Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

LINEE GUIDA SULLA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Versione 1.0 – dicembre 2015

INDICE

1. IL DOCUMENTO INFORMATICO: EVOLUZIONI TECNOLOGICHE, NORMATIVE E PROCEDURALI 4
1.1 INTRODUZIONE 4
1.2 IL DOCUMENTO INFORMATICO 5
1.3 TIPOLOGIE DI FIRME ELETTRONICHE 10
1.4 TIPOLOGIE DI VALIDAZIONI TEMPORALI 18
1.5 IL CONTRASSEGNO ELETTRONICO E ULTERIORI STRUMENTI CORRELATI AL DOCUMENTO INFORMATICO 20
1.6 FORMAZIONE DEL DOCUMENTO INFORMATICO 25
1.7 IL CICLO DI VITA DEL DOCUMENTO INFORMATICO: LE MACRO-FASI CHE COMPONGONO IL CICLO DI VITA DI UN DOCUMENTO 30
1.8 TIPOLOGIE DELLE COPIE, DEI DUPLICATI E DEGLI ESTRATTI ANALOGICI E INFORMATICI E LORO VALORE PROBATORIO 34
1.9 I FASCICOLI INFORMATICI E LORO GESTIONE NEGLI ARCHIVI DIGITALI 39
2. LA CONSERVAZIONE DEI DOCUMENTI E DEI FASCICOLI INFORMATICI 43
2.1 COSA SIGNIFICA CONSERVARE 43
2.2 OBIETTIVI, PROCESSI E STRUMENTI DELLA CONSERVAZIONE 47
3. ORGANISMI DI TUTELA E VIGILANZA 52
3.1 DESCRIZIONE DEL RUOLO, DELLA STRUTTURA E DELLE FUNZIONI DEL MINISTERO DEI BENI E DELLE ATTIVITÀ CULTURALI E DEL TURISMO 52
3.2 DESCRIZIONE DEL RUOLO E DELLE FUNZIONI DELL'AGENZIA PER L'ITALIA DIGITALE 54
4. REQUISITI PER LA CONSERVAZIONE A NORMA E TERMINI DI ADEGUAMENTO DEI SISTEMI ESISTENTI 56
4.1 RIFERIMENTI NORMATIVI AL CAD E AL DPCM 3 DICEMBRE DEL 2013 IN MATERIA DI SISTEMA DI CONSERVAZIONE, STANDARD DI RIFERIMENTO, PROCESSI, FORMATI DEI DOCUMENTI, METADATI. 56
4.2 PIANO E TEMPI DI ADEGUAMENTO DEI SISTEMI PREESISTENTI ALL'ENTRATA IN VIGORE DELLE NUOVE REGOLE TECNICHE. GESTIONE DEGLI EVENTUALI CONTRATTI DI CONSERVAZIONE CHE UTILIZZANO TALI SISTEMI. 59
5. LE PROCEDURE DI ACCREDITAMENTO 60
5.1 REQUISITI DI QUALITÀ E DI SICUREZZA, CONFORMITÀ AGLI STANDARD DI RIFERIMENTO DEI PROCESSI DI CONSERVAZIONE, CARATTERISTICHE TECNICHE E DELL'ORGANIZZAZIONE 60
6. IL SISTEMA DI CONSERVAZIONE: MODELLI DI RIFERIMENTO 63
6.1 LA CONSERVAZIONE GESTITA IN PROPRIO O AFFIDATA, IN PARTE O IN TOTO A TERZI: DESCRIZIONE DEI MODELLI DI RIFERIMENTO DELLE STRUTTURE ORGANIZZATIVE E DELLA RIPARTIZIONE DELLE RESPONSABILITÀ 63
7. ATTIVITÀ PRELIMINARI DEL SOGGETTO PRODUTTORE 68
7.1 DESCRIZIONE DEL MODELLO ORGANIZZATIVO ADOTTATO PER LA CONSERVAZIONE 68
7.2 RICOGNIZIONE DEI DOCUMENTI, LORO CLASSIFICAZIONE E RELATIVO SISTEMA DI GESTIONE 75
7.3 PREDISPOSIZIONE DEL MANUALE DI CONSERVAZIONE 83
7.4 DEFINIZIONE DEL MODELLO APPLICATIVO DI RIFERIMENTO PER IL VERSAMENTO DEI DOCUMENTI 89
7.5 ACQUISIZIONE DEL SERVIZIO DI CONSERVAZIONE DA SOGGETTI PRIVATI TRAMITE GARA D'APPALTO 92
7.6 ACQUISIZIONE DEL SERVIZIO DI CONSERVAZIONE DA SOGGETTI PUBBLICI TRAMITE CONVENZIONE 93
7.7 ACQUISIZIONE DEL SERVIZIO PER LA PROGETTAZIONE E REALIZZAZIONE DEL SISTEMA INTERNO DI CONSERVAZIONE (GARA D'APPALTO) 98

8. ATTIVITÀ DEL SOGGETTO PRODUTTORE NEL CASO DI AFFIDAMENTO DEL SERVIZIO DI CONSERVAZIONE 99

8.1 PREDISPOSIZIONE, INVIO E GESTIONE DEI PACCHETTI DI VERSAMENTO 99
8.2 CONTROLLI E MONITORAGGIO DEL SERVIZIO DI CONSERVAZIONE 104
8.3 GESTIONE DEGLI SCARTI DA COMUNICARE AL CONSERVATORE 106
8.4 GESTIONE DELLA CANCELLAZIONE, PRESSO IL SOGGETTO PRODUTTORE, DEI DOCUMENTI INVIATI IN CONSERVAZIONE 112
8.5 GESTIONE DEGLI ACCESSI DELL'UTENZA (PRIVACY, PROFILI DI AUTORIZZAZIONE) 113
8.6 GESTIONE DEL TRANSITORIO PER L'AVVICENDAMENTO DEI CONSERVATORI 114

9. ALLEGATI 115

ALLEGATO A - MODELLO DI AUTORIZZAZIONE AL TRASFERIMENTO PER LA CONSERVAZIONE DI DOCUMENTI INFORMATICI. 115
ALLEGATO B - METADATI DEL DOCUMENTO INFORMATICO 118
ALLEGATO C - METADATI DEL FASCICOLO INFORMATICO 124
ALLEGATO D - ELENCO DELLE TIPOLOGIE DI DOCUMENTI COMUNI DA CONSERVARE PER TIPOLOGIA DI AMMINISTRAZIONE 128
ALLEGATO E - GENERAZIONE DEL PACCHETTO DI VERSAMENTO 133

1. Il documento informatico: evoluzioni tecnologiche, normative e procedurali

1.1 Introduzione

Il Codice dell'amministrazione digitale, d'ora in poi denominato CAD, D.Lgs. 7 marzo 2005, n. 82, all'art. 40, rubricato "*Formazione di documenti informatici*", introduce un innovativo e fondamentale precetto: "*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71".*

La norma richiamata stabilisce un preciso obbligo: i documenti delle pubbliche amministrazioni devono essere prodotti esclusivamente in modalità informatica. La dematerializzazione dei flussi documentali all'interno delle pubbliche amministrazioni non rappresenta solo un'opportunità o un percorso volto al raggiungimento di livelli di maggior efficienza, efficacia, trasparenza, semplificazione e partecipazione, ma rappresenta anche un preciso ed improrogabile precetto normativo.

Al centro di questo scenario si colloca il documento informatico definito all'art. 1, comma 1, lett. p), del CAD come "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

Per individuare una più completa definizione di documento amministrativo informatico, è necessario richiamare quanto disposto dall'art. 22, comma 1, lett. d), della Legge 7 agosto 1990, n. 241[1], laddove si afferma che per documento amministrativo, si intende "*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*". Tale definizione è stata poi riformulata dal Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, c.d. TUDA[2], dove all'art. 1, comma 1, lett. a), viene stabilito che per documento amministrativo si deve intendere "*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*".

Ciò che contraddistingue il documento informatico è la sua forma elettronica (rappresentazione informatica). Solo in questa forma quindi, il documento informatico può essere formato, acquisito, sottoscritto, trasmesso e conservato.

1 Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (GU n.192 del 18-8-1990).

2 Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (Testo A). (GU n.42 del 20-2-2001 - Suppl. Ordinario n. 30).

Al pari dei documenti analogici[3] anche i documenti informatici sono destinati ad essere conservati nel tempo ma, mentre per i documenti analogici le regole di archiviazione sono relativamente semplici, per i documenti informatici sono richiesti "particolari accorgimenti" in grado di garantire, durante l'intero ciclo di gestione degli stessi, il mantenimento del loro valore giuridico e legale.

Ecco quindi che il governo dei documenti informatici nell'ambito del loro ciclo di vita deve fondarsi sull'adozione di regole, di procedure giuridiche, legali, archivistiche, tecnologiche e funzionali e di strumenti in grado di assicurare, sin dalle prime fasi della loro gestione, una corretta produzione dei medesimi, poiché solo una corretta formazione del documento informatico ne consente una conservazione conforme alla norma a costi ragionevoli. La corretta gestione con strumenti informatici dei flussi documentali nelle pubbliche amministrazioni diviene quindi un momento fondamentale del processo di dematerializzazione[4] dei documenti e dei procedimenti amministrativi, ponendosi come un processo qualificante di efficienza, efficacia e trasparenza dell'azione amministrativa.

1.2 Il documento informatico

Secondo il disposto dell'art. 20, comma 1-bis, del CAD, *"L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio*[5]*, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21"*. Dal punto di vista legale, quindi, il documento informatico è destinato a produrre effetti giuridici diversi a seconda dei requisiti che possiede.

Prerogativa necessaria affinché il documento informatico integri le caratteristiche di qualità e sicurezza, è la sua gestione all'interno di un sistema di gestione documentale ex art. 3, comma 4, lett. d), del DPCM 13 novembre 2014[6]. A tal proposito, occorre fare riferimento all'art. 52 del D.P.R. 28 dicembre 2000, n. 445, che individua le peculiarità che un sistema di gestione

3 Per documento analogico si intende "la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" (Art. 1, comma 1, lett. p-bis, D.Lgs. 7 marzo 2005, n. 82).

4 La dematerializzazione non deve essere intesa solo come tendenza alla sostituzione della documentazione amministrativa cartacea in favore del documento informatico ma anche come gestione totalmente informatica dei documenti amministrativi, con l'obiettivo di limitare (o azzerare del tutto) la produzione di nuova documentazione su supporto analogico.

5 Art. 116, c.p.c. – Valutazione delle prove - Il giudice deve valutare le prove secondo il suo prudente apprezzamento, salvo che la legge disponga altrimenti. Il giudice può desumere argomenti di prova dalle risposte che le parti gli danno a norma dell'art. seguente, dal loro rifiuto ingiustificato a consentire le ispezioni che egli ha ordinate e, in generale, dal contegno delle parti stesse nel processo.

6 Recante "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005", (G.U. n.8 del 12-1-2015).

informatica dei documenti deve possedere, stabilendo che questo deve necessariamente essere in grado di:

a) garantire la sicurezza e l'integrità del sistema;

b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;

c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;

d) consentire il reperimento delle informazioni riguardanti i documenti registrati;

e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di trattamento dei dati personali;

f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

Il governo dei documenti informatici all'interno del sistema di gestione documentale dell'ente, realizzato secondo le prescrizioni del D.P.R. 28 dicembre 2000, n. 445, del DPCM 3 dicembre 2013 in tema di protocollo informatico[7] e del DPCM 13 novembre 2014 in tema di documento informatico, è quindi in grado di garantire il controllo generale e sistematico della documentazione amministrativa e, al contempo, attribuire ai documenti amministrativi informatici quelle caratteristiche di qualità e sicurezza. La qualità può essere intesa anche come la capacità del documento di rendere fruibili le informazioni in esso contenute. Il documento informatico deve essere in grado di garantire la "leggibilità"[8] del suo contenuto, posto che questa dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato, la scelta dei formati risulta estremamente importante e, dal punto di vista della leggibilità dei documenti informatici, decisiva.

Qualsiasi oggetto digitale (ad es. un documento informatico) viene memorizzato sotto forma di *file*, ovvero come una sequenza di *bit* "0" o "1", considerati come un'entità unica dal punto di vista logico e fissati con una certa organizzazione fisica su un supporto di memorizzazione. Il documento informatico, come insieme di *bit*, esiste dunque solo in relazione ad un sistema informatico in grado di visualizzarlo o di trasferirne il contenuto su un supporto materiale

7 Recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005". (GU n.59 del 12-3-2014 - Suppl. Ordinario n. 20).

8 Per leggibilità deve intendersi l'insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.

(stampa), in modo che un essere umano possa prendere conoscenza del suo contenuto. Così, ad esempio, le informazioni contenute in un *file* creato con una data applicazione (word, excel, writer, calc, ecc.) vengono memorizzate secondo un particolare formato. Il formato dipende quindi dall'applicazione utilizzata nella fase di formazione del documento, di conseguenza, una determinata applicazione può interpretare correttamente e operare solo su *file* il cui formato è noto all'applicazione stessa. Diversamente la sequenza di *bit* memorizzata non avrebbe alcun significato e non sarebbe in alcun modo intelligibile se non se ne conoscesse il relativo formato. Comunemente il formato di un *file* è identificato attraverso la sua estensione; si tratta di una serie di lettere, unita al nome del *file* attraverso un punto (ad esempio [nome del file].doc identifica un formato sviluppato dalla Microsoft).Oltre all'estensione, esistono altri metodi per identificare il formato di un *file*, tra cui i più impiegati sono i metadati espliciti, l'indicazione "application/msword" inserita nei tipi MIME che indica un *file* testo realizzato con l'applicazione word di proprietà della Microsoft, e il *magic number*, i primi *byte* presenti nella sequenza binaria del *file*, ad esempio 0xffd8 identifica i *file* immagine di tipo .jpeg.

Si riporta una sommaria catalogazione dei più diffusi formati, secondo il loro specifico utilizzo:

- Testi/documenti (DOC, HTML, PDF,...);
- Calcolo (XLS, ...)
- Immagini (GIF, JPG, BMP, TIF, EPS, SVG, ...);
- Suoni (MP3, WAV, ...);
- Video (MPG, MPEG, AVI, WMV,...);
- Eseguibili (EXE, ...);
- Archiviazione e Compressione (ZIP, RAR, ...);
- Formati email (SMTP/MIME, …).

Per la rappresentazione delle immagini sono disponibili diversi formati, che possono essere distinti secondo la grafica utilizzata:

- La grafica *raster*, dove l'immagine digitale è formata da un insieme di piccole aree uguali (*pixel*), ordinate secondo linee e colonne. I formati più diffusi sono il .tiff (usato dai fax), il .jpg, e il .bmp;
- La grafica vettoriale è una tecnica utilizzata per descrivere un'immagine mediante un insieme di primitive geometriche che definiscono punti, linee, curve e poligoni ai quali possono essere attribuiti colori e anche sfumature. I documenti realizzati attraverso la grafica vettoriale sono quelli utilizzati nella stesura degli elaborati tecnici, come, ad esempio progetti di edifici. Attualmente i formati maggiormente in uso sono:
  - DWG, un formato proprietario per i *file* di tipo *Computer aided design (CAD)*, di cui non sono state rilasciate le specifiche;

- DXF, un formato simile al DWG, di cui sono state rilasciate le specifiche;
- Shapefile, un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con i prodotti che usano i precedenti formati;
- SVG, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

Per determinate tipologie di documenti informatici sono utilizzati specifici formati. In particolare in campo sanitario i formati più usati sono:

- DICOM (immagini che arrivano da strumenti diagnostici);
- HL7 ed in particolare la CDA2 (*Clinical Document Architecture*) che contiene la sua stessa descrizione o rappresentazione.

Le seguenti caratteristiche sono fondamentali nel valutare la scelta dei formati e di conseguenza le applicazioni che li gestiscono:

a) La diffusione, ossia il numero di persone ed organizzazioni che li adotta;
b) La portabilità, ancor meglio se essa è indotta dall'impiego fedele di standard documentati e accessibili;
c) Le funzionalità che l'utente ha a disposizione per elaborare l'informazione e collegarla ad altre (ad esempio gestione di *link*);
d) La capacità di gestire contemporaneamente un numero congruo (in funzione delle esigenze dell'utente) di formati;
e) La diffusione di visualizzatori che consentono una fruibilità delle informazioni in essi contenute indipendentemente dalla possibilità di rielaborarle;
f) La capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili);
g) La possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

La scelta dei formati idonei alla conservazione, oltre al soddisfacimento delle caratteristiche sopra descritte, deve essere strumentale affinché il documento assuma le caratteristiche di immodificabilità[9] e di staticità[10] previste dalle regole tecniche. È pertanto opportuno

9 Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.

privilegiare formati che siano standard internazionali (preferibilmente *de jure*) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche.

I formati per la conservazione adottati per le diverse tipologie di documenti informatici devono essere indicati nel manuale di conservazione. I formati di seguito indicati sono un elenco di quelli che possono essere utilizzati per la conservazione dei documenti informatici, come previsto dall'allegato 2 al DPCM 3 dicembre 2013 in materia di sistema di conservazione[11], che riguarda i "Formati":

- PDF
- PDF/A (da preferire rispetto al PDF)
- TIFF
- JPG
- Office Open XML (OOXML)
- Open Document Format (ODF)
- XML
- TXT

Ai fini della conservazione, per preservare l'autenticità dei messaggi di posta elettronica, lo standard a cui fare riferimento è RFC 2822/MIME. Per quanto concerne il formato degli allegati al messaggio, valgono le indicazioni di cui sopra.

Data la complessità dei diversi formati esistenti è consigliabile utilizzare solo formati indipendenti dalle applicazioni utilizzate per la formazione di documenti, è necessario quindi limitarsi ad utilizzare formati che non siano implicitamente definiti dall'applicazione proprietaria che li adotta, ma che siano invece supportati da una molteplicità di applicazioni e per cui esista una documentazione così completa ed esaustiva da consentire a chiunque ed in qualsiasi momento la realizzazione di un'applicazione per la loro corretta interpretazione e visualizzazione.

Il manuale di gestione assume in questa fase un'importanza fondamentale non solo per le indicazioni in esso contenute, tipicamente rivolte agli operatori interni all'ente impegnati nella produzione dei documenti informatici, ma anche perché, in quanto documento pubblico, consente di rendere edotti i terzi (cittadini, imprese, professionisti, ecc.), su quali formati possono – e devono – essere utilizzati nella produzione dei documenti da destinare alla

10 Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.

11 Recante "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005". (GU n.59 del 12-3-2014 - Suppl. Ordinario n. 20).

pubblica amministrazione. In questo modo, l'ente destinatario ricevendo solo documenti prodotti con "formati ammessi", non si vedrà costretto ad intraprendere complesse operazioni di conversione dei documenti ricevuti (e prodotti) in formati considerati inidonei alla loro conservazione a lungo termine.

Infine un tema da non trascurare riguarda la convalida dei formati prescelti, poiché rappresenta un fattore importante nella gestione documentale di un ente. Per facilitare le operazioni di produzione dei *file* è opportuno scegliere una conformità blanda (cioè di livello non elevato) allo standard, scelto "il livello di conformità", prima di inserire il documento in archivio, è indispensabile verificarne la conformità allo standard di riferimento che, si ribadisce, dovrà essere reso pubblico in una delle modalità sopra descritte. In pratica, in concomitanza dell'ingresso di documenti informatici nel sistema documentale dell'ente, i *file* dovranno essere sottoposti ad un "processo di validazione" durante il quale saranno effettuati tutti i controlli di conformità alle specifiche dichiarate; all'esito di tale processo corrisponderà l'accettazione o (eventualmente) il rifiuto del documento.

1.3 Tipologie di firme elettroniche

Il presente paragrafo tiene conto dell'attuale normativa nazionale e del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE", (c.d. Regolamento eIDAS)[12].

In ragione di quanto prevede il nostro sistema giuridico, l'imputabilità di una determinata rappresentazione ad un soggetto, nella maggior parte dei documenti, è garantita dalla sottoscrizione; per il documento informatico si è reso necessario concepire una sottoscrizione elettronica in grado di assicurare il legame tra il firmatario e il documento informatico. La sottoscrizione elettronica non è semplicemente un atto ma si tratta di un processo, un processo informatico basato su algoritmi crittografici che permettono di rappresentare un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici (documento informatico), utilizzati come metodo di identificazione informatica[13].

