMATICO: IL D.P.R. N. 445/2000 E IL DPCM 31/10/2000

NORMATIVA

- Art. 21 D.P.R. n. 513/1997
- D.P.R. n. 428/1999
- D.P.C.M. 31 ottobre 2000
- D.P.R. n. 445/2000
- D.Lgs. n. 82/2005

LA PRIMA NORMA SUL PROTOCOLLO

La prima norma in materia di “gestione informatica del flusso documentale” è contenuta all’**art. 21 del D.P.R. 10 novembre 1997, n. 513**. Secondo tale disposizione, le Pubbliche Amministrazioni avrebbero dovuto provvedere alla realizzazione di un sistema informatico per la gestione del protocollo e dei documenti entro il 31 dicembre 1998.

IL D.P.R. N. 445/2000

Le pubbliche amministrazioni provvedono entro il **1° gennaio 2004** a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del presente testo unico ed alle disposizioni di legge sulla tutela della riservatezza dei dati personali, nonché dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 e dei relativi regolamenti di attuazione.

(Art. 50, co. 3, D.P.R. n. 445/2000)

LE PRIME REGOLE TECNICHE

Con decreto del Presidente del Consiglio dei Ministri, su proposta dell'Autorità per l'informatica nella pubblica amministrazione di concerto con il Ministro per la funzione pubblica, sono specificate le **regole tecniche**, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione di protocollo.

(Art. 53, co. 4, D.P.R. n. 445/2000)



DPCM 31 ottobre 2000

LE NUOVE REGOLE TECNICHE

NUOVE REGOLE

DPCM 31 ottobre 2000



DPCM 3 dicembre 2013

DPCM 3 DICEMBRE 2013

Stabilisce le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, di cui agli articoli 53, 55 e 66 del D.P.R. n. 445/2000.

Stabilisce altresì le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione di protocollo agli articoli 40 bis, 41 e 47 del CAD.

DPCM 3 DICEMBRE 2013

- Entra in vigore 30 giorni dopo la pubblicazione sulla Gazzetta Ufficiale
- Il DPCM 31 ottobre 2000 cessa di avere efficacia
- Le Amministrazioni in regola con le vecchie regole tecniche hanno 18 mesi di tempo per adeguarsi

ADEMPIMENTI

- a) individuare le **aree organizzative omogenee** e i relativi uffici di riferimento ai sensi dell'articolo 50 del Testo unico;
- b) nominare, in ciascuna delle aree organizzative omogenee individuate ai sensi dell'articolo 50 del Testo unico, il **Responsabile della gestione documentale**, e un suo **vicario**, per casi di vacanza, assenza o impedimento del primo;
- c) nominare eventualmente, nell'ambito delle amministrazioni con più aree organizzative omogenee, il **Coordinatore della gestione documentale** e un suo **vicario** per i casi di vacanza, assenza o impedimento del primo;
- d) adottare il **manuale di gestione** di cui all'articolo 5, su proposta del Responsabile della gestione documentale ovvero, ove nominato, del Coordinatore della gestione documentale;
- e) definire, su indicazione del Responsabile della gestione documentale ovvero, ove nominato, del Coordinatore della gestione documentale, i **tempi, le modalità e le misure organizzative** e tecniche finalizzate all'eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax, e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal Testo unico.

(art. 3 delle regole tecniche)

RESPONSABILE DELLA GESTIONE DOCUMENTALE

A tale figura è assegnato il compito di:

- a) predisporre lo schema del manuale di gestione di cui all'articolo 5;
- b) proporre i tempi, le modalità e le misure organizzative e tecniche di cui all'articolo 3, comma 1, lettera e);
- c) predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza previste nel disciplinare tecnico pubblicato in allegato B del decreto legislativo del 30 giugno 2003, n. 196 e successive modificazioni, d'intesa con il responsabile della conservazione, il responsabile dei sistemi informativi o, nel caso delle pubbliche amministrazioni centrali, il responsabile dell'ufficio di cui all'articolo 17 del Codice e con il responsabile del trattamento dei dati personali di cui al suddetto decreto.

(Art. 4, regole tecniche sul protocollo)

IL MANUALE DI GESTIONE DEL PROTOCOLLO

- Descrive il sistema di gestione dei documenti informatici (anche ai fini della conservazione);
- Fornisce le istruzioni per il corretto funzionamento del servizio.

