Formez PA

IL "NUOVO" CAD

Introduzione alle nuove norme in materia di digitalizzazione della PA

Avv. Prof. Ernesto Belisario

www.ernestobelisario.eu

SLB

BELISARIO

STUDIO LEGALE

Napoli, 3 ottobre 2011

BIBLIOGRAFIA

1) **Giuseppe Cassano – Carmelo Giurdanella**, *Il Codice della Pubblica Amministrazione Digitale*. Giuffrè – 2005.

2) **Angelo Giuseppe Orofino**, *Forme elettroniche e procedimenti amministrativi, Cacucci – 2008.*

3) **Marianna Quaranta**, *Il Codice della Pubblica Amministrazione Digitale*. Liguori – 2007.

4) **Ernesto Belisario**, *La nuova Pubblica Amministrazione Digitale*, Maggioli – 2009.

5) **Gilberto Marzano**, *Conservare il digitale*, Editrice Bibliografica - 2011

5) **Pierluigi Ridolfi**, *Il Nuovo Codice della Amministrazione Digitale*, SIAV - 2011

6) **AA. VV.**, *Il nuovo CAD: manuale d'uso*, ForumPA Edizioni, 2011

SITOGRAFIA

1) **Ministero per la Pubblica Amministrazione e l'Innovazione**
   www.innovazionepa.gov.it

2) **Dossier "Codice Amministrazione Digitale"**
   www.governo.it/GovernoInforma/Dossier/codice_amministrazione_digitale/

3) **Senato della Repubblica - Centro Studi**
   www.senato.it/documenti/repository/dossier/studi/2010/Dossier_251.pdf

4) **DigitPA**
   www.digitpa.gov.it

5) **Egov**
   www.egov.maggioli.it

6) **Diritto 2.0**
   blog.ernestobelisario.eu

7) **Dgit@Lex**
   www.digita-lex.it/

SOMMARIO

- I principi generali
- L'importanza delle leggi
- I "nuovi" diritti e i nuovi "doveri"
- Internet e posta elettronica nella PA
- Riuso
- I dati delle Pubbliche Amministrazioni
- I servizi in rete
- Sanzioni e responsabilità
- Conclusioni

OBIETTIVI

INTRODUZIONE AL NUOVO CAD

- Ripassare il “vecchio” CAD
- Evidenziare le disposizioni maggiormente innovative (D.Lgs. n. 235/2010)
- Fornire gli strumenti per una corretta valutazione delle opportunità e dei profili problematici delle nuove normative

Formez PA

<PREMESSA>

IL PAESE HA BISOGNO DI RIFORME,
MA ANCHE LE RIFORME
AVREBBERO BISOGNO DI UN PAESE.

Formez PA

Commenti

Gio, 13/01/2011 - 09:53 — AF (non verificato)

CAD Modifiche 2010. Testo

Si potrebbe acquistare il volume cartaceo?

Grazie

Augusta Franco
Università degli Studi della Basilicata
Ufficio Protocollo ed Archivio

rispondi

Gio, 13/01/2011 - 13:45 — Francesco (non verificato)

volume cartaceo? è uno scherzo?

Egregia Augusta,
(immagino sia il suo nome di battesimo, a meno che lei non abbia scritto prima il cognome che è comunque confondibile con un nome proprio), colgo l'occasione della sua domanda per sottolineare ancora una volta l'atteggiamento degli operatori delle amministrazioni "contrario" ai dettami della digitalizzazione. Non si è accorta che sta chiedendo la copia di CARTA di un testo che stabilisce per LEGGE DELLO STATO che le amministrazioni devono abbandonare il più possibile la carta e passare a documenti informatici?
Non lo prenda sul personale, ma, il suo, è il tipico esempio del perchè la dematerializzazione delle carte nei procedimenti ha incontrato, a dirlo con un eufemismo, delle resistenze.

rispondi


CARTELLA
ARCHIVIO
Anno 18
chivio Comunale
CONSIGLIO EDILIZIO

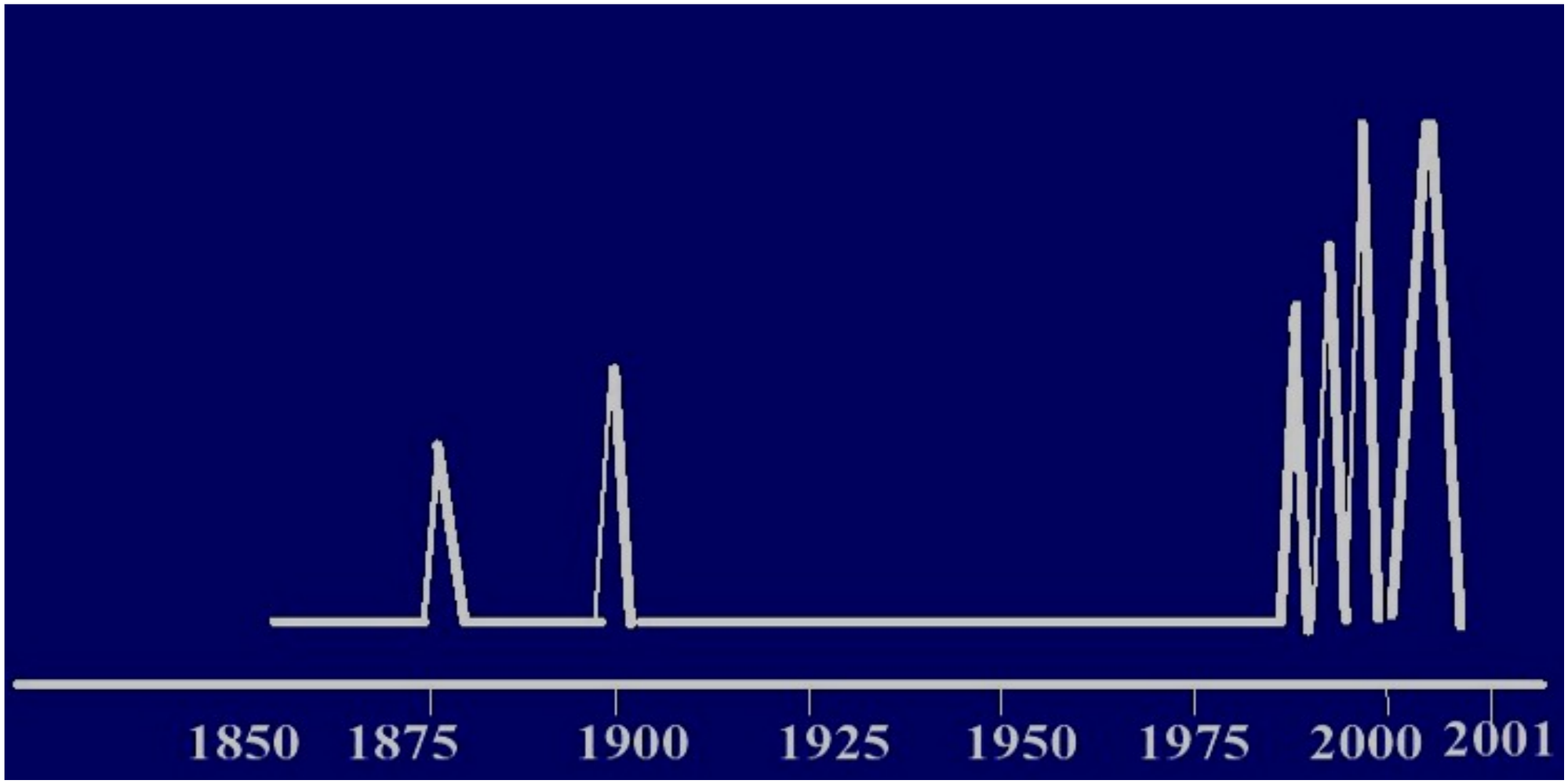
“Gli presentano il progetto per lo snellimento della burocrazia. Ringrazia vivamente. Deplora l’assenza del modulo H. Conclude che passerà il progetto, per un sollecito esame, all’ufficio competente, che sta creando”.

Ennio Flaiano, *Diario Notturno*

“Non è giusto e non è producente continuare a porre sulle spalle del cittadino una quantità sempre crescente di obblighi di sapere e di fare (basti pensare per tutti alla dichiarazione dei redditi e alle difficoltà che comporta la sua compilazione), di sanzioni, di scadenze, di certificazioni e di altri adempimenti di vario genere, come se non avesse altro a cui pensare e come se la vita non fosse già di per se stessa molto più complessa per tutti rispetto a quella di un tempo.”

RENATO BORRUSO

L'ELETTROCARDIOGRAMMA NORMATIVO DELLA PA ITALIANA




OFF

Formez PA

< / PREMESSA>

Formez PA

< IL CONTESTO >

Formez PA

L'AMMINISTRAZIONE DIGITALE

INFORMATIZZAZIONE DELLA P.A.

- “INFORMATICA PARALLELA”
- Eccessiva prolificità normativa (oltre 2.500 atti normativi)
- Mutamento dell’Amministrazione italiana

“Per conseguire maggiore efficienza nella loro attività, le Amministrazioni Pubbliche incentivano l’uso della telematica, nei rapporti interni, tra le diverse Amministrazioni e tra queste e i privati”

Art. 3 –bis, legge 7 agosto 1990, n. 241

Principale normativa su documento e protocollo informatico

- Legge 15 marzo 1997, n. 59, art. 15, comma 2
  - DPR 10 novembre 1997, n. 513
    - DPCM 8 febbraio 1999
      - DPCM 13 gennaio 2004
      - Delibera AIPA 23 novembre 2000, n. 51
      - Circolare AIPA 8 febbraio 2002, n. 39
  - DPR 20 ottobre 1998, n. 403
  - DPR 20 ottobre 1998, n. 428
    - Direttiva PCM 28 ottobre 1999
    - DPCM 31 ottobre 2000
      - Circolare AIPA 7 maggio 2001, n. 28
      - Circolare AIPA 21 giugno 2001, n. 31
  - DPR 28 dicembre 2000, n. 445

Modifiche al DPR 445:

- ~~D.Lgs. 23 gennaio 2002, n. 10~~
- Legge 16 gennaio 2003, n. 3
- DPR 7 aprile 2003, n. 137
- D.Lgs. 30 giugno 2003, n. 196

Modifiche al DPR 445:

- DPCM 30 ottobre 2003
  - Legge 29 luglio 2003, n. 229
  - D.Lgs. 1° agosto 2003, n. 259
  - Legge 11 febbraio 2005, n. 15
  - D.Lgs. 28 febbraio 2005, n. 42
  - DPR 11 febbraio 2005, n. 68
- Delibera CNIPA 19 febbraio 2004, n. 11
- Direttiva MIT 18 dicembre 2003
- Direttiva MIT 19 dicembre 2003
- Direttiva MIT 4 gennaio 2005
- Direttiva MIT 21 dicembre 2001
- Direttiva MIT 9 dicembre 2002
- Direttiva MIT 20 dicembre 2002
- Direttiva MIT 27 novembre 2003
- Decreto MIT 14 ottobre 2003 (2 provv.)
  - D. Lgs. 22 gennaio 2004, n.42
    - D. Lgs. 24 marzo 2006, n. 156
  - D.Lgs. 7 marzo 2005, n. 82
    - D.Lgs. 4 aprile 2006, n. 159

gpd maggio 2006

INFORMATIZZAZIONE DELLA P.A.

"SECONDA FASE DIGITALIZZAZIONE P.A."

Direttiva del Ministro per l'Innovazione e le Tecnologie 4 gennaio 2005

- D. lgs. 28 febbraio 2005, n. 42 (SPC)
- D. lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione digitale)

D. Lgs. 30 dicembre 2010, n. 235

IL CODICE DELL' AMMINISTRAZIONE DIGITALE

Entrato in vigore il 1° gennaio 2006, contiene le disposizioni per garantire il diritto di ogni cittadino a usufruire dei servizi della P.A. anche *on-line* e l'obbligo per la P.A. di snellire le procedure e di rendere tutti i servizi e le comunicazioni interne ed esterne per via telematica.

IL CODICE DELL' AMMINISTRAZIONE DIGITALE

Il CAD ha ordinato e riunito norme già esistenti (in parte già accorpate dal legislatore nel **DPR. 28 dicembre 2000, n. 445**: Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) e ne ha introdotte di nuove per nuovi servizi e nuove opportunità.

IL CODICE DELL' AMMINISTRAZIONE DIGITALE

Nella P.A. digitale le Amministrazioni cooperano tra loro e costituiscono una rete integrata di cui il CAD definisce <u>principi e finalità</u>:

- la riorganizzazione gestionale e dei servizi (art. 12)
- il federalismo efficiente (art. 14)
- la cooperazione (artt. 17, 63, 68)
- la gestione informatica dei procedimenti (art. 41)
- la trasmissione informatica dei documenti (art. 45 ss.)
- la disponibilità dei dati (artt. 50, 58)
- le basi di dati di interesse nazionale (art. 60)

IL CODICE DELL' AMMINISTRAZIONE DIGITALE

NUOVI DIRITTI

- diritto all'uso delle tecnologie (art. 3)
- diritto all'accesso e all'invio di documenti digitali (art. 4)
- diritto ad effettuare qualsiasi pagamento in forma digitale (art. 5)
- diritto a ricevere qualsiasi comunicazione pubblica per *e-mail* (art. 6)
- diritto alla qualità del servizio e alla misura della soddisfazione (art. 7)
- diritto all'alfabetizzazione informatica (art. 8)
- diritto alla partecipazione (art. 9)
- diritto a trovare *on-line* tutti i moduli e i formulari validi (art. 57)

IL CODICE DELL' AMMINISTRAZIONE DIGITALE

I nuovi diritti sono garantiti dalla disponibilità dei seguenti strumenti innovativi:

- i documenti informatici (artt. 1, 20 ss., 39, 40)
- le firme elettroniche (artt. 1, 20, 21, 24 ss.)
- l'archiviazione ottica (artt. 42, 43)
- la posta elettronica certificata (artt. 6, 48)
- i siti *Internet* delle P.A. (artt. 53, 54)

IL CODICE DELL' AMMINISTRAZIONE DIGITALE E' STATO SCARSAMENTE APPLICATO DALLE AMMINISTRAZIONI

PER RISOLVERE LO STALLO DELL'INNOVAZIONE

- Nel "**Libro bianco sulla dematerializzazione**" del 2005 si rileva che

"*La gestione documentale vale oltre il 2% del PIL e quindi un obiettivo di dematerializzazione di appena il 10% genererebbe un risparmio di 3 miliardi di euro, ripetibile ogni anno*".