Il CAD all'art. 1, comma 1, lettere q), q-bis), r), s), individua e disciplina quattro diverse tipologie di sottoscrizione elettronica:

a) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

12 Pubblicato in G.U.U.E. L 257 del 28.8.2014, p. 73.

13 Tale definizione è modificata dal Regolamento n. 910/2014 eIDAS che descrive la firma elettronica come dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.

b) 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;

c) 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;

d) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Evidentemente, l'efficacia giuridica delle firme elettroniche sopra richiamate è diversa in ragione delle caratteristiche possedute da ognuna di esse. Da questo punto di vista, i documenti informatici possono essere distinti in tre categorie:

- documenti non sottoscritti (di cui ci siamo già occupati nel capitolo precedente);
- documenti sottoscritti con firma elettronica;
- documenti sottoscritti con firma elettronica avanzata, qualificata o digitale.

L'art. 21, comma 1, del CAD, stabilisce che *"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 immodificabilità"*.Con questo tipo di firma, detta anche "debole" o "leggera", il documento informatico non assume quelle caratteristiche in grado di garantire provenienza ed integrità; la capacità probatoria del documento informatico così sottoscritto è, quindi, interamente rimessa alla libera valutazione del giudice. In altri termini, il documento informatico non offre alcuna garanzia circa eventuali alterazioni e/o contraffazioni del suo contenuto informativo intervenute dopo la sua formazione.

Per attribuire al documento informatico una maggiore capacità probatoria è necessario ricorrere ad una delle seguenti tre firme, tutte appartenenti alla famiglia delle firme c.d. avanzate: firma avanzata (semplice), firma qualificata o firma digitale. Il comma 2, dell'art. 21 del CAD stabilisce che *"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3,*

che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria".

Analizzando con attenzione la norma sopra richiamata, si possono evidenziare tre aspetti fondamentali che il legislatore introduce con riguardo all'utilizzo delle firme elettroniche avanzate:

I. Requisito di forma

   Il documento informatico deve essere formato *ex* art. 21 garantendo l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento. In questo contesto, la norma focalizza la propria attenzione sulla "corretta formazione" del documento informatico.

II. Efficacia probatoria

Tipologia di firma	**Efficacia probatoria**
Firma qualificata	I documenti informatici sui quali è apposta una firma qualificata, ex art. 21, comma 2, del D.Lgs. 7 marzo 2005, n. 82, hanno l'efficacia prevista dall'art. 2702 del codice civile ai sensi del quale la scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritta. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria si configura quindi l'inversione dell'onere della prova.
Firma digitale	La firma digitale ha la stessa efficacia probatoria della firma qualificata.
Firma elettronica avanzata	L'efficacia probatoria della firma elettronica avanzata, c.d. FEA, è disciplinata dal Titolo V del DPCM 22 febbraio 2013 in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali[14]. Tale firma ha l'efficacia prevista dall'art. 2702 c.c., ex art. 21, comma 2, del D.Lgs. 7 marzo 2005, n. 82, ma la presunzione *ex lege* dell'utilizzo del dispositivo da parte del suo titolare, che pone a carico dell'autore la prova dell'uso illegittimo del dispositivo di firma da parte di un terzo prevista per le firme digitali e qualificate, non si configura per la firma elettronica avanzata.

14 Pubblicato in GU n.117 del 21-5-2013

Firma elettronica semplice	Consente di ricondurre, in qualsiasi forma, dei dati elettronici ad un soggetto, ma non assicura l'integrità del documento stesso. Per tale motivo, ex art. 21, comma 1, del D.Lgs. 7 marzo 2005, n. 82, tali firme sono liberamente valutabili in giudizio, tenendo conto, caso per caso delle oggettive caratteristiche di qualità e sicurezza del documento.

III. Riconducibilità del dispositivo al titolare

Affinché al documento informatico sottoscritto con firma avanzata sia attribuita la stessa efficacia probatoria della scrittura privata, è necessario che la firma sia riconducibile al legittimo titolare.

Il legislatore ricorre al meccanismo della presunzione *ex lege* dell'utilizzo del dispositivo da parte del suo titolare le firme digitali e qualificate, non nel caso di utilizzo di una firma elettronica avanzata, ponendo a carico dell'autore apparente la prova dell'uso illegittimo del dispositivo di firma da parte di un terzo. Rispetto al disconoscimento della firma autografa si configura, quindi, l'inversione dell'onere della prova, poiché fra gli obblighi posti a carico del titolare dei certificati di firma vi sono anche quelli di assicurare la custodia del dispositivo di firma, adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed utilizzare personalmente il dispositivo di firma.

Inoltre, per la validità di alcuni atti, di particolare importanza (individuati dall'art. 1350 c.c., punti 1-12, come ad es. gli atti di compravendita di beni immobili o mobili registrati, le locazioni ultranovenali, le costituzione di società, ecc.) è necessario l'utilizzo della firma qualificata o digitale, mentre non è possibile utilizzare la firma elettronica avanzata.

Tra le altre modalità di riconoscimento l'art. 25 del CAD, prevede che "*Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.*". L'autenticazione della firma elettronica, che può essere esperita anche mediante l'acquisizione digitale della sottoscrizione autografa o di qualsiasi altro tipo di firma elettronica avanzata, consiste nell'attestazione da parte del pubblico ufficiale (Segretario Comunale o Notaio) che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non sia in contrasto con l'ordinamento giuridico. È opportuno rilevare che a differenza di quanto previsto dall'art. 2703 del codice civile, l'art. 24 del CAD impone al Pubblico Ufficiale anche di accertare che l'atto sottoscritto non sia in contrasto con l'ordinamento giuridico.

La libertà di utilizzare indipendentemente una delle firme avanzate, sancita dall'art. 21, comma 2, del CAD, si riduce alle sole firme qualificata e digitale, qualora ci si accinga a sottoscrivere una delle scritture private – se prodotte con documento informatico – di cui all'art. 1350, comma 1, numeri da 1 a 12[15], del cod. civ. L'utilizzo di una firma diversa da quella qualificata o digitale nella sottoscrizione di tali scritture è sanzionata con la nullità dell'atto, *ex* art. 21, comma 2-bis del CAD.

Il sistema di firma qualificata o digitale garantisce all'autore del documento informatico, di renderne manifesta l'autenticità, analogamente a quanto avviene apponendo la firma autografa su un documento cartaceo e al destinatario del documento informatico, di verificarne la provenienza e l'integrità.

Apporre una firma digitale ad un documento elettronico significa sostanzialmente:

- applicare una funzione di *hash* (una funzione matematica che trasforma un testo o un contenuto informatico di lunghezza arbitraria in una stringa binaria o esadecimale a lunghezza fissa) al documento stesso, dalla quale si ottiene l'impronta digitale o *message digest* (un *file* di dimensione fissa che 'sintetizza' le informazioni contenute nel documento, secondo un determinato standard, nella fattispecie, ISO/IEC 10118-3:2004;
- codificare l'impronta mediante la chiave privata disponibile al titolare, basata su un certificato qualificato e realizzata mediante un dispositivo sicuro (*token, smartcard,* ecc.) per la creazione della firma;
- allegare al documento la firma così ottenuta.

Per verificare l'autenticità di un documento firmato digitalmente, qualsiasi soggetto lo abbia ricevuto può, mediante l'utilizzo di specifiche applicazioni messe a disposizione gratuitamente dai Certificatori, verificare la firma del documento utilizzando la chiave pubblica del mittente, ottenendo il *message digest* e confrontando quest'ultimo con quello che si ottiene applicando la stessa funzione di *hash* pubblica al documento medesimo; se le due impronte sono uguali il documento risulta integro e imputabile al sottoscrittore. Il processo di firma come sopra rappresentato può apparire complesso, ma l'utilizzo del

15 "Contratti che trasferiscono la proprietà di beni immobili, contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta, contratti che costituiscono la comunione di diritti indicati dai numeri precedenti, contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione, atti di rinunzia ai diritti indicati dai numeri precedenti, contratti di affrancazione del fondo enfiteutico, contratti di anticresi, contratti di locazione di beni immobili per una durata superiore a nove anni, contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato, atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite dello Stato, atti di divisione di beni immobili e di altri diritti reali immobiliari, le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti.".

dispositivo di firma è in realtà molto semplice e di facile utilizzo. Per procedere in questo senso sarà necessario dotarsi di un "Kit di firma digitale", sommariamente composto da:

- un dispositivo sicuro di generazione delle firme (*smartcard*, *token USB*);
- un lettore di *smartcard*;
- un *software* di firma e verifica.

Fondamentale quando si tratta la materia delle firme qualificata o digitali è il tema della loro validità. Come noto, il certificato del titolare ha un periodo di validità, in genere di 3 anni, ma può anche essere revocato o sospeso prima della naturale scadenza. La revoca sopravviene in diversi casi, quali il guasto, la sottrazione o lo smarrimento del dispositivo di firma, quando il titolare ha perso il controllo esclusivo del dispositivo o quando il titolare abbia il ragionevole dubbio che i certificati qualificati possano essere utilizzati da altri come stabilito dall'art. 8, comma 5, del DPCM 22 febbraio 2013. A norma di quanto disposto dall'art. 21, comma 3, del CAD, "*L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione*[16]". Quindi è assolutamente necessario che il titolare del dispositivo di firma, prima di procedere alla sottoscrizione del documento, verifichi che sulla postazione di sottoscrizione sia attiva una connessione a internet, affinché il software di firma possa accertare che il certificato non risulti revocato. Infatti la verifica, per essere attendibile, deve necessariamente basarsi su informazioni molto aggiornate, e quindi disponibili esclusivamente in rete. La firma digitale ha una scadenza, è necessario quindi sapere come agire per preservare l'autenticità di un documento informatico sottoscritto oltre il termine di scadenza del certificato. Per far ciò è necessario avvalersi di un riferimento temporale opponibile ai terzi, tramite il quale è possibile associare – quando necessario – ad un documento informatico una sorta di "*etichetta elettronica, contenente data e ora certa*", allo scopo di dimostrare che il documento aveva quella specifica forma in quel preciso momento temporale. Fra le diverse tipologie di riferimenti temporali opponibili ai terzi, quello più conosciuto è senza alcun dubbio la c.d. "marca temporale", definita dall'art. 1, comma 1, lettera i), del DPCM 22 febbraio 2013, come *"il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.*" Posto che le marche temporali devono essere conservate dal Certificatore Accreditato per un periodo non inferiore a 20 anni, la firma digitale manterrà la sua validità per un identico lasso temporale. Possiamo affermare che l'apposizione di una marca temporale produce l'effetto giuridico di attribuire ad uno o più documenti informatici una data ed un ora opponibili ai

16 Mancando la sottoscrizione, il valore giuridico sarà quello di mero documento informatico non sottoscritto. Qualora la forma scritta è richiesta *ad substantiam*, il relativo atto giuridico è nullo o inesistente; qualora la forma scritta è richiesta solo *ad probationem*, rimane il limite alla prova testimoniale (art. 2725 c.c.) e per presunzioni (art. 2729 comma 2 c.c.), ma l'atto può essere provato con la confessione o il giuramento.

terzi e, dunque, efficace non solo tra le parti. Potrà essere oggetto di validazione temporale qualsiasi tipo di *file* (documenti, immagini, suoni, filmati, ecc.), a prescindere che sia o meno sottoscritto digitalmente.

Il processo di verifica delle firme è un'attività ineludibile per qualsiasi soggetto (pubblico o privato) che tratti o gestisca documenti informatici sottoscritti con firma qualificata o digitale. Tale procedura consiste sostanzialmente nel verificare che:

1) il documento informatico non sia stato modificato dopo la firma;
2) il certificato del sottoscrittore sia garantito da una *Certification Authority* (CA) inclusa nell'Elenco Pubblico dei Certificatori pubblicato dall'AgID (http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi);
3) il certificato del sottoscrittore non sia scaduto;
4) il certificato del sottoscrittore non sia stato sospeso o revocato.

Nell'ambito della reingegnerizzazione dei processi e delle procedure a supporto del sistema di gestione informatica dei documenti, è necessario prevedere funzioni di sottoscrizione elettronica dei documenti informatici in grado di soddisfare le specifiche esigenze di una pubblica amministrazione quali, ad esempio:

- procedure di firma che richiedono l'intervento, anche in momenti diversi, di più sottoscrittori;
- procedure che consentano l'apposizione di sottoscrizioni relative a specifiche parti di un documento al fine di poter attribuire specifiche responsabilità;
- procedure che permettano di aggiungere dei dati dopo la sottoscrizione (ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo in un documento spedito o ricevuto da una pubblica amministrazione);
- procedure che consentano l'utilizzo di diversi formati di firma[17] (CAdES[18], PAdES[19], XAdES[20]);
- procedure che consentano la sottoscrizione da remoto;
- procedure che permettano la sottoscrizione di un elevato numero di documenti.

La firma remota è una particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM (*Hardware Security Module*), utilizzabile via *web*, sicura e facile da usare. Rispetto ai sistemi di sottoscrizione tradizionali, la firma remota consente di apporre firme

17 Gli *standard* europei (Decisione della Commissione europea 2011/130/EU) prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia.
18 Il file sottoscritto conserva il suo nome e la sua estensione originale, al quale viene aggiunta l'estensione .p7m (ad esempio: nomedocumento.pdf.p7m).
19 File con estensione .pdf. Questo formato è leggibile con i comuni *reader* disponibili per questo formato.
20 File con estensione .xml.

senza la necessità di ricorrere all'installazione di *hardware* o *software* sul supporto utilizzato (PC, *Tablet*, *Smartphone*) a condizione che vi sia un accesso ad internet. Nella procedura di sottoscrizione remota il certificato di firma non è presente su un supporto nelle mani del firmatario ma risiede presso un server sicuro (su di un HSM, nella generalità dei casi presso il Certificatore Accreditato che ha rilasciato i certificati di firma), per sottoscrivere digitalmente i propri documenti informatici il titolare utilizzerà il proprio certificato accedendovi da remoto (via rete), inserendo le proprie credenziali di accesso (*username*, *password*) e un'ulteriore credenziale di autenticazione forte fornita da sistemi c.d. OTP (*One Time Password*). La firma così apposta è una firma qualificata o digitale perfettamente equivalente alla firma apposta utilizzando il Kit di firma tradizionale, col notevole vantaggio che i documenti informatici potranno essere firmati digitalmente utilizzando il servizio di rete messo a disposizione dal Certificatore, rappresentando così una modalità di sottoscrizione pratica, comoda e sicura, fruibile in ogni luogo raggiunto da una connessione internet.

In numerose situazioni il procedimento di sottoscrizione può coinvolgere un elevato numero di documenti, in questi casi è perfettamente legale l'utilizzo di procedure automatiche di sottoscrizione, purché si adottino opportune cautele e ci si attenga alle prescrizioni che seguono:

a) è necessaria la preventiva autorizzazione del titolare delle chiavi di firma destinate alla procedura automatica di sottoscrizione;

b) il soggetto che appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso;

c) l'utilizzo della procedura automatica deve essere indicato esplicitamente nel certificato qualificato;

d) se la procedura automatica fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica;

e) i dispositivi sicuri per la creazione della firma automatica devono essere certificati secondo particolari requisiti di sicurezza.

Il Regolamento eIDAS introduce una novità fondamentale, l'art. 29, infatti, disciplina i dispositivi per la creazione di una firma elettronica qualificata nel rispetto dei requisiti previsti dall'allegato II del citato regolamento.

1.4 Tipologie di validazioni temporali

Il CAD definisce la validazione temporale come "*il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi."* All'art. 20, comma 3, stabilisce poi che "*La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale*." Pertanto, per attribuire a un documento informatico una data ed un orario opponibili ai terzi, è necessario attenersi a quanto riportato nelle regole tecniche che, nella fattispecie, sono quelle contenute nel DPCM 22 febbraio 2013 e nel DPCM 13 novembre 2014.

Il metodo più diffuso di validazione temporale è la c.d. "marca temporale" o *time stamp*, intendendosi con ciò, *"il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica (ad es. un documento informatico) in un tempo certo"*. La marca temporale, in quanto attestazione, ha pieno valore legale solo se ottenuta/apposta mediante l'intervento di una terza parte fidata ed imparziale, ossia di un Certificatore Accreditato (c.d. TSA), che opera nel rispetto delle norme vigenti. Il servizio di apposizione della marca temporale si svolge tramite un servizio di rete e funziona nel seguente modo:

1. l'utente invia alla TSA una richiesta di marcatura temporale;
2. la richiesta contiene l'impronta del documento ed altre informazioni accessorie;
3. la TSA genera la marca temporale e la restituisce all'utente.

La marca temporale, così ottenuta, contiene le seguenti informazioni minime:

a) l'identificativo dell'emittente;
b) il numero di serie della marca temporale;
c) l'algoritmo di sottoscrizione della marca temporale;
d) il certificato relativo alla chiave utilizzata per la verifica della marca temporale;
e) il riferimento temporale della generazione della marca temporale;
f) l'identificativo della funzione di *hash* utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
g) il valore dell'impronta dell'evidenza informatica (*ergo*, del documento).

Tutte le marche temporali emesse dopo il 3 dicembre 2009 hanno una validità minima garantita di 20 anni. Chi fosse interessato ad estendere detto periodo di validità può concordare con la TSA un periodo di validità maggiore. La validazione temporale dei documenti informatici sottoscritti dunque, oltre a rappresentare uno strumento essenziale per la gestione e la conservazione dei documenti stessi, rappresenta uno strumento idoneo a preservarne l'efficacia probatoria nel tempo e a consentirne la verifica anche a distanza di anni.

A norma di quanto disposto dall'art. 41, comma 4, del DPCM 22 febbraio 2013, costituiscono inoltre validazione temporale:

a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del DPCM 3 dicembre 2013 sul protocollo informatico;
b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti;
c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del CAD;
d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adottate dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il D.P.R. 12 gennaio 2007, n. 18.

Si faccia però attenzione al fatto che tutti i sistemi di validazione temporale sopra richiamati sono asincroni rispetto al momento di sottoscrizione; in altre parole sono e possono essere apposti solo in un momento diverso e sicuramente successivo alla sottoscrizione digitale. L'apposizione di una validazione temporale ad un documento informatico sottoscritto quindi, deve essere la più tempestiva possibile. La regola deve essere quella di far trascorrere il minor tempo possibile tra la sottoscrizione digitale e l'apposizione della validazione temporale.

Per quanto riguarda le Pubbliche Amministrazioni, la segnatura di protocollo e la posta elettronica certificata rappresentano due tipologie di validazione temporale largamente presenti e utilizzate nella gestione e trasmissione dei documenti informatici. Pertanto qualora un documento informatico "transiti" per uno di questi due strumenti, acquisirà "automaticamente" una validazione temporale, assumendo con ciò tutti i benefici che ne derivano. L'unica accortezza che l'utente dovrà adottare, sarà quella di verificare che la firma apposta al documento informatico sia valida al momento dell'invio/ricezione della PEC o al momento della segnatura di protocollo. Diversamente, la validazione temporale risulterebbe intempestiva e quindi, non determinante per il prolungamento dell'efficacia giuridica della firma e del documento. Un'altra modalità per garantire e mantenere nel tempo l'efficacia probatoria del documento informatico sottoscritto, è il suo tempestivo versamento in un sistema di conservazione a norma. Tuttavia, anche in questa ipotesi, il tempo intercorrente tra la firma del documento e la sua conservazione, deve essere il più breve possibile, solo in questo modo sarà salvaguardata la validità dei certificati di firma utilizzati nella sottoscrizione dei documenti.

Da ultimo, è necessario sottolineare la differenza esistente tra marca temporale e riferimento temporale. La marca temporale costituisce il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo, il riferimento temporale altro non è che *"un'informazione contenente la data e l'ora con*

riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento." L'unico scopo del riferimento temporale è quello di individuare la data di formazione del documento informatico.

1.5 Il contrassegno elettronico e ulteriori strumenti correlati al documento informatico

Le modalità tecniche di generazione, apposizione e verifica del contrassegno riportato elettronicamente in formato stampabile sulla copia analogica di un documento amministrativo informatico originale, sono contenute nell'art. 23-ter, comma 5, del CAD, il quale stabilisce che *"Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida*[21] *dell'Agenzia per l'Italia Digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità".*

Per Contrassegno elettronico, detto anche "Timbro digitale", "Codice bidimensionale" o "Glifo" si intende una sequenza di bit codificata mediante una tecnica grafica e idonea a rappresentare, alternativamente, un documento amministrativo informatico o un suo estratto o una sua copia o un suo duplicato o i suoi dati identificativi.

Dal punto di vista grafico, il contrassegno elettronico è rappresentato con tecnologie differenti, la cui lettura (decifratura) può essere fatta attraverso un apposito *software* rilasciato dallo sviluppatore della soluzione. In ogni caso, il formato e le caratteristiche del contrassegno generato elettronicamente devono permettere la sua stampa anche con stampanti normalmente reperibili in commercio e la sua verificabilità anche con tecnologie di largo consumo. Il contrassegno elettronico non assicura di per sé la "corrispondenza" della copia analogica al documento amministrativo informatico originale contenuto nel contrassegno stesso o conservato dall'amministrazione che lo ha prodotto, ma costituisce uno strumento mediante il quale è possibile effettuare la verifica della suddetta corrispondenza.