CONTENUTO DEL MANUALE DI GESTIONE

- a) la pianificazione, le modalità e le misure di cui all'articolo 3, comma 1, lettera e);
- b) il piano di sicurezza dei documenti informatici di cui all'articolo 4, comma 1, lettera c);
- c) le modalità di utilizzo di strumenti informatici per la formazione dei documenti informatici, ai sensi dell'articolo 40, comma 1, del Codice, e per lo scambio degli stessi all'interno ed all'esterno dell'area organizzativa omogenea, ivi comprese le caselle di posta elettronica, anche certificata, utilizzate;
- d) la descrizione di eventuali ulteriori formati utilizzati per la formazione del documento informatico in relazione a specifici contesti operativi esplicitati e motivati;**
- e) l'insieme minimo dei metadati associati ai documenti soggetti a registrazione particolare e gli eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce;**
- f) la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione, tra i quali, in particolare, documenti informatici pervenuti attraverso canali diversi da quelli previsti dagli articoli 16 e 17, nonché tramite fax, raccomandata o assicurata;
- g) l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;

CONTENUTO DEL MANUALE DI GESTIONE

- h) le modalità di formazione, implementazione e gestione dei fascicoli informatici relativi ai procedimenti e delle aggregazioni documentali informatiche con l'insieme minimo dei metadati ad essi associati;**
- i) l'indicazione delle unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea;
- j) l'elenco dei documenti esclusi dalla registrazione di protocollo, ai sensi dell'articolo 53, comma 5, del Testo unico;
- k) l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento;
- l) i registri particolari definiti per il trattamento di registrazioni informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, di cui all'articolo 40, comma 4, del Codice;
- m) il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;

CONTENUTO DEL MANUALE DI GESTIONE

- n) le modalità di produzione e di conservazione delle registrazioni di protocollo informatico e, in particolare, l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire l'immodificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione di segnatura ai sensi dell'articolo 55 del Testo unico, nonché le modalità di registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione;
- o) la descrizione funzionale ed operativa del componente "sistema di protocollo informatico" del sistema di gestione informatica dei documenti con particolare riferimento alle modalità di utilizzo;
- p) i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;
- q) le modalità di utilizzo del registro di emergenza ai sensi dell'articolo 63 del Testo unico, inclusa la funzione di recupero dei dati protocollati manualmente.

...E ATTENZIONE!

Il manuale deve essere **obbligatoriamente**
pubblicato sul sito istituzionale

DOVE?

FUNZIONALITÀ MINIMA

Nucleo minimo **obbligatorio** per legge

FUNZIONALITÀ AGGIUNTIVE

Integrazioni del nucleo minimo del protocollo (sono molteplici)

NON È OBBLIGATORIA L'ADOZIONE

REQUISITI MINIMI DI SICUREZZA

Il sistema di protocollo deve assicurare:

- a) l'univoca identificazione ed autenticazione degli utenti;
- b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
- c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
- d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione.

(art. 7, regole tecniche)

REQUISITI MINIMI DI SICUREZZA

- Il sistema di protocollo informatico deve consentire il **controllo differenziato** dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.
- 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 informazioni trattate e di quelle rilevanti per la sicurezza non devono essere rese possibili ai **soggetti non autorizzati**.
- Il sistema di protocollo rispetta 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.

(art. 7, regole tecniche)

REGISTRO GIORNALIERO DI PROTOCOLLO

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

ANNULLAMENTO DELLE INFORMAZIONI

- 1 L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal sistema e registrate in forma immutabile determina l'automatico e contestuale annullamento della intera registrazione di protocollo.
- 2 L'annullamento anche di un solo campo delle altre informazioni registrate in forma immutabile, necessario per correggere errori intercorsi in sede di immissione di dati delle altre informazioni, deve comportare la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione, in modo permanente, del valore precedentemente attribuito unitamente alla data, l'ora e all'autore della modifica. La disposizione di cui al primo periodo si applica per lo stesso campo, od ogni altro, risultato successivamente errato.
- 3 Le informazioni originarie, successivamente annullate, vengono memorizzate secondo le modalità specificate nell'articolo 54 del Testo unico.

