



FIRENZE TECNOLOGIA



## Magazzini Digitali

**“Sistema di  
Digital Preservation  
per il Deposito Legale”**

**54° Congresso nazionale AIB**

Biblioteca Nazionale  
Centrale  
FIRENZE



Fondazione RINASCIMENTO  
digitale  
nuove  
tecnologie  
per i beni  
culturali

Firenze, 8 novembre 2007

Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA



FIRENZE TECNOLOGIA



# Scenario Normativo di riferimento sulla conservazione delle informazioni digitali per la PA

Biblioteca Nazionale  
Centrale  
F I R E N Z E



Fondazione RINASCIMENTO  
digitale  
nuove  
tecnologie  
per i beni  
culturali

Firenze, 8 novembre 2007

Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA



La tematica della **conservazione delle informazioni elettroniche nel lungo periodo** e' attualmente un tema di discussione aperto a livello internazionale in quanto il dinamismo e la complessità del problema non permettono una unica soluzione; tale tematica, che ha assunto negli ultimi anni una rilevanza sempre maggiore, di pari passo con **la migrazione delle informazioni da cartaceo a digitale**, deve essere governata attraverso l'uso di standard internazionali e leggi nazionali di riferimento; in particolare la Pubblica Amministrazione è chiamata ad un **passaggio storico** nella propria organizzazione al fine di garantire la corretta gestione delle informazioni in suo possesso.



# Normativa per la conservazione nella PA

- D.Lgs 30 giugno 2003 n° 196 – Trattamento dei dati personali – Allegato B

19.4. (DPSs) le misure da adottare per garantire l'integrità e **la disponibilità dei dati**, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei **criteri e delle modalità per il ripristino della disponibilità** dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

art. 23. (regole ulteriori per dati sensibili o giudiziari) Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in **tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.**



# Normativa per la conservazione nella PA (1)

- DPR 28 dicembre 2000 n° 445 - SEZIONE III “**Tenuta e conservazione del sistema di gestione dei documenti**”
- Delibera CNIPA n° 11 del 19 febbraio 2004 “Regole tecniche per la riproduzione e **conservazione di documenti su supporto ottico** idoneo a garantire la conformità dei documenti agli originali”
- D.Lgs 8 febbraio 2005, n. 82 e successive modifiche - “Codice della Pubblica Amministrazione Digitale”
  - ➔ Art. 2, comma 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.



# Normativa per la conservazione nella PA (2)

- Giugno 2006, il CNIPA ha rilasciato il Quaderno n° 28 relativo alle "Linee guida alla **continuità operativa nella PA**" che sancisce la necessità per tutte le Pubbliche Amministrazioni di disporre di un Piano per la Continuità Operativa a fronte sia di eventi di piccola sia di grande portata (catastrofi).
- A fine ottobre 2007 sarà presentata la BS 25999-2 sulla Business Continuity
- Lo standard ISO / IEC 27001:2005 (ex. BS7799:2-2002) prevede un dominio specifico - A.14 Business Continuity Management
  - ➔ Sviluppare un processo di gestione del GCO (responsabilità, obiettivi, etc...)
  - ➔ Risk Assessment (BIA): identificazione delle minacce, probabilità di accadimento, valutazione degli impatti per la sicurezza delle informazioni gestite.



FIRENZE TECNOLOGIA



## Magazzini Digitali

Biblioteca Nazionale  
Centrale  
FIRENZE



Fondazione RINASCIMENTO

digitale

nuove  
tecnologie  
per i beni  
culturali

Firenze, 8 novembre 2007

Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA



# Cosa è Magazzini Digitali

- “Magazzini Digitali” - MD è la denominazione del progetto, finanziato da “Fondazione Rinascimento Digitale” e “BNCF – Biblioteca Nazionale Centrale di Firenze”, il cui fine è la **progettazione di un sistema per l'archiviazione** dei contenuti del “**Deposito Legale**” sulla base di quanto stabilito dalla Legge 15 aprile 2004, n. 106 "Norme relative al deposito legale dei documenti di interesse culturale destinati all'uso pubblico" pubblicata nella *Gazzetta Ufficiale* n. 98 del 27 aprile 2004 e del relativo regolamento attuativo pubblicato con DECRETO DEL PRESIDENTE DELLA REPUBBLICA 3 maggio 2006, n.252  
“Regolamento recante norme in materia di deposito legale dei documenti di interesse culturale destinati all'uso pubblico” pubblicato in Gazzetta Ufficiale N. 191 del 18 Agosto 2006.
- Il progetto “MD” coinvolge a pieno titolo sia BNCF, sia la Biblioteca Nazionale Centrale di Roma (**BNCR**) così come previsto dalle disposizioni sul Deposito Legale.



Il sistema “MD” è un *servizio pubblico* la cui finalità principale è il mantenimento della memoria storica del paese attraverso depositi digitali certificati (Trusted Digital Repositories);

per *servizio pubblico* si intende proprio quel **servizio che, ritenuto essenziale e strategico da una determinata comunità, è accessibile indipendentemente dalle possibilità economiche del fruitore** (almeno per quanto riguarda i servizi di base)”.