Il contrassegno elettronico è quindi finalizzato a consentire la verifica della corrispondenza della copia analogica rispetto al documento amministrativo informatico originale per il tempo di disponibilità del servizio di verifica definito dall'Amministrazione o per il tempo di validità giuridica del documento. A tale scopo, sulla copia analogica può essere apposta in chiaro la

21 In attuazione di tale disposizione, l'Agenzia per l'Italia Digitale ha emanato, con Circolare AgID n. 62 del 30 aprile 2013, le "Linee guida per il contrassegno generato elettronicamente ai sensi dell'art. 23-ter, comma 5 del CAD", reperibili sul sito dell'Agenzia, all'indirizzo: http://www.agid.gov.it/sites/default/files/linee_guida/circolare_n._62_recante_linee_guida_contrassegno_elettronico_art_23_ter_cad_0.pdf.

seguente dicitura: *"Ai sensi dell'articolo 23-ter, comma 5, del D.Lgs. 82/2005, le informazioni e gli elementi contenuti nel contrassegno generato elettronicamente sono idonei ai fini della verifica della corrispondenza al documento amministrativo informatico originale. Si precisa altresì che il documento amministrativo informatico originale da cui la copia analogica è tratta è stato prodotto dall'amministrazione ed è contenuto nel contrassegno (oppure, in alternativa, … è conservato dall'amministrazione almeno per il tempo di disponibilità del servizio di verifica suddetta o per il tempo di validità giuridica del documento)."*

Vediamo ora nel dettaglio, quali sono i contenuti del contrassegno elettronico e quali sono le modalità per effettuare la verifica della corrispondenza dello stesso al documento informatico originale detenuto dalla Pubblica Amministrazione:

1. Contrassegno generato elettronicamente contenente i dati identificativi del documento amministrativo informatico	
Contenuto del contrassegno elettronico	In questo scenario il contrassegno generato elettronicamente riporta almeno gli elementi indispensabili all'individuazione del documento amministrativo informatico originale conservato dall'amministrazione.
Elementi minimi da trattare	L'insieme minimo dei metadati di cui all'art. 53 del D.P.R. 28 dicembre 2000, n. 445, fatti salvi i documenti soggetti a registrazione particolare che comunque possono contenere anch'essi il suddetto insieme minimo dei metadati; il riferimento (URI – riferito ad un dominio registrato ed esposto su canale sicuro) che individua il documento amministrativo informatico originale, come definito nella specifica tecnica RFC 3986; i dati che consentono di realizzare l'accesso controllato al documento amministrativo informatico originale.
Dicitura opzionale da riportare in calce alla copia analogica	Il servizio di verifica della corrispondenza della presente copia analogica al documento amministrativo informatico originale prodotto e conservato dall'intestata amministrazione, sarà disponibile sino al …….. ed usufruibile con le seguenti modalità ……...

	-------- --------- -------- Apposizione del codice che permette di identificare la tipologia del contrassegno utilizzato.
Modalità di verifica della corrispondenza	La verifica della corrispondenza potrà essere effettuata accedendo al documento amministrativo informatico originale conservato dall'amministrazione almeno per il tempo di disponibilità del servizio di verifica o per il tempo di validità giuridica del documento.

2. Contrassegno generato elettronicamente contenente l'estratto o la copia o il duplicato del documento amministrativo informatico	
Contenuto del contrassegno elettronico	In questo scenario il contrassegno generato elettronicamente contiene, oltre agli elementi previsti nel primo scenario, anche l'estratto o la copia o il duplicato del documento amministrativo informatico originale conservato dall'amministrazione
Elementi minimi da trattare	1) L'insieme minimo dei metadati di cui all'art. 53 del D.P.R. 28 dicembre 2000, n. 445, fatti salvi i documenti soggetti a registrazione particolare che comunque possono contenere anch'essi il suddetto insieme minimo dei metadati; 2) il riferimento (URI – riferito ad un dominio registrato ed esposto su canale sicuro) che individua il documento amministrativo informatico originale, come definito nella specifica tecnica RFC 3986; 3) i dati che consentono di realizzare l'accesso controllato al documento amministrativo informatico originale; 4) i dati dell'estratto o della copia o del duplicato del documento amministrativo informatico originale.
Dicitura da riportare in calce alla copia analogica	Il servizio di verifica della corrispondenza della presente copia analogica al documento amministrativo informatico originale prodotto e conservato dall'intestata amministrazione, sarà disponibile sino al

	…….. ed usufruibile con le seguenti modalità ……... -------- --------- -------- Apposizione del codice che permette di identificare la tipologia del contrassegno utilizzato.
Modalità di verifica della corrispondenza	La verifica della corrispondenza potrà essere effettuata: a) nel caso in cui nel contrassegno generato elettronicamente sia contenuto un estratto o una copia, accedendo al documento amministrativo informatico originale conservato dall'amministrazione almeno per il tempo di disponibilità del servizio di verifica o per il tempo di validità giuridica del documento. b) nel caso in cui nel contrassegno generato elettronicamente sia contenuto un duplicato del documento amministrativo informatico, la verifica potrà essere effettuata direttamente con il duplicato stesso.

3. Contrassegno generato elettronicamente contenente il documento amministrativo informatico (non conservato dall'Amministrazione)	
Contenuto del contrassegno elettronico	In questo scenario il contrassegno generato elettronicamente contiene, oltre agli elementi previsti nel primo scenario, anche l'estratto o la copia o il duplicato del documento amministrativo informatico originale conservato dall'amministrazione
Elementi minimi da trattare	1) L'insieme minimo dei metadati di cui all'art. 53 del D.P.R. 28 dicembre 2000, n. 445, fatti salvi i documenti soggetti a registrazione particolare che comunque possono contenere anch'essi il suddetto insieme minimo dei metadati; 2) il documento amministrativo informatico originale.
Dicitura da riportare in calce alla copia analogica	Il documento amministrativo informatico originale è stato prodotto dalla seguente Pubblica Amministrazione: ……

	…… …… -------- --------- -------- Apposizione del codice che permette di identificare la tipologia del contrassegno utilizzato.
Modalità di verifica della corrispondenza	La verifica della corrispondenza potrà essere effettuata direttamente con il documento amministrativo informatico originale contenuto nel contrassegno generato elettronicamente.

Qualora il contrassegno elettronico si riferisca a documenti composti da più pagine, lo stesso può essere apposto su ogni singola pagina e, in questo caso, i metadati forniscono le informazioni necessarie a identificare la posizione nel documento della pagina corrente oltre agli altri elementi previsti. Nella fattispecie, le possibili alternative di apposizione del contrassegno possono essere le seguenti:

- contrassegno, apposto su ogni singola pagina, contenente l'intero documento amministrativo informatico, i metadati di contesto della singola pagina rispetto all'intero documento e gli altri elementi previsti;
- contrassegno, apposto su ogni singola pagina, contenente solo il contenuto della pagina stessa, i metadati di contesto della singola pagina rispetto all'intero documento, il riferimento al documento amministrativo informatico archiviato presso l'amministrazione, l'impronta dello stesso e gli altri elementi previsti;
- contrassegno contenente l'intero documento amministrativo informatico apposto in appendice al documento (soluzione che consente di poter utilizzare una superficie maggiore per il contrassegno generato elettronicamente). In questo caso su ogni singola pagina deve essere apposto un contrassegno generato elettronicamente contenente l'impronta del documento e i metadati di contesto della singola pagina rispetto all'intero documento.

Al fine di procedere alla verifica della corrispondenza della copia analogica al documento amministrativo informatico originale, l'utente potrà avvalersi dei software disponibili sulle principali piattaforme di mercato e verificare sul sito dell'Agenzia per l'Italia Digitale le modalità e le istruzioni per l'utilizzo degli stessi.

Il software di verifica deve consentire:

1) l'interpretazione del codice che identifica la tipologia del contrassegno utilizzato;

2) la decodifica del contenuto del contrassegno e il salvataggio di tale contenuto da parte del soggetto che effettua la verifica;
3) nel caso in cui il contenuto del contrassegno sia sottoscritto con firma elettronica qualificata o firma digitale, la verifica della firma utilizzando l'apposito software messo a disposizione dal certificatore accreditato;
4) la visualizzazione in chiaro del contenuto del contrassegno per verificarne la corrispondenza con il contenuto della copia analogica.

Solo la verifica terminata con esito positivo, assicura la corrispondenza della copia analogica al documento amministrativo informatico originale.

In ogni caso, l'ente che vuole utilizzare il contrassegno elettronico, deve:

a) pubblicare in una specifica sezione del proprio sito, secondo le modalità previste dalle "*Linee guida sui siti web delle PA*", l'elenco delle tipologie dei documenti amministrativi informatici su cui è apposto il contrassegno generato elettronicamente;
b) indicare, per ciascuna tipologia di documenti amministrativi informatici, i tempi di disponibilità del servizio di verifica della corrispondenza;
c) rendere possibile l'accesso ad un servizio di supporto ai cittadini e alle imprese (Consulenza; *Help desk*; *Call center*; *Mail*; URP), in caso di rilevazione di non corrispondenza della copia analogica al documento amministrativo informatico originale, per l'analisi e la risoluzione delle difformità riscontrate;
d) prevedere idonee misure atte a consentire un corretto trattamento per la protezione dei dati personali secondo la normativa in materia, in particolare in caso di trattamento di dati sensibili. Queste misure devono prevedere l'utilizzo di dati cifrati all'interno del contrassegno generato elettronicamente e le informazioni riservate, oscurate nella copia analogica, potranno essere memorizzate cifrate all'interno del contrassegno.

1.6 Formazione del documento informatico

Le regole concernenti la formazione dei documenti informatici, contenute nel DPCM 13 novembre 2014, sono in vigore dall'11 febbraio 2015. La formazione del documento informatico e del documento amministrativo informatico è regolata, rispettivamente, dagli articoli 3 e 9 del DPCM appena citato e il documento amministrativo informatico può essere classificato come una particolare *species* del documento informatico. L'importanza che assume il momento di formazione dei documenti informatici è fondamentale, poiché solo una corretta formazione del documento è in grado di garantirne un'efficace gestione e una valida conservazione a lungo termine. In ambito digitale infatti, la conservazione dei documenti informatici non può essere considerata un'attività *ex-post*, ma deve necessariamente costituire

una componente irrinunciabile della fase di formazione dei documenti stessi. Nella fase di formazione dei documenti si dovranno adottare tutti gli accorgimenti e gli strumenti opportuni per la loro corretta produzione, anche in ragione delle diverse tipologie documentali, della loro differente natura e contenuto o della loro destinazione. Dovrà essere garantita la loro integrità, immodificabilità, identificazione, classificazione, fascicolazione, leggibilità, memorizzazione e conservazione in conformità alle norme e alle regole tecniche che presidiano la corretta tenuta e gestione dei documenti di una Pubblica Amministrazione.

Ai sensi dell'art. 3, del DPCM 13 novembre 2014, il documento informatico può essere formato mediante una delle seguenti quattro modalità: redazione, acquisizione, registrazione informatica di informazioni o dati e generazione o raggruppamento di un insieme di dati o registrazioni.

a) Redazione

La formazione del documento informatico mediante la sua redazione tramite l'utilizzo di appositi strumenti *software*, rappresenta oggi la principale modalità di produzione di documenti informatici da parte di una Pubblica Amministrazione; si tratta della più tradizionale modalità di formazione di un documento che interviene utilizzando applicazioni di *office automation* deputate, il più delle volte, alla redazione di documenti contenenti testo.

Una volta memorizzato nel suo formato originale di produzione, il documento informatico potrà essere consolidato in una o più versioni, sino ad arrivare alla sua versione definitiva, ossia la versione che non subirà alcuna ulteriore modifica di contenuto da parte del suo autore. Solo dopo questa fase, il documento assumerà anche una forma definitiva o, meglio, un formato definitivo in grado di rendere immodificabile il suo contenuto e, ove necessario, predisposto per una eventuale sottoscrizione digitale. Immodificabilità e staticità sono, quindi, due caratteristiche essenziali che devono essere obbligatoriamente garantite. Le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

1) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
2) l'apposizione di una validazione temporale;
3) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
4) la memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
5) il versamento ad un sistema di conservazione.

b) Acquisizione

Con questa modalità il documento è formato mediante acquisizione:

- di un documento informatico per via telematica o su supporto informatico;
- della copia per immagine su supporto informatico di un documento analogico;
- della copia informatica di un documento analogico.

c) Registrazione informatica di informazioni o dati.

Fra le diverse modalità di formazione dei documenti informatici vi è anche quella di cui all'art. 3, comma 1, lett. c), del DPCM 13 novembre 2014, che si realizza attraverso la *"registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente". Con riferimento ai moduli e formulari, è opportuno richiamare quanto precisato nella circolare AgID del 29 marzo 2013, n. 61, rubricata "Accessibilità siti web e documenti amministrativi".* A norma dell'art. 9, comma 4, del DPCM 13 novembre 2014, le istanze, le dichiarazioni e le comunicazioni, se pervenute all'ente per mezzo di moduli o formulari, devono essere identificate e trattate nel sistema di gestione informatica dei documenti come i documenti amministrativi informatici ovvero, se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto, memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione.

d) Generazione o raggruppamento di un insieme di dati o registrazioni

Il documento informatico, infine, può essere prodotto tramite la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica (art. 3, comma 1, lett. c), del DPCM 13 novembre 2014). In entrambe le modalità da ultimo commentate *"Registrazione informatica di informazioni o dati e generazione o raggruppamento di un insieme di dati o registrazioni"* di cui, rispettivamente, alle lettere c) e d), comma 1, dell'art. 3, del DPCM 13 novembre 2014, le caratteristiche di immodificabilità e di integrità sono determinate dalle operazioni di registrazione dell'esito della medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione. Relativamente ai documenti amministrativi informatici, le caratteristiche di immodificabilità e di integrità, oltre che con le modalità sopra descritte, possono essere ottenute anche con la loro registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti

di cui al Capo IV del D.P.R. 28 dicembre 2000, n. 445. In ogni caso, al termine della sua formazione, il documento informatico dovrà possedere le seguenti cinque caratteristiche fondamentali:

1. staticità;
2. integrità;
3. immodificabilità;
4. leggibilità;
5. autenticità.

Così formato, il documento informatico dovrà essere identificato in modo univoco e persistente e dovrà essere memorizzato in un sistema di gestione informatica dei documenti. L'art. 3, comma 9, del DPCM 13 novembre 2014 stabilisce, infatti, che *"al documento informatico immodificabile vengono associati i metadati che sono stati generati durante la sua formazione"*. I metadati[22] altro non sono che un insieme di dati (informazioni) associati ad un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne: contesto, contenuto e struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione.

Il DPCM 13 novembre 2014, individua un insieme minimo di metadati da associare ad ogni documento informatico, in particolare il comma 9, dell'art. 3, stabilisce che tale insieme è costituito dalle seguenti informazioni:

a) l'identificativo univoco e persistente;
b) il riferimento temporale (data di chiusura);
c) l'oggetto;
d) il soggetto che ha formato il documento;
e) l'eventuale destinatario;
f) l'impronta del documento informatico.

Il successivo art. 9, comma 7, dello stesso DPCM, prevede che i metadati "minimi" da associare ad un documento amministrativo informatico di cui all'art. 53 del D.P.R. 28 ottobre 2000 n. 445:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;

22 Nella letteratura tecnica il metadato viene semplicemente e genericamente definito come un "dato su un (altro) dato", ossia sono informazioni che descrivono un insieme di dati, possono far parte del dato (ergo, documento) o possono essere archiviati come oggetti esterni al data a cui si riferiscono.

- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;
- l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

In riferimento alle richiamate regole tecniche sul protocollo informatico (DPCM 3 dicembre 2013):

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- codice identificativo del registro;
- data di protocollo secondo il formato individuato in base alle previsioni di cui all'art. 20, comma 2;
- progressivo di protocollo secondo il formato specificato all'art. 57, del D.P.R. 28 dicembre 2000, n. 445.

Informazioni relative alla segnatura:

- l'oggetto;
- il mittente;
- il destinatario o i destinatari.

Nella segnatura di un documento protocollato in uscita da un ente possono essere specificate una o più delle seguenti ulteriori informazioni:

- indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.

Relativamente ai metadati previsti per il fascicolo informatico o aggregazione documentale informatica, l'allegato 5, al DPCM 13 novembre 2014, individua i seguenti metadati minimi:

- Identificativo univoco e persistente;
- Cod. Amministrazione titolare;
- Cod. Amministrazioni partecipanti;
- Responsabile del procedimento (Nome, Cognome, Codice Fiscale);

- Oggetto;
- Identificativo dei documenti contenuti nel fascicolo.

Eventuali ulteriori metadati rilevanti ai fini amministrativi, definiti per ogni tipologia di documento nell'ambito del contesto a cui esso si riferisce, potranno essere associati al documento amministrativo informatico, purché puntualmente descritti nel manuale di gestione dell'ente.

Per quanto riguarda i documenti informatici rilevanti ai fini delle disposizioni tributarie, l'art. 3, comma 1, lettera b), del Decreto del Ministero dell'Economia e delle finanze del 17 giugno 2014, "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto"[23], stabilisce che per questa particolare tipologia di documenti (ad esempio, registri IVA, fatture di vendita, fatture di acquisto, ecc.) siano presenti almeno i seguenti metadati:

- cognome, nome o denominazione;
- codice fiscale;
- partita IVA;
- data del documento o associazioni logiche di questi ultimi, laddove tali informazioni siano obbligatoriamente previste.

Indipendentemente dalla quantità e dalla tipologia di metadati utilizzati, l'importante è che queste informazioni siano costantemente aggiornate in ragione degli eventi che coinvolgono il documento informatico nel corso del suo ciclo di vita. Infine, è importante ricordare che l'allegato 3, al DPCM 13 novembre 2014, rubricato "Standard e specifiche tecniche", individua nello standard ISO 15836:2009 - *Information and documentation - The Dublin Core metadata element set*, il modello di metadati da adottare per la conservazione, in quanto compatibile con lo standard OAIS, utilizzato come modello di riferimento per i sistemi di conservazione digitale in Italia.

1.7 Il ciclo di vita del documento informatico: le macro-fasi che compongono il ciclo di vita di un documento

Il ciclo di vita di un documento amministrativo informatico può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte. Lo schema che segue ben sintetizza come l'insieme di tali fasi ed attività si articola.

23 Pubblicato in GU n.146 del 26-6-2014.

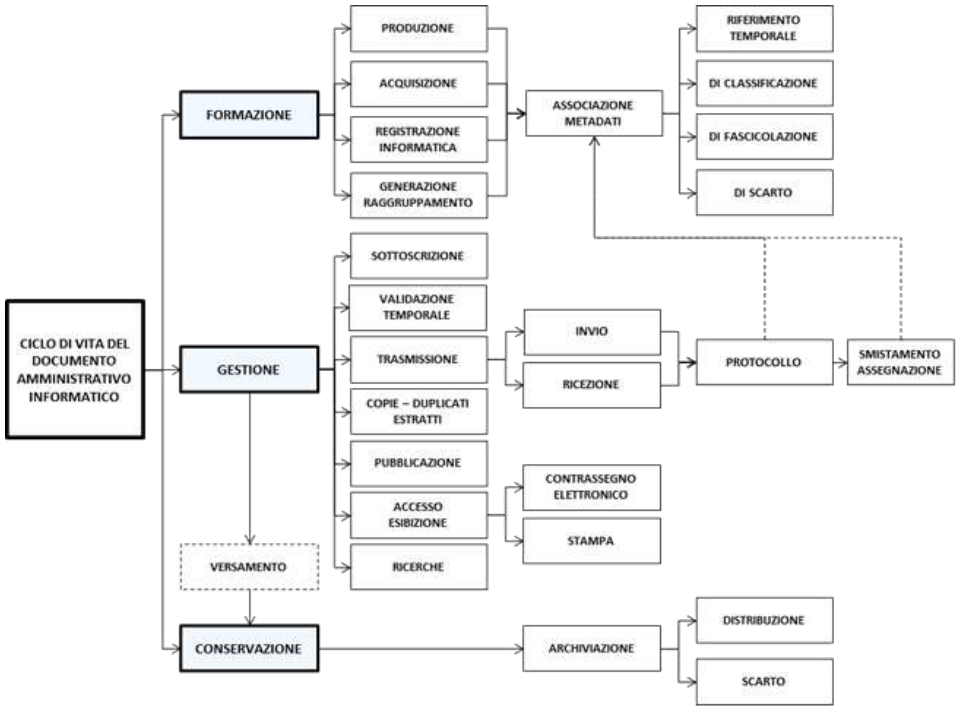

Figura 1 - Schema ciclo di vita documento amministrativo informatico

La gestione del ciclo di vita di un documento informatico, affinché possa essere efficiente e sicura, deve essere necessariamente presidiata da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita di un documento informatico. Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica ed archivistica tipici della gestione degli archivi pubblici.

