

TESI DI LAUREA, TESI DI DOTTORATO E DISSERTAZIONI ELETTRONICHE
LINEE GUIDA PER LA DIGITALIZZAZIONE E CONSERVAZIONE ARCHIVISTICA A
NORMA

1. PREMESSA	1
1.1. <i>Considerazioni introduttive</i>	1
1.2. <i>Il quadro normativo di riferimento per la produzione e conservazione di documenti informatici</i>	2
1.2.1. La definizione dei termini rilevanti (nella regolamentazione tecnica):.....	2
1.2.2. La validità giuridica.....	3
1.2.3. La conservazione.....	4
2. IL DEPOSITO LEGALE DELLE TESI DI DOTTORATO	6
2.2. <i>Formato strutturato dei metadati nel caso di tesi costituite da più file</i>	6
2.3. <i>Formato dei file</i>	6
2.4. <i>Protocollo di rappresentazione per lo scambio dei metadati</i>	7
2.5. <i>Accesso</i>	7
2.6. <i>Procedura e tempistica</i>	7
2.7. <i>Procedure di validazione</i>	7
2.8. <i>Metadati descrittivi</i>	7
3. TESI DI DOTTORATO, DI LAUREA E DISSERTAZIONI ELETTRONICHE: VALIDITÀ GIURIDICA E GESTIONE/CONSERVAZIONE ARCHIVISTICA	8
4. DEFINIZIONE DEI FLUSSI	8
5. RIFERIMENTI BIBLIOGRAFICI	9

1. PREMESSA¹

1.1. *Considerazioni introduttive*

Le linee guida definiscono i processi di digitalizzazione e conservazione dei prodotti della ricerca scientifica in ambito accademico e didattico. Hanno l'obiettivo di fornire indicazioni di massima per la loro produzione in forma digitale nativa in conformità con quanto stabiliscono i requisiti archivistici standard previsti a livello nazionale (delibera CRUI) e internazionale, la più recente normativa italiana (dlgs 235/2010 e regole tecniche ai sensi dell'articolo 71 in corso di approvazione, legge sul deposito legale). Sono escluse dalla trattazione le questioni connesse al diritto d'autore.

Tenendo conto della specificità delle risorse digitali trattate, in particolare della diversità di trattamento prevista dalla normativa italiana e dalle indicazioni internazionali ed europee in materie di tesi di dottorato, le linee guida sono articolate in tre parti: la **prima** dedicata al deposito legale delle tesi di dottorato, per il quale è stata definita (e qui adottata) una specifica regolamentazione finalizzata a consentire il deposito presso le Biblioteche nazionali centrali di Firenze e Roma nella forma di *harvesting*; la **seconda** per tutte le forme di prodotti digitali riconducibili alla produzione di prodotti della ricerca scientifica identificabili come documenti rilevanti dal punto di vista giuridico e archivistico. Rientrano in questa categoria anche le tesi di dottorato per quanto concerne il loro valore giuridico e la loro

¹ Cfr Biblioteca nazionale centrale di Roma e Fondazione Rinascimento digitale, *Consegna alle Biblioteche nazionali delle Tesi di Dottorato in formato digitale indicazioni tecniche per la raccolta automatica (harvesting)*; A. Bollini, N. De Paoli, *Harvesting delle tesi di dottorato delle Biblioteche Nazionali tramite DSpace*, Cilea, 14 settembre 2010; MinervaEurope, *Linee guida tecniche per i programmi di creazione di contenuti culturali digitali*, Ministero per i beni e le attività culturali, Edizione italiana 2.0, 2006, www.minervaeurope.org; *Linee guida per il deposito delle tesi di dottorato negli archivi aperti*, <https://www.cru.it/HomePage.aspx?ref=1149#>) approvate dalla CRUI. Per le indicazioni di dettaglio si veda *Pagina informativa sulle procedure di deposito legale delle tesi di dottorato in formato digitale presso le Biblioteche nazionali centrali*, <http://depositolegale.it/oai.html#h2a>.

trattazione archivistica conforme a quanto stabilito dal dpr 445/2000. La **terza** parte è dedicata a definire – a mero titolo indicativo – scenari operativi di flusso per la formazione e tenuta nell'archivio corrente delle tesi di dottorato e di laurea in forma digitale.