- "*Nella sola Pubblica Amministrazione Centrale (uffici giudiziari esclusi) si producono ogni anno circa: 110 milioni di documenti, che danno luogo a 160 milioni di registrazioni di protocollo e 147 milioni di archiviazioni.*"

Fonte: NetConsulting 2007

PER RISOLVERE LO STALLO DELL'INNOVAZIONE

PIANO E-GOV 2012

Il Piano di E-government 2012 lanciato a gennaio 2009 dal Ministro per la Pubblica Amministrazione e l'Innovazione Renato Brunetta definisce un insieme di progetti di innovazione digitale che, nel loro complesso, si propongono di modernizzare, rendere più efficiente e trasparente la Pubblica Amministrazione, migliorare la qualità dei servizi erogati a cittadini e imprese e diminuirne i costi per la collettività, contribuendo a fare della Pubblica Amministrazione un volano di sviluppo dell'economia del Paese.

Il Piano definisce definisce 27 obiettivi di Governo da raggiungere entro la fine della legislatura.

PER RISOLVERE LO STALLO DELL'INNOVAZIONE

PIANO E-GOV 2012

OBIETTIVO n. 20 - DEMATERIALIZZAZIONE

Stato di attuazione del piano e-gov 2012

I progetti e-gov 2012

- Obiettivi Settoriali
- Obiettivi Territoriali
- Obiettivi Di Sistema
  - 19 - Trasparenza PA
  - **20 - Dematerializzazione ->**
  - Casella Elettronica Certificata
  - Fatturazione Elettronica
  - Pagamenti On-Line Verso La PA
  - DURC On-Line
  - Operazione Trasparenza
  - Gestione Documentale
  - Attuazione Codice Amministrazione Digitale
  - 22-Rapporto Cittadino-PA
  - 23 - Trasferimento Know-How Innovazione
  - 24 - Sicurezza Sistemi Informativi E Reti
- Obiettivi Internazionali
- Progetti Speciali

Home » Obiettivi di sistema

Dematerializzazione

Entro il 2012 saranno ridotti i flussi cartacei a favore di processi documentali totalmente informatizzati.

Referente per l'obiettivo: Notarmuzi (DIT) c.notarmuzi@governo.it - Pontevolpe (CNIPA) pontevolpe@cnipa.it

I progetti previsti:

- Casella elettronica per i cittadini, le amministrazioni pubbliche, le imprese e i professionistio
- Fatturazione elettronica
- Pagamenti on-line
- DURC on-line
- Operazione trasparenza
- Gestione documentale
- Attuazione del Codice di Amministrazione Digitale

http://www.e2012.gov.it/egov2012/?q=content/dematerializzazione-0

PER RISOLVERE LO STALLO DELL'INNOVAZIONE

MODIFICA E AGGIORNAMENTO CAD

art. 33 Legge. n. 69/2009

IL “NUOVO” CAD

D. LGS. n. 235/2010

Con il decreto legislativo 30 dicembre 2010, n. 235 sono state apportate sostanziali modifiche ed integrazioni al Codice dell’Amministrazione Digitale del 2005.

Tale intervento normativo trae ragione da:

- l’evoluzione delle tecnologie informatiche;
- la necessità di coordinamento con le nuove norme in tema di trasparenza, organizzazione e merito;
- l’urgenza di elevare i livelli di efficacia, efficienza ed economicità del sistema pubblico;
- la decisione di accelerare i processi di digitalizzazione.

QUALI SONO LE PRINCIPALI NOVITA' INTRODOTTE DAL D. LGS. N. 235/2010?

ORGANIZZAZIONE INTERNA

Non può esservi vera innovazione senza reingegnerizzazione dei processi; per questo le PA centrali saranno obbligate ad istituire un ufficio unico responsabile delle attività ICT e la costituzione di detto Ufficio è altresì raccomandata anche alle Regioni e agli Enti Locali.

Tale istituzione si rende opportuna, tanto più che l'attuazione delle disposizioni del CAD è comunque rilevante ai fini della misurazione e della valutazione della performance organizzativa e individuale dei dirigenti. Alle opportunità si accompagnano quindi sia gli incentivi, sia le sanzioni: l'innovazione diventa così - in modo cogente - materia di valutazione del personale, da cui dipendono sanzioni ed incentivi.

L'introduzione delle nuove tecnologie diviene poi obbligatoria nella gestione dei procedimenti amministrativi (con l'espresso obbligo di protocollare la posta elettronica certificata e di creare il fascicolo elettronico del procedimento)

RAPPORTI CON CITTADINI E IMPRESE

Gli Enti dovranno utilizzare le comunicazioni cartacee solo quando sia impossibile utilizzare quelle telematiche (soprattutto via Posta Elettronica Certificata); ogni amministrazione dovrà poi consentire a cittadini ed imprese i pagamenti informatici e l'inoltro di istanze per via telematica.

Gli Enti dovranno curare maggiormente i contenuti dei propri siti Web, che diventano sempre più il vero front-office; molto importante, a riguardo, la disposizione che prevede che le PA promuovano progetti volti alla diffusione e al riutilizzo dei dati pubblici: si tratta della prima norma nazionale in materia di Open Data.

RAPPORTI CON CITTADINI E IMPRESE

I cittadini e le imprese hanno diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Non sarà più possibile quindi per un Ente o per un gestore di pubblico servizio obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale sicuro (nella maggior parte dei casi costituito dalla PEC), certificato e con piena validità giuridica che permetta di dialogare con la PA dal proprio computer; il nuovo Codice amplia questo diritto anche verso i gestori di servizi pubblici.

La riforma permette poi di esigere questo diritto anche mediante l'uso dell'azione collettiva e introduce l'effettiva disponibilità degli strumenti necessari nella valutazione dei dirigenti e delle organizzazioni.

RAPPORTI CON CITTADINI E IMPRESE

Già il Codice del 2005 imponeva alle amministrazioni di consentire i pagamenti ad esse spettanti con le tecnologie digitali, ma non diceva come. Il nuovo CAD prevede una serie di strumenti operativi (ad es. le carte di credito) e consente di avvalersi di soggetti anche privati per la riscossione, aprendo di fatto un nuovo mercato dei servizi.

Il digitale diventa la regola nei rapporti tra imprese ed amministrazioni e il cartaceo l'eccezione. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

RAPPORTI CON CITTADINI E IMPRESE

La PEC (Posta Elettronica Certificata) diventa, per tutte le imprese e i professionisti, che per legge devono esserne dotati e per i cittadini che lo desiderano il mezzo più veloce, sicuro e valido per comunicare con le amministrazioni pubbliche. Da lì passano comunicazioni, atti e provvedimenti, ma anche istanze e dichiarazioni che un cittadino può trasmettere usando la propria casella PEC anche come strumento di identificazione che può evitare, nella maggior parte dei casi, l'uso della firma digitale.

SICUREZZA INFORMATICA

Il digitale diventerà la regola ed il cartaceo l'eccezione; di conseguenza, le amministrazioni dovranno – necessariamente – dedicare sempre maggiore attenzione alla sicurezza dei dati e alla privacy dei cittadini.

Se la PA diventa digitale la sicurezza dei dati, dei sistemi e delle infrastrutture è sempre più un obiettivo chiave, anche per costruire quella fiducia nei servizi pubblici on line che ancora manca; il codice introduce disposizioni importanti sia sulla continuità operativa, sia sul disaster recovery dettando le modalità per il coordinamento delle azioni delle singole amministrazioni e per la predisposizione di piani operativi.

QUALI SONO LE PRINCIPALI SCADENZE DELLA RIFORMA?

ENTRO IL 25 APRILE 2011

- Le pubbliche amministrazioni utilizzeranno la posta elettronica certificata o altre soluzioni tecnologiche per tutte le comunicazioni che richiedono una ricevuta di consegna ai soggetti che hanno preventivamente dichiarato il proprio indirizzo.

ENTRO IL 25 MAGGIO 2011

- Le amministrazioni centrali individueranno un unico ufficio responsabile dell'attività ICT.

ENTRO IL 25 LUGLIO 2011

- Le PA centrali pubblicheranno sui propri siti istituzionali i bandi di concorso e tutta una serie di informazioni sul proprio funzionamento nell'ottica della total disclosure.
- Le amministrazioni consentiranno ovunque i pagamenti ad esse spettanti per via telematica.
- Le amministrazioni e le imprese comunicheranno tra loro esclusivamente per via telematica.

ENTRO IL 25 GENNAIO 2012

- Le Pubbliche Amministrazioni non potranno richiedere l'uso di moduli e formulari che non siano stati pubblicati sui propri siti istituzionali.

- Il cittadino fornirà una sola volta i propri dati alla pubblica amministrazione. Sarà onere delle Amministrazioni (in possesso dei dati) assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre Amministrazioni richiedenti.

- Saranno emanate le regole tecniche che consentiranno di dare piena validità alle firme elettroniche diverse da quella digitale, nonché, alle copie cartacee e, soprattutto, a quelle digitali dei documenti informatici, dando così piena effettività al processo di dematerializzazione dei documenti della PA.

- Saranno emanate le regole tecniche per la conservazione sostitutiva dei documenti in forma digitale dando il via agli archivi informatizzati.

ENTRO IL 25 MARZO 2012

- Gli Enti dovranno predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire servizi e il ritorno alla normale operatività.

Formez PA

I DIRITTI DIGITALI

I PRINCIPI

1. 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.

2. 2. 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.

3. *(art. 2, commi 1 e 2, D. lgs. n. 82/2005)*

I NUOVI DIRITTI

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all'articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.

1-*ter*. *La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.*

(art. 3, D. lgs. n. 82/2005)

I NUOVI DIRITTI

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

(art. 4, D. lgs. n. 82/2005)

I NUOVI DIRITTI

1. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

(art. 5-bis, D. lgs. n. 82/2005)

I NUOVI DIRITTI

Le PA devono provvedere al necessario adeguamento tecnologico ed organizzativo

✓ Piena attuazione normativa in materia di digitalizzazione (CAD, protocollo informatico);

✓ Conservazione dati e leggibilità dei documenti;

✓ Libertà delle forme e autonomia organizzativa (strumenti di identificazione);

✓ Non invocabili difficoltà organizzative (CdS, VI, sent. 635/1998);

✓ Responsabilità (T.A.R. Basilicata, sent. 478/2011).

Formez PA

< / IL CONTESTO >

CENTRALITA' DEL DOCUMENTO INFORMATICO

GESTIRE IL CAMBIAMENTO

✓ La scrittura ha sempre un ruolo fondamentale nel procedimento amministrativo. Essa rappresenta la testimonianza e ha portato nel tempo alla definizione di registri, libri, formulari, repertori, etc.

✓ Nell'informatica gli eventi hanno prevalente corrispondenza con i processi automatizzati.

✓ La registrazione informatica diventa quindi quell'insieme di informazioni "chiuse", rilevanti per l'organizzazione e che tiene traccia documentando e qualificando un evento o una transazione.

✓Un altro elemento cruciale è la conservazione documentale indispensabile per garantire un ciclo di vita "lungo" al documento informatico.

I LIVELLI DEL CAMBIAMENTO

Una schematizzazione può essere descritta mediante quattro livelli di maturità.

- Livello 0: introduzione dell'informatica (la I di ICT).
- Livello 1: diffusione degli strumenti di comunicazione (la C di ICT).
- Livello 2: attivazione di procedure automatiche di gestione documentale.
- Livello 3: riconoscimento totale della registrazione informatica (superamento del cartaceo).

Formez PA

< I SUPPORTI>

SCIENTIFIC AMERICAN

Ensuring the Longevity of Digital Documents

The digital medium is replacing paper in a dramatic record-keeping revolution. But such documents may be lost unless we act now

by Jeff Rothenberg

SCIENTIFIC AMERICAN *January 1995*

The year is 2045, and my grandchildren (as yet unborn) are exploring the attic of my house (as yet unbought). They find a letter dated 1995 and a CD-ROM. The letter says the disk contains a document that provides the key to obtaining my fortune (as yet unearned). My grandchildren are understandably excited, but they have never before seen a CD—except in old movies. Even if they can find a suitable disk drive, how will they run the software necessary to interpret what is on the disk? How can they read my obsolete digital document?

This imaginary scenario reveals some fundamental problems with digital documents. Without the explanatory letter, my grandchildren would have no reason to think the disk in my attic was worth deciphering. The letter possesses the enviable quality of being readable with no machinery, tools or special knowledge beyond that of English. Because digital information can be copied and recopied perfectly, it is often extolled for its supposed longevity. The truth, however, is that because of changing hardware and software, only the letter will be immediately intelligible 50 years from now.

I SUPPORTI FISICI

✓ Falso mito: la carta è eterna

✓ Il dato elettronico per essere consultato nel tempo deve essere gestito opportunamente

✓ E’ breve - molto più di quanto si pensi - il ciclo di vita dei supporti più diffusi (Floppy, CD/DVD, Hard disk, pen drive, memoria flash: da 5 a 10 anni di vita media con picchi negativi di 2 anni per CD economici mal conservati; Nastro VHS, Nastro Mini-DV: da 10 a 15 anni di vita media; Nastro magnetico, Dvd-RAM: da 20 a 340 anni di vita media).

LA TECNOLOGIA NON E' TUTTO

- ✓ Importanza dei profili organizzativi
- ✓ Censimento delle informazioni da conservare
- ✓ Ridondanza e backup
- ✓ Importanza del riversamento
- ✓ Controlli e verifiche periodici
- ✓ Importanza della qualità nelle forniture

Formez PA

</ I SUPPORTI>

Formez PA

< I FORMATI >


P7M

DEFINIZIONE

In informatica, un formato di file è la convenzione che viene usata per leggere, scrivere e interpretare i contenuti di un file.

Poiché i file non sono altro che insiemi ordinati di byte, cioè semplici numeri, per poter associare al loro contenuto cose diverse si usano convenzioni che legano i byte ad un significato.

