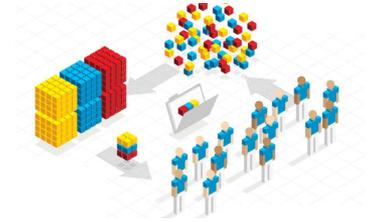
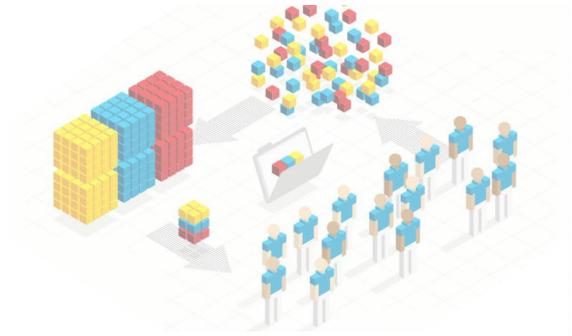


Agenda



- 14.30 **Benvenuto e introduzione**
Federico Bissolotti, IBM ECM Sales
- 14.40 **Scenario sulle normative di archiviazione e conservazione dati.
Sprone o freno per le aziende?**
Andrea Lisi – Presidente ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti)
- 15.00 **Tre esperienze, con angolazioni diverse, a confronto.**
Intervengono:
Giuseppe Alibrandi – Banca Popolare di Milano
Andrea Dubini – Compagnia Generale Trattori
Eugenio Mariotto - Cobra
- 15.45 **IBM Smart Archive: soluzioni leader già integrate.**
Claudio Balestri, IBM Data Management Sales
Sergio Resch – IBM Storage Sales
Giancarlo Sassi – IBM ECM Sales
- 16.30 **Soluzioni dai Business Partner IBM**
Stefano Gandolfi – IBM ECM Channel Manager
- 17.15 **Cos'è archiviato in un bicchiere di vino?**
Degustazione guidata e analisi sensoriale di gruppo





IBM Smart Archive

Selezione Vincente, Archivio Intelligente

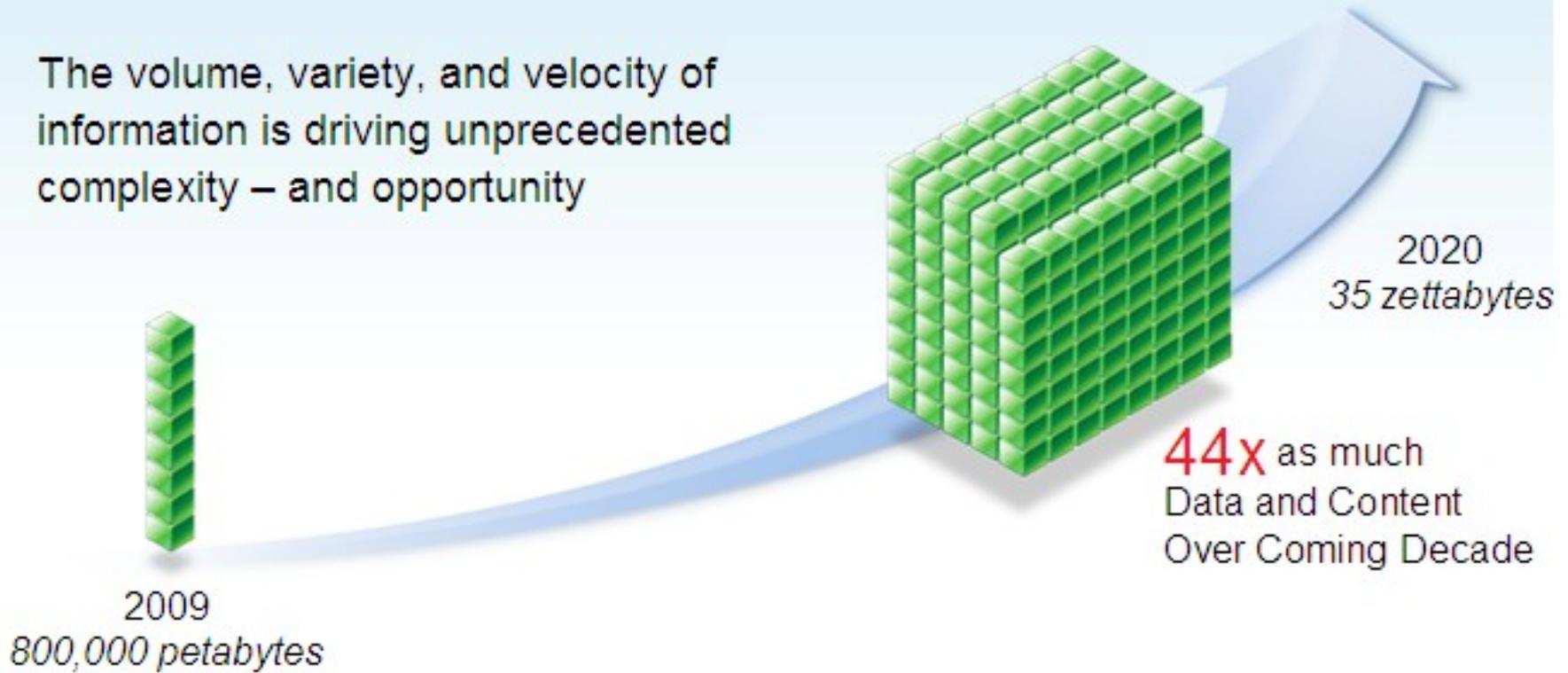
Milano, 19 Gennaio 2011



The Continued Explosion of Information

80% of new information growth is unstructured content – with 90% of that unmanaged

The volume, variety, and velocity of information is driving unprecedented complexity – and opportunity



Source: IDC, The Digital Universe Decade – Are You Ready?, May 2010

The data deluge: businesses, governments and society are only starting to tap its vast potential (from The Economist)