Si sottolinea che gran parte delle fattispecie documentarie qui considerate (in particolare le tesi di laurea e di dottorato) costituiscono per i soggetti produttori (le Università, in questo caso) documenti giuridicamente rilevanti in quanto “contenuti di atti e fatti prodotti nell'esercizio dell'attività amministrativa” (articolo 1 del dpr 445/2000) e sono quindi sottoposti (per quanto riguarda i processi di informatizzazione e di conservazione digitale) alle disposizioni del dpr 445/2000 sul documento amministrativo, del Codice dell'amministrazione digitale e della successiva regolamentazione tecnica. Hanno infatti **sempre** un duplice profilo, biblioteconomico e archivistico.

1.2. Il quadro normativo di riferimento per la produzione e conservazione di documenti informatici

Il quadro normativo di riferimento è alquanto complesso nel caso della produzione digitale nativa di documenti informatici giuridicamente rilevanti. Le principali disposizioni (che qui si riportano sinteticamente riguardano la **definizione dei termini rilevanti**, la **validità giuridica dei documenti** (provenienza/origine, data certa opponibile a terzi, identità, contesto amministrativo e integrità nel tempo dei contenuti e dei metadati che attestano la provenienza, la data, l'identità e il contesto amministrativo) e la loro **conservazione a lungo termine**. Si riportano di seguito le norme di cui è obbligatorio tenere conto nel definire linee guida generali di produzione e tenuta dei documenti in questione.

1.2.1. La definizione dei termini rilevanti (nella regolamentazione tecnica):

- *autenticità* (caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche; l'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico),
- *ciclo di gestione* (arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo),
- *conservazione* (insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione),
- *identificativo univoco* (sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione),
- *integrità* (insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato nei suoi elementi essenziali),
- *pacchetto di archiviazione* (pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione),
- *pacchetto di distribuzione* (pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta),
- *pacchetto di versamento* (pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione),

- *pacchetto informativo* (contenitore che racchiude uno o più oggetti da conservare - documenti informatici, fascicoli informatici, aggregazioni documentali informatiche -, oppure anche i soli metadati riferiti agli oggetti da conservare),
- *rapporto di versamento* (documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore).

1.2.2. La validità giuridica

Il tema della validità giuridica è molto complesso, poiché riguarda aspetti tecnologici, giuridici e organizzativi che includono tra l'altro l'utilizzo di firme elettroniche per assicurare la provenienza dei documenti ovvero l'imputabilità certa nel tempo dei contenuti del documento e della sua forma a un autore riconosciuto e il riferimento temporale opponibile a terzi (marcatura temporale, protocollazione, posta certificata). In questa sede ci si limiterà a trattare il problema della tipologia di firma elettronica che il Cad consente di utilizzare nel caso della fattispecie documentaria qui considerata e il nodo del riferimento temporale, nelle modalità proposte dal dpcm 30 marzo 2009 e dalla regolamentazione tecnica in corso di approvazione. Poiché i documenti qui considerati sono generalmente a conservazione illimitata, le due questioni sono impegnative non solo sul piano organizzativo e in termini di costi (ad esempio l'impiego massivo di firme digitali da distribuire agli studenti appare in questa fase improponibile sia per ragioni economiche che gestionali), quanto per i rischi di verificabilità della validità della firma e della data nel lungo periodo.

Le regole tecniche sul documento informatico (in corso di approvazione) stabiliscono il principio generale in base al quale **qualunque documento informatico debba essere identificato in modo univoco e persistente e memorizzato all'interno del sistema di gestione documentale**. Stabiliscono inoltre le modalità concrete di memorizzazione che garantiscono il carattere di **immodificabilità** (in termini di non alterabilità nelle fasi di tenuta, accesso e conservazione). Riprendendo precedenti indicazioni (presenti ad esempio nel dpcm 30 marzo 2009) prevedono l'obbligo di "eliminare o rendere statiche, anche attraverso procedure automatiche, tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, e le informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione".

Successivamente specificano le modalità operative che garantiscono l'immodificabilità in relazione alla tipologia di formazione del documento. Le indicazioni sono molto flessibili, lasciando i produttori (gli atenei) liberi di scegliere le modalità di gestione del processo: in particolare prescrivono che, nel caso di *redazione tramite l'utilizzo di appositi strumenti software*, l'immodificabilità si ottiene mediante operazioni quali la sottoscrizione con firma digitale ovvero con firma elettronica qualificata o l'apposizione di una validazione temporale o ancora il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa o la memorizzazione su sistemi di gestione documentale che adottino politiche di sicurezza o il versamento ad un sistema di conservazione.