(art. 8, regole tecniche sul protocollo)

FORMATO DELLA SEGNATURA DI PROTOCOLLO

- a) codice identificativo dell'amministrazione;
- b) codice identificativo dell'area organizzativa omogenea;
- c) codice identificativo del registro;
- d) data di protocollo secondo il formato individuato in base alle previsioni di cui all'articolo 20, comma 2;
- e) progressivo di protocollo secondo il formato specificato all'articolo 57 del Testo unico.

(art. 9, regole tecniche protocollo)

PROTOCOLLO E IPA

- Le Amministrazioni devono accreditarsi presso l'Indice delle Amministrazioni
- Ciascuna Amministrazione aggiorna **immediatamente** ogni modifica delle variazioni sulle AOO
- Il codice identificativo dell'Amministrazione (che viene assegnato automaticamente) deve essere riportato nei dati della segnature di protocollo

MODALITÀ DI TRASMISSIONE DEI DOCUMENTI INFORMATICI

Posta elettronica: messaggi PEC / messaggi PEO
compatibili con il protocollo SMTP/MIME

Cooperazione applicativa: SPC

MODALITÀ DI REGISTRAZIONE DEI DOCUMENTI INFORMATICI

Alla registrazione di protocollo vengono associate le ricevute generate dal sistema di protocollo informatico e, nel caso di registrazione di messaggi di posta elettronica certificata spediti, anche i dati relativi alla consegna rilasciati dal sistema di posta certificata correlati al messaggio oggetto di registrazione.

(art 18, regole tecniche)

MODALITÀ DI REGISTRAZIONE DEI DOCUMENTI INFORMATICI

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'articolo 40-bis del Codice. L'indirizzo di tali caselle è riportato nell'indice delle amministrazioni e nel manuale di gestione di cui all'articolo 5, nonché pubblicato sul sito dell'amministrazione.

(art 18, regole tecniche)

MODALITÀ DI REGISTRAZIONE DEI DOCUMENTI INFORMATICI

Ciascuna amministrazione può istituire specifiche caselle di posta elettronica, anche certificata, per trattare peculiari tipologie documentali, anche oggetto di registrazione particolare. Gli indirizzi di tali caselle sono riportati nell'indice delle amministrazioni e nel manuale di gestione, nonché pubblicati nel sito dell'amministrazione.

(art 18, regole tecniche)

MODALITÀ DI REGISTRAZIONE DEI DOCUMENTI INFORMATICI

Per i documenti informatici pervenuti ad una area organizzativa omogenea ai sensi dall'articolo 40-bis del Codice, è responsabilità dell'amministrazione decidere, secondo quanto previsto dal manuale di gestione di cui all'articolo 5, comma 2, lettera f), quali documenti sono oggetto di registrazione di protocollo ovvero di registrazione particolare.

(art 18, regole tecniche)

INFORMAZIONI DA INCLUDERE NELLA SEGNATURA

1. Oltre alle informazioni di cui all'articolo 9, il file di cui all'articolo 20, comma 1 contiene le seguenti informazioni minime:

- a) l'oggetto;
- b) il mittente;
- c) il destinatario o i destinatari.

2. Nella segnatura di un documento protocollato in uscita da una Amministrazione possono essere specificate una o più delle seguenti informazioni incluse anch'esse nello stesso file:

- a) indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- b) indice di classificazione;
- c) identificazione degli allegati;

(art. 21, regole tecniche)

TEMPISTICA PER L'ADEGUAMENTO

SISTEMI CONFORMI ALLA DELIBERAZIONE 11/2004

Devono essere adeguati entro e non oltre 18 mesi dall'entrata in vigore delle nuove regole tecniche.

Fino al completamento di tale processo troverà applicazione il DPCM 31/10/2000, recante le precedenti regole tecniche in materia di protocollo informatico.

SISTEMI NON CONFORMI AL DPCM 31/10/2000

Chi, alla data di entrata in vigore delle nuove regole tecniche, non ha un sistema di protocollo a norma (o non lo ha proprio) dovrà adeguarsi tempestivamente alle nuove regole tecniche.