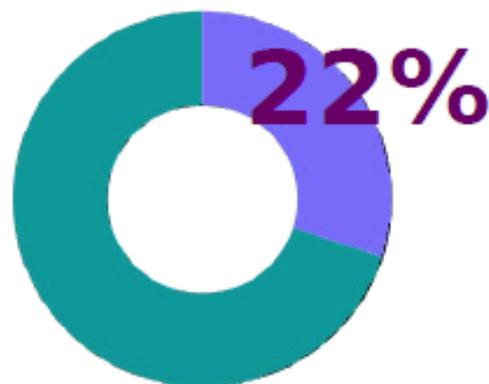


Explosion of Information and Related Legal Obligations Make Legal Information Governance A Pressing Problem

Companies that cite defensible disposal as key result of governance programs

98%

Companies that can defensibly dispose today

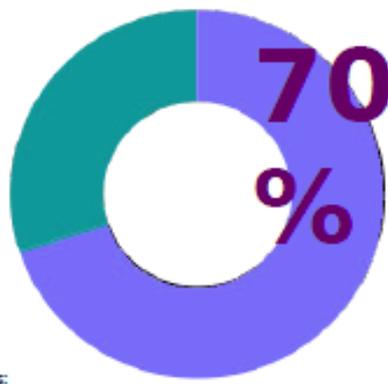


Source: CGOC Benchmark Report on Information Governance

Average cost to collect, cull and review information per legal case¹

\$3M

Portion of information unnecessarily retained²



Sources:

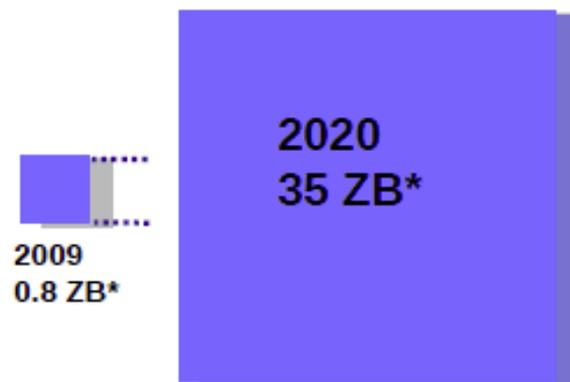
1. *Litigation Cost Survey of Major Companies, 2010* (from Conference on Civil Litigation, Duke Law School, May 2010)
 2. Industry estimates

Amount of IT budgets consumed by storage³

17%

Projected future information growth⁴

44x



* Zettabyte = 1 trillion gigabytes

Sources:

3. *Information Week Survey, December 2009*
 4. *IDC Digital Universe Study, May 2010, sponsored by EMC*

Qualche problema...

Furto documenti in Comune, procura conferma l'indagine

luglio 7th, 2010 • Articoli Correlati • Pubblicato in



WikiLeaks

@wikileaks Everywhere

We open governments.

<http://wikileaks.org>

E' stata confermata dalla Procura di Genova l'apertura di un'indagine sulla sottrazione di documenti riservati dagli uffici del Comune nel palazzo del Matitone a Genova. L'inchiesta, anticipata oggi dal Secolo XIX parte da una denuncia

Il sito di Wikileaks sotto attacco, ma i giornali pubblicheranno ugualmente le notizie tra poche ore.

CORRIERE DELLA SERA*it*

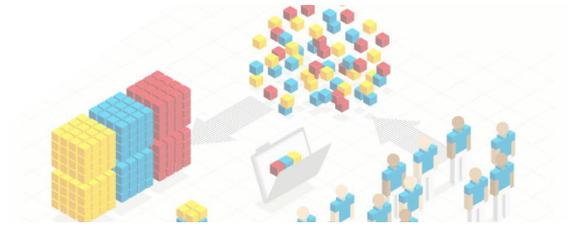
pubblicato: domenica 28 novembre 2010 da natrium  Mi piace  119

Nell'agosto scorso c'è stato un tentativo di forzare la porta e un armadio dell'ufficio del capo dei qip



ROMA - Tennisti, stilisti, banchieri, imprenditori: si concentra su nuovi nomi l'indagine sugli italiani titolari di un conto presso la filiale di Ginevra della banca britannica Hsbc. Persone che avevano occultato parte dei propri beni al fisco e si sono ritrovate nella famigerata «lista Falciani», **l'elenco dei clienti ceduto dal responsabile informatico dell'Istituto di credito Hervé Falciani, 38 anni, alle autorità francesi.** Migliaia e migliaia di correntisti di mezzo mondo tra i quali ci sono, appunto, 6.963 nostri connazionali che hanno trasferito oltre confine oltre sei miliardi e nove milioni di dollari. Su di loro indagano adesso Procure e Guardia di Finanza per ricostruire la movimentazione e verificare quanti abbiano scelto di usufruire dello «scudo» e così evitare conseguenze penali.

La condivisione e il furto di dati sensibili nei social network. La crescita dei servizi e delle piattaforme Web 2.0 impone una riflessione su cosa andrebbe (o non andrebbe) pubblicato nelle community. **Negli Stati Uniti, il 23% delle imprese ha registrato una fuga di informazioni sensibili.**



Le novità normative su archiviazione e conservazione dei dati e documenti: *sprone o freno per le aziende?*

Avv. Andrea Lisi – Presidente ANORC – www.anorc.it

Milano, 19 gennaio 2011



valore di una comunicazione
e-mail?

certificati medici
on line

fattura elettronica

valore della PEC?