A fronte di un così ampio margine di scelta, non si ritiene di dover fornire in questa sede indicazioni tassative. Si richiamano tuttavia le indicazioni specifiche delle nuove regole tecniche:

- nel caso di documenti amministrativi informatici gestiti dalle pubbliche amministrazioni la caratteristica di immodificabilità è assicurata *anche mediante la registrazione nel registro di protocollo, negli ulteriori registri, ove opportunamente normati, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti*, secondo quanto previsto nel Capo IV del D.P.R. 28 dicembre 2000, n. 445 e come descritti e documentati nel manuale di gestione;
- si prevede che ai documenti siano associati *riferimenti temporali del tipo UTC* (Tempo Universale Coordinato) in grado di assicurare data certa al contenuto digitale;

- si stabilisce l'obbligo di utilizzare formati (indicati in un apposito allegato) in grado di assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la longevità dei dati in termini di accesso e di leggibilità;
- si definisce un nucleo minimo di metadati (indicati anch'essi in un allegato tecnico) che includono un **identificativo univoco e persistente** del documento, la **data nel formato indicato** in precedenza, **l'oggetto, il soggetto che ha formato il documento**;
- si definiscono le modalità di versamento nel sistema di conservazione mediante la creazione di un cosiddetto *pacchetto di versamento* le cui caratteristiche (inclusi i tempi del versamento) sono concordate con il responsabile della conservazione e definite nel manuale di conservazione oltre che descritte a conclusione del processo nel cosiddetto *rapporto di versamento*.

1.2.3. La conservazione

L'**articolo 43 del Cad** (*conservazione dei documenti*) – fermo restando l'obbligo previsto dall'articolo 41 comma 1 di produrre i documenti delle pubbliche amministrazioni in forma digitale – ne prescrive la tenuta nel tempo nella medesima modalità per tutti i casi per i quali sia “prescritta la conservazione per legge o regolamento”, anche qualora gli originali siano stati formati su altri supporti: la loro validità giuridica e rilevanza è assicurata a condizione che “la riproduzione e la conservazione nel tempo siano effettuate in modo da garantire la conformità dei documenti agli originali nel rispetto della specifica regolamentazione tecnica”, fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi tutelati (pubblici o privati dichiarati di notevole interesse storico).

L'**articolo 44 del Cad** (*requisiti per la conservazione dei documenti informatici*), dopo aver confermato quanto già stabilito dal CAD nel 2005 – ovvero che il sistema di conservazione dei documenti informatici garantisce l'identificazione certa del soggetto che ha formato il documento o che lo ha acquisito, l'integrità del documento e la leggibilità e agevole reperibilità dei documenti stessi e delle informazioni identificative inclusi i dati di registrazione e classificazione originari e il rispetto delle misure di sicurezza – introduce due nuovi importanti commi: il comma 1-bis che prescrive la collaborazione tra i responsabili rispettivamente del sistema di conservazione e del servizio per la tenuta del protocollo informatico e il comma 1-ter che stabilisce a livello di norma generale quanto già indicato nella normativa tecnica del 2004 in materia di affidamento della funzione conservativa “ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche”.

L'**articolo 44-bis del Cad** (*conservatori accreditati*) stabilisce un duplice livello di qualità del servizio prevedendo la possibilità di richiedere l'accreditamento presso DigitPA per “i soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza” (comma 1). I dettagli tecnici, tutt'altro che secondari anche se non esaurienti, sono presenti nel comma seguente allorché si richiamano “in quanto compatibili”, gli articoli 26 (requisiti dei certificatori), 27 (certificatori qualificati), 29 (accreditamento, ad eccezione del comma 3, lettera a) e 31 (vigilanza) ovvero gli obblighi e i controlli previsti dal CAD per gli enti certificatori che rilasciano certificati di firma digitale. Nel caso specifico si riconosce che tale funzione possa essere affidata anche a soggetti pubblici e che i soggetti privati (comma 3) che intendano accreditarsi debbano essere “costituiti in società di capitali con capitale sociale non inferiore a euro 200.000”.