Per poter considerare i “MD” un deposito digitale accreditato si è stabilito che tale sistema deve essere conforme almeno ai seguenti standard:

- 1) Il processo di Governance di MD deve essere unico, centralizzato e in diretto coordinamento fra BNCF e BNCR con il Ministero dei Beni Culturali.
- 2) La sicurezza delle informazioni contenute in MD deve essere gestita in conformità allo standard ISO/IEC 27001:2005 (ISMS – Information Security Management System)
- 3) La metodologia di archiviazione delle informazioni deve essere conforme allo standard ISO 14721 – OAIS Open Archival Information System



- 4) “MD” deve essere conforme a quanto disposto da RLG-NARA in “Criteria for Measuring Trustworthiness of Digital Repositories & Archives: an Audit & Certification Checklist” - TRAC.
- 5) Leggi e regolamenti nazionali in materia di Archiviazione Digitale nella Pubblica Amministrazione
- 6) Tutto il software utilizzato nell'infrastruttura informatica che conserva i dati deve essere rilasciato con licenza GNU/GPL o similari, così da garantire l'accesso al codice sorgente.



MD ha l'obiettivo di conservare e rendere fruibili nel lungo periodo le informazioni contenute nell'archivio.

- tutelare l' **integrità delle informazioni**: proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione
- tutelare la **confidenzialità delle informazioni**: assicurare che le informazioni siano accessibili solo a chi e' autorizzato
- tutelare la **disponibilità delle informazioni**: assicurare che gli utenti autorizzati possano effettivamente accedere alle informazioni e beni collegati nel momento in cui lo richiedono



- **sostenibilità economica:** programmare con cadenza almeno biennale i budget necessari per il mantenimento e miglioramento del sistema
- **conservazione di lungo periodo:** si rende necessario adottare quelle misure di sicurezza che, in funzione al budget disponibile, minimizzano i rischi anche accidentali
- tutelare la **fruibilità delle informazioni:** assicurare che le informazioni siano realmente fruibili alla comunità di riferimento



**“Deposito Legale Elettronico di Magazzini Digitali”** e' composto da:

- Deposito Legale Elettronico di BNCF – Biblioteca Nazionale Centrale di Firenze
- Deposito Legale Elettronico di BNCR – Biblioteca Nazionale Centrale di Roma
- Deposito Legale Elettronico presso dark archive, amministrato da un terzo Ente



- **PC/Sever di tipo industriale** montati su rack ognuno di quali dotato di 4 dischi SATA da 500 GB (non viene fatto uso di nessun tipo di scheda particolare, di RAID ecc proprio per evitare qualsiasi tipo di dipendenza); e' stato installato un sistema operativo **open source** (una comune distribuzione **Linux**) e un software di base – anche questo open source - per la replica automatica dei dati (rsync).  
Selezione del Software Applicativo (ADORE)
- **Architettura Multisito** (5 macchine sono state installate presso BNCF, 5 presso BNCR); è previsto anche un terzo sito (*dark archive*) che fa una copia dei dati su nastri magnetici del tipo LTO Ultrium3
- Il modello di architettura ipotizzato fa riferimento a Google e a PetaByte; si tratta di PC-Server facilmente amministrabili e sostituibili con dischi hot swap in raid fra di loro
- Per ogni file, **per ogni sequenza di bit, esistono complessivamente 5 repliche** (2 a Firenze, 2 a Roma e 1 nel *dark archive*)



# Dimensionamento di MD

- L'ipotesi di dimensionamento fatta si basa sull'edizione di circa 5.000 CD anno (600MByte cad.) che corrispondono a circa 3 TeraByte/Anno. Per gestire 3TByte sono necessari n° 3 PC server con 4 alloggiamenti per HD da 500GB per ciascuna sede.
- **Banda Internet** 4Mbit/s



- Il processo di analisi del rischio deve essere **documentato, ripetibile** e soprattutto deve **dimostrare di gestire il rischio** in funzione delle finalità del sistema “MD”
- La stima del rischio, a partire da un'esauriente e completa **identificazione di minacce e relative vulnerabilità**, deve riguardare tutti gli **asset** compresi nell'ambito di applicazione
- Gli impatti devono essere valutati verso la **Confidenzialità, l'Integrità, la Disponibilità** e tutti gli altri parametri che vengono definiti all'interno della Politica di Sicurezza del Sistema.
- La **scelta dei controlli** da adottare deve essere bilanciata con il resto dell'organizzazione e deve essere rivista con periodicità da parte del Responsabile della Sicurezza & Audit.



- Digital Repository Audit Method Based on Risk Assessment – DRAMBORA
- Presentata a L'Aja 3 e 4 maggio 2007
- HATII – University of Glasgow
- Maggio 2007 – versione provvisoria su cui svolgere test presso le organizzazioni



**FIRENZE TECNOLOGIA**

# Grazie per l'attenzione

Ivano Greco  
tel. 055 2661025

i.greco at firenzetecnologia punto it  
<http://www.sicurinfo.it>

Firenze, 8 novembre 2007  
Ivano Greco – Firenze Tecnologia, Azienda Speciale della CCIAA