Ad esempio, un formato di file per immagini può stabilire che i primi due byte sono l'altezza e la larghezza dell'immagine, e i seguenti i colori secondo uno schema preordinato.

DEFINIZIONE

- Spesso identifichiamo il formato dall'estensione del file
- Sono note oltre 15.000 estensioni, ma solo alcune centinaia sono documentate e solo alcune decine sono utilizzate quotidianamente negli uffici pubblici
- Ad es. formato testi TXT, DOC, HTML, PDF, RTF, TEX, ecc.).
- Di norma, vengono scelti i formati più diffusi… ma una PA non può fare questo.

STANDARD E FORMATI

Adeguamento tecnologico ed organizzativo

Conservazione dei dati e leggibilità dei documenti

FORMATI (*art. 16 DPCM 31 ottobre 2000*)

REQUISITI (*art. 4 Deliberazione Aipa n. 51/2000*)

- non alterabilità

- immutabilità

- interoperabilità

I FORMATI IDONEI ALLA CONSERVAZIONE

1. *Devono essere "open" e non proprietari*
2. *Devono essere auto-consistenti e autoesplicativi*
3. *Non devono contenere istruzioni interne (ad es. macro) in grado di modificarne il contenuto*
4. *Devono essere bene documentati*

NON PROPRIETA’

- Un formato è proprietario quando è stato creato da una organizzazione privata (ad es. un’azienda, una software house, etc.), che ne detiene i diritti di proprietà intellettuale; di conseguenza le sue specifiche vengono gestite esclusivamente da tale organizzazione.

- Un formato è, invece, non proprietario (o libero) quando la gestione delle sue specifiche non è prerogativa di un’organizzazione privata ma è affidata ad una comunità di sviluppatori che cooperano per la gestione condivisa delle stesse, o ad un organismo di standardizzazione.

- E’ preferibile utilizzare formati non proprietari che non sono legati all’esistenza di una specifica azienda che ne detiene la proprietà e che potrebbe, in qualsiasi momento, modificarne le specifiche, renderle inaccessibili, o imporre restrizioni sul loro utilizzo.

APERTURA

- Un formato è aperto (o pubblico) quando le sue specifiche sono pubbliche, liberamente accessibili (ad esempio perché sono state pubblicate sul web).
- Viceversa, un formato è chiuso (o segreto) quando le sue specifiche non sono pubbliche.
- Un formato adatto per la produzione di documenti informatici compatibili con un processo di conservazione digitale non solo deve essere aperto ma deve essere anche completamente documentato.

STANDARDIZZAZIONE

Un formato è standard quando:

- le sue specifiche sono definite o approvate da un organismo di standardizzazione (ad esempio l'ISO, l'ANSI, l'ECMA, il W3C, etc.) e quindi ha ottenuto un riconoscimento ufficiale (c.d. "standard de jure");
- le sue specifiche non sono state ratificate da nessun organismo di normazione, ma è diventato, di fatto, uno standard grazie alla sua ampia diffusione (c.d. "standard de facto").

I formati che sono standard sono meno soggetti ad obsolescenza.

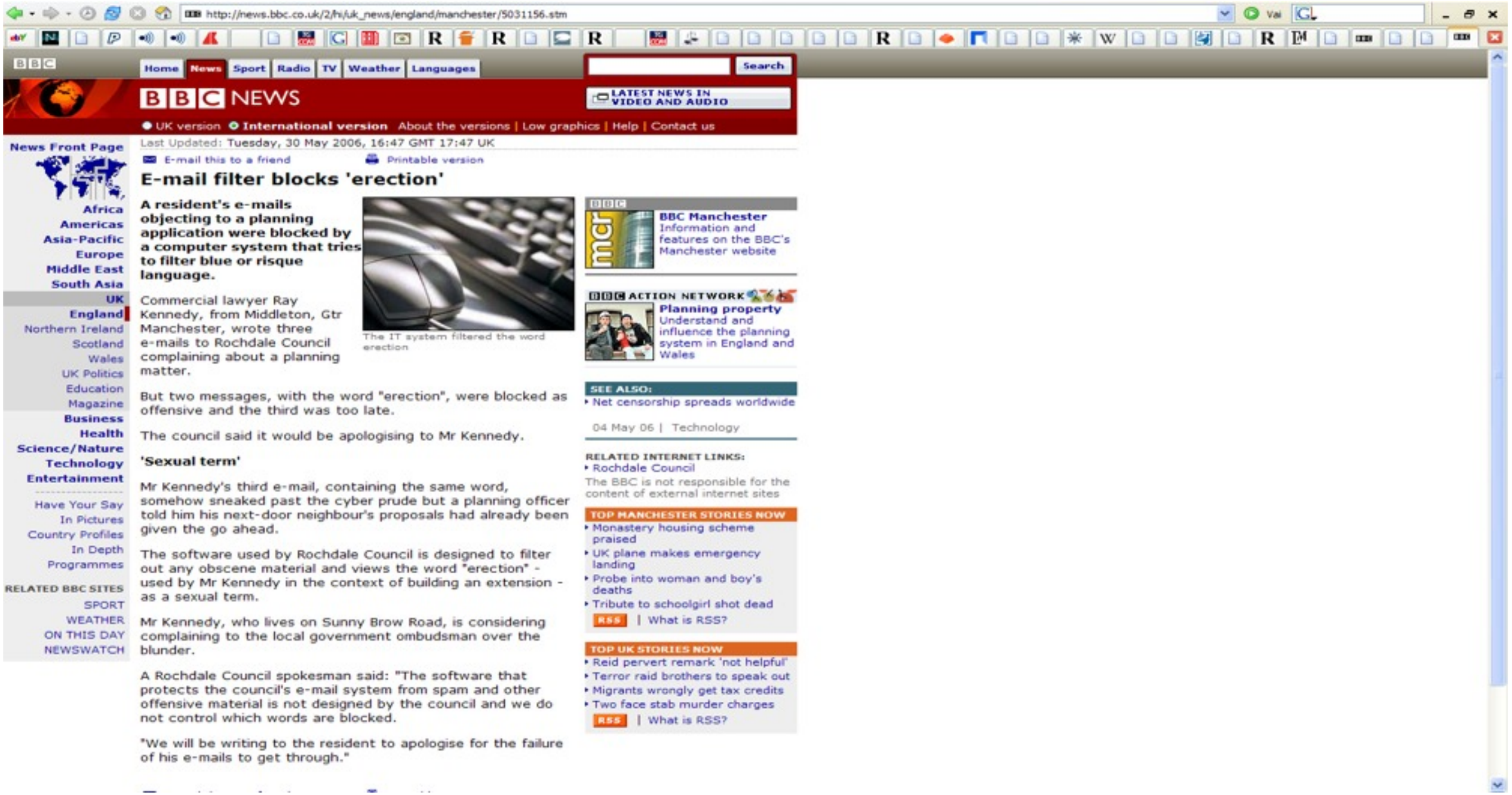
Gli standard de jure sono da preferire agli standard de facto, dal momento che solo il processo ufficiale di standardizzazione garantisce che non vi siano interessi di parte nella definizione ed implementazione di un formato.

DIGITPA ED I FORMATI

4. Il DigitPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.

(art. 68, D. Lgs. n. 82/2005)

IMPREVISTI DA EVITARE...



http://news.bbc.co.uk/2/hi/uk_news/england/manchester/5031156.stm

Formez PA

< / I FORMATI>

< IL DOCUMENTO INFORMATICO >

[DOCUMENTO] + [INFORMATICO]

SOSTANTIVO E AGGETTIVO

COMINCIAMO DAL DOCUMENTO...

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

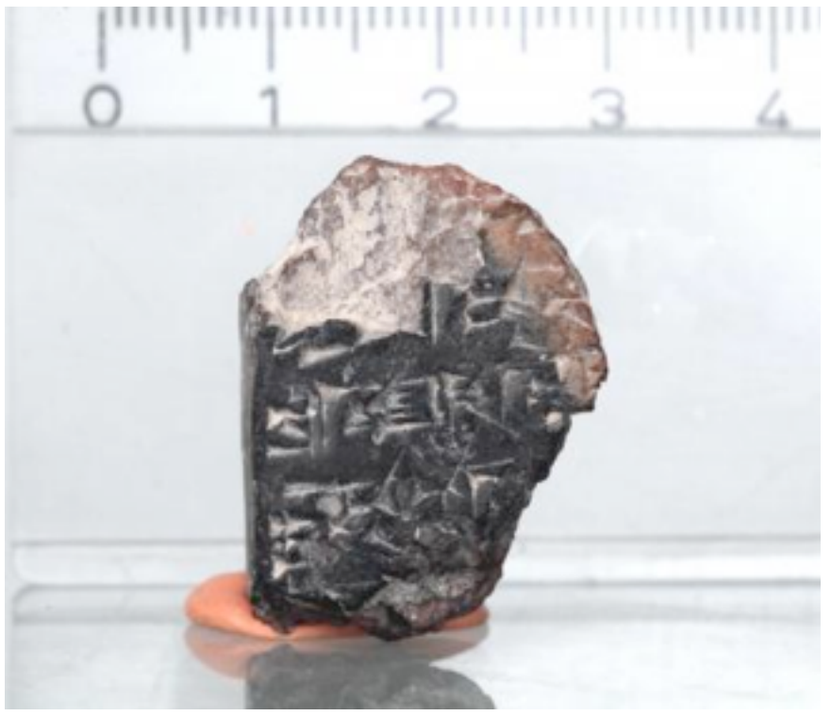
(*art. 1, comma 1, lett. A, D.P.R. 28-12-2000 n. 445*

Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa)

L'ETIMOLOGIA

documénto = *lat.* DOCUMÈNTUM da DOCÈRE *informare, far sapere, insegnare* (v. *Docente*). — Insegnamento, Ammaestramento, Regola concernente checchessia.

Deriv. *Documentàre.*



DOCUMENTO SCRITTO, XIV SECOLO A.C., GERUSALEMME

CONTRATTO CON GLI ITALIANI

tra Silvio Berlusconi,

nato a Milano il 29 settembre 1936,

leader di Forza Italia e della Casa delle Libertà,

che agisce in pieno accordo con tutti gli alleati della coalizione,

e

i cittadini italiani

si conviene e si stipula quanto segue.

Silvio Berlusconi, nel caso di una vittoria elettorale della Casa delle Libertà, si impegna, in qualità di Presidente del Consiglio, a realizzare nei cinque anni di governo i seguenti obiettivi:

1. Abbattimento della pressione fiscale
   - con l'esenzione totale dei redditi fino a 22 milioni di lire annui;
   - con la riduzione al 23 per cento dell'aliquota per i redditi fino 200 milioni;
   - con la riduzione al 33 per cento dell'aliquota per i redditi sopra i 200 milioni;
   - con l'abolizione della tassa di successione e della tassa sulle donazioni.
2. Attuazione del "Piano per la difesa dei cittadini e la prevenzione dei crimini" che prevede tra l'altro l'introduzione dell'istituto del "poliziotto o carabiniere o vigile di quartiere" nelle città, con il risultato di una forte riduzione del numero di reati rispetto agli attuali 3 milioni.
3. Innalzamento delle pensioni minime ad almeno 1 milione di lire al mese.
4. Dimezzamento dell'attuale tasso di disoccupazione con la creazione di almeno 1 milione e mezzo di nuovi posti di lavoro.
5. Apertura dei cantieri per almeno il 40 per cento degli investimenti previsti dal "Piano decennale per le Grandi Opere" considerate di emergenza e comprendente strade, autostrade, metropolitane, ferrovie, reti idriche e opere idro-geologiche per la difesa dalle alluvioni.

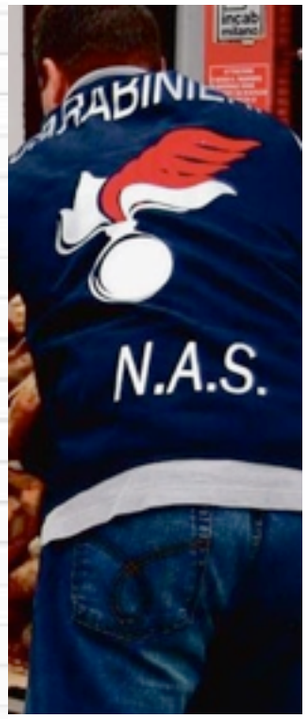
Nel caso in cui al termine dei cinque anni di governo almeno 4 su 5 di questi traguardi non fossero stati raggiunti, Silvio Berlusconi si impegna formalmente a non ripresentare la propria candidatura alle successive elezioni politiche.

In fede,

Silvio Berlusconi

Il contratto sarà reso valido e operativo il 13 maggio 2001 con il voto degli elettori italiani.

Il contratto con gli italiani



Acqua minerale da sottoporre ad esame chimico

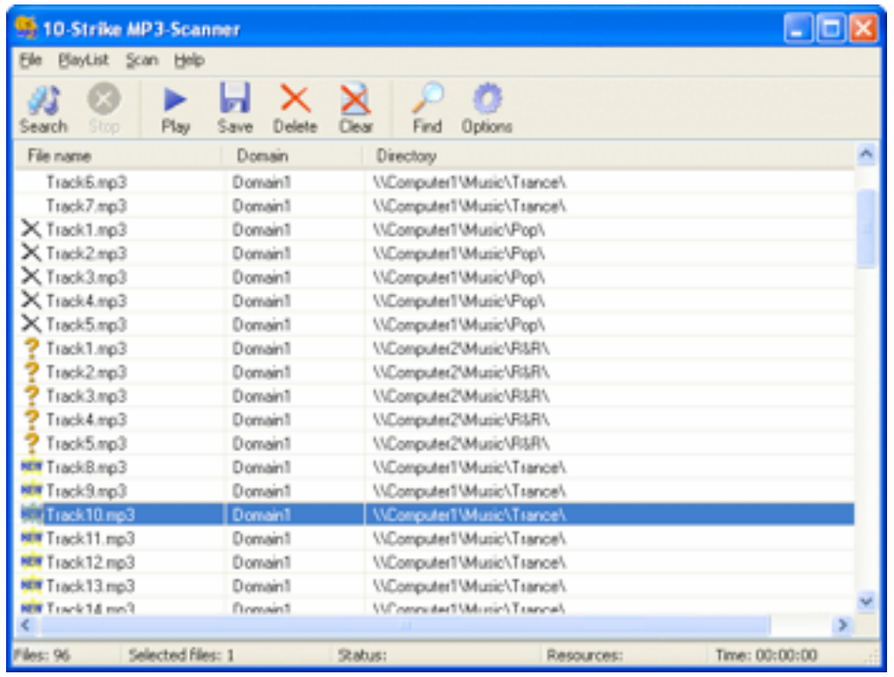
DEFINIZIONE

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

(art. 1, D. LGS. n. 82/2005)

Formez PA

I DOCUMENTI INFORMATICI



IL DOCUMENTO INFORMATICO

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71.