L'**articolo 50 bis** (*continuità operativa*) prevede che “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 predispongano i *piani di emergenza* in grado di assicurare la *continuità delle operazioni* indispensabili per il servizio e il ritorno alla normale operatività” (comma 1); che il Ministro per la pubblica amministrazione e l'innovazione *assicuri l'omogeneità delle soluzioni* di continuità operativa definite dalle diverse Amministrazioni e ne informi con cadenza almeno annuale il

Parlamento (comma 2); che le pubbliche amministrazioni definiscano (sulla base di *studi di fattibilità* valutati da DigitPA):

- 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; si prevede che DigitPA, sentito il Garante per la protezione dei dati personali, definisca le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifichi annualmente il costante aggiornamento dei piani di *disaster recovery* delle amministrazioni interessate e ne informi annualmente il Ministro per la pubblica amministrazione e l'innovazione.

L'**articolo 51** (*sicurezza dei dati, dei sistemi, delle infrastrutture delle pubbliche amministrazioni*) stabilisce principi generali per le norme di sicurezza (definite in dettaglio nelle regole tecniche di cui all'articolo 71) con riferimento all'esigenza di rispettare criteri di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati (comma 1); stabilisce l'obbligo di DigitPA di raccordare le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici e promuovere intese con le analoghe strutture internazionali, segnalare al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni (comma 1-bis) e gli obblighi delle amministrazioni di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi (comma 2-bis).

La regolamentazione tecnica (in via di definitiva approvazione) traduce operativamente gli articoli ora citati, propone – come si è visto – un sistema chiaro ed esaustivo di definizioni e individua le modalità concrete per gestire i documenti digitali, trasferirli a terzi e conservarli, oltre a stabilire un sistema certo di responsabilità, incluse le forme obbligatorie di collaborazione interne alla p.a. (ad esempio tra responsabile dell'archivio e protocollo, responsabile del sistema di sicurezza e responsabile del sistema di conservazione). In particolare prescrive che:

- le modalità e i tempi per i versamenti nel sistema di conservazione siano concordate con il responsabile della conservazione e siano opportunamente documentate in un **rapporto di versamento**;
- si predisponga un **manuale di conservazione** (di cui si stabiliscono le componenti principali);
- si conservino i **metadati essenziali** previsti in sede di formazione della risorsa (**identificativo univoco e persistente** del documento, **riferimento temporale** nel formato indicato, **l'oggetto**, **il soggetto che ha formato il documento**, **il riferimento al fascicolo di riferimento** che nel caso in questione è riferito al fascicolo dello studente);

Sono inoltre stabilite le fasi e i requisiti minimi del **processo di versamento** (peraltro conformi con i principali standard internazionali):

- acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico,
- verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione,
- rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b. abbiano evidenziato delle anomalie,

- generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione,
- eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove previsto nel manuale di conservazione,
- preparazione e gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nel pacchetto di archiviazione (definito in allegato alle regole) e secondo le modalità riportate nel manuale della conservazione,
- preparazione e sottoscrizione con la firma digitale o firma elettronica qualificata, ove previsto nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione,
- produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione al fine di garantire l'interoperabilità tra sistemi di conservazione,
- produzione dei duplicati informatici o delle copie informatiche effettuati a fini di distribuzione,
- eliminazione dal sistema di conservazione del pacchetto di archiviazione alla decorrenza dei termini previsti dalla norma dandone informativa al produttore secondo quanto previsto dalla normativa vigente, che, nel caso degli archivi pubblici o archivi privati, che rivestono interesse storico particolarmente importante, implica anche la previa autorizzazione allo scarto da parte del Ministero per i beni e le attività culturali.

E' inoltre importante sottolineare che in quanto pubbliche amministrazioni gli atenei possono scegliere tra due modelli di conservazione: la gestione interna o l'affidamento a sistemi di conservazione esterni che tuttavia devono essere oggetto di accreditamento presso DigitPA, essere conservati, ai fini della vigilanza da parte di DigitPA sul territorio nazionale e in modo da garantire l'accesso presso la sede del produttore.

2. IL DEPOSITO LEGALE DELLE TESI DI DOTTORATO

2.1. Architettura di base

Si riportano in sostanza le indicazioni suggerite dal Ministero per i beni e le attività culturali per il deposito legale mediante *harvesting* da parte delle Biblioteche nazionali centrali di Roma e Firenze. Si tratta di procedure operative già adottate da numerosi atenei che rispettano la conformità al modello stabilito dallo standard ISO 14721 – OAIS.

Si ribadisce che tali indicazioni non sono sufficienti a garantire il valore giuridico delle tesi e la loro conservazione in quanto documento archivistico collegato al contesto amministrativo di ciascun ateneo. Per il trattamento di tali aspetti si rinvia al capitolo 3.