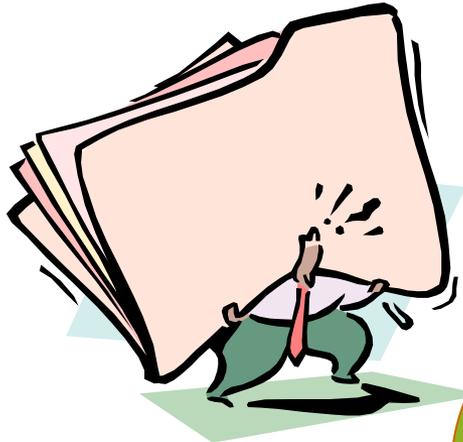
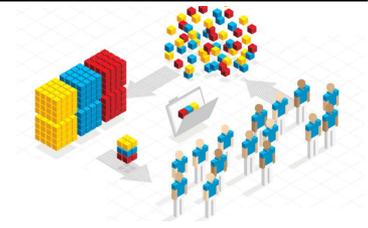
differenze tra firme elettroniche
e firme digitali

pec e cec pac:
di cosa stiamo parlando?

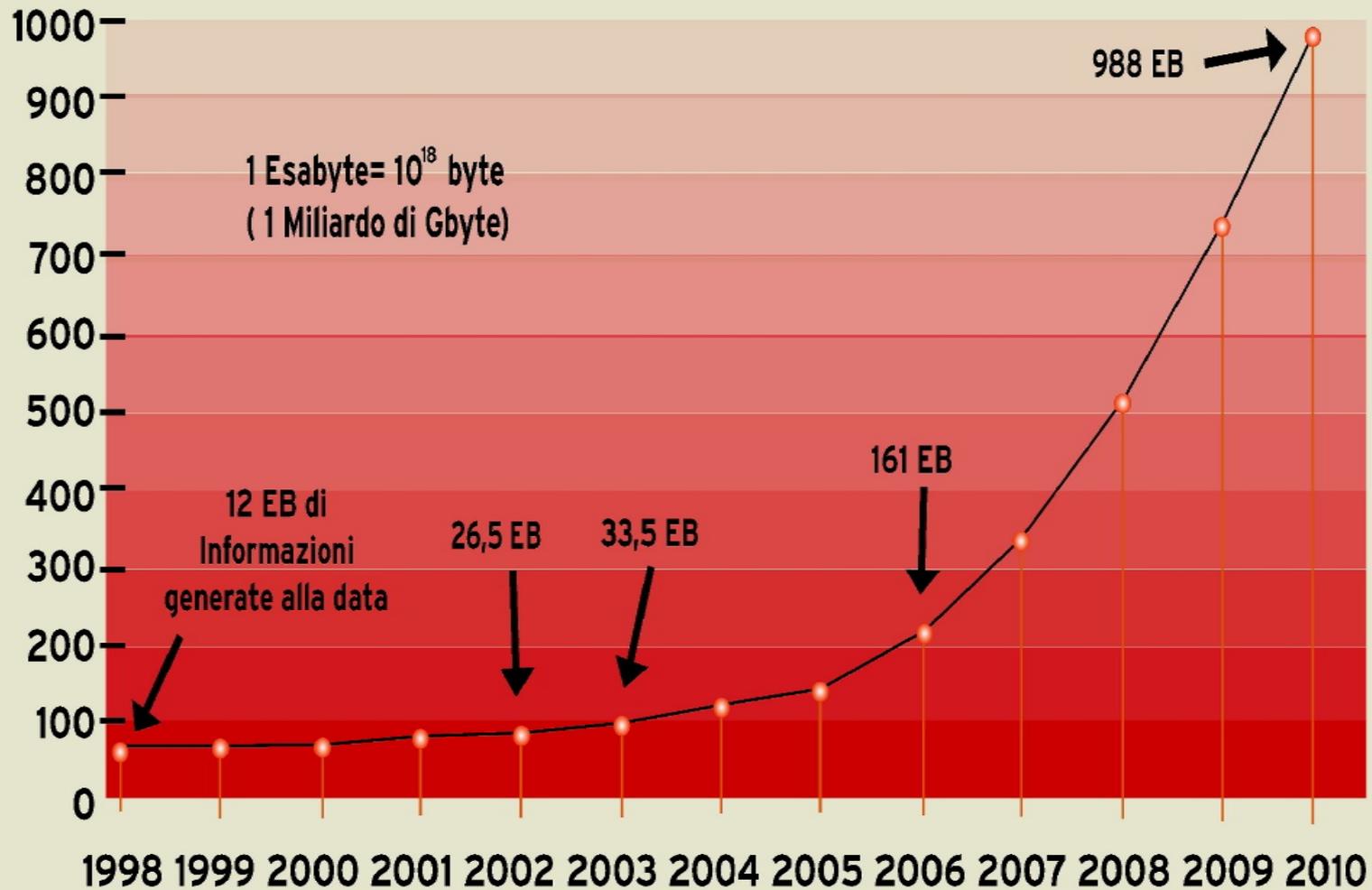
albo pretorio on line

cartella clinica
elettronica

di cosa stiamo parlando?

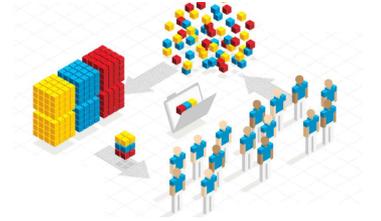


...del passaggio culturale, sociologico, economico e, quindi, giuridico da un documento pesante e statico ad un documento dinamico, che si condivide e che diventa “partecipativo”...



La crescita delle informazioni

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



mentre le informazioni crescono
la nostra memoria evapora?