(art. 20, D. LGS. n. 82/2005)

IL DOCUMENTO INFORMATICO

VALIDITA'

- ☑ Liberamente valutabile in giudizio se sprovvisto di firma digitale o con firma elettronica
- ☑ 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. è richiesta la firma elettronica qualificata o digitale a pena di nullità

IL DOCUMENTO INFORMATICO

TITOLARE

- ☑ Chi forma un documento informatico, anche parzialmente

TEMPO DI FORMAZIONE

- ☑ Nelle quasi totalità dei casi è all'attivazione del procedimento e quindi i riferimenti sono il protocollo informatico e la PEC; raramente viene utilizzata la marca temporale.

DEFINIZIONE

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

(art. 1, D. LGS. n. 82/2005)

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.

(art. 22, D. LGS. n. 82/2005)

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)

LE COPIE INFORMATICHE

VALIDITA'

- ☑ 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

DEFINIZIONE

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

(art. 1, D. LGS. n. 82/2005)

COPIE PER IMMAGINE

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.

(art. 22, D. LGS. n. 82/2005)

LE COPIE INFORMATICHE

VALIDITA'

- ☑ 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

DEFINIZIONE

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

(art. 1, D. LGS. n. 82/2005)

COPIE ANALOGICHE DI DOCUMENTO INFORMATICO

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'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.
2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

(art. 23, D. LGS. n. 82/2005)

COPIE ANALOGICHE DI DOCUMENTO INFORMATICO

5. Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico.

(art. 23-ter, D. LGS. n. 82/2005)

COPIE ANALOGICHE DI DOCUMENTO INFORMATICO

VALIDITA'

- ☑ 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

[FIRMA] + [ELETTRONICA]

SOSTANTIVO E AGGETTIVO

Formez PA

LA FIRMA AUTOGRAFA

DOCUMENTO INFORMATICO E FIRME

DPR 513/1997

- Firma digitale

Dir. 1999/93/CE

- Firma elettronica
- Firma elettronica avanzata

D.Lgs. 10/2002

- Firma elettronica
- Firma elettronica avanzata

DPR 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

ESISTONO MOLTI MODI DI FIRMARE...

DEFINIZIONI

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
q-bis) firma elettronica avanzata: 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;
r) firma elettronica qualificata: 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;
s) firma digitale: un particolare tipo di firma elettronica qualificata basata 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;

(art. 1, D. LGS. n. 82/2005)

FIRME ELETTRONICHE

Liberamente valutabile

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

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

FIRMA ELETTRONICA

Insieme di dati usati per l'identificazione

FIRMA ELETTRONICA AVANZATA

FE + connessione univoca con il soggetto, mezzo a controllo esclusivo

FIRMA ELETTRONICA QUALIFICATA

FEA + SSCD + certificato qualificato

FIRMA DIGITALE

FEA + certificato qualificato + crittografia asimmetrica

TIPOLOGIE DI FIRME

Fonte: DigitPA

Formez PA

LA FIRMA ELETTRONICA

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.

La firma autografa SI riferisce in maniera univoca ad un solo soggetto ed al documento…cui è apposta….

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.

Per la firma autografa deve adoperarsi una penna, un foglio di carta ed il braccio del suo titolare e soprattutto non scade…

NON CHIAMIAMOLA “FIRMA” MA TITOLO RAPPRESENTATIVO DELL’IDENTITÀ DIGITALE CERTIFICATA

< / IL DOCUMENTO INFORMATICO >

< LA TRASMISSIONE DEL DOCUMENTO INFORMATICO >

POSTA ELETTRONICA

VANTAGGI

La posta elettronica rappresenta uno strumento di amplissima diffusione per le caratteristiche di semplicità, immediatezza ed efficacia

POSTA ELETTRONICA

PROFILI PROBLEMATICI

- Possibilità di falsificazione di mittente, orario di invio, notifica di ricezione, ecc.

- Mancata standardizzazione delle ricevute e dei comportamenti dei gestori (attribuzione delle caselle, trattamento delle anomalie)

- Debolezze ⟶ Valore legale

POSTA ELETTRONICA CERTIFICATA

PERCHE' NASCE

La posta elettronica certificata (PEC) è un sistema di posta che supera le debolezze della posta elettronica tradizionale e può essere utilizzata in qualsiasi contesto nel quale sia necessario avere prova dell'invio e della consegna di una determinata comunicazione

POSTA ELETTRONICA CERTIFICATA

DEFINIZIONE

"*sistema elettronico di trasmissione di documenti informatici nel quale è fornita al mittente la documentazione elettronica attestante l'invio e la consegna di documenti informatici*"

(art. 1, comma 2, lett. g-h, DPR n. 68/2005)

POSTA ELETTRONICA CERTIFICATA

DEFINIZIONE

"*sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi*"

(art. 1, comma 1, lett. v-bis, D. Lgs. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

VALORE DELLA TRASMISSIONE

Il documento informatico trasmesso per via telematica si intende

- ✓ SPEDITO DAL MITTENTE: se inviato al proprio gestore di PEC

- ✓ CONSEGNATO AL DESTINATARIO: se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione del gestore di PEC

POSTA ELETTRONICA CERTIFICATA

CONFRONTO CON LA RACCOMANDATA A/R

L’attestazione di invio e ricezione, rilasciata dal gestore di PEC, ha lo stesso valore dell’avviso di ricevimento della raccomandata postale, ed è opponibile a terzi

POSTA ELETTRONICA CERTIFICATA

CONFRONTO CON LA RACCOMANDATA A/R

RACCOMANDATA

- non si può sapere chi spedisce una raccomandata
- non si può sapere cosa è stato spedito

PEC

- certezza della casella del mittente (e, quindi, del suo titolare)
- legame certo tra la trasmissione e il documento stesso

POSTA ELETTRONICA CERTIFICATA

PUNTI DI FORZA

- ✓ Certificazione di avvenuta consegna del messaggio e dei suoi allegati
- ✓ Archiviazione di tutti gli eventi da parte del proprio gestore
- ✓ Semplicità di inoltro, riproduzione, archiviazione e ricerca
- ✓ Economicità della trasmissione
- ✓ Velocità della consegna
- ✓ Garanzia dell'identità del mittente

POSTA ELETTRONICA CERTIFICATA

PRECISAZIONI

- La PEC non può sostituire la firma digitale
- La PEC può essere utilizzata anche per scambiare comunicazioni con caselle di posta elettronica c.d. tradizionale (sebbene con differente valore legale)

POSTA ELETTRONICA CERTIFICATA

LE NORME RILEVANTI

- Legge n. 59/1997
- D.P.R. n. 445/2000
- D.P.R. n. 68/2005
- D. LGS. n. 82/2005 (come modificato dal D. Lgs. 23/2010)
- Legge n. 2/2009
- Legge n. 69/2009
- D. Lgs. n. 150/2009
- Circolare Min. Innovazione n. 1/2010

POSTA ELETTRONICA CERTIFICATA

LEGGE SULLA SEMPLIFICAZIONE AMMINISTRATIVA

"Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge."

(art. 15, comma 2, Legge n. 59/1997)

POSTA ELETTRONICA CERTIFICATA

"1. 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.

2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi.

3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge"

(art. 14, D.P.R. n. 445/2000 abrogato dall'art. 75 D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

DECRETO DEL PRESIDENTE DELLA REPUBBLICA

11 febbraio 2005 n.68

Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3

POSTA ELETTRONICA CERTIFICATA

CODICE DELL'AMMINISTRAZIONE DIGITALE

"1. *Le Pubbliche Amministrazioni centrali utilizzano la posta elettronica certificata, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.*

2. Le disposizioni di cui al comma 1 si applicano anche alle Pubbliche Amministrazioni regionali e locali salvo che non sia diversamente stabilito."

(art. 6, D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

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

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 protocollo informatizzato;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.”

(art. 47, D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

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. La 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.

(art. 47, D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

(art. 48, D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

(art. 48, D. LGS. n. 82/2005)

POSTA ELETTRONICA CERTIFICATA - GLI OBBLIGHI

MONOPOLY

SOGGETTI OBBLIGATI ALLA PEC

PUBBLICHE AMMINISTRAZIONI

“ Le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, qualora non abbiano provveduto ai sensi dell'articolo 47, comma 3, lettera a), del Codice dell'Amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, istituiscono una casella di posta certificata o analogo indirizzo di posta elettronica di cui al comma 6 per ciascun registro di protocollo e ne danno comunicazione al Centro nazionale per l'informatica nella pubblica amministrazione, che provvede alla pubblicazione di tali caselle in un elenco consultabile per via telematica. Dall'attuazione del presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica e si deve provvedere nell'ambito delle risorse disponibili.”

(art. 16, comma 8, Legge n. 2/2009)

SOGGETTI OBBLIGATI ALLA PEC

LE IMPRESE

“ Le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell’invio e della ricezione delle comunicazioni e l’integrità del contenuto delle stesse, garantendo l’interoperabilità con analoghi sistemi internazionali. Entro tre anni dalla data di entrata in vigore del presente decreto tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, comunicano al registro delle imprese l'indirizzo di posta elettronica certificata. L'iscrizione dell'indirizzo di posta elettronica certificata nel registro delle imprese e le sue successive eventuali variazioni sono esenti dall'imposta di bollo e dai diritti di segreteria.”

(art. 16, comma 6, Legge n. 2/2009)

SOGGETTI OBBLIGATI ALLA PEC

I PROFESSIONISTI

“ I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6 entro un anno dalla data di entrata in vigore del presente decreto. Gli ordini e i collegi pubblicano in un elenco riservato,consultabile in via telematica esclusivamente dalle pubbliche amministrazioni,i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.”

(art. 16, comma 7, Legge n. 2/2009)

Formez PA

LA PEC PER I PROFESSIONISTI

TERMINE PER L'ADEGUAMENTO

29 novembre 2009

CONSEGUENZE PER IL MANCATO ADEGUAMENTO

sanzioni disciplinari

CONOSCIBILITA' DEGLI INDIRIZZI PEC

appositi elenchi

Accesso Ascachannel
Utente Registrato
nome utente password
ENTRA
non sei registrato clicca qui

economia
finanza
tecnologia
politica
sociale
esteri
archivio news
news@mail
» ascachannel

multimedia

salute oggi

- Home Page
- Copertina
- Focus
- Speciali
  - Ricostruzione Abruzzo
- Abruzzo/la ripresa
- Breaking News
- Economia
- Borse&Mercati
- Politica
- Enti Locali
- Sport
- Attualitá
- Energia e Mercati
- Terzo Settore
- Leggi&Regioni
- Cooperazione decentrata
- Vetrinaitaliana
- Attività di Governo
- Edizione Radiofonica
  - Governo.it
  - Governo.it focus
  - Governo.it estero
- Autonomie Locali
- Multimedia
- Ambiente e turismo
- Stampa estera
- Famiglia

economia
comunicati stampa

Torna al minisito "ICT"

19-03-10

P.A.: BRUNETTA, AL VIA CONTROLLI SU ORDINI PROFESSIONALI PER 'PEC'

(ASCA) - Roma, 19 mar - Il Ministro per la Pubblica Amministrazione e l'Innovazione Renato Brunetta ha incaricato l'Ispettorato per la Funzione Pubblica di accertare se e in quale modo gli Ordini e i Collegi Professionali abbiano adempiuto a tutti gli obblighi di legge nell'attivazione della PEC (Posta Elettronica Certificata) dei loro iscritti.

Tale strumento, spiega una nota, e' volto a semplificare i rapporti fra i professionisti e la Pubblica Amministrazione, oltre a ridurre tempi e costi delle comunicazioni, a garantire la certezza del mittente, l'integrita' e la riservatezza dei messaggi (alla stregua di una raccomandata con ricevuta di ritorno).

Il comma 7 dell'articolo 16 del decreto legge n. 185/2008 stabilisce che i professionisti iscritti in Albi o Elenchi istituiti con legge comunichino il proprio indirizzo di PEC ai rispettivi Ordini o Collegi, che li raccolgono in un "elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni". Tale norma prescriveva che gli elenchi fossero predisposti entro la fine dello scorso anno. Rilevata da un primo monitoraggio la diffusa inadempienza di tale disposizione, il ministro Brunetta ha quindi disposto la verifica dell'Ispettorato di Palazzo Vidoni.