GLI ADEMPIMENTI TECNOLOGICI ED ORGANIZZATIVI

PRINCIPALI ADEMPIMENTI

- Individuare le AOO
- Nominare il/i responsabile/i della gestione documentale
- Nominare (eventualmente) il coordinatore della gestione documentale
- Redigere il manuale di gestione
- Eliminare i protocolli di settore, multipli e telefax

(Art. 3, regole tecniche)

AREE ORGANIZZATIVE OMOGENEE

Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.

(Art. 50, co. 4, D.P.R. n. 445/2000)

INDIVIDUAZIONE DELLE AOO

- AOO come settore dell'organizzazione caratterizzato da esigenze di gestione della documentazione e dei procedimenti tendenzialmente omogenee
- AOO non ha solo unico sistema per il registro di protocollo ma anche sistema unitario per gestione documenti, archiviazione, diffusione informazioni verso esterno
- AOO ha responsabilità unitaria
- Compresenza di aspetti geografici e funzionali

COSA DEVE GARANTIRE IL SISTEMA?

1. Il sistema di gestione informatica dei documenti, in forma abbreviata "sistema" deve:
 - a) garantire la sicurezza e l'integrità del sistema;
 - b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
 - c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
 - d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
 - e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
 - f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

(Art. 52, D.P.R. n. 445/2000)

REGISTRAZIONE DI PROTOCOLLO

1. La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni e' effettuata mediante la memorizzazione delle seguenti informazioni:
 - b) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
 - b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
 - c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
 - d) oggetto del documento, registrato in forma non modificabile;
 - e) data e protocollo del documento ricevuto, se disponibili;
 - f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

(Art. 53, D.P.R. n. 445/2000)

BISOGNA PROTOCOLLARE ANCHE LE EMAIL

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. 40-bis, D. Lgs. n. 82/2005)

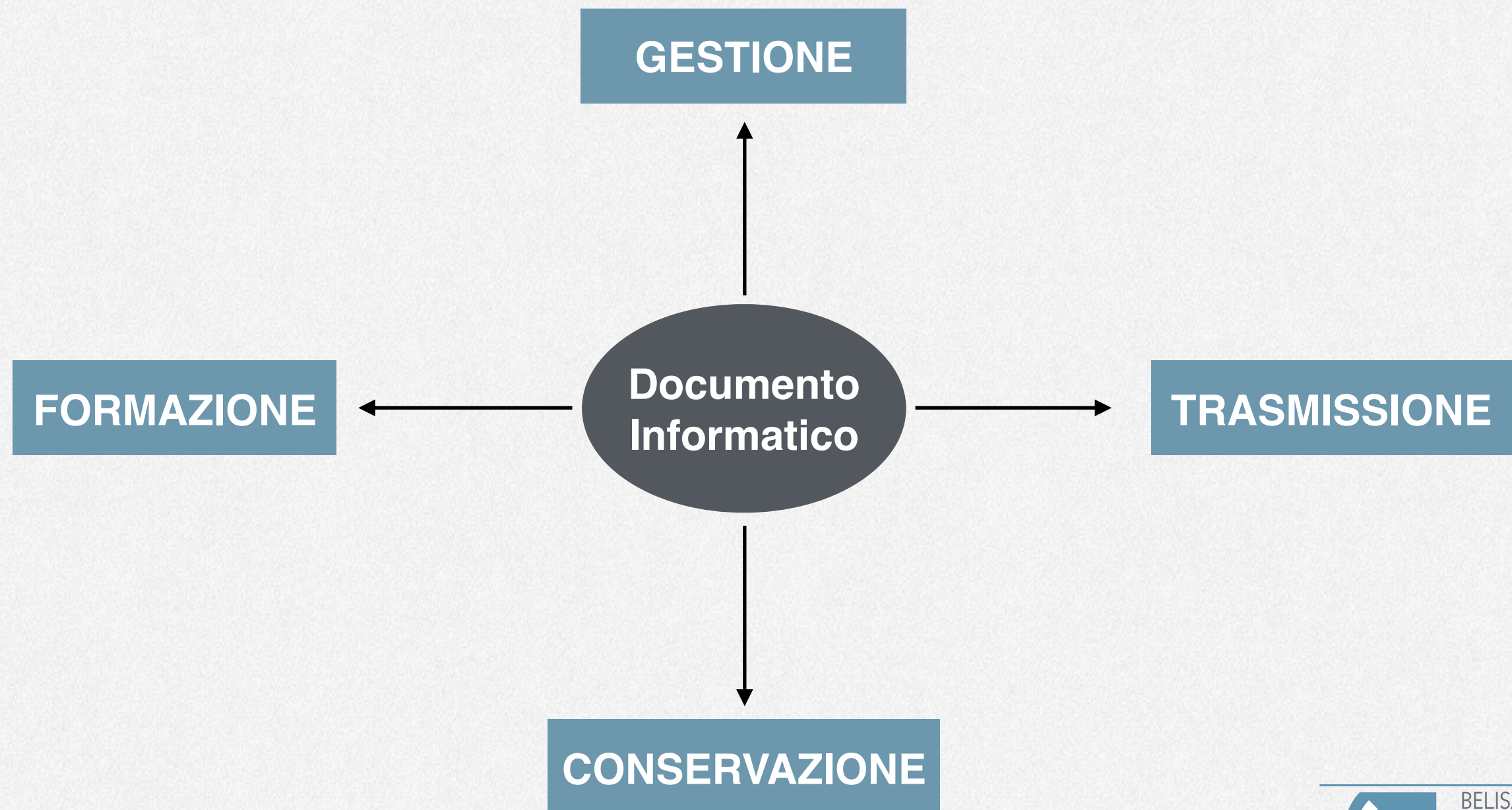
LA CONSERVAZIONE DEL DOCUMENTO INFORMATICO