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

I testi in dvd si rovinano presto

I dati su supporti elettronici scompaiono più facilmente

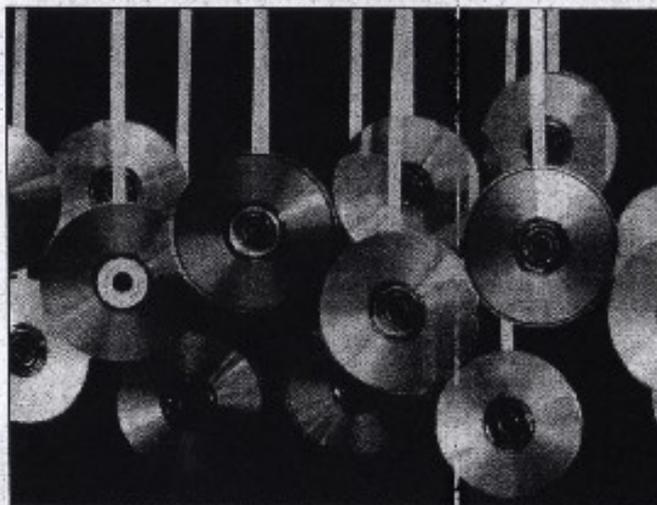
DI MASSIMO GALLI

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

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

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

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



Corsa contro il tempo per salvare gli archivi digitali

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

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

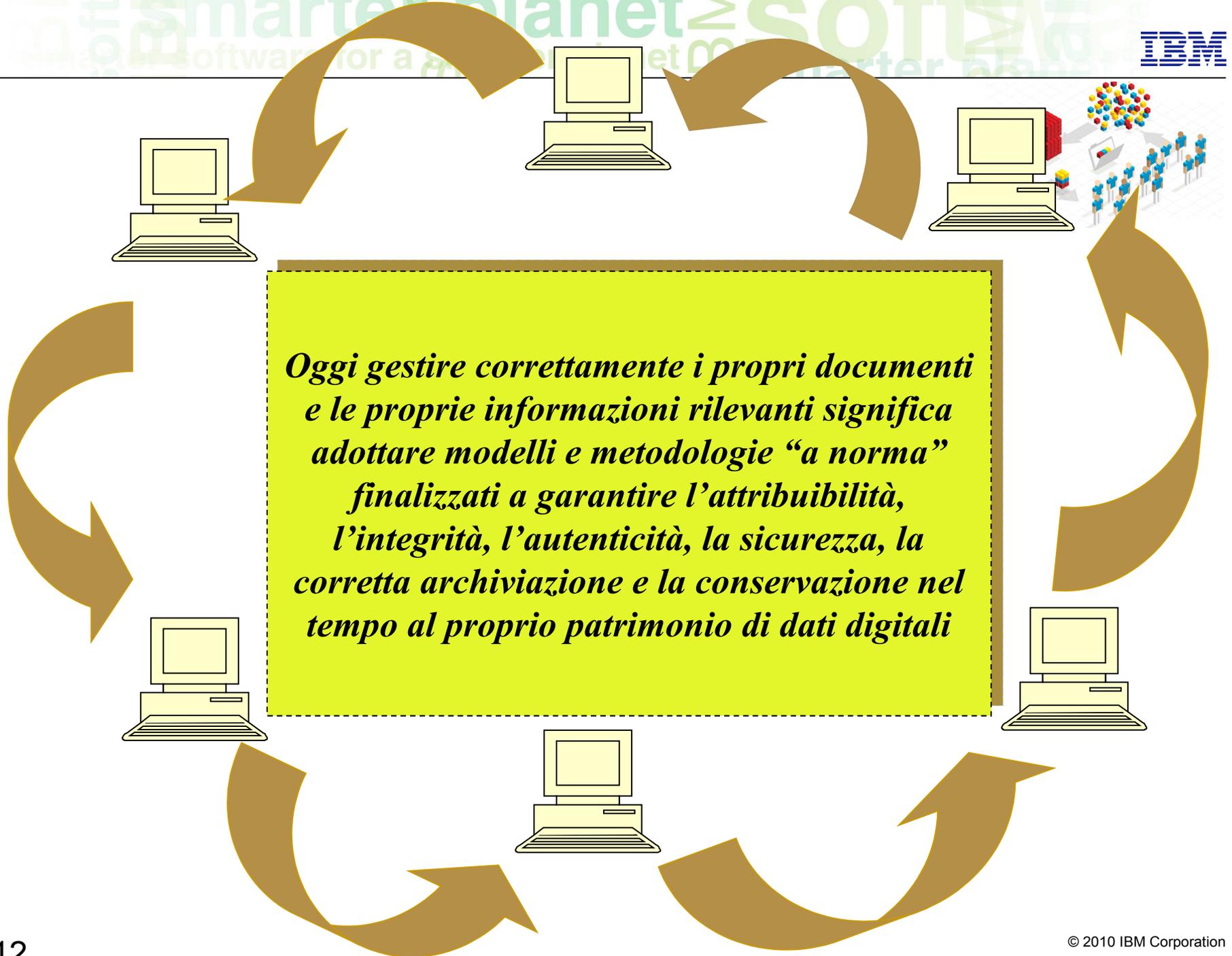
quelle questioni che tiene molte gente sveglia di notte.

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

© Riproduzione riservata

Il partito Ump propone di tornare a legalizzare la professione

Nelle case d'asta si riaffaccia l'ottimismo



Sistema di gestione e conservazione informatica dei documenti

Sviluppo di un sistema informatico

Analisi organizzativa

Change Management

Sicurezza informatica

privacy

Analisi dei processi di gestione dei flussi documentali

- Mappatura processi
- Rilevazione ruoli e responsabilità

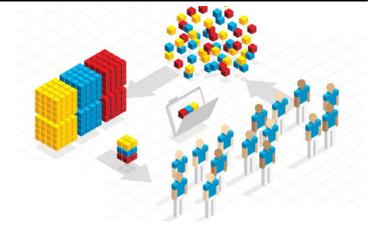
Reingegnerizzazione di tutti i procedimenti