Le Associazioni professionali coinvolte negli accertamenti sono in tutto 25: entro il 30 marzo dovranno comunicare il nominativo del responsabile del procedimento (incaricato dell'attuazione delle disposizioni di legge), che deve verificare il numero dei professionisti iscritti che non hanno ancora provveduto a segnalare il proprio indirizzo di PEC e individuare le opportune sanzioni nei loro confronti.

res-rus/sam/bra

notizie correlate

articoli

- P.A. LOCALE: ANCI, RIUNITA COMMISSIONE VALUTAZIONE
- EPIFANI, CERTIFICATI MEDICI VIA WEB? BENE MA RIFORMA E' ALTRO
- BRUNETTA AVVIA MONITORAGGIO ATTUAZIONE PEC
- A FEBBRAIO STABILI ASSENZE PER MALATTIA DIPENDENTI
- BRUNETTA, PEC SEMPLIFICA RAPPORTI CON CITTADINI E IMPRESE
- GARANTE PRIVACY, OK A CARTA NAZIONALE SERVIZI E TUTELE CITTADINI
- BRUNETTA, CON CERTIFICATO MEDICO ONLINE 200MLN PEZZI CARTA IN MENO
- A FEBBRAIO STABILI ASSENZE PER MALATTIA DIPENDENTI (2)
- A FEBBRAIO STABILI ASSENZE PER MALATTIA DIPENDENTI
- BRUNETTA, AL VIA CONTROLLI SU ORDINI PROFESSIONALI PER 'PEC'
- GARANTE PRIVACY, OK A CARTA NAZIONALE SERVIZI E TUTELE... (2)
- GARANTE PRIVACY, OK A CARTA NAZIONALE SERVIZI E TUTELE CITTADINI

fonte: www.asca.it

SOGGETTI OBBLIGATI ALLA PEC

COMUNICAZIONI TRA I SOGGETTI OBBLIGATI ALLA PEC

“ Salvo quanto stabilito dall'articolo 47, commi 1 e 2, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, le comunicazioni tra i soggetti di cui ai commi 6, 7 e 8 del presente articolo, che abbiano provveduto agli adempimenti ivi previsti, possono essere inviate attraverso la posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo”

(art. 16, comma 9, Legge n. 2/2009)

LA PEC PER I CITTADINI

“ Per favorire la realizzazione degli obiettivi di massima diffusione delle tecnologie telematiche nelle comunicazioni, previsti dal codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai cittadini che ne fanno richiesta e' attribuita una casella di posta elettronica certificata o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell’invio e della ricezione delle comunicazioni e l’integrità del contenuto delle stesse, garantendo l’interoperabilità con analoghi sistemi internazionali. L'utilizzo della posta elettronica certificata avviene ai sensi degli articoli 6 e 48 del citato codice di cui al decreto legislativo n. 82 del 2005, con effetto equivalente, ove necessario, alla notificazione per mezzo della posta. Le comunicazioni che transitano per la predetta casella di posta elettronica certificata sono senza oneri.”

(art. 16,-bis comma 5, Legge n. 2/2009)

Formez PA

...UN FUTURO PROSSIMO?

NEWS
14/3/2011

Pec per ogni neonato, proposto ddl

L'iniziativa del Pd prevede un budget annuo di 7 milioni di euro

ROMA

A tutto Internet, fin dalla nascita. La casella di posta elettronica certificata non può aspettare: deve essere assegnata fin dalla nascita. Lo prevede un disegno di legge presentato dalla senatrice del Pd Maria Leddi a palazzo Madama. «La crescita della nostra competitività e il miglioramento della qualità della vita e dei servizi -spiega- sono legati alla diffusione delle tecnologie digitali».

E alla diffusione di massa delle tecnologie dell'informazione, aggiunge l'esponente dell'opposizione, «è legata la possibilità di garantire in modo generalizzato ai cittadini l'accesso alla rete e a quell'enorme miniera di informazioni e di conoscenze che il Web offre. La condizione pregiudiziale perchè il processo parta è che si diffonda tra i cittadini l'accesso a Internet, l'alfabetizzazione informatica, l'utilizzo

ULTIMI ARTICOLI | RUBRICHE

Il canale Tecnologia è a cura di **Anna Masera**

marzo 2011
febbraio 2011
gennaio 2011
dicembre 2010
novembre 2010
ottobre 2010
settembre 2010
agosto 2010
luglio 2010
giugno 2010
maggio 2010
aprile 2010

CERCA >> FEED RSS

ISTANZE E DICHIARAZIONI PER VIA TELEMATICA

ISTANZE E DICHIARAZIONI PER VIA TELEMATICA

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica 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, 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;

(art. 65, D. Lgs. n. 82/2005)

ISTANZE E DICHIARAZIONI PER VIA TELEMATICA

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.

ISTANZE E DICHIARAZIONI PER VIA TELEMATICA

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 e' richiesta la sottoscrizione mediante firma digitale.

2. Le istanze e le dichiarazioni inviate o compilate su 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.

ISTANZE E DICHIARAZIONI PER VIA TELEMATICA

2. Le istanze e le dichiarazioni inviate per via telematica, ivi 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. La copia dell'istanza sottoscritta dall'interessato e la copia 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.

3-bis. Il potere di rappresentanza per la formazione e la presentazione di istanze, progetti, dichiarazioni e altre attestazioni nonche' per il ritiro di atti e documenti presso le pubbliche amministrazioni e i gestori o esercenti di pubblici servizi puo' essere validamente-conferito ad altro soggetto con le modalita' di cui al presente articolo

(art. 38, D.P.R. n. 445/2000)

SANZIONI & RESPONSABILITA’

MANCATA PUBBLICAZIONE INDIRIZZO PEC

☐ Azione ex art. 3, comma 1-ter, D. Lgs. n. 82/2005

☐ Class Action ex D. Lgs. n. 198/2009

☐ Omissione d'atti d'ufficio ex art. 328 C.P.

☐ Mancato raggiungimento performance e responsabilità disciplinare

D.Lgs. n. 198/2009:

***class action* amministrativa**

diffida a provvedere entro 90 gg.

diversamente G.E. del T.A.R.

pubblicazione online del ricorso e delle azioni di ottemperanza alla sentenza

venerdì 6 agosto 2010

di *Claudio Tamburrino*

A+ A-

Commenti (11)

PEC, class action radicale

Il Ministero dell'Economia. Il Comune di Roma, la Regione Basilicata e la Campania. Tutti non si sono adeguati alla normativa: impedendo ai cittadini di comunicare per via telematica. Agorà Digitale avvia la procedura legale

Roma – I Radicali hanno avviato la procedura per la **prima Class Action italiana per i diritti digitali dei cittadini**: a essere chiamati in causa il Ministero dell'Economia e delle Finanze, le Regioni Basilicata e Campania e il Comune di Roma. Al centro della questione l'uso della Posta Elettronica Certificata (PEC), che sarebbe impedito ai cittadini: nonostante la normativa in materia abbia garantito il diritto di utilizzare la PEC nelle comunicazioni con le pubbliche amministrazioni, le inadempienze degli enti coinvolti hanno di fatto impedito la possibilità di goderne.

Questi enti, infatti, **non hanno pubblicato in homepage l'indirizzo di PEC cui avrebbero**

LEGGI ANCHE ULTIME NOTIZIE

DIRITTO & INTERNET
Copyright, la condanna di Yahoo!

ATTUALITÀ
Gioventù ribelle, dubbi sul videogame per i 150 anni

AMMINISTRATIVO 28 SETTEMBRE 2011, 20:08

Il diritto all'uso delle nuove tecnologie entra in vigore… grazie alla class action amministrativa

Dalla Basilicata un segnale forte a tutta l'amministrazione italiana

```
Codice dell'Amministrazione Digitale

Art. 3
Diritto all'uso delle tecnologie

1. I cittadini e le imprese hanno diritto a
richiedere ed ottenere
l'uso delle tecnologie telematiche nelle
comunicazioni con le
pubbliche amministrazioni...
```

Il Ministro Stanca ed il suo staff (il capo dell'ufficio legislativo Enrico De Giovanni e tutti gli altri) l'avevano previsto nel lontano 2005 (*l'alba del C.A.D.*): "**il diritto di richiedere e ottenere** l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni".

Quanti altri diritti conoscete che contengano nella loro descrizione *"richiedere"* e, a seguire, a rischio di sembrare un po' tardi… *"ottenere"*?

Condividi questo Articolo

MANCATA PUBBLICAZIONE PEC

La mancata individuazione di almeno un indirizzo istituzionale di posta elettronica certificata sul sito web… nonché la mancata attuazione del diritto degli utenti di comunicare elettronicamente tramite l'utilizzo della stessa determina un disservizio, costringendo gli interessati a recarsi personalmente presso gli uffici e ad utilizzare lo strumento cartaceo per ricevere ed inoltrare comunicazioni e/o documenti.

Va peraltro precisato che il disservizio lamentato estende i suoi riflessi negativi anche sulle modalità di esercizio del diritto del privato di partecipare al procedimento amministrativo poiché l'art. 4, comma 1, del codice dell'amministrazione digitale consente, infatti, di esercitare tali diritti procedimentali anche attraverso strumenti di comunicazione telematici.

(*T.A.R. Basilicata, 23 settembre 2011, n. 478*)

Agenzia Entrate

Direzione Regionale della Toscana

Settore Servizi e Consulenza
Ufficio Gestione Tributi

Firenze, 13 gennaio 2010

Conferenza degli Ordini dei Dottori Commercialisti e degli Esperti Contabili della Toscana

Consulta Regionale dei Consigli Provinciali dei Consulenti del Lavoro della Toscana

Prot. n. 695/10/GT

OGGETTO: Corrispondenza per posta elettronica

Si comunica che, al momento, gli Uffici dell'Agenzia delle Entrate non sono abilitati all'utilizzo della casella di posta elettronica certificata.

Pertanto, si prega di raccomandare ai professionisti che fanno capo alla Conferenza ed alla Consulta in indirizzo di non utilizzare per comunicare con gli Uffici della D.R. Toscana (sia interni, che locali) la casella PEC, ma quella ordinaria di posta elettronica.

Al momento abilitato alla PEC è esclusivamente il Centro Operativo di Venezia.

Ringraziando per la collaborazione, si inviano cordiali saluti.

La presente viene inviata esclusivamente via e-mail.

MANCATA PROTOCOLLAZIONE COMUNICAZIONI PEC

- Profili di illegittimità azione amministrativa
- Responsabilità disciplinare
- Omissione d’atti d’ufficio ex art. 328 C.P.

CORRIERE DELLA SERA

IL MINISTRO PER L' INNOVAZIONE

Stanca: ogni lettera di un ministero costa 20 euro

Sempre più messaggi elettronici e sempre meno carta per la pubblica amministrazione. Con significativi risparmi. L' aumento delle e-mail nei primi dieci mesi del 2003 rispetto allo stesso periodo del 2002 è stato del 94%, a quasi 22 messaggi scambiati. I dati sono stati forniti ieri dal ministro per l' Innovazione e le tecnologie Lucio Stanca. Stanca ha anche anticipato la prossima direttiva per l' ammodernamento della pubblica amministrazione: dalla fine della legislatura, sarà obbligatorio l' uso della posta elettronica, al posto della carta, per tutte le comunicazioni interne. Ciò permetterà non solo un recupero d' efficienza e un incremento della produttività - ha ricordato Stanca - ma anche significativi risparmi: ogni lettera inviata con i sistemi tradizionali comporta infatti per l' amministrazione una spesa stimato in 20 euro, una volta calcolati anche i costi d' archiviazione.

Pagina 23
(23 novembre 2003) - Corriere della Sera

MANCATO USO PEC

- ✓ Responsabilità per danno erariale

MANCATA FORMAZIONE PEC

Sussiste danno erariale nel caso in cui i dirigenti non provvedono a disporre un’adeguata formazione del personale in materia informatica.

(*Corte Conti, Reg. Lazio, 28 febbraio 2006, n. 635*)

< / LA TRASMISSIONE DEL DOCUMENTO INFORMATICO >

< LA CONSERVAZIONE DEL DOCUMENTO INFORMATICO >

I costi e le inefficenze nella gestione del documento cartaceo in Italia

Acquisizione documenti

Stampa/ Produzione documenti

- 115 miliardi di pagine stampate, di cui 19,5 miliardi inutilizzate

Costo: 287 milioni di euro all'anno

Distribuzione documenti

- Ogni documento viene duplicato da 9 a 11 volte

=> costo: 18 euro per documento

Archiviazione documenti

- 1 documento perduto su 20
- 3% dei documenti archiviati erroneamente
- Costo per recuperare un documento non archiviato correttamente: 120 euro

40%:
Percentuale media del tempo di ogni impiegato speso in attività di gestione documentale

Fonte: ***Elaborazioni NetConsulting su fonti ISTAT, 2006***

FACCIAMO CHIAREZZA?

- ✓ Dematerializzazione
- ✓ Smaterializzazione
- ✓ Archiviazione sostitutiva
- ✓ Archiviazione elettronica
- ✓ Archiviazione digitale
- ✓ Conservazione sostitutiva
- ✓ Conservazione digitale
- ✓ Archiviazione ottica
- ✓ Archiviazione ottica sostitutiva
- ✓ Conservazione ottica sostitutiva

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.

DEMATERIALIZZAZIONE

- *"la macchina della dematerializzazione è partita, ma appare ancora frenata: si tratta di convincere le persone, con l'informazione e con la formazione, che una amministrazione << full digital >> è possibile. Ci sono ancora troppi << se >> e troppi << ma >>: si tratta di convincere gli incerti con la forza dei fatti*" (CNIPA, aprile 2006).

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.

FORMAZIONE DI DOCUMENTI INFORMATICI

1. Le pubbliche amministrazioni [che dispongono di idonee risorse tecnologiche] 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. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.]

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

FORMAZIONE DI DOCUMENTI INFORMATICI

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)

PROTOCOLLO INFORMATICO

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, nonche' le istanze e le dichiarazioni di cui all'articolo 65 in conformita' alle regole tecniche di cui all'articolo 71.

(art. 40-BIS, D. Lgs. n. 82/2005)

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.

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

PROCEDIMENTO E FASCICOLO INFORMATICO

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.

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.

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

PROCEDIMENTO E FASCICOLO INFORMATICO

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.

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

DEMATERIALIZZAZIONE DEI DOCUMENTI DELLE PA

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 DELLE PA

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.

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

RIPRODUZIONE E CONSERVAZIONE DEI DOCUMENTI DELLE PA

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 DELLE PA

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 ì 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.