Dal punto di vista archivistico, possono essere individuate tre ulteriori fasi di vita del documento in ragione delle diverse fasi di organizzazione e utilizzo in cui i documenti si vengono a trovare nel corso della loro vita:

- archivio corrente: insieme dei documenti necessari alle attività correnti;
- archivio di deposito: insieme dei documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: insieme dei documenti storici selezionati per la conservazione permanente.

Fra le diverse fasi del ciclo di vita di un documento informatico, la fase di formazione rappresenta probabilmente la fase più delicata dell'intero processo di gestione; in questa fase, infatti, devono essere operate delle scelte che risulteranno decisive, per le successive fasi di gestione e conservazione. Nella fase di formazione dovranno essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità e coerenza alle regole tecniche che presidiano la formazione dei documenti informatici, tenendo in debito conto le esigenze e i bisogni pratici

del lavoro quotidiano tipico di un'amministrazione pubblica. Al tal fine, risulta decisivo avvalersi di un valido e completo manuale di gestione documentale, di *workflow* documentali e applicazioni di *Document & Content Management* e di applicativi informatici progettati e realizzati specificamente per la pubblica amministrazione che si basino su elevati livelli di automazione ed interoperabilità in grado di operare nel web. In un contesto in continua trasformazione il manuale di gestione dovrà essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti informatici utilizzati. Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici, dovranno essere sottoposti ad un costante lavoro di valutazione, monitoraggio, ri-progettazione e reingegnerizzazione. L'adozione del manuale di gestione non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo sancito dall'art. 5, del DPCM 3 dicembre 2013, contenente le regole tecniche sul protocollo informatico, al quale fa seguito l'ulteriore obbligo della sua pubblicazione sul sito istituzionale dell'ente.

Un momento cruciale della fase di vita di un documento informatico, cioè quello della sua trasmissione, che integra in sé le attività di invio o di ricezione dei documenti informatici che, in quanto tali, possono essere trasmessi esclusivamente con strumenti informatici (generalmente, e-mail o PEC). L'utilizzo di questi "mezzi di trasmissione" è previsto dallo stesso Legislatore che attraverso specifiche norme contenute nel CAD, ha stabilito che:

- *"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"* (all'art. 5-bis, comma 1);
- *"Per le comunicazioni di cui all'art. 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano"* (Art. 6);
- *"Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza"* (Art. 47).

Pur riconoscendo a ciascun ente un elevato grado di autonomia nella scelta del "mezzo di trasmissione" da utilizzare, non può essere sottaciuto il disposto di cui agli artt. 45 e 48 del CAD dove, rispettivamente, viene stabilito che:

- *"I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale. 2. 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"* (Art. 45);
- *"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, [omissis]. 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. 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).*

Una particolare attenzione dovrà essere posta alla fase di protocollazione dei documenti informatici spediti o ricevuti. Nello specifico, dovrà essere garantita la conformità dei processi di trasmissione al DPCM 3 dicembre 2013, nel quale sono contenute le regole tecniche relative alle operazioni di registrazione e segnatura di protocollo che, come noto, devono essere effettuate esclusivamente in modalità informatica.

In particolare, il sistema di protocollo informatico oltre a garantire le "funzionalità minime" richieste dalla normativa, deve essere in grado di assicurare:

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

Inoltre il sistema di gestione informatica dei documenti, opportunamente progettato e realizzato, deve garantire:

- l'individuazione di tutti i documenti in entrata e in uscita;
- l'attribuzione ad ogni documento ricevuto o spedito di una specifica e univoca identificazione (Art. 53 del D.P.R. 28 dicembre 2000, n. 445);
- la data e l'ora di invio/ricezione dei documenti;
- la sequenza cronologica dei documenti ricevuti e spediti (garantire l'ordine cronologico);
- l'immodificabilità dei documenti registrati a protocollo;
- la riservatezza delle informazioni contenute nei documenti;
- la certezza, qualora necessaria, dell'avvenuto recapito dei documenti inviati (gestione delle ricevute di accettazione e consegna previste dal sistema PEC);
- l'usabilità delle procedure e degli strumenti informatici utilizzati.

L'obiettivo è quello di attribuire alla ricezione/invio dei documenti, nonché alle rispettive date di spedizione e ricevimento, la certezza assoluta e l'efficacia probatoria richieste dalla normativa.

In ambito digitale, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale devono essere assolti con la pubblicazione, da parte delle amministrazioni e degli enti pubblici obbligati, nei propri siti informatici, o nei siti informatici di altre amministrazioni ed enti pubblici obbligati, ovvero di loro associazioni. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere agli obblighi di pubblicità legale è necessario quindi che esso garantisca la conformità di quanto pubblicato all'originale, l'autorevolezza dell'ente emanatore e del sito *web*, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

Il ciclo di gestione di un documento informatico termina con il suo versamento in un sistema di conservazione che, inevitabilmente, deve essere realizzato in ottemperanza a quanto disposto dal CAD e dalle regole tecniche e, fra tutte, in conformità a quanto stabilito dal DPCM 3 dicembre 2013. Chiude il ciclo di vita di un documento informatico la sua conservazione a norma o, eventualmente, il suo definitivo scarto, ossia l'operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale.

1.8 Tipologie delle copie, dei duplicati e degli estratti analogici e informatici e loro valore probatorio

L'art. 23-ter, comma 1, del CAD, stabilisce che *"gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge".*

Questo significa che i documenti amministrativi informatici, qualora prodotti in formato digitale, sono documenti originali da cui è possibile ricavare duplicati, copie o estratti sia analogici che informatici.

Il CAD individua:

1. *la copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto*, ovvero, ad esempio, il risultato dell'operazione di trascrizione al computer di un documento cartaceo, per il quale il contenuto è identico, ma la forma può differire (posso copiare l'intero contenuto di un foglio A4 cartaceo in una pagina Word o in tre slide PowerPoint o in due fogli Excel o in qualsiasi altra forma);
2. *la 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*, ovvero, ad esempio, la scansione di un documento in TIFF o JPG;
3. *la copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari*, ovvero, ad esempio, un file Word che viene salvato in formato PDF, per cui il contenuto resta invariato, ma differisce la sequenza di valori binari che formano il *file*;
4. *la copia analogica di documento informatico*, che è la semplice stampa;
5. *la copia analogica di documento analogico*, che è la semplice fotocopia.

Il CAD dedica ben 5 articoli alla disciplina di copie, estratti e duplicati dall'art. 22 all'art. 23 quater, a cui si devono aggiungere le disposizioni contenute nelle Regole tecniche, ed in particolare quelle contenute nel DPCM 13 novembre 2014, agli artt. 4, 5 e 6.

Con riferimento ai documenti elettronici che costituiscono copia di originali analogici, ossia formati in origine sulla carta, occorre per prima cosa distinguere:

- la copia informatica di documento analogico (che costituisce il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto);
- dalla copia per immagine su supporto informatico di documento analogico (rappresentata dal documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto).

In entrambi i casi, possiamo parlare di "dematerializzazione", ossia della sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico.

L'art. 22, comma 1, del CAD, stabilisce che le copie informatiche di documenti analogici (nella generalità dei casi realizzate attraverso la digitalizzazione mediante sistemi OCR[24] o semplice "digitazione" del testo), hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad esse è apposta o associata, da parte di colui che le spedisce o le rilascia, una firma digitale o altra firma elettronica qualificata. In tal caso la loro esibizione e produzione sostituisce quella dell'originale. Il comma 2, dell'articolo sopra citato, attribuisce anche alle copie per immagine su supporto informatico di documenti analogici, (risultato di un processo di acquisizione dell'immagine del documento originale analogico, per esempio, mediante l'utilizzo di uno *scanner*), 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. In questi casi, per vedersi riconosciuta l'efficacia probatoria dell'originale, è necessario che la conformità del risultato informatico dell'immagine relativa all'originale analogico sia attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato e la dichiarazione di conformità sia formata e asseverata secondo quanto disposto dalle regole tecniche.

L'art. 22, comma 3, stabilisce altresì che le copie per immagine su supporto informatico di documenti originali analogici, formate nel rispetto delle regole tecniche, hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta. La differenza sostanziale tra il processo di copia di cui al comma 2, rispetto a quello previsto al comma 3, consiste nel fatto che: nel primo caso la copia informatica ha la medesima efficacia probatoria dell'originale da cui è tratta, nel secondo caso, invece, il valore probatorio della copia informatica può essere disconosciuto. In entrambi i casi, la copia per immagine deve essere prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, qualora siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia, attraverso certificazione di processo.

Per quanto riguarda l'attestazione di conformità delle copie per immagine di cui all'art. 22, comma 2, del CAD, questa può essere inserita nel documento informatico contenente la copia per immagine. In questo caso, il documento informatico così formato è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato; oppure essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. In questo caso il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

24 I sistemi di riconoscimento ottico dei caratteri.

Si tenga però presente che il comma 5, dell'art. 22, in commento stabilisce regole particolari in riferimento ai documenti analogici originali unici. La copia informatica di un documento analogico formato in origine da una pubblica amministrazione assume il medesimo valore giuridico dell'originale da cui è tratto, qualora il funzionario delegato a tale compito:

a) sottoponga il contenuto della copia informatica ad un processo di conformità (che può essere effettuato per raffronto visivo dei due documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia);

b) rilasci apposita attestazione di conformità:

   - inserendola nel documento informatico contenente la copia informatica; il documento informatico così formato deve essere sottoscritto con firma digitale o firma elettronica qualificata del funzionario delegato;

   - producendola come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia; il documento informatico contenente l'attestazione di conformità deve essere sottoscritto con firma digitale o con firma elettronica qualificata del funzionario delegato;

c) sia nella formazione della copia informatica che nell'apposizione della sottoscrizione digitale, si attenga a quanto disposto delle regole tecniche sul documento informatico (DPCM 13 novembre 2014);

d) proceda alla corretta conservazione (a norma) della copia informatica.

Nel processo di dematerializzazione dei documenti analogici è in ogni caso necessario prestare molta attenzione a quelli sottoscritti con firma autografa. Pur tenendo presente la previsione di cui all'art. 22, comma 4, del CAD, infatti, è comunque doveroso essere estremamente prudenti nell'eliminare (ergo, distruggere) gli originali analogici sottoscritti. L'operazione di distruzione dell'originale analogico sottoscritto (che comunque non può che intervenire solo dopo aver correttamente conservato la relativa copia informatica), deve essere valutata attentamente in ragione della possibilità o meno di vedersi contestata l'autenticità dell'originale ormai distrutto.

Fa da contraltare alla fattispecie che precede, la copia analogica di documento informatico, ossia la riproduzione su carta (normalmente effettuata a mezzo stampa) di un documento informatico. In questo caso, passando da un documento informatico digitalmente sottoscritto ad uno analogico, viene a perdersi la cosiddetta "catena del valore" della firma digitale, pertanto è necessario che la conformità all'originale sia attestata da un pubblico ufficiale a ciò autorizzato. Tuttavia, se la copia è conforme alle vigenti regole tecniche, anche con riguardo alle disposizioni sulla conservazione dell'originale informatico, è sufficiente che la conformità all'originale non sia espressamente disconosciuta, ex art. 23, comma 2, del CAD.

Per quanto riguarda le copie analogiche di documenti amministrativi informatici, il comma 5, dell'art. 23-ter, del CAD, lascia la possibilità di apporre a stampa sulle copie analogiche un contrassegno elettronico, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. In alternativa all'uso del contrassegno elettronico, si può fare ricorso a quanto previsto dall'art. 3, del D.Lgs. 12 febbraio 1993, n. 39, col quale si dispone che gli atti amministrativi prodotti con sistemi informatici o telematici, nel pieno controllo dell'amministrazione, possono essere accompagnati, per la loro validità, dall'indicazione a stampa della fonte e del nominativo del soggetto responsabile, nonché dell'eventuale dicitura che specifica che il documento informatico da cui la copia analogica è tratta è stato prodotto ed è conservato dall'amministrazione secondo le regole tecniche previste dal CAD.

L'art. 23-bis, del CAD, si occupa dei duplicati e delle copie informatiche di documenti informatici. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se sono prodotti mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la stessa sequenza di bit del documento informatico di origine. Il comma 2, dell'art. 23-bis, in commento, si occupa delle copie e degli estratti informatici del documento informatico. Diversamente, un estratto di un documento informatico si realizza quando in un "nuovo" documento si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti informatici in possesso di una pubblica amministrazione. In questi casi, se la copia o l'estratto informatico di un documento informatico sono prodotte in conformità alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale da cui sono tratte solo qualora la loro conformità all'originale, in tutte le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Le regole tecniche stabiliscono che la copia e gli estratti informatici di un documento informatico devono essere prodotti:

- attraverso l'utilizzo di uno dei formati idonei (ad esempio: PDF, PDF/A, TIFF, JPG, OOXML, ODF, XML, ecc.);
- mediante processi e strumenti che assicurino la corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine;
- o previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia.

La copia o l'estratto di uno o più documenti informatici così realizzato, se sottoscritto con firma digitale o firma elettronica qualificata da chi effettua la copia ha la stessa efficacia probatoria dell'originale, salvo che la conformità allo stesso non sia espressamente disconosciuta.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o dell'estratto informatico di un documento informatico può essere inserita nel documento informatico contenente la copia o l'estratto. Il documento informatico così formato è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può anche essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

1.9 I fascicoli informatici e loro gestione negli archivi digitali

Come noto, la formazione dei fascicoli e delle altre aggregazioni di documenti[25] è strettamente legata allo svolgimento quotidiano delle attività di un organismo pubblico. Il fascicolo, infatti, consolida e fotografa tutto ciò che una pubblica amministrazione ha effettivamente prodotto nel corso della sua attività. L'elevata quantità e la complessità della documentazione prodotta all'interno di un'organizzazione complessa, quale è quella di una pubblica amministrazione, implica la necessità di ricorrere a sistemi di classificazione e fascicolazione in grado di garantire, fra l'altro, un rapido rinvenimento dei documenti.

L'art. 65, del D.P.R. 28 dicembre 2000, n. 445, stabilisce che lo stesso sistema per la gestione dei flussi documentali, oltre a possedere i requisiti indicati all'art. 52, deve:

a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;

b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento.

La regola generale è che ogni documento deve essere individuato attraverso un'apposita e puntuale classificazione per poi essere inserito necessariamente in un fascicolo. Dal punto di vista pratico, attraverso l'attività di classificazione e fascicolazione[26] dovrà essere attribuito a ciascun documento un indice (indice di classificazione) desunto da una struttura di voci (piano

25 Per aggregazione documentale informatica si intende "l'aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente".

26 Classificazione e fascicolazione non devono essere confuse, avendo diversa natura e funzione: la prima fornisce una struttura logica, la seconda aggrega i documenti.

di classificazione) per poi essere associato ad un fascicolo (unità archivistica). Questa attività ha l'obiettivo di ordinare i documenti cartacei in modo fisico e i documenti informatici in modo logico, nonché il loro inserimento in un sistema di gestione documentale in grado di governare i processi/procedimenti amministrativi nel corso dei quali i documenti sono prodotti o acquisiti. Possiamo quindi definire fascicolo, l'insieme ordinato di documenti, riferiti in modo stabile a uno stesso affare/procedimento/processo amministrativo, a una stessa materia, a una stessa tipologia, che si forma sempre nel corso delle attività amministrative dell'ente, allo scopo di riunire, a fini decisionali o informativi, tutti i documenti utili allo svolgimento di tali attività e in grado di garantire la conservazione delle relazioni tra i documenti in esso contenuti.

L'allegato 1, al DPCM 13 novembre 2014, definisce il fascicolo informatico una *"Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del CAD".* Dalla richiamata definizione si evince che l'aggregazione dei documenti in fascicoli deve essere:

a) strutturata, ossia deve basarsi su tecnologie, infrastrutture e soluzioni concepite e realizzate a tale scopo;

b) governata da precise regole e criteri in grado di assicurare uniformità nella gestione dei documenti informatici;

c) idonea a garantire l'organicità, le funzioni e le finalità dell'archivio.

Diventa irrinunciabile avvalersi di specifici programmi informatici in grado, ad esempio, di mettere a disposizione dell'utente specifiche funzioni capaci di classificare/organizzare i fascicoli:

- per oggetto (materia o nominativo),
- per processo o per procedimento, (in questo caso il fascicolo include tutti i documenti [ricevuti, spediti o interni] relativi a un procedimento o a una specifica attività, che può coincidere con la gestione di un vero e proprio procedimento amministrativo),
- per tipologia o forma del documento, (in questo caso il fascicolo include un insieme ordinato di documenti sciolti, raggruppati in base alla loro tipologia o forma secondo criteri predefiniti).

L'obiettivo è quello di realizzare un sistema in grado di indicizzare, ordinare ed organizzare funzionalmente i documenti informatici in fascicoli affinché risulti agevole la loro ricerca ed il loro reperimento ottemperando, al contempo, anche alle esigenze di natura operativa, organizzativa ed archivistica. Nel ridisegnare/reingegnerizzare i processi, quindi, può risultare fondamentale coinvolgere, gli utenti che saranno chiamati ad utilizzare il sistema. I fascicoli

informatici, in quanto parte del sistema di gestione informatica dei documenti, sono unità fondamentali dell'archivio di un ente, pertanto la loro corretta formazione e gestione deve essere garantita, specialmente in ambiente digitale, dove i documenti informatici sono privi della consistenza materiale della carta. Le modalità di attribuzione o, meglio, di associazione dei documenti ai rispettivi fascicoli, è una prerogativa di ogni singolo ente che a tal fine dovrà definire adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo. Tuttavia, tenuto conto del disposto di cui all'art. 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445, dovranno essere adottati principi di coerenza funzionale nell'ambito di ciascuna area organizzativa omogenea.

Per quanto riguarda la formazione, il comma 2-bis, dell'art. 41, del CAD, il fascicolo informatico deve:

- garantire la possibilità di essere direttamente consultato;
- garantire la possibilità di essere alimentato da tutte le amministrazioni coinvolte nel procedimento;
- essere formato, identificato e utilizzato in conformità ai principi di corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico (DPCM 13 novembre 2014), ivi comprese le regole concernenti il protocollo informatico (DPCM 3 dicembre 2013), ed il sistema pubblico di connettività;
- rispettare i criteri di interoperabilità e di cooperazione applicativa;
- poter contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati;
- essere formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto e alle finalità dei singoli documenti;
- essere realizzato in modo da garantire l'esercizio in via telematica dei diritti previsti in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.

All'atto della sua costituzione, al fascicolo informatico deve essere associato un *"insieme minimo di metadati",* riconducibile alle seguenti informazioni:

a) l'identificativo univoco e persistente;
b) l'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
c) le altre amministrazioni partecipanti all'iter del procedimento;
d) il Responsabile del procedimento (nome, cognome e codice fiscale);
e) l'oggetto del procedimento;

f) l'elenco dei documenti contenuti, salvo il caso in cui il fascicolo contenga aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati.

Oltre al set minimo di metadati espressamente richiesto dall'art. 41, comma 2-ter, del CAD, è opportuno associare ad ogni fascicolo informatico anche le seguenti ulteriori informazioni:

- data di apertura (o di istruzione);
- data di chiusura;
- i riferimenti di classificazione;
- le coordinate geografiche della posizione fisica dei fascicoli cartacei dove sono contenuti gli originali analogici riconducibili al fascicolo informatico;
- i riferimenti (*link*) ad altri documenti informatici, con la possibilità di accedervi;
- i riferimenti (*link*) ad altri fascicoli corrispondenti a procedimenti connessi a quello oggetto del fascicolo principale, con la possibilità di accedervi;
- i riferimenti (*link*) ad eventuali sotto-fascicoli.

In ogni caso, l'ente produttore dovrà preliminarmente effettuare un'adeguata analisi delle proprie esigenze organizzative e funzionali e poi decidere una struttura predefinita di metadati e la loro quantità.