- Ridefinizioni ruoli e responsabilità
- Analisi costi/benefici

**Formazione
Comunicazione**

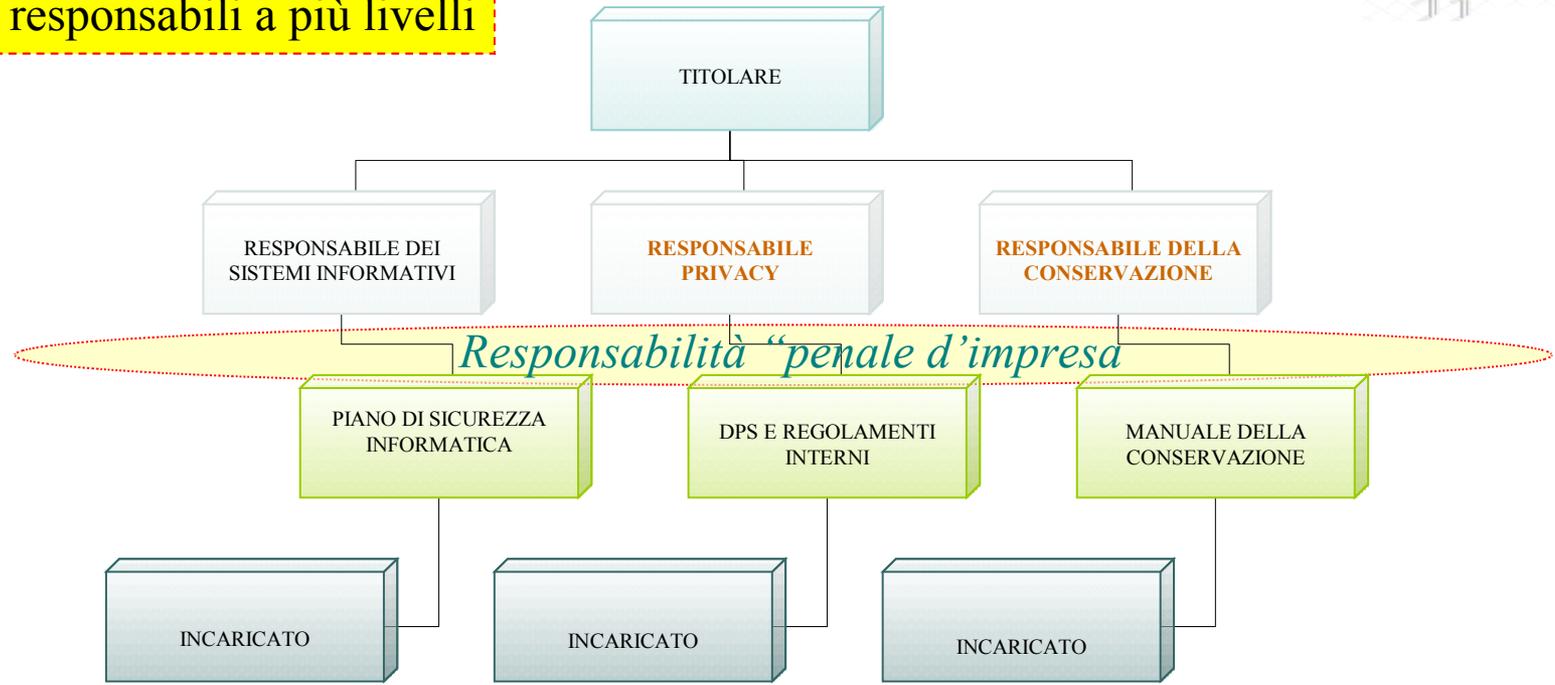
**Conservazione
sostitutiva/digitale**

*D. Lgs
231/2001*

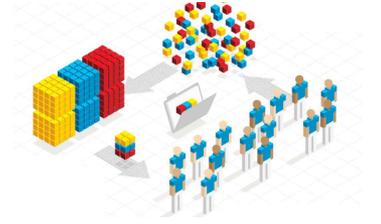


L'ORGANIZZAZIONE

In strutture complesse:
gerarchia di responsabili a più livelli



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



*la strada normativa
verso la digitalizzazione documentale
è segnata*

Recenti Normative in vigore

Libro Unico del Lavoro:

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

- Decreto Ministero Lavoro 9 luglio 2008

- Circolare n. 20/2008 Ministero Lavoro 21/08/2008

- Note Inail 26/08/2008 e 10/09/2008

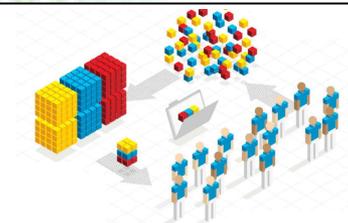
- Registri e contratti assicurativi:

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

- ***Nuove Regole Tecniche ai sensi dell'art. 71 CAD (in fase di "finalizzazione")***

- **Finanziaria 2005**: comma 197 – e-cedolino
- **Finanziaria 2006**: comma 51 – dematerializzazione corrispondenza
- **Finanziaria 2007** : trasparenza retribuzioni
- **Finanziaria 2008**: commi 209-214 – obbligo di fatturazione elettronica alla PA
commi 589-593 – obbligo di PEC e telefonia VOIP
- **Manovra Fine Estate** (DL 112/2008): artt. 39-40 – digitalizzazione Libro unico del Lavoro
- Legge 18 giugno 2009 n. 69 – “taglia carta, **revisione CAD**, Voip”
- **DL anticrisi 78/2009** – convertito in Legge 3 agosto 2009, n. 102
- **D.L. 185/08 (L. 28 gennaio 2009 n. 2) – PEC obbligatoria per tutti e Documenti originali unici smaterializzabili senza notaio!**

L. 2/2009 - Art. 16, c. 6,7,8, 9 e 10:
PEC obbligatoria per professionisti, società e PA
e CEC PAC gratis per tutti!!



Il dubbio:
Chi conserverà la **PEC**?