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

REQUISITI PER LA CONSERVAZIONE DEI DOCUMENTI DELLE PA

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 attivita' di rispettiva competenza.
1-ter. Il responsabile della conservazione puo' chiedere la conservazione dei documenti informatici o la certificazione della conformita' del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonche' dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

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

CONSERVAZIONE SOSTITUTIVA

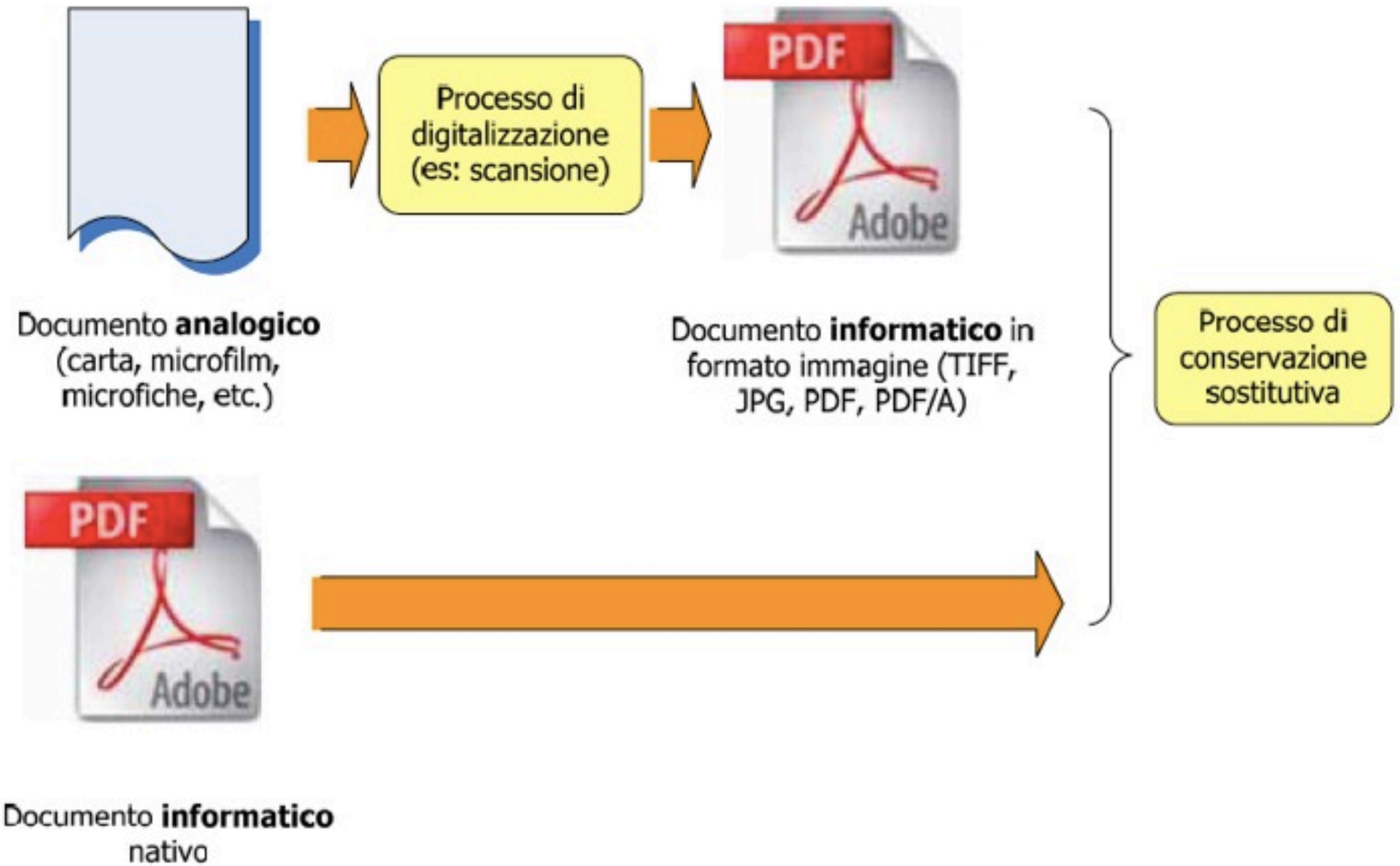
- La conservazione sostitutiva è un processo, definito normativamente, attraverso il quale è possibile garantire nel tempo la validità legale di un documento informatico, sia che si tratti di un documento nativo digitale, sia che si tratti di un documento informatico ottenuto da un documento analogico (ad es.mediante scansione)
- Nel secondo caso, la conservazione sostitutiva equipara, sotto certe condizioni, i documenti cartacei con quelli elettronici e permette alla PA e alle aziende di risparmiare sui costi di stampa, stoccaggio e archiviazione.
- Il risparmio è particolarmente alto per la documentazione che deve essere, a norma di legge, conservata per più anni.
- La conservazione sostitutiva di fatto legalizza il documento informatico ottenuto mediante digitalizzazione, equiparandolo a quello cartaceo.

CONSERVATORI ACCREDITATI

1. I soggetti pubblici e privati che svolgono attivita' 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 piu' elevato, in termini di qualita' 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 societa' di capitali con capitale sociale non inferiore a euro 200.000.

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

IL PROCESSO DI CONSERVAZIONE SOSTITUTIVA



COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA

Processo di conservazione dei documenti informatici nativi

- Secondo la Delibera del Cnipa n. 11 del 19 febbraio 2004 la conservazione sostitutiva di documenti informatici avviene attraverso la loro memorizzazione (o “archiviazione”), ed eventualmente anche della loro impronta, su supporti ottici o su altri supporti idonei e si completa con l’apposizione del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.

COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA

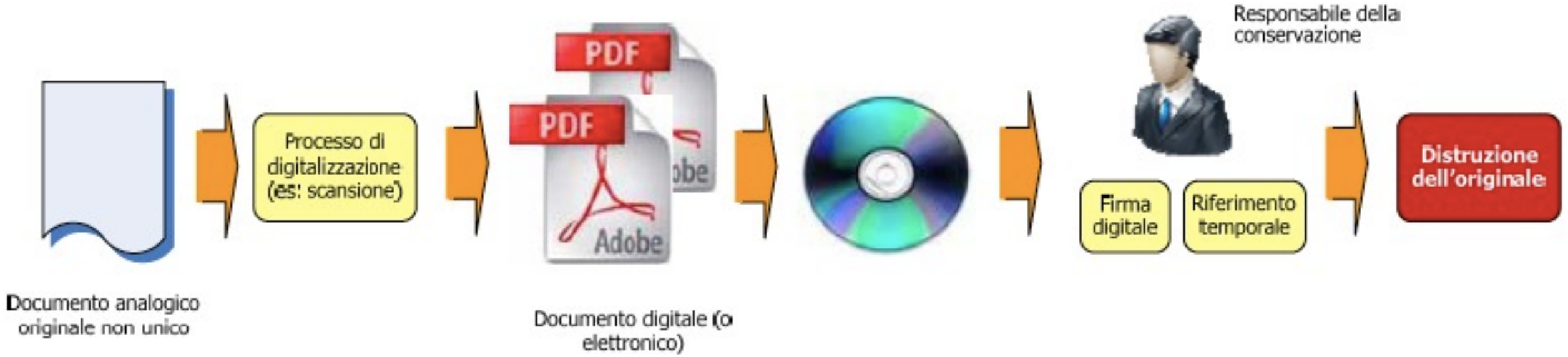
COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA

Processo di conservazione dei documenti analogici

- Secondo la Delibera CNIPA n. 11 del 19 febbraio 2004, la conservazione sostitutiva di documenti analogici avviene mediante memorizzazione delle relative immagini direttamente su supporti ottici (o altri supporti idonei) e termina con l'apposizione, sull'insieme dei documenti, o su un'evidenza informatica contenente una o più impronte dei documenti, o di un insieme di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta così lo svolgimento corretto del processo.

Formez PA

COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA



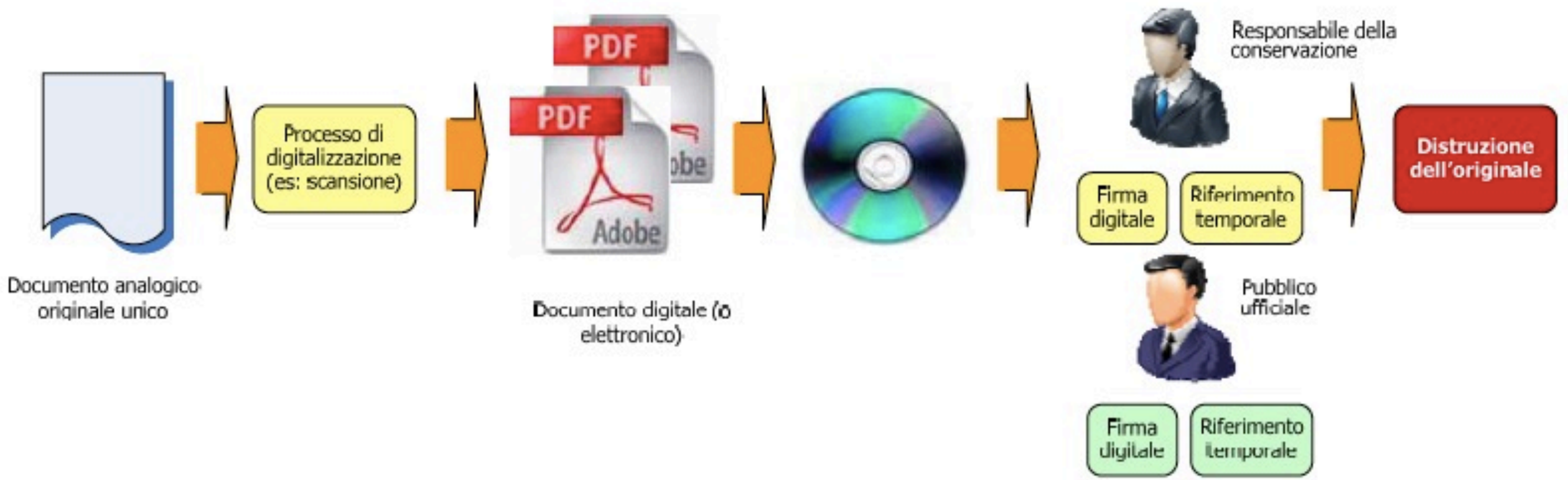
COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA

Processo di conservazione dei documenti analogici

- Per i documenti analogici considerati “originali unici" il processo prevede anche l’apposizione ulteriore del riferimento temporale e della firma digitale da parte di un pubblico ufficiale che attesti la conformità tra documento originale e quanto registrato.
- Nelle pubbliche amministrazioni il ruolo del pubblico ufficiale è svolto dal dirigente dell’ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati

Formez PA

COME AVVIENE LA CONSERVAZIONE SOSTITUTIVA



LA DISTRUZIONE DEI DOCUMENTI ANALOGICI

- La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo quanto previsto dal comma 4 dell'art. 43 del D.Lgs. 82/2005,
- ovvero: "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"
- …. il valore storico-culturale?

IL RESPONSABILE DELLA CONSERVAZIONE

L'art. 5 della Deliberazione CNIPA 11/2004 introduce la figura del Responsabile della conservazione, denominato anche Responsabile del procedimento di conservazione sostitutiva, e gli vengono assegnati i compiti di:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza;
- organizzare il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni: la descrizione del contenuto dell'insieme dei documenti, l'identificazione del Responsabile della conservazione, gli estremi identificativi delle persone eventualmente delegate dal Responsabile della conservazione con l'indicazione dei compiti alle stesse assegnati, l'indicazione delle copie di sicurezza;

COMPITI DEL RESPONSABILE DELLA CONSERVAZIONE

- mantenere e rendere accessibile un archivio del software in gestione nelle eventuali diverse versioni;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
- verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

COMPITI DEL RESPONSABILE DELLA CONSERVAZIONE

In particolare, l'attività del responsabile della conservazione risulta determinante in diverse fasi del processo di conservazione:

- nella fase di acquisizione in formato immagine (scansione) dei documenti analogici, in assenza di ulteriori specificazioni normative, sarà sua la scelta di un formato tale da consentire l'effettiva leggibilità dei documenti conservati sui supporti, da verificare periodicamente, con cadenza non superiore ai cinque anni (art.5, comma 1, lett.h Delibera CNIPA n.11/2004)
- nella fase di apposizione di firma digitale e marca temporale, dovrà scegliere se operare sull'insieme dei documenti, sull'unica impronta di essi oppure su più impronte che rappresentano i singoli documenti o insiemi di essi (art.3, comma 2 DM 23 gennaio 2004)
- nel caso in cui sia previsto l'intervento di un pubblico ufficiale, spetta al responsabile della conservazione richiederne la presenza ed assicurare allo stesso assistenza e risorse per l'espletamento delle attività a lui attribuite (art. 5 comma 1 lett.f Delibera CNIPA n.11/2004)
- se appositamente designato, spetta al responsabile della conservazione l'invio dell'impronta dell'archivio oggetto di conservazione alle competenti agenzie fiscali, ai sensi dell'art. 5 comma 1 DM 23 gennaio 2004.

LA DELEGA

Il Responsabile della conservazione può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone di specifica competenza ed esperienza

Allo stesso modo, il processo di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati.

LA FORMAZIONE

È logico ritenere che la responsabilità della conservazione debba essere affidata ad una figura professionale dotata di idonee conoscenze in materia di:

- **archivistica**, perché si tratta di garantire la formazione, conservazione e fruizione di archivi digitali;
- **informatica**, per fare le giuste scelte relativamente ai supporti di memorizzazione, ai formati elettronici, al sistema di conservazione digitale;
- **diritto e diplomatica del documento contemporaneo**, per avere la capacità di valutare l'autenticità, gli elementi intrinseci ed estrinseci, l'accessibilità, l'intelligibilità e la riproducibilità dei documenti informatici;
- **organizzazione**, in quanto la produzione dei documenti informatici comporta necessariamente la rimodulazione degli assetti organizzativi e il re-engineering dei processi operativi.

</LA CONSERVAZIONE DEL DOCUMENTO INFORMATICO>

< LA SICUREZZA INFORMATICA>

PRIVACY

- **LA TUTELA DEI DATI PERSONALI ED IL TESTO UNICO n. 196/2003**

- LA SICUREZZA DEI DATI: MISURE MINIME, MISURE IDONEE E SANZIONI

- SISTEMI INFORMATIVI E TRATTAMENTO DATI PERSONALI

PRIVACY

Diritto di essere lasciati tranquilli

Tutela della riservatezza

PRIVACY

- Diritto ad essere lasciato solo (1890 Warren e Brandeis)

↓

- Diritto a chiedere di se stesso
- Diritto di scegliere quel che si è disposti a rivelare agli altri
- Diritto di controllare l'uso delle informazioni che ci riguardano

PRIVACY

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla *tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*

in ITA legge 31 dicembre 1996, n. 675 (c.d. "legge privacy")

Diritto a:

non fare circolare i propri dati personali;

controllarne l'utilizzazione;

far cessare il trattamento illecito.