In questa fase di "passaggio" dall'analogico al digitale, il sistema dovrà essere in grado di gestire tre distinte situazioni dove saranno presenti:

a) solo documenti nativi digitali: in questo caso il fascicolo raggruppa solo documenti informatici prodotti e gestiti in formato digitale;
b) documenti sia informatici che analogici - situazione ibrida: è l'ipotesi in cui i fascicoli sono composti sia da documenti prodotti su supporto cartaceo che da documenti nativi digitali;
c) documenti solo analogici: in questa circostanza esiste solo il tradizionale fascicolo cartaceo.

In ambito informatico, la consultazione di un fascicolo elettronico avviene attraverso la presentazione (a video o a stampa) dei metadati che lo identificano, ne descrivono il contesto di produzione e lo collegano al titolario di classificazione. A queste informazioni si aggiungono quelle relative ai documenti associati al fascicolo e alle informazioni che descrivono i flussi documentali e i flussi di lavoro che hanno interessato il fascicolo. È necessario prevedere specifiche funzioni in grado di accedere ai singoli documenti informatici e di rappresentare (a video o in stampa) il loro contenuto in un forma leggibile all'uomo. Come avviene per il documenti informatici, anche i fascicoli e le aggregazioni documentali in genere, al termine della loro gestione corrente, devono essere trasferiti in un sistema di conservazione "a norma", ossia realizzato in conformità a quanto stabilito dal CAD e dalle regole tecniche. A tal fine, l'art. 15, del DPCM 13 novembre 2014, stabilisce che il Responsabile della gestione

documentale, ovvero, ove nominato, il coordinatore della gestione documentale deve stabilire, per le diverse tipologie di fascicoli, in conformità con le norme vigenti in materia, con il sistema di classificazione e con il piano di conservazione, i tempi entro cui i documenti debbono essere versati in conservazione.

2. La conservazione dei documenti e dei fascicoli informatici

2.1 Cosa significa conservare

Conservare documenti è una funzione essenziale insita nella produzione documentale stessa.

La produzione di documenti implica infatti la conservazione degli stessi nel tempo. Lo storico Jacques Le Goff ha definito il documento come *"una cosa che resta"*[27], cioè è prodotta proprio per essere conservata nel tempo e resa disponibile a chi ha interesse a conoscere l'atto o il fatto rappresentato nel documento.

Nella normativa italiana tale concetto fondamentale è declinato e normato in maniera differente per documenti prodotti o acquisiti dalla pubblica amministrazione, rispetto a documenti prodotti o acquisiti da privati. La conservazione dei documenti rappresenta per le pubbliche amministrazioni una funzione di carattere istituzionale. Esse sono infatti tenute per legge a conservare i propri documenti e archivi sia come testimonianza diretta delle loro azioni al servizio della collettività che come memoria storica, in quanto gli archivi e i documenti degli enti pubblici sono beni culturali[28].

La normativa in materia di archivi e documenti pubblici è stata sempre ispirata al principio della salvaguardia della documentazione prodotta dalla pubblica amministrazione, tutelata come bene culturale e individuata come rappresentativa di atti o fatti giuridicamente rilevanti. L'obbligo di conservazione dei documenti d'archivio è inteso a salvaguardare diritti soggettivi,

27 J. Le Goff, Storia e memoria, Torino, Einaudi, 1977, pag. 454.

28 In un testo di archivistica si legge: "Ogni persona che appartiene ad una Comunità ha il diritto di conoscere come la Comunità viene gestita e per soddisfare tale esigenza deve poter conoscere, attraverso la documentazione prodotta, quali sono state le operazioni poste in essere . La conservazione è quindi un preciso impegno di coloro che svolgono compiti attivi e di coordinamento all'interno dei soggetti pubblici… anche per l'esigenza di un rispetto dei diritti della collettività" [Antonio Romiti Archivistica generale, Civita Editoriale , Lucca 2003, p. 44. Tale affermazione è ribadita dalla recente legge 7 agosto 2015 n. 124, art. 7 comma 1 lettera h) : "riconoscimento della libertà di informazione attraverso il diritto di accesso, anche per via telematica, di chiunque, indipendentemente dalla titolarità di situazioni giuridicamente rilevanti, ai dati e ai documenti detenuti dalle pubbliche amministrazioni, salvo i casi di segreto o di divieto di divulgazione previsti dall'ordinamento e nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati, al fine di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche".

interessi legittimi, il diritto d'accesso, la ricerca a fini storici, culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico.

Il Codice dei beni culturali (D.Lgs. 22 gennaio 2004, n. 42 e s.m.i.) definisce senza alcuna distinzione cronologica tutti *"gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico"* (art. 10, comma 2 lett. b), come beni culturali, cioè testimonianze aventi valore di civiltà, facenti parte del patrimonio culturale tutelato e valorizzato in attuazione dell'art. 9 della Costituzione. La tutela e la valorizzazione del patrimonio culturale concorrono a preservare la memoria della comunità nazionale e a promuovere lo sviluppo della cultura. Lo Stato, le regioni e gli altri enti territoriali debbono assicurare e sostenere la conservazione di tale patrimonio e ne favoriscono la pubblica fruizione. In particolare gli enti citati ed ogni altro ente pubblico hanno l'obbligo di conservare i propri archivi nella loro organicità e di ordinarli (art. 30, comma 4). Il significato di "ordinare" comprende due aspetti: obbliga a predisporre mezzi e procedure perché l'archivio corrente nasca ordinato, quindi ci siano procedure per la corretta formazione ed aggregazione dei documenti e per l'altro aspetto impone di ordinare l'archivio già esistente ove si trovi in stato di disordine.

Questo ultimo aspetto risulta particolarmente complesso nel caso di documentazione informatica, che deve quindi essere correttamente e ordinatamente gestita fin dal momento della produzione per garantirne una corretta conservazione nel tempo. È stato notato che la documentazione informatica è molto meno resiliente di quella tradizionale in caso di abbandono e trascuratezza.

Inoltre l'art. 53 del Codice dei beni culturali stabilisce che i beni culturali appartenenti allo Stato, alle regioni e agli altri enti territoriali rientranti, come gli archivi, nelle tipologie indicate all'art. 822 del codice civile costituiscono il demanio culturale. Come tali gli archivi e i singoli documenti degli enti pubblici in base al successivo art. 54 sono beni inalienabili e non possono formare oggetto di diritti a favore di terzi, ma possono solo essere oggetto di trasferimento tra lo Stato, le regioni e gli altri enti pubblici territoriali ed essere utilizzati ai fini di fruizione e valorizzazione pubblica secondo le modalità stabilite dal titolo II del Codice dei beni culturali.

In particolare deve essere garantito un accesso gratuito per finalità di lettura, studio e ricerca, soprattutto per scopi storici, regolamentando anche la consultazione degli archivi correnti (art. 124).

In ogni caso, come obbligo conservativo è previsto l'obbligo di inventariare i propri archivi storici (art. 30). Tutto quanto detto vale a prescindere dalla forma e dal supporto dei documenti quindi ha pieno valore anche per i documenti informatici. Le regole del codice dei beni culturali sono applicabili anche ad archivi privati dichiarati di rilevante interesse storico.

Nel caso invece di soggetti privati generalmente intesi, quali società o individui che svolgono una attività economica, il principio generale di conservazione deriva dalle norme del codice civile sulla tenuta della corrispondenza e delle scritture contabili, in particolare l'art. 2214, che impone di *"conservare ordinatamente per ciascun affare"* la corrispondenza ricevuta e spedita oltre alle fatture e alle scritture contabili. Gli articoli 2220 e 2312 specificano che le scritture e i documenti devono essere conservate per dieci anni *"dalla data dell'ultima registrazione"* o a decorrere dalla cancellazione della società dal registro delle imprese. Ai soggetti privati si applicano ovviamente tutte le norme in materia di conservazione di documenti a rilevanza fiscale o tributaria.

L'art. 43 del CAD stabilisce che i documenti informatici di cui è prescritta la conservazione per legge o regolamento sono conservati *"in modo permanente con modalità digitali"* nel rispetto delle regole tecniche. Pertanto la produzione di documenti informatici implica anche la loro conservazione in modalità informatica e pone in evidenza la necessità di evolvere la tradizionale funzione conservativa dei documenti in modalità idonee a conservare i documenti informatici con sistemi informatici. La conservazione costituisce un fattore fondamentale per la sostenibilità del processo di dematerializzazione, a garanzia che documenti e informazioni in formato digitale siano conservati nel lungo periodo, in modo autentico e accessibile, come avviene per i documenti cartacei. Se non ci fosse la garanzia che i documenti digitali prodotti siano conservati e resi accessibili nel lungo termine, infatti, non sarebbe possibile ipotizzare una reale diffusione del processo di dematerializzazione. La realizzazione di archivi accessibili e strutturati, con la messa a disposizione dell'enorme patrimonio informativo della PA, costituisce, quindi, uno strumento indispensabile per tutte le pubbliche amministrazioni. La conservazione dei documenti informatici rientra quindi a pieno titolo nella funzione essenziale di mantenimento nel tempo dei documenti con alcune specifiche peculiarità, che derivano dalle caratteristiche del documento informatico stesso.

In estrema sintesi si può ricordare che nel caso dei documenti informatici il contenuto non può essere letto e compreso direttamente ma - essendo rappresentato da simboli digitali - deve essere decodificato mediante specifiche risorse di calcolo (hardware e software). Tali risorse sono determinate da una costante evoluzione tecnologica che può ostacolare la conservazione dei documenti elettronici rendendone difficile la leggibilità nel tempo. Cambia inoltre il rapporto tradizionale tra contenuto e supporto, non più legati da un nesso fisico, ma collegati solo logicamente. Il supporto per quanto piccolo deve sempre essere presente ma può mutare senza incidere sul contenuto. Se la conservazione dei documenti tradizionali (cartacei o su altro supporto: tavolette di argilla, papiro, pergamena, pietra ecc.) si basa essenzialmente sul mantenimento inalterato nel tempo del supporto e dei segni su di esso apposti, organizzati in modo da poterne comprendere il contenuto in relazione al contesto giuridico-amministrativo di produzione, la conservazione dei documenti informatici deve affrontare la sfida di mantenere

nel tempo oggetti che richiedono una molteplicità di strumenti e risorse tecniche di mediazione per essere letti e compresi dall'uomo, ma anche da altri sistemi. Sono inoltre necessarie informazioni ulteriori per ricostruirne la provenienza e valutarne l'autenticità e l'integrità.

Le risorse digitali per loro natura sono soggette a un continuo, più o meno frequente, ma comunque inevitabile processo di trasformazione che ne consente l'accesso nel tempo, ma implica rischi gravi di perdite e manipolazioni. Conservare documenti e archivi informatici deve evolversi da un modello di conservazione passiva o inerte, anche se sono sempre presenti idee di risolvere il problema con la scoperta di supporti per il digitale di lunghissima durata, ad un modello di conservazione attiva basato su un sistema complessivo dedicato alla conservazione. Si può quindi dire che in ambiente digitale l'attenzione della conservazione deve spostarsi dal supporto al contenuto e sono necessarie attive politiche ed efficienti pratiche per conservare e tramandare documenti informatici garantendo nel lungo termine il mantenimento del valore giuridico, delle caratteristiche di integrità ed autenticità e nel contempo il loro accesso, la loro leggibilità e intelligibilità nel contesto di relazioni e vincoli originari. La conservazione in ambiente digitale è dunque una funzione attiva e continua nel tempo che deve iniziare fin dalla nascita stessa dei documenti. La conservazione deve prevedere sia la cosiddetta conservazione dei *bit* (*Bit preservation*), cioè la capacità di accedere ai *bit* come erano stati originariamente registrati, anche in caso di degrado del supporto, di obsolescenza dell'*hardware* e/o disastri di sistema, ma soprattutto la conservazione logica (*Logical preservation*) intesa come la capacità di comprendere e utilizzare l'informazione in futuro, conservando il contenuto intellettuale anche in presenza di futuri cambiamenti tecnologici e di conoscenza. Deve supportare il tracciamento della provenienza dei documenti e la garanzia della loro autenticità e integrità.

Accanto ai molti vantaggi in termini, per esempio, di capacità di ricerca e di riproduzione, la diffusione delle tecnologie digitali in ogni campo porta certi svantaggi. La rapida obsolescenza delle tecnologie digitali crea considerevoli pericoli tecnici, in particolare un maggiore rischio rispetto al passato di perdita della possibilità di recuperare, restituire o interpretare informazioni.

Non sarebbe saggio considerare il problema solo dal lato tecnico. Ci sono anche elementi organizzativi, legali, industriali, scientifici e culturali che devono essere considerati. Ignorare i problemi generati dalla conservazione delle informazioni in formato digitale condurrà inevitabilmente alla perdita di tali informazioni. Come ricorda un testo sulla conservazione della memoria digitale, con lo sviluppo dei documenti informatici e dei sistemi informatici di gestione documentale si può affermare che: in conclusione, con il passare del tempo, con un'accelerazione sempre maggiore e grazie proprio agli strumenti usati per registrare le informazioni, si è avuta sempre maggior facilità di produzione delle informazioni, una sempre maggior capacità di trasferirle, di renderle disponibili, di duplicarle e di integrarle. Di contro, la

possibilità di perderle, o di veder alterata (per qualunque motivo) l'informazione originale, diventa sempre più probabile[29].

2.2 Obiettivi, processi e strumenti della conservazione

La conservazione dei documenti e dei fascicoli informatici è dunque l'attività volta a proteggere e mantenere, cioè custodire, nel tempo gli archivi di documenti e dati informatici. Il tempo di conservazione, come ricordato dall'art. 43 del CAD può essere "permanente", cioè indefinito nel futuro o come viene spesso indicato "a lungo termine", cioè un arco temporale sufficientemente ampio da essere interessato da cambiamenti tecnologici[30]. Il suo obiettivo primario è di impedire la perdita o la distruzione non autorizzata dei documenti e di mantenere nel tempo le loro caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità. Per fare ciò è necessario offrire effettive garanzie di mantenimento delle caratteristiche dei documenti che assicurano il valore di fonte attendibile e di prova giuridicamente rilevante, avendo la capacità di dimostrare in sede giuridica che il processo conservativo è stato correttamente eseguito e il risultato è stato realmente conseguito. La sfida è garantire che in un futuro anche lontano i documenti informatici prodotti oggi possono continuare ad essere letti e utilizzati assicurando il loro valore giuridico e la loro corretta collocazione nell'ambito dell'archivio dei soggetti produttori.

Le caratteristiche sopra riportate sono definite nel glossario allegato alle regole tecniche emanate con i DPCM 3 dicembre 2013 e 13 novembre 2014.

Per riassumere in breve si può dire che:

- Autenticità: è la caratteristica di un documento informatico che fornisce la garanzia che il documento sia ciò che dichiara di essere, senza avere subito alterazioni o modifiche. Insieme di identità (identificazione e provenienza) e integrità;
- Integrità: è la qualità di un documento di essere completo e inalterato, cioè non avere subito modifiche non autorizzate;
- Affidabilità: esprime il livello di fiducia che l'utente, cioè colui che legge il documento ripone, o può riporre nel documento informatico, in particolare nella sua visualizzazione leggibile allo stesso;

29 Vincenzo Gambetta, La conservazione della memoria digitale, Collana Siav di Minigrafie, 2009. Tale conclusione risulta quanto mai simile alle parole che troviamo nel testo di Eugenio Casanova, Archivistica, Siena 1928: "In progresso di tempo, le ulteriori generazioni si appigliarono a sostanze, fossero più fragili, ma meglio rispondenti all'attività sempre più febbrile che veniva impossessandosi dell'umanità". Nello stesso testo si legge che "la conservazione degli atti corrisponde ad un bisogno innato dell'unanimità, bisogno che l'ignoranza potrà calpestare, ma sopprimere non mai" (p. 505). Lo stesso Casanova sottolinea anche che "La conservazione degli atti in archivio … ha uno scopo positivo, ben determinato, tangibile, vale a dire quello di renderli utili alla generalità degli individui e agli individui stessi" (p. 21).

30 In coerenza con la definizione di "lungo termine" data nello standard ISO 14721, relativo al modello OAIS di sistema informativo aperto per l'archiviazione.

- Leggibilità: è la caratteristica che definisce il mantenimento della fruibilità delle informazioni contenute nel documento durante l'intero ciclo di gestione dei documenti, cioè al momento della sua formazione o produzione, nella sue forme di diffusione, nella sua memorizzazione e archiviazione e nella sua conservazione; in certi casi si può distinguere tra leggibilità da parte di sistemi informatici o leggibilità da parte di un essere umano;
- Reperibilità: esprime la capacità di reperire ed esibire il documento con le caratteristiche sopra riportate.

Quindi un documento correttamente conservato deve essere reperibile ed avere le caratteristiche di autenticità, integrità, affidabilità e leggibilità.

In una prima fase l'attenzione conservativa dei documenti informatici si è concentrata soprattutto sul tema della integrità, intesa come mantenimento della immodificabilità della sequenza di bit originari, fidando soprattutto su tecniche quali la firma digitale e sul mantenimento di supporti non riscrivibili.

Si è compreso successivamente che tali azioni, se a breve termine garantivano il mantenimento dei documenti, proteggendoli da manipolazioni e alterazioni, non erano sufficienti per garantire una corretta conservazione permanente o nel lungo termine poiché non assicuravano il mantenimento della reperibilità, affidabilità e leggibilità degli oggetti conservati, rendendo in certi casi difficile anche verificarne l'autenticità soprattutto in rapporto al contesto di provenienza.

Il problema conservativo non era risolvibile con il solo mantenimento dell'immodificabilità dei singoli documenti, ma doveva allargarsi al mantenimento delle aggregazioni documentali e delle informazioni di contesto di produzione dei documenti. Tale consapevolezza ha trovato la sua prima definizione nell'art. 44 del CAD che ha introdotto il concetto di "sistema di conservazione", definendolo come sistema che deve assicurare:

- l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento, quindi identificazione della provenienza per valutarne le caratteristiche di autenticità;
- l'integrità del documento;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari, quindi dei metadati associati ai documenti e la definizione delle aggregazioni documentali e delle articolazioni d'archivio di riferimento;
- il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D. Lgs. 30 giugno 2013, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Un sistema è un insieme di persone, apparecchiature, applicazioni e procedure dedicate in questo caso ad assicurare la conservazione, anche nel lungo termine, dei documenti e delle aggregazioni documentali informatiche, con i rispettivi metadati garantendo il mantenimento delle caratteristiche sopra citate.

Nello specifico grande rilevanza hanno le regole e le procedure che si applicano, la professionalità delle persone addette e la qualità, in particolare in termini di robustezza, sicurezza ed affidabilità, delle tecnologie applicate.

Questo concetto è stato sviluppato nel DPCM 3 dicembre 2013 contenente le Regole tecniche in materia di sistema di conservazione che ha esplicitamente definito che gli oggetti della conservazione, per i quali il sistema di conservazione deve garantire, dalla presa in carico dal produttore, le caratteristiche sopracitate, sono:

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati;

Tali oggetti, conformemente allo standard OAIS sono trattati dal sistema in pacchetti informativi distinti in: pacchetti di versamento (*Submission Information Package*, SIP)[31], pacchetti di archiviazione (*Archival Information Package*, AIP)[32], pacchetti di distribuzione (*Dissemination Information Package*, DIP)[33].

Tali pacchetti secondo il modello OAIS sono entità composte di quattro elementi:

- il contenuto informativo, cioè l'oggetto da conservare, il quale comprende: l'oggetto dati (*data object*) e l'insieme delle informazioni che ne permettono la rappresentazione e la comprensione (*representation information*);
- le informazioni sulla conservazione (*preservation description information*);
- le informazioni sull'impacchettamento;
- le informazioni descrittive sul pacchetto utilizzate per ricercare il pacchetto.

In sintesi si può dire che la conservazione di un contenuto informativo presuppone la formazione e il mantenimento di un pacchetto informativo che, oltre al contenuto, contiene i metadati che lo identificano, lo qualificano sotto il profilo dell'integrità e lo collocano nel contesto di provenienza.

31 Il pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione.

32 Il pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3 dicembre 2013 secondo le modalità riportate nel manuale di conservazione.

33 Il pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta.

Per conservare la memoria digitale occorre dunque avere attenzione non soltanto agli oggetti digitali, intesi come sequenze di bit, ai formati elettronici e ai requisiti di validità di natura giuridica, ma anche all'insieme dei metadati da valorizzare per rendere evidenti le caratteristiche documentali e il *"vincolo archivistico"* rappresentato dall'insieme delle relazioni logiche e formali che esistono tra i documenti di un archivio. Le funzioni dei metadati per la conservazione degli archivi vanno dall'identificazione permanente degli oggetti e delle loro relazioni, alla memorizzazione dei meccanismi tecnici e procedurali di formazione, tenuta e conservazione, ai privilegi di accesso, alle logiche di selezione, alla descrizione del contesto di produzione e di successiva custodia e conservazione. Il numero e la varietà degli standard e degli insiemi di metadati testimoniano la difficoltà di definire un *set* applicabile in qualsiasi contesto e a qualsiasi tipologia. Le relazioni tra oggetti da conservare e metadati appaiono assolutamente necessarie quanto particolarmente complesse, articolate e dinamiche.