- *è un formato adatto?*
- *chi garantisce la fascicolazione?*
- *chi garantisce l'autenticità e l'integrità?*

ART. 43 CAD (Riproduzione e conservazione dei documenti)

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

Disposizioni in materia di semplificazione dei rapporti della Pubblica amministrazione con cittadini e imprese e delega al Governo per l'emanazione della carta dei doveri delle amministrazioni pubbliche

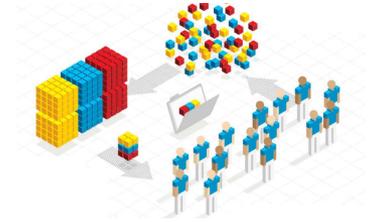
TITOLO I: DISPOSIZIONI IN MATERIA DI INNOVAZIONE E DI SEMPLIFICAZIONE DEI RAPPORTI DELLA PUBBLICA AMMINISTRAZIONE CON CITTADINI E IMPRESE

Art. 6

(Conservazione delle cartelle cliniche)

1. La conservazione delle cartelle cliniche, senza nuovi e maggiori oneri a carico dello Stato, è effettuata esclusivamente in forma digitale. Esse sono rilasciate agli interessati, su richiesta, anche in forma cartacea, previo pagamento di un corrispettivo stabilito dall'amministrazione che le detiene.
2. La presente disposizione entra in vigore il 1° luglio 2010. Entro tale data possono essere stabilite modalità uniformi di attuazione del presente articolo **con regolamento da emanarsi ai sensi dell'art. 17, comma 3, della legge 23 agosto 1988 n. 400** su proposta dei Ministri per il lavoro, la salute e le politiche sociali e per la pubblica amministrazione e l'innovazione, di concerto con i Ministri dell'economia e delle finanze, **della difesa** e per la semplificazione normativa, **nel rispetto di quanto previsto dall'art. 41 del decreto legislativo 7 marzo 2005, n. 82.**

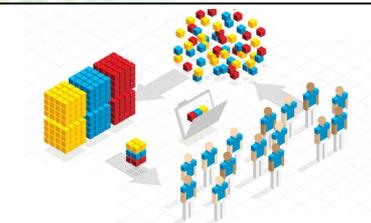
Conservazione cartelle cliniche elettroniche



I dubbi:

- Con quale normativa conservo?
- Come rispetto la normativa privacy?

Certificati medici on line

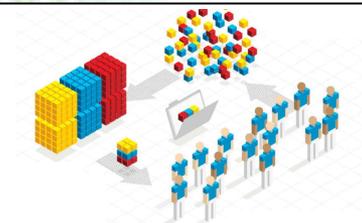


PRESIDENZA DEL CONSIGLIO DEI MINISTRI

CIRCOLARE 11 marzo 2010, n. 1 (in G.U. n. 112 del 15 maggio 2010)

Indicazioni operative per la trasmissione per via telematica dei certificati di malattia, ai sensi dell'articolo 55-septies del decreto legislativo 30 marzo 2001, n. 165, introdotto dall'articolo 69 del decreto legislativo 27 ottobre 2009, n. 150.

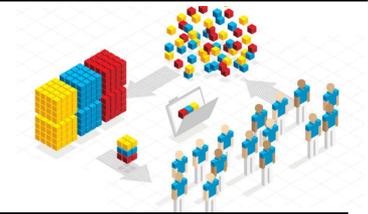
L'ultima novità



DECRETO LEGISLATIVO 30 dicembre 2010, n. 235

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

...ma la normativa deve ritenersi completa?



La normativa deve essere rigida e precisa?
.....o è preferibile che sia flessibile?

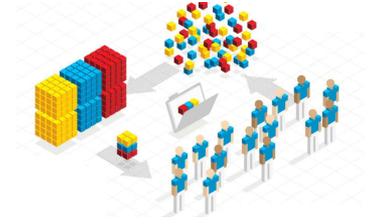
Dal punto di vista tecnico l'approccio deve essere specifico?
...oppure è meglio che sia neutrale?

LA NORMATIVA E' COMPLETA (anche se "a pacth")!

Ruolo del giurista



- Contratti
- Buone prassi
- ...es. *ius gentium*



Il Sistema di Conservazione Digitale dei documenti

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



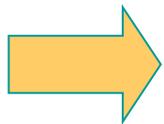
*E solo un sistema di conservazione digitale a norma può
consentire un futuro giuridicamente rilevante ai nostri
documenti informatici!*

Al Codice della Amministrazione Digitale ...:

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

1. Il sistema di conservazione dei documenti informatici **assicura**:

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



Chiave interpretativa per la normativa sulla conservazione sostitutiva e sulla fatturazione elettronica

Al Codice della Amministrazione Digitale ...:

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

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'art. 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'art. 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attivita' di rispettiva competenza.

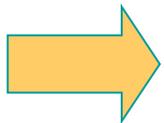
1-ter. Il responsabile della conservazione puo' chiedere la conservazione dei documenti informatici o la certificazione della conformita' del relativo processo di conservazione a quanto stabilito dall'art. 43 e dalle regole tecniche ivi previste, nonche' dal comma 1 ad altri soggetti, pubblici o privati,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

Sicurezza informatica nella conservazione dei documenti ...:

51. *Sicurezza dei dati.*

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.



Non c'è conservazione senza sicurezza informatica

Schema di Modifica al CAD – delega contenuta nell’art. 33 L. 69/20098

Dopo l’articolo 50 del decreto legislativo 7 marzo 2005, n. 82, è inserito il seguente: “**Art. 50-bis** - (*Continuità operativa*). - 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 :

a) **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;

b) **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 assicura l’omogeneità delle 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.”.