PRIVACY

art. 1. primo comma Direttiva 95/46/CE “Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle *persone fisiche* e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali”

art. 1. primo comma legge del 31 dicembre 1996 n. 675 “La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle *persone fisiche*, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle *persone giuridiche* e di ogni altro ente o associazione”

PRIVACY

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al *trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.*

Decreto legislativo 30 giugno 2003, n. 196 -
Codice in materia di protezione dei dati personali

CODICE PRIVACY

Parte generale — Art. 1 – 45 — Tutti i trattamenti

Parte speciale

Ambito giudiziario	art. 46 – 52
Forze di polizia	art. 53 – 57
Difesa e sicurezza dello stato	art. 58
Ambito pubblico	art. 59 – 74
Ambito sanitario	art. 75 – 96
Scopi storici, statistici, scientifici	art. 97 – 110
Lavoro e Previdenza Sociale	**art. 111 – 116**
Bancario, finanziario e assicurativo	art. 117 – 120
Comunicazioni elettroniche	**art. 121 – 133**
Videosorveglianza	**art. 134**
Giornalismo	art. 136–139

AMBITO DI APPLICAZIONE

- **QUALI MISURE ?**
- **CHI E' TENUTO AD ADOTTARLE ?**

Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque e' stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.
(art. 5, comma 1, d. lgs. n. 196/2003)

fini esclusivamente personali

Definizioni

A CHI SI APPLICA?

CHIUNQUE E' STABILITO NELLO STATO → anche " dati all'estero"

NON SI APPLICA

PERSONE FISICHE

- Fini esclusivamente personali
- No comunicazione sistematica
- No diffusione

Definizioni

TRATTAMENTO (art. 4 lett. a)

Anche se non sono contenuti in una banca dati

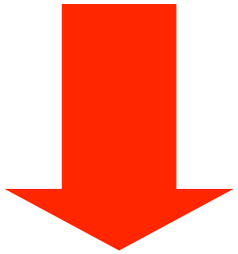
- Raccolta
- Registrazione
- Organizzazione
- Conservazione
- Consultazione
- Elaborazione
- Modificazione
- Selezione
- Estrazione
- Raffronto
- Utilizzo
- Interconnessione
- Blocco
- **Comunicazione**
- **Diffusione**
- Cancellazione
- Distruzione

COMUNICAZIONE → A persone determinate

DIFFUSIONE → A persone indeterminate

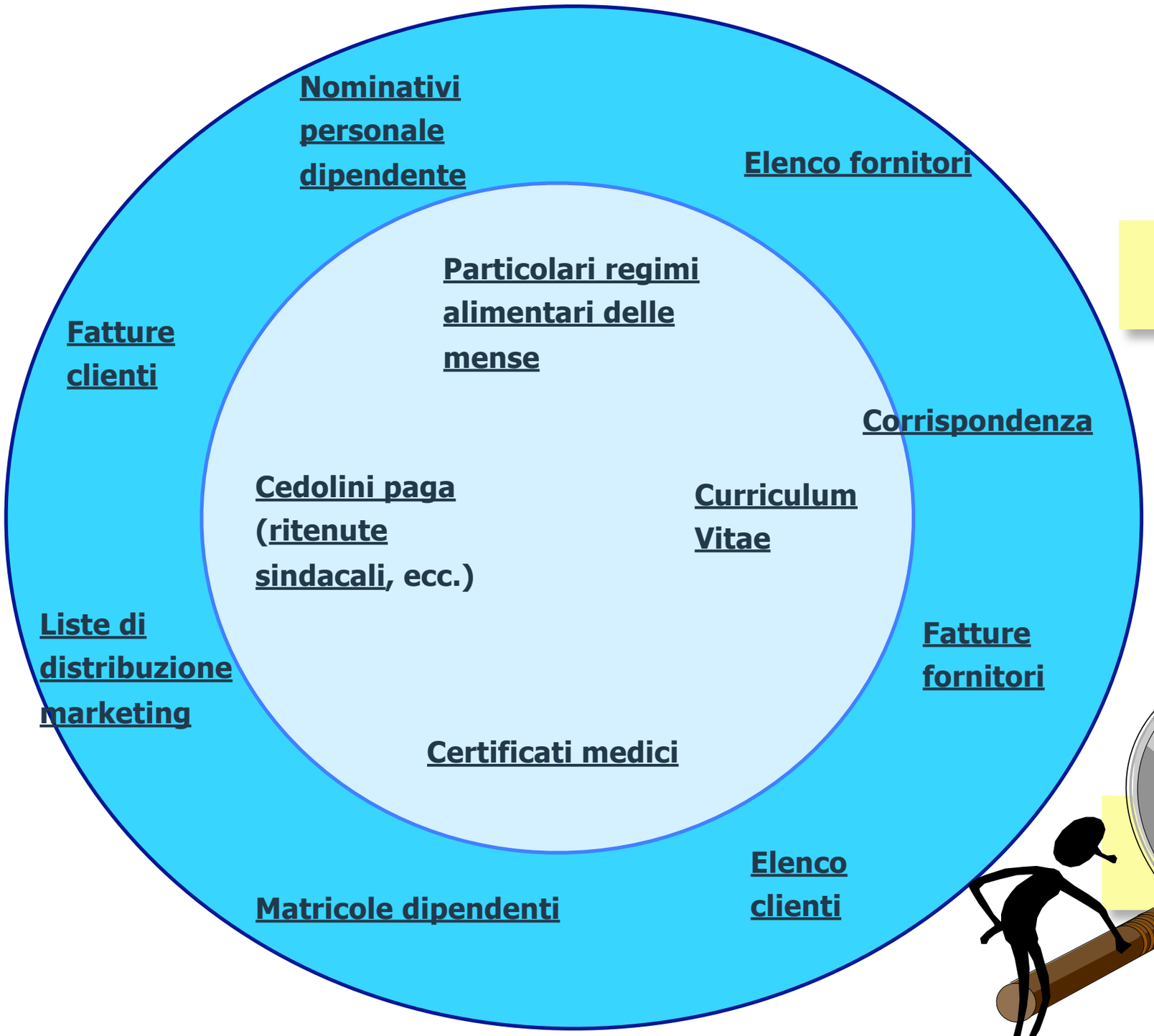
DEFINIZIONI

- **Dato personale**: qualunque informazione relativa a persona fisica, giuridica, ente o associazione identificate o identificabili

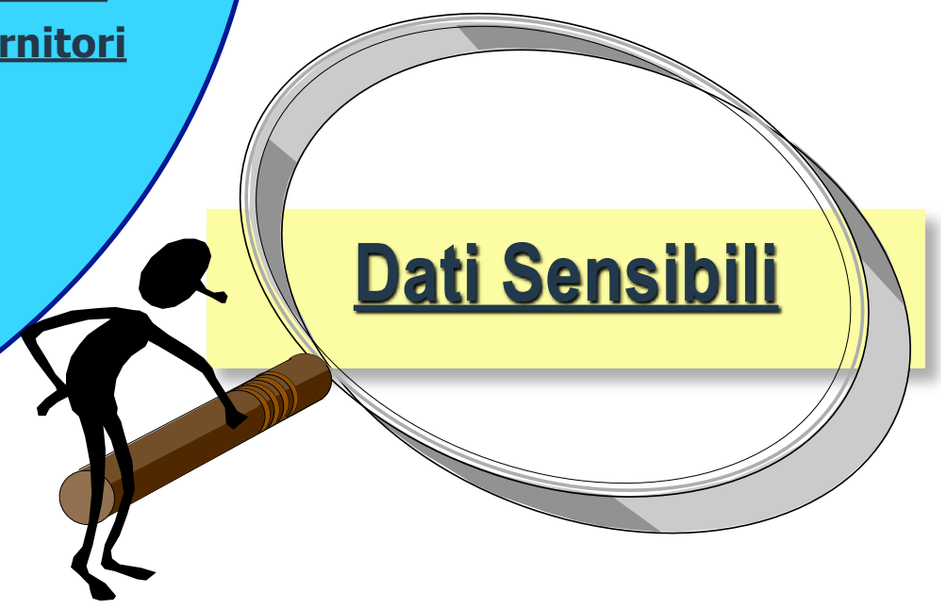


- Codice fiscale
- Recapiti
- Lavoro
- Attività economiche
- Istruzione

QUADRO RIEPILOGATIVO



Dati Personali



ENTI PUBBLICI

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

ADEMPIMENTI BASE

- *DESIGNAZIONI*
- *INFORMATIVA*
- **CONSENSO**
- *NOTIFICAZIONE*
- *MISURE DI SICUREZZA*

ORGANIZZAZIONE DELLA PRIVACY

IL TITOLARE DEL TRATTAMENTO DEVE INDIVIDUARE FORMALMENTE, CON ATTO SCRITTO, I SOGGETTI CHE HANNO TITOLO A TRATTARE I DATI

LE DESIGNAZIONI

- *responsabili del trattamento (interni ed esterni):* questa figura, la cui designazione è facoltativa, ricorre frequentemente in presenza di articolazioni interne delle realtà produttive ovvero in presenza di servizi in outsourcing (es. gestione buste paga)
- *incaricati:* questa figura, la cui designazione è obbligatoria, individua le persone fisiche che - materialmente - compiono operazioni di trattamento dati all'interno dell'azienda

LA SICUREZZA INFORMATICA

"Complesso di tutte le operazioni e accorgimenti adottati al fine di rendere vani i tentativi di attacchi (passivi ed attivi) che possono essere perpetrati ai danni di un sistema informatico ".

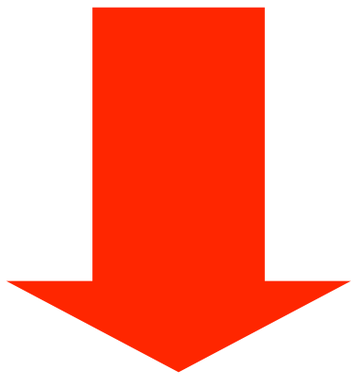
LA SICUREZZA INFORMATICA

SICUREZZA DEI DATI E DELLE INFORMAZIONI

Confidenzialità

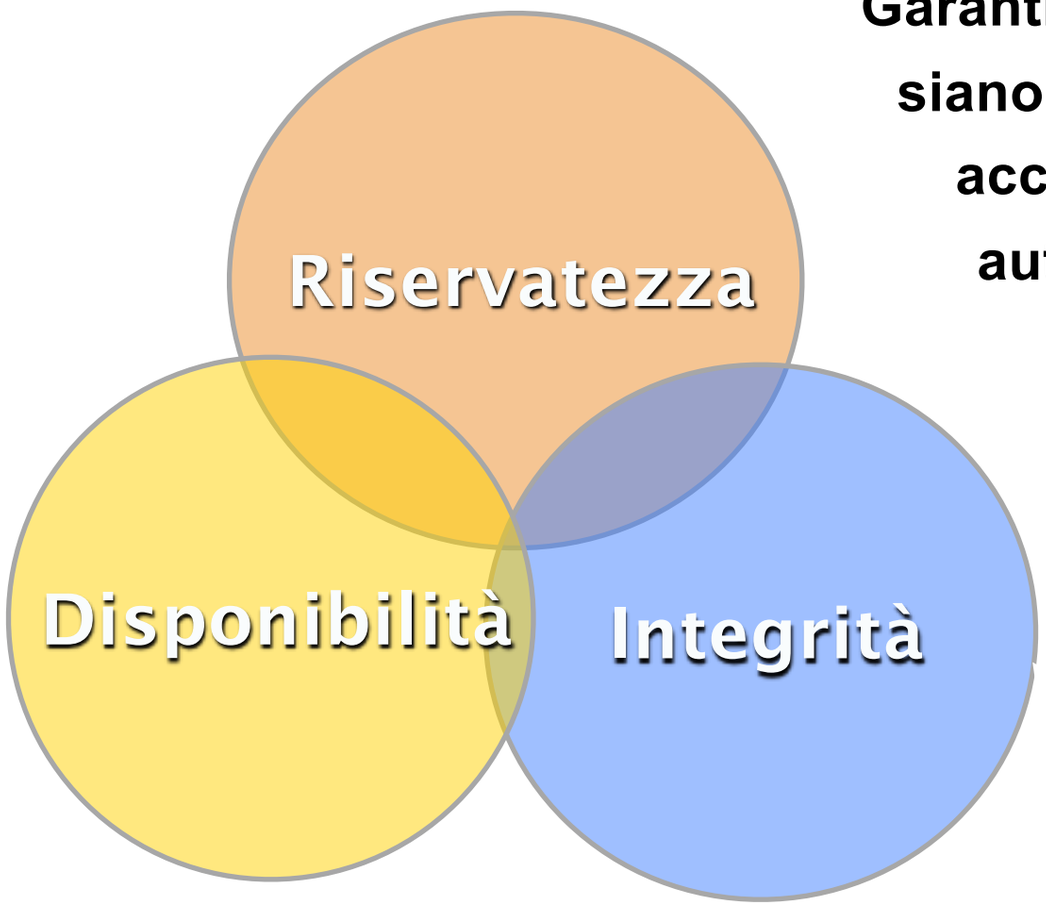
Integrità

Disponibilità



- ☐ Legge di Ranum (il software non basta)
- ☐ La sicurezza informatica totale non esiste