La conservazione inoltre va inquadrata in una visione sistemica più ampia che ricomprende il produttore, cioè, in termini archivistici, il soggetto che ha prodotto l'archivio, costituito dai documenti ricevuti o prodotti nel corso della sua attività, e gli utenti, cioè coloro che richiedono di fruire delle informazioni di interesse conservate. Infatti per poter garantire la conservazione della memoria digitale è necessario che già in fase di produzione e di gestione documentale corrente vengano rispettati alcuni requisiti fondamentali, quali l'utilizzo di formati idonei e corrette azioni di gestione documentale, quali identificazione e registrazione dei documenti e loro organizzazione in base al piano di classificazione e fascicolazione. Una visione conservativa orientata agli utenti permette di valutare le necessità di reperibilità e leggibilità, con garanzia di autenticità ed integrati, dei futuri utenti dei documenti prodotti e conservati.

Nel modello OAIS si definisce un "*Open Archival information System*" come un archivio, inteso come struttura organizzata di persone e sistemi che accetta la responsabilità di conservare informazioni e renderle disponibile ad una Comunità di riferimento, garantendo che l'informazione conservare sia comprensibile in maniera autonoma da detta comunità di utenti, che quindi deve essere messa in grado di comprendere anche in futuro le informazioni conservate senza conoscere o avere assistenza da chi le ha prodotte.

In questo quadro si comprende come i pacchetti di versamento siano il modo di trasferire gli oggetti da conservare dal produttore, in particolare dal suo sistema di gestione documentale, al sistema di conservazione e i pacchetti di distribuzione siano la modalità di esibizione agli utenti degli oggetti conservati. Nelle logiche di conservazione tali pacchetti sono distinti perché per rendere disponibile e comprensibile in maniera autonoma un oggetto conservato il sistema di conservazione potrebbe dover compiere delle operazioni che vanno oltre lo statico mantenimento dei pacchetti di versamento, ma possono prevedere azioni di migrazione, cioè di produzione di copie per adeguare il formato dei documenti a formati conservabili e leggibili in futuro. Deve inoltre produrre metadati e informazioni a testimonianza del corretto svolgimento

del processo di conservazione per garantire il mantenimento del valore giuridico degli oggetti conservati e corredare il pacchetto di distribuzione di ulteriori informazioni per rendere l'oggetto conservato comprensibile in maniera autonoma. Tali azioni possono essere ricomprese anche nella preparazione del pacchetto di archiviazione conservato nel sistema di conservazione. Viene quindi a delinearsi un processo conservativo digitale che si può articolare in tre macro fasi:

- formazione della memoria digitale presso il soggetto produttore;
- trasferimento degli oggetti da conservare dal soggetto produttore al conservatore;
- conservazione, accesso e fruizione del patrimonio informativo e documentale conservato.

La formazione degli oggetti da conservare (documenti informatici e aggregazioni documentale informatiche) presso il soggetto produttore deve avvenire in un sistema di gestione documentale che rispetti la normativa e garantisca l'applicazione di idonei strumenti archivistici (piano di classificazione, piano di conservazione, manuale di gestione), garantendo la corretta formazione degli oggetti da conservare. Particolare attenzione deve essere dedicata alla memorizzazione in formati idonei alla conservazione e alla valutazione degli oggetti da conservare nell'ottica di un archivio unico, strutturato secondo una logica condivisa da tutta l'organizzazione, evitando o opportunamente monitorando, la produzione di oggetti digitali in diversi sistemi. Il trasferimento al conservatore deve avvenire a seguito di specifici accordi tra produttore e conservatore che definiscano, oltre alle rispettive responsabilità, le tipologie dei documenti e degli oggetti informatici da conservare, stabilendo in particolare le modalità di preparazione e trasmissione del pacchetto di versamento.

Occorre inoltre stabilire il momento in cui eseguire il trasferimento, garantendo da un lato il mantenimento delle caratteristiche di integrità e validità giuridica dei documenti e dall'altro la completezza delle aggregazioni documentali. La prima esigenza spinge ad azioni di trasferimento molto precoci e ravvicinate al momento di formazione dei documenti, mentre la seconda porta a momenti potenzialmente molto più lontani. Bisogna inoltre tenere conto in certi casi dei tempi definiti dalla normativa, sia per garantire la sicurezza delle informazioni che il rispetto di norme fiscali e tributarie.

Una possibile soluzione potrebbe essere quella di eseguire il trasferimento in due tempi: le unità documentarie con i relativi metadati prima che rischino di subire trattamenti non idonei o perdano alcune caratteristiche di validità giuridica, a causa ed esempio di scadenza o revoca di certificati di firma, o rischino di subire gli effetti della obsolescenza tecnologica; le unità archivistiche (fascicoli e serie o altre aggregazione documentali informatiche) con l'insieme dei metadati che le identificano e le organizzano rispetto alle attività del soggetto produttore quando sono chiuse e complete. In questo caso il sistema di conservazione dovrà avere

opportune funzionalità che permettano di ricomporre i vincoli tra unità documentarie e unità archivistiche per poter fornire una visione unitaria, organica e senza duplicazioni del complesso archivistico che viene a formarsi.

Il trasferimento dovrà essere svolto utilizzando canali di comunicazioni efficienti, sicuri e riservati. La fase della conservazione e quello che le regole tecniche identificano come processo di conservazione inizia con l'acquisizione e la presa in carico da parte del conservatore dei pacchetti di versamento trasferiti dai produttori. L'acquisizione e la presa in carico dei pacchetti di versamento implicano la necessità di opportune verifiche che gli oggetti contenuti e i metadati siano coerenti con quanto concordato e che non vi siano anomalie o errori. Al termine della fase di acquisizione verrà preparato il pacchetto di archiviazione, da cui poi deriveranno i pacchetti di distribuzione. Tale processo, oltre alla struttura organizzativa e tecnologica, ai soggetti coinvolti, agli oggetti da conservare deve essere descritto nel manuale di conservazione, da redigere nel rispetto delle regole tecniche.

La funzione di conservazione non è quella di mantenere inalterate nel tempo le sequenze binarie degli oggetti trattati, ma soprattutto quella di assicurare nel tempo la possibilità di accesso e fruizione. In prospettiva dunque il sistema di conservazione dovrà sempre più offrire idonee funzionalità per soddisfare le richieste di consultazione e di esibizione in primo luogo dei produttori e sempre più in futuro dei cittadini, studiosi e altri portatori d'interesse. Per la memoria digitale pubblica dovrà essere garantita in futuro il massimo livello di consultabilità nel rispetto delle norme sulla tutela dei dati personali e della riservatezza. In particolare dovrà essere garantita la confrontabilità dei documenti e degli archivi secondo le norme del Titolo II, Capo III del Codice dei Beni Culturali. La conservazione dovrà infatti giungere a costituire per le pubbliche amministrazione gli archivi storici del futuro e garantire la piena fruizione e valorizzazione del patrimonio documentale conservato.

3. Organismi di tutela e vigilanza

3.1 Descrizione del ruolo, della struttura e delle funzioni del Ministero dei beni e delle attività culturali e del turismo

Il Ministero per i Beni Culturali e Ambientali fu istituito, con D.L. 14 dicembre 1974, n. 657, convertito dalla Legge 29 gennaio 1975, n. 5 - G.U. 14 febbraio 1975, n. 43, con il compito di affidare unitariamente alla specifica competenza di un dicastero appositamente costituito la gestione del patrimonio culturale e dell'ambiente al fine di assicurare l'organica tutela di interesse di estrema rilevanza sul piano interno e nazionale. (Organizzazione del Ministero per i beni culturali e ambientali con D.P.R. 3 dicembre 1975 n. 805). Raccolse le competenze e le funzioni in materia di Archivi di Stato del Ministero degli Interni, anche se con il DPCM 29 agosto 2014, n. 171 è possibile ricostruire l'organigramma del Ministero che vede alle sue

direttе dipendenze, a livello centrale, le dodici direzioni generali, che comprendono, tra le altre la Direzione Generale Archivi.

Oggi il Ministero per i beni e le attività culturali e del turismo (MIBACT) esercita funzioni di tutela e vigilanza dei sistemi di conservazione degli archivi di enti pubblici o di enti privati dichiarati di interesse storico particolarmente importante e autorizza le operazioni di scarto e trasferimento della documentazione conservata ai sensi del D.Lgs 22 gennaio 2004, n. 42[34].

La tutela e vigilanza sugli archivi di enti pubblici non statali è esercitata dal MIBACT, tramite le Soprintendenze archivistiche competenti per territorio. "*Lo spostamento, anche temporaneo dei beni culturali mobili"* compresi gli archivi storici e di deposito è soggetto ad autorizzazione della Soprintendenza archivistica (D.Lgs 22 gennaio 2004, n. 42, art. 21, comma 1, lett. b). Anche "*Il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi di privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13"*, sia che comporti o non comporti uno spostamento, rientra tra gli interventi soggetti ad autorizzazione della Soprintendenza archivistica (D.Lgs 22 gennaio 2004, n. 42, art.21, comma 1, lett. e).

La disposizione si applica anche:

- all'affidamento a terzi dell'archivio (*outsourcing*), ai sensi del D.Lgs 22 gennaio 2004, n. 42, art.21, comma 1, lett. e);
- al trasferimento di archivi informatici ad altri soggetti giuridici, nell'ottica della conservazione permanente sia del documento sia del contesto archivistico[35].

Per richiedere tale autorizzazione, da presentare in ogni caso prima dell'affidamento del servizio di conservazione, le Pubbliche Amministrazioni ed i conservatori accreditati possono far riferimento al modello in allegato (Allegato A).

La Soprintendenza può, in seguito a preavviso, effettuare ispezioni per accertare lo stato di conservazione e custodia degli archivi e può emettere prescrizioni per la tutela degli archivi. Inoltre l'eliminazione di documenti di archivi pubblici o degli archivi privati per i quali sia intervenuta la dichiarazione di interesse culturale è soggetta alla preventiva e vincolante autorizzazione della Soprintendenza archivistica, secondo quanto disposto dall'art. 21 del Codice dei beni culturali e del paesaggio relativo agli *"interventi soggetti ad autorizzazione"* che alla lett. d) include tra tali interventi anche l'operazione di scarto dei documenti d'archivio. Lo scarto è l'operazione con cui vengono eliminati quei documenti che hanno esaurito la loro

34 Si fa riferimento in particolare agli art. 4, 10, 18 e 21 del citato Decreto legislativo. Il mantenimento delle competenze del Mibact in materia di tutela dei sistemi di conservazione degli archivi pubblici è ribadito dall'art. 6 comma 9 e dall'art. 9 comma 2 delle regole tecniche sulla conservazione (DPCM 3 dicembre 2013).

35 Dal sito della Soprintendenza archivistica per l'Emilia-Romagna, http://www.sa-ero.archivi.beniculturali.it/index.php?id=21.

validità giuridica o amministrativa e che, allo stesso tempo, non sono considerati di rilevanza storica tale da renderne opportuna la conservazione illimitata. Tale eliminazione si rende necessaria per una ordinata tenuta dell'archivio che eviti l'accumulo di masse ingenti di documentazione effimera. Ma essa è anche un'operazione culturale mediante la quale si selezionano le fonti storiche che verranno utilizzate in futuro per conoscere il nostro presente. Tale operazione è soggetta ad un procedimento di autorizzazione che prevede la compilazione di un elenco dettagliato della documentazione da parte dell'ente che propone lo scarto. Tale elenco deve essere trasmesso alla competente Soprintendenza per l'autorizzazione. La Soprintendenza ha l'obbligo di concludere il procedimento, entro 60 giorni dalla ricezione della richiesta, fatte salve le richieste di maggiori informazioni sulla proposta di scarto, che interrompono il termine del procedimento.

L'autorizzazione allo scarto può essere totale o parziale. In questo caso nella risposta della Soprintendenza dovranno essere motivate le ragioni di esclusione dallo scarto dei documenti indicati. Per un'analisi della procedura operativa di scarto in caso di depositi digitali vedi capitolo 8.

Bisogna infine ricordare che, secondo quanto disposto dall'art. 36, comma 2 lett. a) del recente regolamento di organizzazione del MIBACT (DPCM 29 agosto 2014, n. 171), il Soprintendente archivistico *"svolge, sulla base delle indicazione e dei programmi definiti dalla competente Direzione generale, attività di tutela dei beni archivistici presenti nell'ambito del territorio di competenza nei confronti di tutti i soggetti pubblici e privati, ivi inclusi i soggetti di cui all'articolo 44-bis del Codice dell'amministrazione digitale di cui al D. Lgs. 7 marzo 2005, n. 82, e successive modificazioni",* cioè i conservatori accreditati. Il D.M. 27 novembre 2014 ha ridisegnato la distribuzione degli istituti periferici accorpando, in cinque casi, le Soprintendenze di due regioni sotto un'unica direzione: Abruzzo e Molise, Calabria e Campania, Puglia e Basilicata, Umbria e Marche, Veneto e Trentino Alto Adige, che si sommano alla già esistente Piemonte e Valle d'Aosta. Detta riforma ha comportato anche l'unificazione delle Soprintendenze archivistiche per l'Emilia-Romagna, la Liguria e la Sicilia rispettivamente con gli Archivi di Stato di Bologna, Genova e Palermo. In questi tre regioni le Soprintendenze e gli Archivi di Stato citati costituiscono ora un unico Istituto.
Attualmente, dunque, operano in Italia 14 Soprintendenze archivistiche.

3.2 Descrizione del ruolo e delle funzioni dell'Agenzia per l'Italia Digitale

L'Agenzia per l'Italia Digitale, detta AgID, è stata istituita con il D.L. 22 giugno 2012, n. 83, convertito dalla legge 7 agosto 2012, n. 134. I compiti dell'Agenzia sono definiti in primo luogo dalle competenze degli enti che essa ha assorbito nel momento della loro soppressione: il Dipartimento Digitalizzazione e Innovazione della Presidenza del Consiglio dei Ministri, l'Agenzia per la diffusione delle tecnologie per l'innovazione, DigitPA, l'Istituto superiore delle

comunicazioni e delle tecnologie dell'informazione per le competenze sulla sicurezza delle reti, e in secondo luogo dalle prescrizioni contenute nel D. L. 18 ottobre 2012, n. 179, convertito dalla legge 17 dicembre 2012, n. 221. L'Agenzia per l'Italia Digitale è lo snodo necessario per la realizzazione dell'Agenda Digitale, cui assicura il coordinamento di competenze finora sparse su enti diversi: si è semplificata la gestione delle politiche dell'innovazione, con unitarietà di orientamento e controllo dei processi di digitalizzazione e ammodernamento della P.A. Tra questi processi particolare rilevanza per la connessione con l'Agenda Digitale europea hanno:

- la diffusione delle tecnologie dell'informazione e della comunicazione
- l'interoperabilità dei sistemi informativi pubblici
- la vigilanza sulla qualità dei servizi
- la razionalizzazione della spesa informatica
- il coordinamento delle iniziative strategiche per la digitalizzazione dei servizi pubblici per cittadini e imprese.

L'Agenzia, che opera attraverso un Direttore Generale, è, inoltre, dotata di un Comitato di indirizzo, composto da un rappresentante della Presidenza del Consiglio dei Ministri, un rappresentante del Ministero dello sviluppo economico, un rappresentante del Ministero dell'istruzione, dell'università e della ricerca, un rappresentante del Ministro per la pubblica amministrazione e la semplificazione, un rappresentante del Ministero dell'economia e finanze e due rappresentanti designati dalla Conferenza Unificata.

L'AgID ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana in coerenza con l'Agenda digitale europea e contribuisce alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, allo scopo di favorire l'innovazione e la crescita economica. Coordina inoltre le attività dell'amministrazione statale, regionale e locale, progettando e monitorando l'evoluzione del Sistema Informativo della Pubblica Amministrazione, anche adottando infrastrutture e standard che riducano i costi sostenuti dalle singole amministrazioni e migliorino i servizi erogati a cittadini e imprese. Definisce linee guida, regolamenti e standard e svolge attività di progettazione e coordinamento di iniziative strategiche per un'efficace erogazione di servizi online della pubblica amministrazione a cittadini e imprese, assicurando, fra l'altro, l'uniformità tecnica dei sistemi informativi pubblici. L'Agenzia sostiene la diffusione dell'innovazione digitale per contribuire allo sviluppo economico, culturale e sociale del Paese. Collabora con le istituzioni e gli organismi europei, nazionali e regionali aventi finalità analoghe, anche attraverso la stipula di accordi strategici, promuovendo l'alfabetizzazione digitale di cittadini e imprese, creando nuove conoscenze e opportunità di sviluppo. L'AgID svolge, inoltre, i compiti necessari per l'adempimento degli

obblighi internazionali assunti dallo Stato in materia di innovazione digitale, informatica e internet.

Per quanto attiene alla conservazione ne definisce le modalità operative per realizzare l'attività di conservazione. Si tratta della definizione di natura e funzione del sistema, modelli organizzativi, ruoli e funzioni dei soggetti coinvolti, descrizione del processo. I soggetti, pubblici e privati, che svolgono attività di conservazione dei documenti informatici che intendono accreditarsi, devono presentare all'Agenzia per l'Italia Digitale domanda di accreditamento. Le modalità di presentazione della domanda sono state definite dall'Agenzia stessa con apposita Circolare[36], su cui si sofferma il successivo paragrafo 5, al quale si rinvia.

4. Requisiti per la conservazione a norma e termini di adeguamento dei sistemi esistenti

4.1 Riferimenti normativi al CAD e al DPCM 3 dicembre del 2013 in materia di sistema di conservazione, standard di riferimento, processi, formati dei documenti, metadati

I requisiti per la conservazione informatica dei documenti si trovano all'art. 44 del CAD:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'art. 50, comma 4, del D.P.R. 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 artt. da 31 a 36 del D. Lgs. 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto. Inoltre è necessario rispettare le regole tecniche del DPCM 3 dicembre del 2013 in materia di sistema di conservazione ai sensi degli artt. 20, commi 3 e 5 -bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al D. Lgs. n. 82 del 2005 e la Circolare AgID del 10 aprile 2014 n. 65 sulle modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del D. Lgs. 7 marzo 2005, n. 82.

1) D. Lgs. 7 marzo 2005, n. 82

Codice dell'amministrazione digitale (CAD)

Articoli:

36 Circolare AgID n. 65 del 10 aprile 2014, pubblicata in GU n. 89 del 16-4-2014.

- 20, comma 3, 5 bis - Documento informatico
- 22, comma 4, 5 - Copie informatiche di documenti analogici
- 23, comma 2 - Copie analogiche di documenti informatici
- 23 bis, comma 2 - Duplicati e copie informatiche di documenti informatici
- 23 ter, comma 4 - Documenti amministrativi informatici
- 41, comma 2 bis, 2 ter - Procedimento e fascicolo informatico
- 42 - Dematerializzazione dei documenti delle pubbliche amministrazioni
- 43 - Riproduzione e conservazione dei documenti
- 44 - Requisiti per la conservazione dei documenti informatici
- 44-bis - Conservatori accreditati
- 50, comma 1 - Disponibilità dei dati delle pubbliche amministrazioni
- 51, comma 2, 2 bis - Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni
- 71 - Regole tecniche

2) Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013

Regole tecniche in materia di sistema di conservazione ai sensi degli artt. 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al D. Lgs. n. 82 del 2005.