2.2. Formato strutturato dei metadati nel caso di tesi costituite da più file

Si indica come formati per l'impacchettamento lo standard ISO 28500 - WARC (aggregatore di oggetti digitali a fini di stoccaggio in un file system convenzionale) o il contenitore xml MPEG21-DIDL, una modalità semplice e indipendente per acquisire e gestire insiemi di metadati conformi a schemi e a standard diversi, dato che permette di identificare i singoli componenti (didl:Component) della risorsa (didl:Item) e url della pagina web, detta JOP (jump off page) che riporta le informazioni utili alla consultazione della risorsa mediante un browser. In questo caso il Dublin Core viene utilizzato per identificare (dc:identifier) la JOP che conterrà le ulteriori informazioni sui componenti.

2.3. Formato dei file

E' consigliato il PDF-A; sono suggeriti altri formati aperti, tra cui il formato ODS.

2.4. Protocollo di rappresentazione per lo scambio dei metadati

Per il servizio di deposito legale attuato con raccolta automatica dei metadati (*harvesting*) i metadati devono essere esposti da ogni ateneo utilizzando il protocollo OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting)² in quanto in grado di rappresentare risorse digitali costituite da molteplici file e sostenute; si suggerisce l'uso di applicativi software open source per la gestione di open archives (Dspace, Eprints).

2.5. Accesso

Mantenimento delle scelte di embargo dell'autore per ogni file nella struttura dei metadati; esposizione dei metadati oggetto di validazione da parte degli atenei (segreterie) con particolare riferimento alla presenza di

- un identificativo univoco (URL del deposito),
- un profilo di autorizzazione per ogni file depositato al fine di gestire opportunamente le tesi (o parti di esse) soggette a embargo, consentendo in questo caso l'accesso solo presso le sale di consultazione delle Biblioteche nazionali centrali di Roma e Firenze mediante PC privi di periferiche.

2.6. Procedura e tempistica

L'Università dichiara alla BNCF la propria disponibilità ad accettare la raccolta automatica dei metadati e dei file relativi alle proprie tesi di dottorato, utilizzando l'applicativo presente sul sito (<http://register-oai.depositolegale.it/>) per registrare l'url oai-pmh del proprio repository.

La BNCF esegue la procedura di raccolta una volta al mese in maniera incrementale.

2.7. Procedure di validazione

La BNCF invia, a conferma della ricezione, una mail con allegati due file, in formato xml e xls, contenenti la lista delle URI delle tesi depositate la relativa impronta digitale in formato SHA-1 base32. Meccanismi ulteriori di validazione dipendono dal software utilizzato: ad esempio nel caso di DSpace è possibile prevedere processi di autenticazione di determinati indirizzi IP.

2.8. Metadati descrittivi

Si tratta solo delle informazioni di rappresentazione sintattica e semantica utili esclusivamente ai fini del deposito legale e della ricerca online (per i metadati rilevanti a fini archivistici si veda il capitolo 3). È ritenuto obbligatorio il ricorso allo standard Dublin Core secondo lo schema di seguito indicato:

Dataset	Dublin Core	NOTE
title	DC:title	Titolo della tesi
creator	DC:creator	Autore dell'opera (nel formato cognome, nome); non obbligatorio, ma raccomandato è l'indicazione dell'anno di nascita dell'Autore inserito con la seguente sintassi cognome, nome <anno>
description	DC:description	Abstract (meglio se in inglese)

² La Open Archives Initiative ha elaborato nel 1999 un quadro di riferimento finalizzato a promuovere la diffusione e l'interoperabilità degli archivi aperti di tipo *e-prints*. Il modello è stato successivamente utilizzato come modello di riferimento per l'architettura della biblioteca digitale.

language	Dc:language	Lingua (nel formato ISO639-1);
identifier	DC: identifier	URL a cui raggiungere il full-text della tesi o a una pagina intermedia
type	DC:type	Tipologia di materiale, da impostare di default come Doctoral Thesis è importante per il recupero dei dati usare la forma inglese
contributor	DC:contributor	Nome del tutor (nella forma cognome, nome)
date	DC:date	Data di discussione della tesi (min. Anno)
publisher	DC:publisher	Nome dell'università (è importante perché l'università di provenienza rende esplicito il valore della tesi)
format	DC:format	Dimensione in byte/MIME type
subjects	DC:subject	Settore scientifico disciplinare MIUR
rights	DC:rights	EMBARGO yy-mm-dd Item availability restricted