COS'È

Processo informatico attraverso il quale è possibile garantire nel tempo la validità legale di un documento informatico.

DEMATERIALIZZAZIONE E CONSERVAZIONE

IL CICLO DI VITA DEL DOCUMENTO INFORMATICO



NORMATIVA IN MATERIA DI CONSERVAZIONE

- Deliberazione AIPA 30 luglio 1998, n. 24 relativa ai supporti ottici;
- Deliberazione CNIPA 19 febbraio 2004, n. 11, contenente le precedenti regole tecniche;
- DPCM 3 dicembre 2013 - NUOVE REGOLE TECNICHE.

DOCUMENTI ANALOGICI E DIGITALI

ART. 1 CAD

DOCUMENTO ANALOGICO

p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

DOCUMENTO INFORMATICO

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

DOCUMENTI ANALOGICI E DIGITALI

DOCUMENTO ANALOGICO

- materiale
- è l'unico originale
- può essere sottoscritto con firma autografa

DOCUMENTO INFORMATICO

- immateriale
- tutti i duplicati sono originali
- può essere sottoscritto digitalmente

DEMATERIALIZZAZIONE

- Il termine “dematerializzazione” ha fatto la sua prima comparsa durante gli anni ‘80 nel settore finanziario, con particolare riferimento ai titoli di credito al fine di superarne la fisicità e consentire forme di circolazione virtuali.
- Da allora è entrato a far parte del lessico giuridico: il termine “dematerializzazione” (o “smaterializzazione”) viene utilizzato per identificare la progressiva perdita di consistenza fisica da parte dei documenti e degli archivi, tradizionalmente costituiti da documentazione cartacea, all’atto della loro sostituzione con documenti informatici.

UN PO' DI DATI

- il costo della gestione e della conservazione nella pubblica amministrazione centrale è stimato intorno ai 3 miliardi di euro/anno;
- il costo per la gestione documentale dei soli documenti protocollati nelle PA locali non è inferiore a 1,5 miliardi di euro/anno;
- il costo per la gestione dei cedolini per 1,5 milioni di dipendenti pubblici è stimato oltre i 40 milioni di euro/anno;
- le grandi organizzazioni perdono un documento ogni 12 secondi;
- il 7% dei documenti è perduto in modo definitivo;
- un dirigente spende in media 9 ore all'anno per ricercare documenti male archiviati, male indicizzati o persi;
- il 3% dei documenti sono archiviati in modo errato.

DEMATERIALIZZAZIONE DEI DOCUMENTI DELLE PUBBLICHE AMMINISTRAZIONI

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.

(Art. 42, D.Lgs. n. 82/2005)

RIPRODUZIONE E CONSERVAZIONE DEI DOCUMENTI

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è 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 conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
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'articolo 71.
4. 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.