SICUREZZA DEI DATI E DEI SISTEMI



Garantire che i dati siano protetti da accessi non autorizzati

Garantire che i dati siano disponibili agli utenti autorizzati

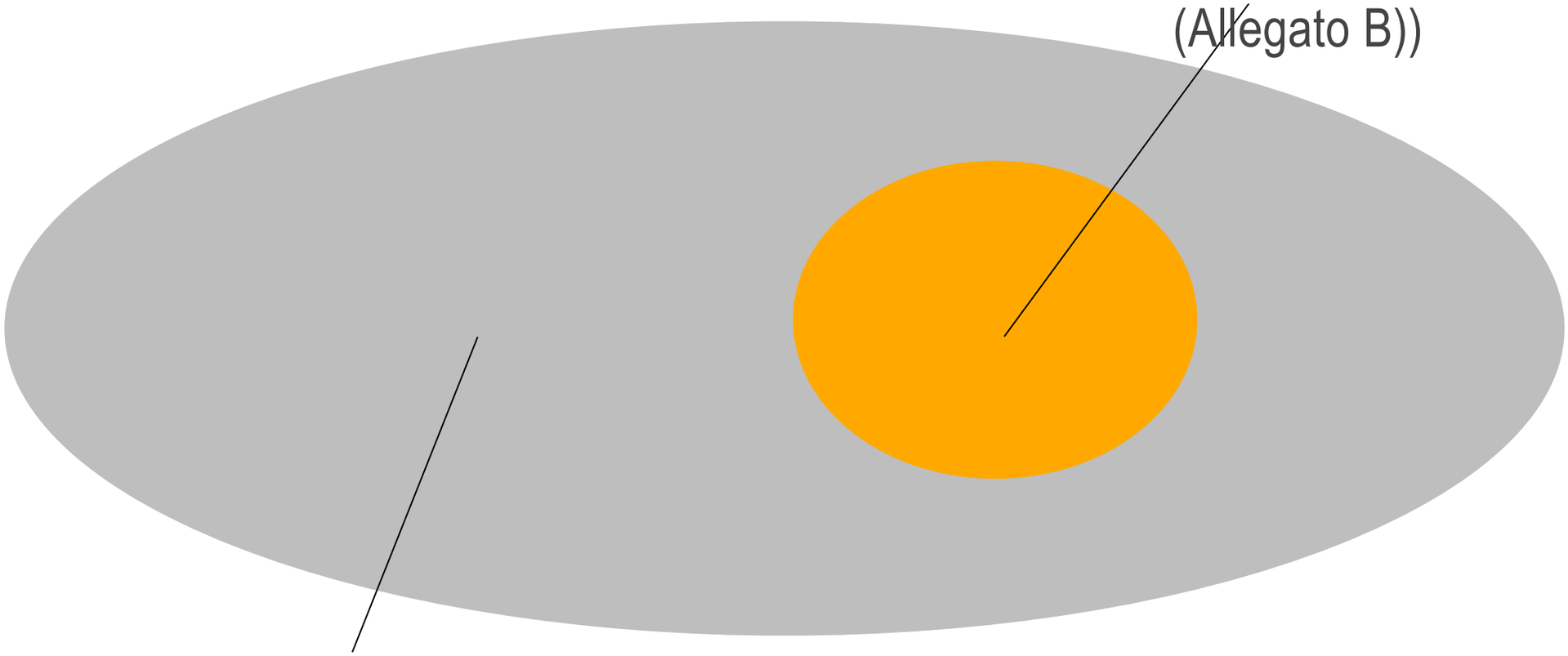
Garantire che i dati siano aggiornati ed integri

MISURE DI SICUREZZA

il D. Lgs. n. 196/2003 prevede due distinti tipi di misure di sicurezza

- ***misure minime (All. B)***: il mancato rispetto costituisce reato
- ***misure idonee (art. 31)***: la mancata adozione di esse espone al risarcimento dei danni

SICUREZZA DEI DATI E DEI SISTEMI



IDONEE

(art. 31, 1)

OBBLIGHI DI SICUREZZA

Art. 31 D. Lgs. n. 196/2003

In relazione a:

- conoscenze acquisite dal progresso tecnico
- natura dei dati
- specifiche caratteristiche del trattamento

IDONEE E PREVENTIVE MISURE DI SICUREZZA

riducono al minimo

rischi di:

- distruzione/perdita di dati
- accesso non autorizzato
- trattamento non consentito/non conforme

MISURE MINIME DI SICUREZA

Art. 33 D. Lgs. n. 196/2003

Obblighi di sicurezza (art. 31)

↓

MISURE MINIME

↓

Livello minimo di protezione dei dati

ALLEGATO B

1-26 Trattamenti **con** strumenti elettronici

27-29 Trattamenti **senza** strumenti elettronici

Strumenti elettronici **>** elaboratore

MISURE MINIME

Trattamento con strumenti elettronici

Autenticazione (1-11) - parola chiave

- rilevazione biometrica

Autorizzazione (12-14)

Altre misure (15-18) - antivirus

- patch, upgrade

- back up

Documento programmatico sulla sicurezza (19)

Dati sensibili o giudiziari (20-24)

Misure di tutela e garanzia (25-26)

STRUMENTI ELETTRONICI

Riguardo agli ELABORATORI

- credenziali di **autenticazione informatica** (user-id e password)
- sistema di **autorizzazione** (singole operazioni)
- misure di **protezione** e **ripristino** dati (antivirus; firewall; back-up)

AUTENTICAZIONE INFORMATICA

La ***password*** (o altro dispositivo di autenticazione che può essere anche una caratteristica biometrica) deve essere conosciuta esclusivamente dall'incaricato, restare in suo esclusivo possesso ed essere modificata almeno ogni 6 mesi, o ogni 3 mesi se i dati trattati sono sensibili o giudiziari.

Anche il codice di identificazione è unico e una volta assegnato ad un incaricato non può essere assegnato ad altri.

Codice di identificazione e password sono disattivate se non sono utilizzate da almeno 6 mesi o in caso di perdita della qualità che consente all'incaricato di accedere ai dati.

Agli incaricati vengono impartite indicazioni sul trattamento ed è prescritto di adottare le cautele necessarie per assicurare la segretezza della password e dei dispositivi di accesso, nonché di non lasciare incustodito ed accessibile a terzi lo strumento elettronico durante il trattamento.

PAROLA CHIAVE

Fattori di sicurezza

lunghezza (8 caratteri)

composizione, scelta e digitazione (non ha riferimenti all’incaricato)

distribuzione e modifica (modificata al 1° utilizzo)

vita utile (6 mesi/3 mesi)

titolarità (individuale)

FIREWALL

Dispositivo che inserisce una barriera che blocca ogni accesso non autorizzato tra la propria Azienda e la rete Internet (hacker, virus, spyware, ecc.).

AGGIORNAMENTO

- **Annuale** per dati comuni
- **Semestrale** per dati sensibili

BACK UP

PREVENZIONE

DISTRUZIONE O PERDITA DATI

Back - up automatizzati
giornalieri o massimo settimanali

RECUPERO

IN CASO DI DANNEGGIAMENTO

ANTIVIRUS

I dati personali devono essere protetti **contro il rischio di intrusione e dall'azione dei programmi di cui all'art. 615-quinquies** c.p. mediante l'attivazione di idonei strumenti elettronici da aggiornare almeno ogni 6 mesi.

Controllo mediante computer non collegato alla rete dei floppy-disk provenienti dall'esterno.

Interazione solo con sistemi dotati di programmi antivirus

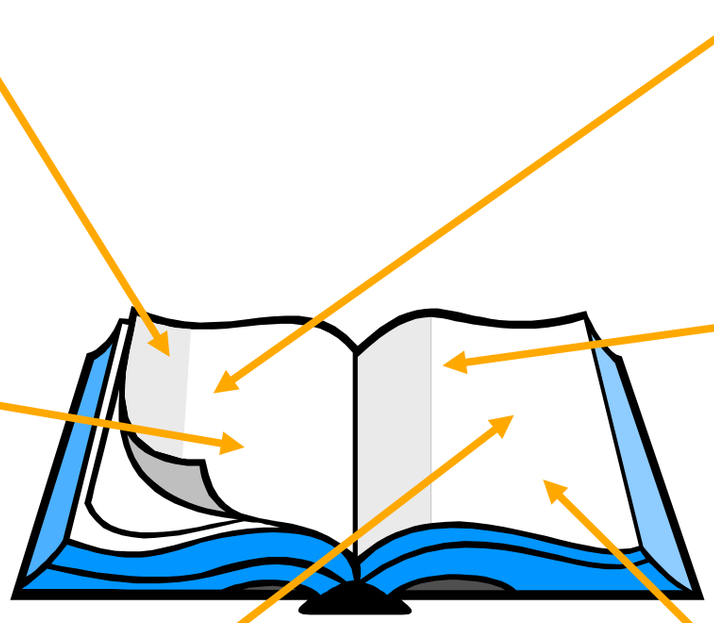
DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Analisi dei rischi

Compiti e responsabilità

Criteri e procedure per l'integrità dei dati

Criteri tecnici ed organizzativi per la protezione dei locali



Criteri e procedure per la sicurezza delle trasmissioni

Piano di formazione per gli incaricati

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Entro il 31 marzo di ogni anno:

elenco dei trattamenti

distribuzione dei compiti

analisi dei rischi

misure da adottare

ripristino dei dati

interventi formativi

SANZIONI PENALI

Art. 169 (Misure di sicurezza) 1° comma

Mancata adozione delle misure MINIME (art.33)

arresto fino a 2 anni o

ammenda da 10 a 50 mila euro

SANZIONI PENALI

Art. 169 (Misure di sicurezza) 2° comma

Termine per regolarizzarsi (> 6 mesi)

adempimento e

pagamento di 12.500 euro

estinzione del reato

SANZIONI CIVILI

Risarcimento del danno

Mancata adozione delle misure IDONEE (art.31)

Art.15: il danno è risarcito ai sensi dell'art. 2050 c.c.

(se non prova di aver adottato tutte

le misure idonee a evitarlo)

+

danno non patrimoniale


Chelmsford (A 414)
Chipping Ongar A 128
Brentwood
Kelvedon Hatch A 128
Industrial Estates
Secret Nuclear Bunker

SISTEMI INFORMATIVI PUBBLICI

Adeguamento tecnologico ed organizzativo

- Piena attuazione normativa protocollo informatico e gestione automatizzata dei procedimenti (*Dpr n. 445/2000*; *Dpcm 31 ottobre 2000*)
- Sicurezza dei dati e dei sistemi (*art. 51*)

> *"1. Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71, garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.*
>
> *2. I documenti informatici delle Pubbliche Amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta."*

E’ IMPORTANTE

Art. 20 CAD

1-bis. L'idoneita' 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 qualita', sicurezza, integrita' ed immodificabilita', fermo restando quanto disposto dall'articolo 21

Art. 21 CAD

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 immodificabilita

SISTEMI INFORMATIVI PUBBLICI

La diffusione delle tecnologie informatiche nelle PA e la tenuta di archivi informatizzati rende necessario:

- Individuare procedure per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture

- Garantire la continuità del servizio anche quando erogato mediante tecnologie ICT (art. 50 bis)

- Individuare le procedure da mettere in atto in situazioni di emergenza, che devono riguardare le risorse umane, le risorse strumentali, le strutture e le infrastrutture

DEFINIZIONE DI CONTINUITÀ OPERATIVA E DI DISASTER RECOVERY

Dalle "Linee guida per la continuità operativa della Pubblica Amministrazione" (Quaderno n. 28 DigitPA):

- *Continuità operativa: insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.*

- *Disaster Recovery: insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.*

NORME IN MATERIA DI CONTINUITÀ OPERATIVA

- Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)

- Decreto legislativo 30 dicembre 2010, n. 235 (Gazz. Uff. 10 gennaio 2011, n. 6):

  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.

NORMATIVA PRIVACY

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

(Art. 31, D. Lgs. n. 196/2003)

NUOVO CAD

1.In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono :

il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.".

DEFINIZIONE

Disastro: Una calamità improvvisa e non pianificata che causa gravi danni o perdite.

QUALCHE ESEMPIO...

- Calamità naturali (es. terremoti)
- Problemi nell'alimentazione elettrica
- Guasti della rete
- Eventi fortuiti (es. incendi)
- Inagibilità dei locali
- Malfunzionamenti del sistema informatico
- ... combinazione di due o più degli eventi sopra descritti.

CONTENUTI DEL PIANO

- ☑ Scopo e campo di applicazione, dove si identificano gli elementi fisici (quali le sedi, le aree all'interno delle sedi, il data center, ecc.) e funzionali (le attività di business o i servizi) dell'organizzazione coperti dal piano

- ☑ Obiettivi di continuità degli elementi coperti dal piano

- ☑ Ruoli e responsabilità nella gestione dell'emergenza, con particolare evidenza dei ruoli decisionali di vertice dell'organizzazione;

- ☑ Criteri di attivazione delle procedure di emergenza (le condizioni che determinano la dichiarazione di disastro)

- ☑ Procedure di attuazione in risposta alla condizione di di emergenza (la reperibilità del personale chiave, le modalità di comunicazione ai dipendenti, le modalità di comunicazione agli esterni interessati –nel caso di PA: cittadini, imprese, altre PA-, il piano di disaster recovery);

- ☑ Flusso di informazioni e processi di documentazione

- ☑ Modalità di verifica e di aggiornamento del Piano

Formez PA

</LA SICUREZZA INFORMATICA>

Formez PA

REGOLE TECNICHE E ATTUATIVE

LE NORME CHE PREVEDONO L'ADOZIONE DI REGOLE TECNICHE

- art. 2, comma 6
- art. 5, comma 3,
- art. 5-bis,comma 2
- art. 6, comma 1-bis
- art. 20, comma 3
- art. 22, comma 3-ter
- art. 23-ter
- art. 28, comma 3-bis
- art. 58, comma 2
- art. 60, comma 3
- art. 71

150 ANNI DALL'UNITA' D'ITALIA.

E ASPETTIAMO ANCORA I DECRETI ATTUATIVI.

SANZIONI E RESPONSABILITA’

NON DEVE TRARRE IN INGANNO

L'ASSENZA DI SANZIONI DIRETTE

- *misurazione performance*
- *responsabilità disciplinare*
- *responsabilità amministrativa*
- *responsabilità penale*

To Do List:

- Weekly college
- weekly self portrait
- Scan negative for Royko Print
- Work out
- Clean Yuki's Cage
- Take out garbage

ABBIAMO CAPITO CHE…

- le norme tracciano una *check list*

- è necessaria un'adeguata organizzazione (più che la tecnologia)

- il mancato rispetto delle norme espone l'ente e gli agenti pubblici a sanzioni e responsabilità

- cittadini e imprese possono pretendere la concreta attuazione dei propri diritti digitali

“È assurdo pensare che una locomotiva possa andar più veloce di una carrozza a cavalli”

Wiliam Preece, *1876*

GIVE US SOME FEEDBACK

GRAZIE

SLB

BELISARIO

STUDIO LEGALE

www.ernestobelisario.eu

facebook.com/amministrazionedigitale

edu@ernestobelisario.eu

ernesto.belisario@pec.studiobelisario.it