Tutti gli articoli presenti del Decreto

Allegati:

- 1 - Definizioni/Glossario
- 2 - Formati
- 3 - Standard e specifiche tecniche
- 4 - Specifiche tecniche del pacchetto di archiviazione
- 5 – Metadati

3) Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013

Regole tecniche per il protocollo informatico ai sensi degli artt. 40 -bis, 41, 47, 57-bis e 71, del Codice dell'amministrazione digitale di cui al D. Lgs. n. 82 del 2005

Articoli:

- 5, comma 2, lettera m) - Manuale di gestione
- 7, comma 5 - Requisiti minimi di sicurezza dei sistemi di protocollo informatico
- 9 - Formato della segnatura di protocollo

4) Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014

Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni

Articoli:

- 3, comma 2, 3, 4, 5, 8, 9 - Formazione del documento informatico
- 7 - Trasferimento nel sistema di conservazione
- 8 - Misure di sicurezza
- 9, comma 1, 6, 7, 8 - Formazione del documento amministrativo informatico
- 11 - Trasferimento nel sistema di conservazione
- 12 - Misure di sicurezza
- 13 - Formazione dei fascicoli informatici
- 15 - Trasferimento in conservazione
- 16 - Misure di sicurezza

5) Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze

Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto

Articoli:

- 2 - Obblighi da osservare per i documenti informatici rilevanti ai fini delle disposizioni tributarie

- 3 - Conservazione dei documenti informatici, ai fini della loro rilevanza fiscale
- 4, comma 1, 3 - Obblighi da osservare per la dematerializzazione di documenti e scritture analogici rilevanti ai fini tributari
- 5 - Obbligo di comunicazione e di esibizione delle scritture e dei documenti rilevanti ai fini tributari

Inoltre è necessario rispettare gli standard internazionali:

- ISO 14721:2012 OAIS (*Open Archival Information System*), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems – Requirements,* Requisiti di un ISMS (*Information Security Management System*);
- ETSI TS 101 533-1 V1.3.1 (2012-04) *Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management*, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04) *Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors*, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 *Information and documentation - The Dublin Core metadata element set*, Sistema di metadati del Dublin Core.

4.2 Piano e tempi di adeguamento dei sistemi preesistenti all'entrata in vigore delle nuove regole tecniche. Gestione degli eventuali contratti di conservazione che utilizzano tali sistemi.

Con riferimento alla disposizione contenuta all'art. 14 del DPCM 3 Dicembre 2013, "Disposizioni Finali", tutti i sistemi di conservazione già esistenti dovranno essere adeguati entro o non oltre 36 mesi dalla data di entrata in vigore del Decreto.

Il conservatore non accreditato, che abbia messo in opera sistemi di conservazione conformi alla Deliberazione CNIPA del 19 febbraio 2004 n. 11[37], dovrà predisporre un piano di aggiornamento dei propri sistemi allo scopo di documentare all'Autorità ed ai propri Clienti, qualora lo richiedano, le modalità e i tempi di aggiornamento dei propri servizi alle nuove disposizioni.

I conservatori accreditati e quelli che intendono intraprendere la procedura di accreditamento invece dovranno fare riferimento esclusivamente a quanto disposto dal DPCM 3 dicembre 2013.

Suddetto piano dovrà pertanto contenere, oltre alla time-line di completamento delle attività, indicazione della modalità di adeguamento tecnico, ovvero riportare indicazione se l'attività comporti:

- il versamento dei vecchi archivi nel nuovo sistema: in tal caso il conservatore dettaglierà le modalità in cui suddetto versamento avverrà, quali controlli verranno applicati nella fase di versamento e quali evidenze verranno conservate,

oppure, in via alternativa,

- il mantenimento dei vecchi sistemi fino al termine di scadenza della conservazione: in tal caso il conservatore evidenzierà con quali modalità verrà garantito l'accesso ai documenti conservati con piattaforma già esistente.

Il conservatore dovrà inoltre indicare le modalità di accesso al nuovo sistema di conservazione, qualora tale modalità differisca da quella utilizzata per l'accesso alla piattaforma già esistente.

Nel caso di erogazione del servizio in outsourcing e qualora l'adeguamento del sistema comporti una modifica degli SLA[38] di servizio e/o della ripartizione delle responsabilità (tra produttore, Responsabile della conservazione e conservatore esterno), il conservatore dovrà comunicare le variazioni intervenute e aggiornare la documentazione contrattuale così come la manualistica del servizio.

5. Le procedure di accreditamento

5.1 Requisiti di qualità e di sicurezza, conformità agli standard di riferimento dei processi di conservazione, caratteristiche tecniche e dell'organizzazione

L'art. 44-bis del D. Lgs. 7 marzo 2005, n. 82 e s.m.i. (CAD), attribuisce all'Agenzia per l'Italia Digitale il compito di accreditare *"i soggetti pubblici e privati che svolgono attività di*

37 Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.(G.U. 9 marzo 2004, n. 57).
38 *Service Level Agreement*, in italiano: Accordo sul livello del servizio.

conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi e intendono conseguire il riconoscimento dei requisiti del livello più elevato, in termini di qualità e sicurezza". I soggetti, pubblici e privati, che svolgono attività di conservazione dei documenti informatici che intendono accreditarsi devono, quindi, presentare all'Agenzia per l'Italia Digitale domanda di accreditamento. Le modalità di presentazione della domanda sono state definite, come già accennato, dall'Agenzia per l'Italia Digitale, con la Circolare del 10 aprile 2014 n. 65; tutta la documentazione necessaria ivi richiamata (moduli per la domanda e schemi di documenti da allegare alla stessa) è disponibile sul sito AgID, alla pagina "Accreditamento e conservatori"[39], in cui è reperibile, tra l'altro, anche il documento esplicativo "Documentazione per accreditamento conservatori".

Possono richiedere l'accreditamento i conservatori di cui all'art. 44-bis del CAD che, al fine di conseguire tale riconoscimento, devono:

1. dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l'attività di conservazione;
2. utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti: in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della gestione documentale e conservazione documenti informatici e che abbia dimestichezza con le procedure di sicurezza appropriate e che si attenga alle norme del CAD e al DPCM 3 dicembre 2013 recante le regole tecniche in materia di sistema di conservazione;
3. applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
4. utilizzare sistemi affidabili e sicuri di conservazione di documenti informatici realizzati e gestiti in conformità alle disposizioni e ai criteri, standard e specifiche tecniche di sicurezza e di interoperabilità contenute nelle regole tecniche previste dal CAD;
5. adottare adeguate misure di protezione dei documenti idonee a garantire la riservatezza, l'autenticità, l'immodificabilità, l'integrità e la fruibilità dei documenti informatici oggetto di conservazione, come descritte nel manuale di conservazione, parte integrante del contratto/convenzione di servizio.

Il conservatore, se soggetto privato, in aggiunta a quanto previsto dai precedenti punti, deve inoltre:

1. avere forma giuridica di società di capitali e un capitale sociale di almeno 200.000 Euro;

39 http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/accreditamento-conservatori

2. garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e da parte dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'art. 26 del D. Lgs. 1 settembre 1993, n. 385 recante "Testo unico delle leggi in materia bancaria e creditizia".

Sul sito dell'Agenzia per l'Italia Digitale alla pagina "Accreditamento e conservatori" sono altresì disponibili il modulo per la domanda e gli schemi di documenti, richiamati nella suddetta Circolare, da allegare alla stessa. È necessario che ogni ente che richieda l'accreditamento sia in possesso dei requisiti necessari previsti dalla legge, sia conforme agli standard internazionali come riportato nel documento "Requisiti di qualità e sicurezza " e si avvalga di personale dotato di specifiche competenze come riportato nel documento "Elenco profili professionali per la conservazione".

La domanda, redatta in lingua italiana e secondo lo schema pubblicato sul sito dell'Agenzia, deve essere predisposta in formato elettronico, o fornita in copia ai sensi dell'art. 22, comma 2, del CAD, sottoscritta con firma digitale, o firma elettronica qualificata, dal legale rappresentante del conservatore ed inviata alla casella di posta elettronica certificata all'indirizzo protocollo@pec.agid.gov.it.

Con le medesime modalità deve essere predisposta la documentazione, atta a dimostrare il possesso dei requisiti richiesti, allegata alla domanda. Tale documentazione è elencata nel documento "Documentazione per l'accreditamento", pubblicato sul sito istituzionale dell'Agenzia.

La domanda deve indicare:

- la denominazione della società;
- la sede legale;
- le sedi operative;
- il/i rappresentante/i legale/i;
- il nominativo e i recapiti (numeri telefonici, indirizzo e indirizzo di PEC) di uno o più referenti tecnici cui rivolgersi in presenza di problematiche tecnico-operative che possono essere risolte per le vie brevi;
- l'elenco dei documenti allegati, con preciso riferimento a quanto indicato nel documento "Documentazione per l'accreditamento".

L'istruttoria relativa alle domande e la valutazione della documentazione prodotta sono effettuate dall'Agenzia ai sensi dell'art. 29, ad eccezione del comma 3, lett. a), del CAD. Infatti

la domanda di accreditamento si considera accolta qualora non venga comunicato al conservatore il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa, tale termine può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità dell'Agenzia o che questa non possa acquisire autonomamente. L'Agenzia, quindi, si riserva di richiedere integrazioni alla documentazione presentata e di effettuare le opportune verifiche su quanto dichiarato. L'attività istruttoria è svolta sulla base del documento "Requisiti di qualità e sicurezza per l'accreditamento" e al termine dell'istruttoria, l'Agenzia accoglie la domanda ovvero la respinge, con provvedimento motivato, e ne dà apposita comunicazione al conservatore. A seguito dell'accoglimento della domanda, l'Agenzia dispone l'iscrizione del conservatore nell'apposito elenco, ai fini dell'applicazione della disciplina in questione, il conservatore una volta accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni. Qualora invece la domanda venga respinta il conservatore non può presentare una nuova domanda se non siano cessate le cause che hanno determinato il mancato accoglimento della precedente e comunque non prima di 6 mesi.

L'elenco dei conservatori accreditati ai sensi della Circolare AgID del 10 aprile 2014 n. 65, pubblicato sul sito istituzionale dell'Agenzia, contiene per ogni soggetto iscritto le seguenti informazioni:

a) denominazione della società;

b) indirizzo della sede legale;

c) nominativo del rappresentante legale;

d) il manuale di conservazione del soggetto;

e) data di iscrizione;

f) stato dell'accreditamento (attivo, se in corso di validità, o revocato, nel caso in cui sia intervenuta la revoca con indicazione della data di revoca).

6. Il sistema di conservazione: modelli di riferimento

6.1 La conservazione gestita in proprio o affidata, in parte o in toto a terzi: descrizione dei modelli di riferimento delle strutture organizzative e della ripartizione delle responsabilità

I modelli organizzativi di riferimento della conservazione sono definiti, in attuazione dell'art. 44 del CAD, all'art. 5 del DPCM 3 dicembre 2013 in tema di conservazione. La conservazione può essere realizzata all'interno della struttura organizzativa del soggetto produttore dei

documenti informatici da conservare (modello interno) ovvero affidandola (modello esterno), in tutto o in parte, a soggetti pubblici e privati che offrano idonee garanzie organizzative e tecnologiche. Le pubbliche amministrazioni che vogliano esternalizzare il servizio di conservazione, sono tenute per legge ad affidarlo ad una società, sia essa pubblica o privata, accreditata presso AgID, di cui all'articolo 44-bis del CAD.

I modelli organizzativi:

- ***In house*** per cui il processo/sistema di conservazione è realizzato all'interno della struttura organizzativa del soggetto produttore dei documenti informatici.
- ***Outsourcing*** dove il Responsabile della conservazione può affidare il processo/sistema di conservazione, in modo totale o parziale, a soggetti terzi pubblici o privati che offrono idonee garanzie organizzative e tecnologiche.

A prescindere dal modello adottato, rimane l'obbligo di nominare all'interno dell'organizzazione la figura del Responsabile della conservazione, il quale, sotto la propria responsabilità, può delegare in outsourcing il processo/sistema di conservazione. In caso di outsourcing, la delega è formalizzata, esplicitando chiaramente il contenuto della stessa, ed in particolare, le specifiche funzioni e competenze affidate; viene stipulato un contratto o una convezione di servizio che prevede l'obbligo del rispetto del manuale della conservazione predisposto dal Responsabile della stessa da parte del soggetto/i delegati. Rimane comunque in carico al Responsabile della conservazione vigilare sulla corretta esecuzione del processo di conservazione: sul fornitore graverà la sola responsabilità contrattuale nei confronti del Responsabile della conservazione.

Le regole tecniche all' art. 6 del DPCM 3 dicembre 2013 in materia di sistema di conservazione, coerentemente con quanto indicato nello standard OAIS "*Open Archival Information System*"[40] al quale si ispirano, individuano i seguenti soggetti coinvolti nei processi di conservazione: il produttore, l'utente e il Responsabile della conservazione.

Si tratta dei soggetti definiti nell'allegato 1 – "Glossario/Definizioni" delle Regole Tecniche come:

1. **Produttore:**

   Il produttore - il quale non coincide necessariamente con il soggetto che ha formato il documento - è definito nella normativa come la persona fisica o giuridica alla quale si affida il compito di predisporre e inviare il pacchetto di versamento prodotto nel contesto del sistema di gestione documentale e contenente i documenti corredati dei necessari metadati descrittivi, il quale viene quindi trasmesso al sistema di conservazione. All'interno delle

40 Standard ISO 14721:2012.

pubbliche amministrazioni il produttore è rappresentato dal dirigente o dal funzionario Responsabile della gestione documentale.

Le attività infatti poste in capo al produttore riguardano:

a) la produzione del pacchetto di versamento;

b) la responsabilità del trasferimento del contenuto del pacchetto di versamento nel sistema di conservazione.

Il pacchetto di versamento deve essere infatti trasferito ai fini della sua acquisizione al sistema di conservazione. Il produttore si assume quindi la responsabilità di produrre il pacchetto di versamento e di trasferirne correttamente il contenuto nel sistema.

Questo implica che il produttore del pacchetto di versamento si assume una serie di responsabilità, quali ad esempio quella di produrre i pacchetti di versamento secondo il formato concordato, attribuendo una nomenclatura univoca e identificativa del file stesso ed eventualmente generando il *file* in formato XML che riporta i metadati caratteristici di ciascun documento, inviando il tutto con la tempistica e secondo i canali concordati con il soggetto conservatore. Eventuali errori nel trasferimento del contenuto nei sistemi di conservazione saranno riferibili in via diretta ed immediata al produttore del pacchetto di versamento. I rischi per il soggetto che forma il documento, e che si occupa anche di trasferirlo al sistema di conservazione in qualità di produttore, risiedono ad esempio nel consegnare un pacchetto di versamento non in linea con le indicazioni/accordi presi con il Responsabile del servizio di conservazione ovvero nel consegnare un file di metadati non coincidente con i documenti riversati nel sistema di conservazione. Ciò implica che il sistema di conservazione genererà il rilascio di un rapporto di versamento negativo. In capo al soggetto che ha formato il documento, e che è anche produttore del pacchetto di versamento, ciò determina la necessità di presidiare anche le fasi di generazione del pacchetto di versamento e di verificarne il contenuto e la sua leggibilità in fase di trasferimento e consegna.

In estrema sintesi, laddove il titolare del contenuto documentale dovesse rivestire anche la qualità di produttore del pacchetto di versamento, senza delegarla ad un soggetto terzo, si troverebbe a dovere garantire il rispetto di una serie di requisiti di matrice sia legale che operativa. Secondo quanto già descritto in precedenza, dal punto di vista del rispetto delle disposizioni normative e regolamentari vigenti, il soggetto che ha formato il documento sarebbe in questo caso tenuto a:

a) rispettare i termini di conservazione di natura civilistica e fiscale, monitorando le tempistiche correlate al corretto invio in conservazione a norma della documentazione;

b) curare l'acquisizione del pacchetto di versamento nel sistema di Conservazione, monitorando eventuali anomalie rilevate a valle dei controlli di accettazione del sistema di conservazione con conseguente rifiuto del pacchetto stesso, provvedendo di conseguenza a "normalizzare" i pacchetti di versamento secondo le specifiche concordate con il conservatore;

c) in quanto Responsabile del versamento del pacchetto informativo all'interno del sistema di conservazione, resta ferma la sua esclusiva responsabilità laddove provveda all'invio di pacchetti di versamento, e questi siano accettati dal sistema, contenenti documenti non validi o illeggibili. Una volta conservati a norma, tali documenti sono immodificabili e non possono essere rimossi dal sistema di conservazione.

Naturalmente, il rispetto dei requisiti legali e regolamentari comporta anche l'effettuazione da parte del soggetto che ha formato il documento, che rivesta anche le funzioni di produttore del pacchetto di versamento, di tutta una serie di attività operative dovendosi occupare di:

a) risolvere eventuali anomalie a seguito del rifiuto del pacchetto di versamento da parte del sistema di conservazione;

b) classificare la documentazione secondo il piano della conservazione concordato con il Responsabile della conservazione, rispettando altresì gli accordi tecnici intercorsi con il Responsabile stesso;

c) produrre i file contenenti i metadati necessari all'indicizzazione dei documenti curandosi della corrispondenza tra gli stessi e l'oggetto conservato;

d) garantire l'effettiva leggibilità della copia informatica di documenti analogici inviati in conservazione (a seguito delle attività di scannerizzazione o renderizzazione);

e) assicurare la continuità dei documenti inviati in conservazione senza salti di numerazione degli archivi (numeri mancanti).

2. Utente:

L'utente è la persona fisica o giuridica, interna o esterna al sistema di conservazione che richiede l'accesso alla documentazione dell'archivio. Il recupero dell'informazione presso il produttore avviene principalmente per finalità amministrative e a scopo di controllo.

L'utente dev'essere sempre opportunamente autenticato ed ogni attività di accesso e recupero dei documenti dev'essere definita sulla base del livello di autorizzazione concesso.

Il ruolo di Utente del sistema di conservazione è rivestito da tutti quei soggetti che, avendone diritto, possono interrogare il sistema al fine di ottenerne il Pacchetto di

Distribuzione. L'art. 6, comma 4 delle regole tecniche dispone infatti il potere dell'Utente di richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Utente può essere una persona fisica, un ente o un sistema in grado di interagire con i servizi del sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse. Solitamente si tratta di personale amministrativo e gestionale del soggetto titolare delle informazioni conservate, ovvero del personale appartenente alle Autorità preposte alle attività di controllo e verifica nei confronti dei titolari dei documenti. A tale proposito, l'eventuale individuazione di Utenti con privilegi di "esibizione a norma" deve essere concordata con il soggetto titolare dei contenuti documentali.

3. Responsabile della conservazione:

Il Responsabile della conservazione è la persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato. Il Responsabile della conservazione definisce le caratteristiche e i requisiti generali del sistema, gestisce e monitora i processi conservativi al fine di salvaguardare gli aspetti fisici, logici e tecnologici, garantendo l'integrità e la leggibilità degli archivi nel tempo. Interviene nei casi di produzione di copie e estratti di documenti informatici, per garantire la possibilità di attestazione da parte di un pubblico ufficiale della loro conformità agli originali; spetta a lui sottoscrivere con firma digitale o firma elettronica qualificata il rapporto di versamento ove richiesto, predisporre e sottoscrivere, se previsto, il pacchetto di distribuzione e preparare e sottoscrivere il pacchetto di archiviazione, la cui sottoscrizione digitale è invece obbligatoria. Tale figura, inoltre, qualora il produttore sia una pubblica amministrazione o un ente pubblico, vigila sulle procedure di versamento della documentazione presso gli Archivi di Stato e presso l'Archivio Centrale dello Stato. Fornisce, infine, supporto per le attività di verifica da parte degli organi di controllo. Il Responsabile della conservazione ha facoltà di delegare il coordinamento dell'intero processo o una parte delle mansioni a lui affidate a soggetti terzi in possesso delle necessarie conoscenze e competenze. Tale delega deve essere formalizzata e debitamente documentata all'interno del manuale di conservazione.

Nelle pubbliche amministrazioni il ruolo di Responsabile della conservazione può essere svolto dal Responsabile della gestione documentale, ovvero dal coordinatore della gestione documentale, ove nominato. Se il Responsabile della conservazione, di una Pubblica Amministrazione o anche di un privato, affida il processo di conservazione ad un conservatore esterno, nel caso di una PA che abbia ottenuto l'accreditamento presso

l'Agenzia per l'Italia Digitale, si interfaccerà con il Responsabile del servizio di conservazione.

Il Responsabile del servizio di conservazione opera d'intesa con il Responsabile del trattamento dei dati personali, con il Responsabile della sicurezza del sistema, con il Responsabile dei sistemi informativi e, nel caso in cui il soggetto produttore sia una pubblica amministrazione o un ente pubblico, anche con il Responsabile della gestione documentale, le cui attività sono definite in riferimento al sistema di gestione documentale. Il Responsabile del servizio di conservazione si occupa delle politiche complessive del sistema di conservazione e ne determina l'ambito di sviluppo e le competenze. A tal fine, anche in coerenza con OAIS, provvede alla pianificazione strategica, alla ricerca dei finanziamenti, alla revisione periodica dei risultati conseguiti e ad ogni altra attività gestionale mirata a coordinare lo sviluppo del sistema.

Gli obiettivi che persegue sono :

- garantire la conservazione, archiviazione e gestione dei documenti informatici e degli altri oggetti digitali;
- erogare servizi di accesso basati sui contenuti digitali conservati;
- fornire supporto, formazione e consulenza ai produttori per i processi di dematerializzazione.