Lo scopo della Normativa

Garantire al Documento Informatico:

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

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

attraverso una complessa procedura di conservazione

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

Riferimento temporale/marca temporale

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



Outsourcing
(art. 5 Del. CNIPA)

Attribuibilità e immutabilità del documento



Formazione del documento o sua "riproduzione sostitutiva"

Conservazione documento

Sicurezza della conservazione



Firme Elettroniche/ Digitali e Riferimenti Temporali su singoli documenti

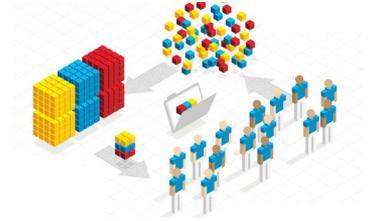
Archiviazione Elettronica



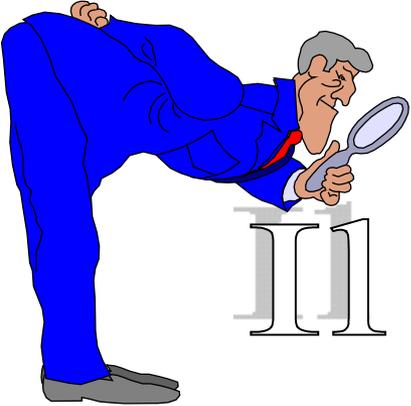
Firma digitale + Marca Temporale sul lotto di documenti



Misure di sicurezza: Business Continuity, Back up, Disaster Recovery, e Restore



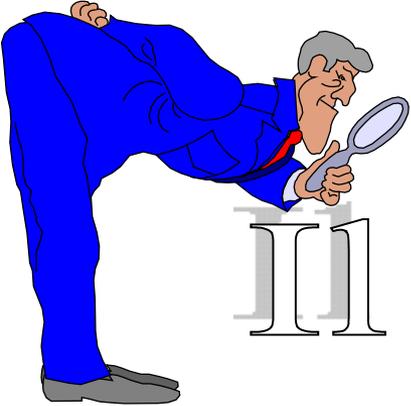
*i rischi:
tutto semplice?*



Il caso concreto

Un gruppo di ASL italiane decide di avviare un importante progetto di gestione informatica e conservazione permanente di Referti e Immagini (sviluppate nei sistemi RIS e PACS) e di affidarne il processo (previo Bando di Gara) ad una multinazionale che si avvale di un outsourcer locale per sviluppare le dinamiche di gestione, disaster recovery, mirroring e conservazione. Si decide di evitare un salvataggio su supporti ottici e di garantire la custodia attraverso un processo di conservazione su un archivio centrale. Ma le difficoltà di trasmissione di dati non permettono il processo di salvataggio in disaster recovery delle immagini...





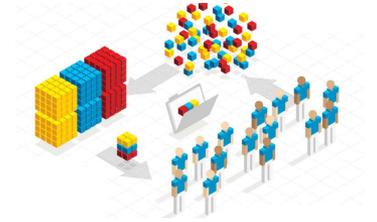
Il caso concreto

Alcuni server (anche quello di mirroring) vanno in crash e le immagini diagnostiche di interi mesi si perdono!

I file risultano irrecuperabili!

Chi è responsabile?

Il Responsabile
della
Conservazione Digitale
dei documenti e delle informazioni rilevanti



Art. 5 (Del. 11 CNIPA) Responsabile della conservazione

1. Il responsabile del procedimento di conservazione sostitutiva:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;

b) archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:

1) descrizione del contenuto dell'insieme dei documenti;

2) estremi identificativi del responsabile della conservazione;

3) estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;

4) indicazione delle copie di sicurezza; (continua...)

- c) mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- d) verifica la corretta funzionalità del sistema e dei programmi in gestione;
- e) adotta 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;
- f) richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- g) definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- h) verifica 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.

(continua)

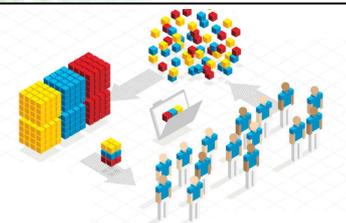
Le 2 figure a confronto:

Il Responsabile privacy

- È PREPOSTO DAI VERTICI AZIENDALI ALLA GESTIONE, SUPERVISIONE E CONTROLLO **DELLA PRIVACY**
- DEFINISCE E IMPLEMENTA IL **MODELLO DI GESTIONE PRIVACY**
- DEFINISCE MODALITA' E STRUMENTI PER IL TRATTAMENTO
- NOMINA E IMPARTISCE ISTRUZIONI AGLI INCARICATI
- NOMINA E DELEGA COMPITI E FUNZIONI A RESPONSABILI ESTERNI
- DEFINISCE E ADOTTA LE MISURE DI SICUREZZA
- REDIGE O AGGIORNA IL **DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**
- REFERENTE IN CASO DI ACCESSI, ISPEZIONI, CONTROLLI

Il Responsabile della conservazione

- È PREPOSTO DAI VERTICI AZIENDALI ALLA GESTIONE, SUPERVISIONE E CONTROLLO **DEL SISTEMA DI CONSERVAZIONE SOSTITUTIVA**
- DEFINISCE E IMPLEMENTA IL **MODELLO DI CONSERVAZIONE SOSTITUTIVA**
- DEFINISCE MODALITA' E STRUMENTI PER IL TRATTAMENTO
- NOMINA E IMPARTISCE ISTRUZIONI AGLI INCARICATI
- NOMINA E DELEGA COMPITI E FUNZIONI A RESPONSABILI ESTERNI
- DEFINISCE E ADOTTA LE MISURE DI SICUREZZA
- REDIGE O AGGIORNA IL **MANUALE DELLA CONSERVAZIONE SOSTITUTIVA**
- REFERENTE IN CASO DI ACCESSI, ISPEZIONI, CONTROLLI



Pertanto, gli obblighi imposti al responsabile della conservazione (i quali paiono essere prevalentemente tecnico-informatici, manageriali e organizzativi e non più solo operativo-fisici), analiticamente elencati al primo comma dell'art. 5 della deliberazione CNIPA attengono ad ambiti eterogenei, che si sostanziano nel compimento delle seguenti attività (tutte delegabili):

- attività di programmazione e di natura esecutiva;
- attività di mantenimento, di verifica e di controllo;
- attività di documentazione e di studio normativo;
- attività di protezione e sicurezza.

outsourcing?

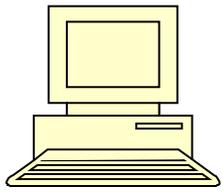
I commi 2 e 3 dell'articolo 5 della deliberazione CNIPA consentono al responsabile del procedimento di conservazione di delegare in tutto o in parte le proprie attività ad altri soggetti interni alla struttura e a soggetti terzi.