3. TESI DI DOTTORATO, DI LAUREA E DISSERTAZIONI ELETTRONICHE: VALIDITÀ GIURIDICA E GESTIONE/CONSERVAZIONE ARCHIVISTICA

Da sviluppare sulla base della normativa esistente (capitolo 1)

4. MODELLI DI FLUSSO

4.1. Il flusso per la formazione e gestione nell'archivio corrente delle tesi di dottorato e di laurea

ATTIVITÀ	RESPONSABILE	DOCUMENTO/AGGREGAZIONE	MODALITÀ DI GESTIONE	MODALITÀ DI GESTIONE IN ESSE3
Registrazione titolo tesi/lavoro finale	Studente	Documento/metadati (?) nel fascicolo studente	Da definire in base ai sistemi esistenti. Garantisce la gestione dei seguenti metadati:	interfaccia studente in relazione al sistema di protocollo informatico
Approvazione da parte del docente relatore	Docente relatore	Comunicazione allo studente, minuta nel fascicolo studente	Verifica requisiti, autorizzazione; comunicazione studente	verifica requisiti, autorizzazione; comunicazione studente
Registrazione domanda di laurea	Segreteria	Documento con firma elettronica (tipologia da definire) nel fascicolo studente (data accertabile)	Mediante il sistema di protocollo o altri sistemi in grado di garantire data certa	Titulus/protocollo informatico
Completamento metadati tesi: profilo CRUI, classificazione e fascicolazione (corso di laurea, indicazioni ciclo dottorato); impronta e dati di protocollazione e dati di validazione, metadati sull'impacchettamento dei file in caso di file plurimi	Studente/segreteria	Metadati nel sistema di gestione delle tesi		
Upload della tesi e degli allegati: completamento dei metadati, form di	Studente/segreteria	Documento di autorizzazione nel fascicolo studente	Mediante il sistema di protocollo o altri sistemi in grado di garantire data certa e di fornire	TITULUS: repertorio/protocollo

autorizzazione alla consultazione e riproducibilità (ad esempio dati relativi all'embargo per le tesi di dottorato e al diritto d'autore); gestione degli allegati analogici o in formati non consentiti			adeguato supporto operativo	
Approvazione da parte del docente (utilizzo di firma digitale o di elettronica avanzata da parte del docente)	Docente/segreteria	Archiviazione della tesi come serie tipologica repertoriata nel protocollo (riferimento temporale opponibile a terzi) e annotazione nel fascicolo studente; in alternativa apposizione di marcatura temporale	Repertorio ufficiale/protocollazione o altro sistema di archiviazione con data certa opponibile a terzi	Repertorio ufficiale/protocollazione
Invio documento allo studente e al correlatore (copia analogica?)	Segreteria	Comunicazione		
Produzione statino per la commissione esami	Segreteria	Statino per la commissione esami		
Predisposizione del verbale della Commissione esami	Segreteria	Verbale della Commissione/serie tipologica dei verbali (in forma analogica?)		
Imputazione conseguimento titolo	Segreteria	Metadati nel sistema di gestione e nel fascicolo studente	in ESSE 3 (manuale?)	
Gestione stampa pergamena	Segreteria	Serie tipologica		

5. RIFERIMENTI BIBLIOGRAFICI

CRUI, Gruppo di lavoro Open Access, *Linee guida per il deposito delle tesi di dottorato negli archivi aperti*, 2007, <<http://www.crui.it/HomePage.aspx?ref=1149>>.

CRUI, Gruppo di lavoro Open Access, *Tesi di dottorato e diritto d'autore*, <<http://www.crui.it/HomePage.aspx?ref=1149#>>.

Depositolegale.it, *Magazzini digitali*, <<http://depositolegale.it/>>.

Magazzini Digitali: un'infrastruttura per la conservazione permanente, Venezia, Biblioteca Nazionale Marciana, 23 aprile, 2010, <<http://marciana.venezia.sbn.it/internal.php?codice=684>>.

Marialaura Vignocchi, *Linee guida per l'accesso aperto alle tesi di dottorato*, in "AIDAInformazioni", 26 (2008), 3-4, <<http://www.aidainformazioni.it/pub/arabito-etala342008.pdf>>.

Cristalli di esperienza. Nuove prospettive e scenari per le tesi di dottorato: conservazione, accessibilità, certificazione, formati, integrazione con Open Access, giornata di studio del CNBA, Parma, CNBA, 2008, <<http://digital.casalini.it/17240611>>.