(Art. 43, D.Lgs. n. 82/2005)

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 originari;
- 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.

1-bis. Il sistema di conservazione dei documenti informatici e' 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.

1-ter. 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.

(Art. 44, D.Lgs. n. 82/2005)

LE NUOVE REGOLE SULLA CONSERVAZIONE NEL TEMPO DEL DOCUMENTO INFORMATICO

NUOVE REGOLE TECNICHE

Deliberazione CNIPA 19 febbraio 2004 N. 11



DPCM 3 dicembre 2013

SISTEMA DI CONSERVAZIONE

1. In attuazione di quanto previsto dall'articolo 44, comma 1, del Codice, il sistema di conservazione assicura, dalla presa in carico dal produttore di cui all'articolo 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**.
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.

(Art. 3, regole tecniche)

COSA CAMBIA

- Non più distinzione tra conservazione sostitutiva di documenti informatici e conservazione sostitutiva di documenti analogici;
- Obbligatoria la redazione del Manuale di conservazione;
- Redazione di un Piano della sicurezza del sistema di conservazione all'interno del Piano generale di sicurezza;
- Nomina di specifiche figure professionali.

CONSERVATORI ACCREDITATI

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.
2. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.

(Art. 44-bis, D. Lgs. n. 82/2005)

GLI OGGETTI DELLA CONSERVAZIONE

- 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.

MODELLI ORGANIZZATIVI

- a) **Conservazione interna:** all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare;
- b) **Conservazione esterna, affidata a soggetti accreditati:** esternalizzata, 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.

GLI OGGETTI DEL SISTEMA DI CONSERVAZIONE

- a) **pacchetti di versamento:** pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
- b) **pacchetti di archiviazione:** pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 delle regole tecniche e riportate nel manuale di conservazione
- c) **pacchetti di distribuzione:** pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta

I RUOLI DEL SISTEMA DI CONSERVAZIONE

- a. produttore;
- b. utente;
- c. responsabile della conservazione.

CONSERVAZIONE AFFIDATA A SOGGETTO ESTERNO

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'articolo 5, mediante contratto o convenzione di servizio che preveda l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della stessa.

8. Il soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali.

(art. 6, regole tecniche)

IL RESPONSABILE DELLA CONSERVAZIONE

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'articolo 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.

(Art. 7, regole tecniche)

IL RESPONSABILE DELLA CONSERVAZIONE

- 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;
- 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;

IL RESPONSABILE DELLA CONSERVAZIONE

- 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'articolo 12;
- 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, per gli organi giudiziari e amministrativi dello Stato, 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 di cui all'articolo 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

IL MANUALE DI CONSERVAZIONE

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.

(Art. 8, comma 1, regole tecniche)

FIGURE NECESSARIE

- Responsabile della conservazione
- Responsabile per il trattamento dei dati personali
- Responsabile del protocollo

SICUREZZA DEL SISTEMA DI CONSERVAZIONE

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'articolo 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'articolo 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.

(Art. 12, regole tecniche)

DPCM 3 DICEMBRE 2013

- Entra in vigore 30 giorni dopo la pubblicazione sulla Gazzetta Ufficiale
- Le Amministrazioni in regola con le vecchie regole tecniche hanno 36 mesi di tempo per adeguarsi

TEMPISTICA PER L'ADEGUAMENTO

SISTEMI CONFORMI ALLA DELIBERAZIONE II/2004

Devono essere adeguati entro e non oltre 36 mesi dall'entrata in vigore delle nuove regole tecniche.

Fino al completamento di tale processo troverà applicazione la deliberazione CNIPA n. II/2004, recante le precedenti regole tecniche in materia di conservazione sostitutiva.

SISTEMI NON CONFORMI ALLA DELIBERAZIONE II/2004

Chi, alla data di entrata in vigore delle nuove regole tecniche, non ha un sistema di conservazione a norma (o non lo ha proprio) dovrà adeguarsi tempestivamente alle nuove regole tecniche.

Q&A

PUT YOUR QUESTIONS

THANKS
FOR YOUR ATTENTION

WWW.E-LEX.IT

EBELISARIO@E-LEX.IT