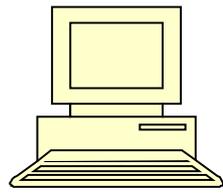
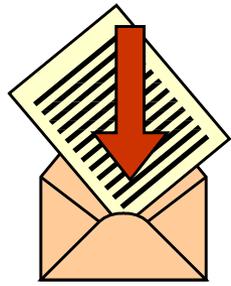
Processo di outsourcing

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

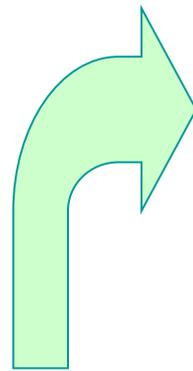
i servizi in outsourcing



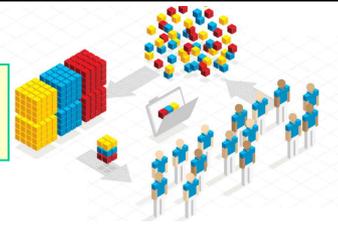
Cliente



Outsourcer



Fatturazione



Chi firma?

Chi controlla?

Chi è responsabile?



L'“esternalizzazione” di alcuni processi aziendali fortemente specializzati e complessi

Servizi di conservazione con nomina quale responsabile esterno della conservazione sostitutiva

Verifica e certificazione dei processi



2. Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.

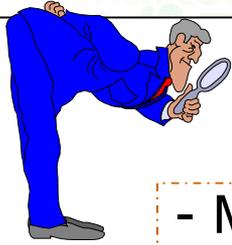
3. Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione.

(art. 5 Del. CNIPA)

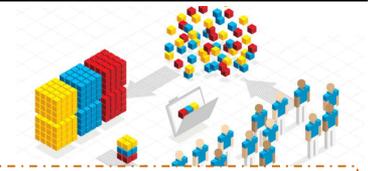


***Contratto di outsourcing: si delega
all'esterno il procedimento di conservazione***

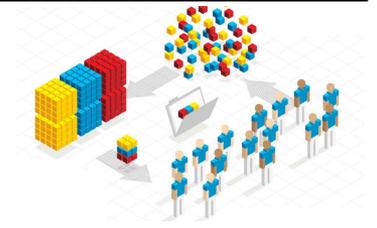
*Il Responsabile della Conservazione è un **Team Manager** di alto profilo che va controllato da un Organismo di Vigilanza e i cui compiti vanno contrattualizzati nel dettaglio*



Outsourcing...a cosa prestare attenzione?



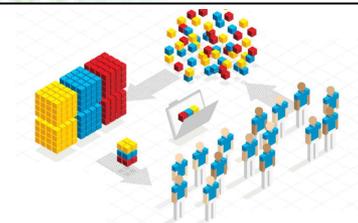
- Manuale e DPS: *documenti che si parlano*
- Attenzione agli allegati tecnici... *che siano coordinati con il contratto!*
- Specificate bene la fase di formazione del documento e le modalità di trasmissione dei flussi
- Definite i formati adatti alla conservazione e specificate le responsabilità in caso di consegna di formati inadatti alla conservazione a lungo termine
- Definite bene la fase eventuale di cessazione del servizio
- Attenzione alle deleghe di firma in remoto sempre allo stesso soggetto conservatore
- In caso di utilizzo di certificati di firma non italiani le procedure vanno verificate nel dettaglio e così i software di verifica della firma
- Evitate i copia-incolla...piuttosto non fate il contratto!



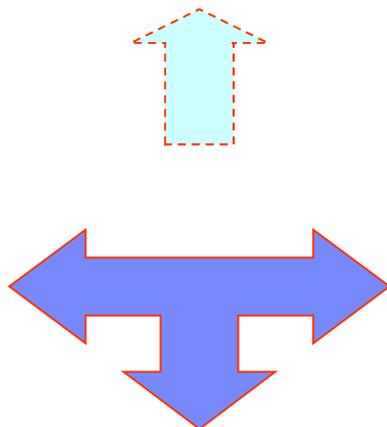
Outsourcing...a cosa prestare attenzione?

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

Titolare dei Documenti e dei Dati
(nomina Responsabile interno
della conservazione)



Responsabile del
procedimento di
conservazione
(referente interno)



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

***Organismo di
Vigilanza e
Certificazione***

art. 26 DIRETTIVA 2006/123/CE
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 12 dicembre 2006
relativa ai servizi del mercato interno

1. Gli Stati membri, in collaborazione con la Commissione, adottano misure di accompagnamento volte ad incoraggiare i prestatori a garantire, su base volontaria, la qualità dei servizi, in particolare:

a) facendo certificare o valutare le loro attività da organismi indipendenti o accreditati.

11) i sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito possono offrire ai prestatori di servizi di certificazione il quadro appropriato per l'ulteriore sviluppo dei loro servizi verso i livelli di fiducia, sicurezza e qualità richiesti dall'evoluzione del mercato; tali sistemi dovrebbero incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; questi ultimi dovrebbero essere liberi di aderire a tali sistemi di accreditamento e i trarne vantaggio (direttiva 1999/93/CE).

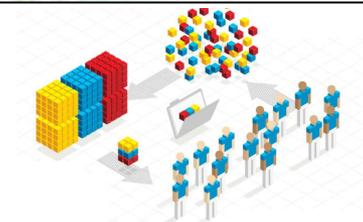
Dal nuovo Codice della Amministrazione Digitale:

44-bis (Conservatori accreditati).

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.

2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31. 3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.

Grazie per l'attenzione



...e per contatti o ulteriori informazioni:



Avv. Andrea Lisi
Digital&Law Department Studio Legale Lisi

www.studiolegalelisi.it

Tel. 0832/256065 – Fax 0832/244802

e.mail: andrealisi@studiodl.it



Digital & Law

Department

www.studiolegalelisi.it