Di fatto, quindi il soggetto conservatore si impegna alla conservazione dei documenti trasferiti e ne assume la funzione di Responsabile de servizio di conservazione ai sensi della normativa vigente, garantendo il rispetto dei requisiti previsti dalle norme in vigore nel tempo per i sistemi di conservazione, e svolge l'insieme delle attività elencate nell'art. 7 comma 1 delle Regole tecniche, in particolare quelle indicate alle lettere a), b), c), d), e), f), g), h), i), j), k) e m).

7. Attività preliminari del soggetto produttore

7.1 Descrizione del modello organizzativo adottato per la conservazione

Secondo quanto disposto dalla normativa primaria e tecnica le realtà pubbliche e private hanno facoltà di scegliere tra due possibili soluzioni conservative: all'interno della struttura organizzativa del soggetto produttore ovvero affidandola, in tutto o in parte, a soggetti pubblici e privati.

Il Responsabile del servizio di conservazione incaricato dal soggetto produttore della documentazione, inteso quest'ultimo come l'ente pubblico o privato che produce il pacchetto di

versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione e, sotto la propria responsabilità, definisce un sistema di conservazione che sia da esso gestito e monitorato direttamente all'interno della propria struttura organizzativa, oppure opta per l'affidamento a terzi di tutto o parte del processo conservativo. Il sistema di gestione documentale risulta in ogni caso logicamente distinto da quello di conservazione, in termini di infrastrutture informatiche adottate e metodologie organizzative, procedurali e descrittive degli archivi formati. Il Responsabile del servizio di conservazione, quindi, non si preoccuperà della gestione del documento ma solo della presa in carico del pacchetto di versamento e della sua successiva conservazione nel tempo.

La definizione del modello organizzativo deve essere valutata in termini di efficienza e sostenibilità e attuata in considerazione delle risorse finanziarie, tecnologiche e professionali disponibili. La costituzione di un sistema affidabile comporta la definizione di procedure capaci di fronteggiare nel tempo le evoluzioni e la rapida obsolescenza delle tecnologie, a cui sono soggetti i documenti trattati con modalità informatiche. Inoltre, la costituzione e l'adeguamento degli impianti, dei formati e dei supporti di memorizzazione, per garantire la conservazione a norma degli originali e la produzione delle necessarie copie di *backup*, per preservare il vincolo esistente tra i documenti e il loro valore giuridico fin dalla fase della loro formazione, implica l'affidamento delle attività a personale specializzato in diverse discipline scientifiche. La valutazione, dunque, non può che essere operata in funzione delle risorse economiche e organizzative a disposizione, considerando le reali capacità di fronteggiare l'inevitabile investimento iniziale e stimando il rapporto tra costi e benefici.

Ai fini della completa valutazione del modello organizzativo da adottare, non si può prescindere dal considerare anche elementi specifici del sistema di conservazione che si deve realizzare.

La definizione del modello organizzativo da adottare deve tener conto dei requisiti di un sistema di conservazione dei documenti informatici declinati dall'art. 44 del CAD:

a) garantire l'identificazione certa del soggetto che ha formato il documento conservato;
b) garantire l'integrità del documento conservato;
c) garantire la leggibilità e l'agevole reperibilità del documento conservato;
d) garantire la continuità di disponibilità nel tempo, la tutela del documento conservato e la protezione dei suoi contenuti in conformità a quanto disposto dagli artt. da 31 a 36 e dall'allegato b del D.Lgs. n. 196 del 2003[41].

41 Codice in materia di protezione dei dati personali. (GU n.174 del 29-7-2003 - Suppl. Ordinario n. 123).

È palese che per rispettare tali requisiti è necessario non solo l'attività ma anche la collaborazione delle aree direttamente interessate attraverso i loro responsabili:

- per i requisiti a, b e c il Responsabile dell'area del protocollo informatico, gestione flussi documentali e archivi; in tal senso anche il Testo Unico, all'art. 68, richiama quest'area al compito di elaborare e aggiornare il piano di conservazione degli archivi, integrato con il sistema di classificazione, definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti;
- per il requisito d, il Responsabile del trattamento dei dati personali ex art. 29 D.Lgs. n. 196 del 2003.

Si rende inoltre necessaria una figura di governo dell'intero processo di conservazione il Responsabile della conservazione, che deve operare d'intesa con il Responsabile del trattamento dei dati personali e con il Responsabile del protocollo informatico, flussi documentali e archivio.

Quindi, per l'aspetto funzionale, si delinea una struttura di questo tipo:

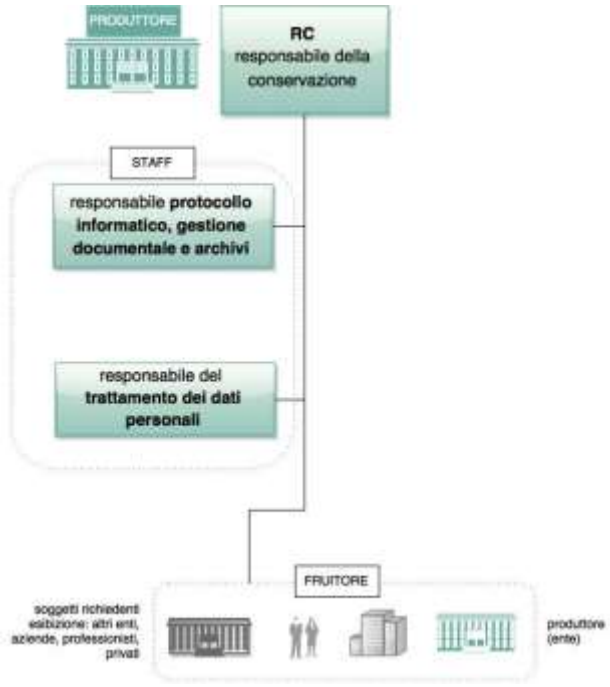

Figura 2 - Ruoli e responsabilità nel processo di conservazione (parziale)

Ai commi 3 e 4 dell'art. 7 delle regole tecniche per la conservazione, DPCM 3 dicembre 2013, è stabilito che il ruolo di Responsabile della conservazione deve essere ricoperto da un dirigente o da un funzionario formalmente designato; può trattarsi anche dello stesso Responsabile della gestione documentale o dal coordinate della gestione documentale ove

nominato. Tale ruolo in ogni caso non può essere ricoperto da un soggetto terzo ed esterno all'amministrazione.

Trattandosi poi di conservazione digitale di documenti e fascicoli informatici, è senza dubbio necessario arricchire lo staff, a supporto del Responsabile della conservazione, con il Responsabile dei sistemi informativi dell'amministrazione; pertanto l'organizzazione va a delinearsi come in Figura 3 - Ruoli e responsabilità nel processo di conservazione (completo).

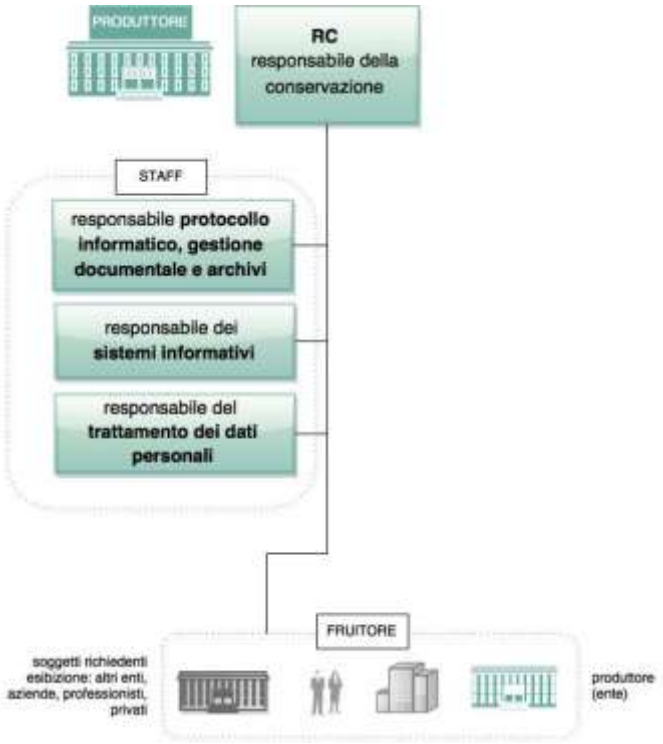

Figura 3 - Ruoli e responsabilità nel processo di conservazione (completo)

L'organizzazione così delineata ha cura di applicare le regole tecniche per la conservazione e quindi di adottare la soluzione tecnologica più adatta alle proprie esigenze per conservare i propri documenti nel rispetto dei requisiti richiamati all'inizio del presente paragrafo.

Infatti, la norma lascia al produttore libertà di decidere, in base alle proprie esigenze e capacità di investimento, di allestire il sistema di conservazione con mezzi propri (*in house* – vedi Figura 4 - Modello organizzativo della conservazione svolta "in house") oppure di affidarlo a soggetti terzi (*outsourcing* – vedi Figura 5 - Modello organizzativo della conservazione svolta "in outsourcing") a patto che questi ultimi abbiano ottenuto l'accreditamento ai sensi art. 44-bis del Codice.

Come è evidente dalle figure 4 e 5, il Responsabile della conservazione rimane una figura interna al produttore; nel caso dell'affidamento al soggetto esterno (Figura 5 - Modello organizzativo della conservazione svolta "in outsourcing"), il Responsabile della conservazione rimane sempre in seno al produttore ma delega la funzione di Responsabile del servizio di

conservazione. Ciò significa che la fase operativa della conservazione, individuata nel sistema ICT allestito in totale aderenza alle regole tecniche DPCM 3 dicembre 2013, può essere delegata a terzi in caso di *outsourcing* ma risponde sempre al Responsabile della conservazione del produttore.

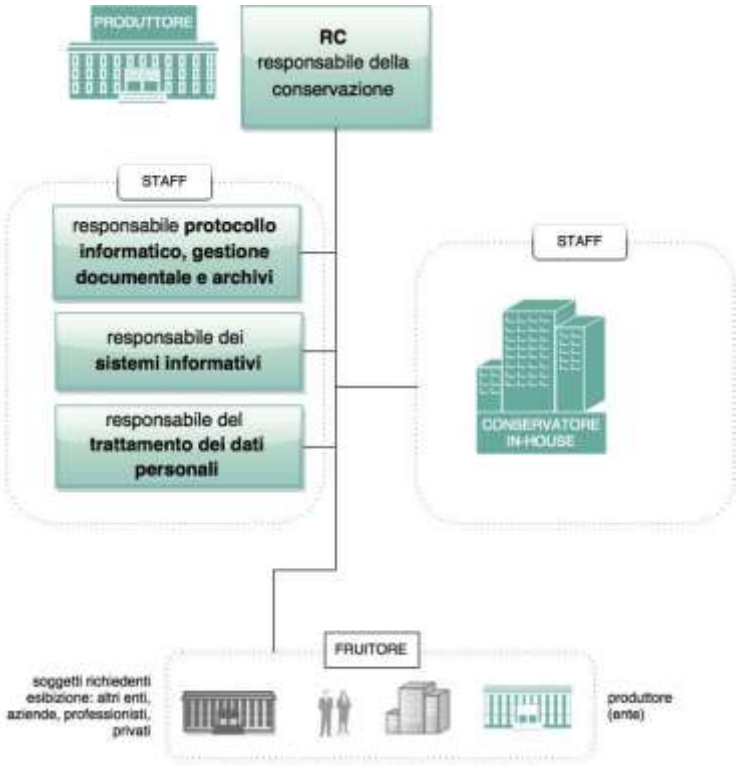

Figura 4 - Modello organizzativo della conservazione svolta "in house"

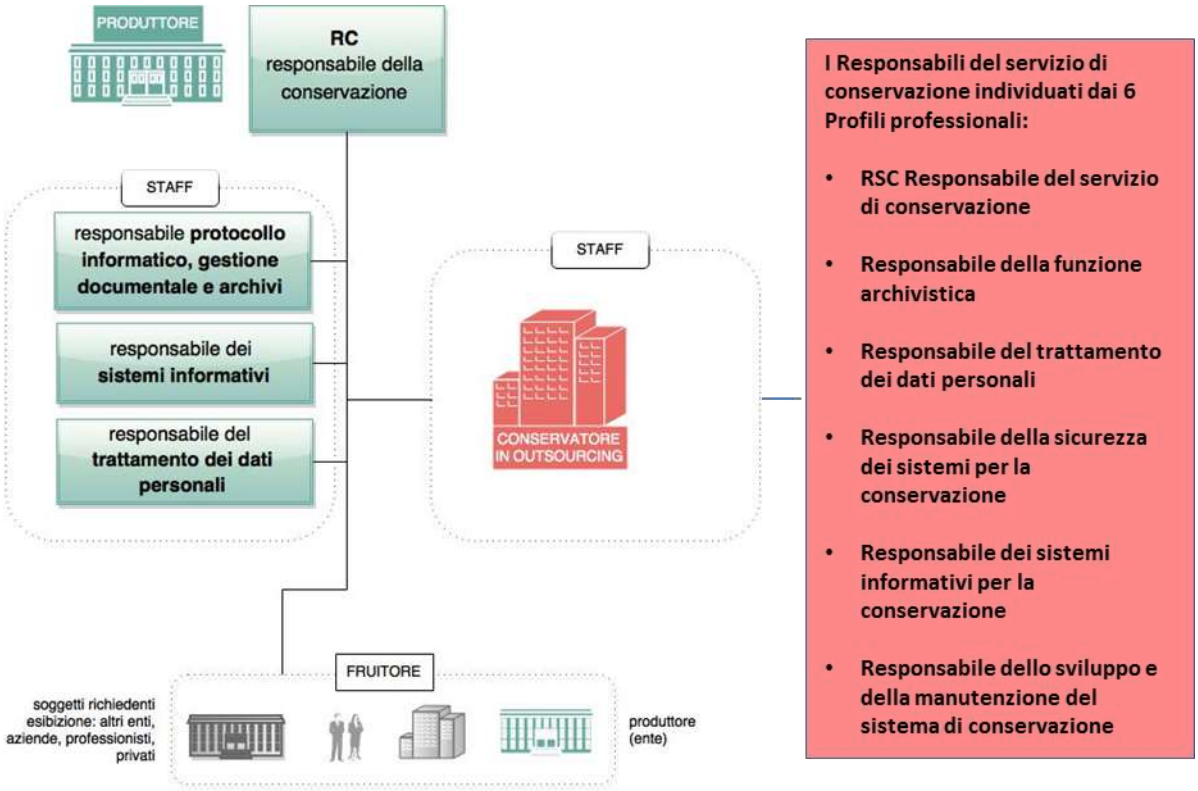

Figura 5 - Modello organizzativo della conservazione svolta "in outsourcing"

In ottica di riduzione della spesa e di razionalizzazione delle risorse ICT, è certamente molto più performante, in termini di rapporto tra qualità del servizio che obbligatoriamente occorre raggiungere e mantenere nel tempo e spesa per allestire e mantenere tale livello, il modello con *outsourcing* per i seguenti motivi:

- il soggetto terzo a cui viene affidato il servizio di conservazione si fa carico di affrontare gli investimenti necessari per garantire i livelli attesi, sia in termini di qualità che di sicurezza, dalle regole tecniche per la conservazione ed imposti dal DPCM 3 dicembre 2013;
- il soggetto terzo a cui viene affidato il servizio deve ottenere l'accreditamento dall'Agenzia per l'Italia Digitale per operare in tal senso ed è soggetto a verifiche nel tempo da parte della stessa per assicurare che i livelli, di qualità e sicurezza del servizio, siano sempre garantiti e coerenti con la normativa cogente.

Il Responsabile della conservazione ha l'onere di coordinare il rapporto con il conservatore affinché siano assicurati metodi per avviare e conservare i documenti nel rispetto della norma; quando il conservatore è un soggetto esterno deve farsi carico quindi di:

- concordare con il conservatore gli elementi contenuti nel manuale di conservazione (tipologie documentali, tempi di versamento e conservazione, formati e metadati descrittivi)

- concordare con il conservatore la struttura e le modalità di produzione dei pacchetti di documenti da avviare in conservazione (quindi quando il produttore trasmette al conservatore) e da esibire (quindi quando il conservatore trasmette al produttore)
- definire con il conservatore quali siano canali di comunicazione dati che possono essere utilizzati per scambiarsi i pacchetti di documenti.

Il Responsabile del protocollo informatico, gestione documentale e archivi ha il compito di :

- produrre il pacchetto di versamento secondo le regole pattuite tra Responsabile della conservazione ed il conservatore;
- assicurare la trasmissione del contenuto del pacchetto di versamento nel rispetto di quanto definito, tra Responsabile della conservazione e conservatore, nel suo (ndr - del produttore) manuale di conservazione.
- Il Responsabile del trattamento dei dati ha il compito di tutela delle informazioni contenute nei documenti da conservare; tale ruolo deve essere svolto sia dal produttore che dal conservatore nelle forme previste dal Codice in materia di protezione dei dati personali.

Infine l'utente può essere un soggetto esterno al produttore, pubblico o privato, che desidera accedere ad un documento conservato; in tale condizione va applicato quanto previsto dal Codice in tema di disponibilità dei dati con le tutele previste per garantire l'accesso alle informazioni in esso contenute solo se l'utente è autorizzato.

Per quanto concerne la sicurezza fisica e logica dei contenuti è necessario prevedere la predisposizione di soluzioni complesse, in grado di garantire una corretta gestione della continuità operativa del sistema anche attraverso l'individuazione di almeno due distinti siti, uno principale e uno secondario, attraverso i quali gestire in sicurezza il sistema di conservazione, e garantendo la replica e l'eventuale ripristino del sistema stesso, dei dati in esso contenuti e delle infrastrutture in grado di trattarli anche in caso di gravi emergenze che ne possano compromettere il corretto funzionamento. Per quanto attiene alle risorse umane non è possibile prescindere da uno studio della pianta organica del personale, attuando attività di mappatura delle competenze specifiche delle figure professionali interne in funzione dei ruoli previsti dalla normativa e vagliando eventuali piani di assunzione di nuovo personale qualificato.

I soggetti pubblici e privati che intendono erogare servizi di conservazione in outsourcing rivolti ad una pubblica amministrazione devono obbligatoriamente sottoporsi all'iter di valutazione dell'Agenzia per l'Italia Digitale - che verifica l'effettivo possesso di elevati livelli

di qualità e sicurezza dei sistemi di conservazione - e risultare inseriti nell'elenco dei conservatori accreditati predisposto e pubblicato dalla stessa AgID ai sensi dell'art. 44 bis del CAD.

7.2 Ricognizione dei documenti, loro classificazione e relativo sistema di gestione

L'art. 53 del D.P.R. 28 dicembre 2000, n. 445 prevede che *"Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione."*

La frase *"e tutti i documenti informatici"* lascia spazio a dubbiose interpretazioni, ma il legislatore voleva certo intendere "tutti i documenti amministrativi informatici", cioè quelli prodotti dall'amministrazione o comunque utilizzati a fini amministrativi.

Tutti i documenti attinenti all'azione amministrativa dell'ente devono quindi essere registrati nel protocollo informatico, ricevendo così una segnatura di protocollo che include alcuni elementi (metadati) essenziali da associarsi in modo permanente al documento sia in fase di gestione sia in fase di conservazione. Possono non essere registrati a protocollo i documenti già soggetti a registrazione particolare, organizzati in repertori/serie particolari. In questo caso le serie dei documenti soggetti a registrazione particolare devono essere elencati in specifico allegato del manuale di gestione.

Gli elementi obbligatori, in quanto giuridicamente rilevanti, della registrazione a protocollo sono:

- numero di protocollo
- data di registrazione
- mittente per il documento in arrivo/ destinatario per il documento in partenza
- oggetto
- indicazione del registro nell'ambito del quale è stata effettuata la registrazione.[42]

Altri elementi utili da includere nella registrazione sono:

- numero degli allegati

42 Previsto dalla Circolare n. 60 del 2013 "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni".

- descrizione degli allegati
- data del documento ricevuto (se disponibile)
- numero di protocollo del documento ricevuto (se disponibile).

Si ricorda che il registro di protocollo, anche in forma digitale, è atto pubblico di fede privilegiata che certifica l'effettivo ricevimento e l'effettiva spedizione di un documento ad una certa data, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici a favore o a danno delle parti. Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente. Deve quindi essere sottoposto a conservazione digitale a norma.

La segnatura di protocollo è l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo per consentire di individuare ciascun documento in modo inequivocabile (art. 55 del D.P.R. 28 dicembre 2000, n. 445). La registrazione a protocollo e la segnatura costituiscono un'operazione unica e vengono effettuate contemporaneamente; hanno entrambe natura di atto pubblico. La segnatura di protocollo deve rispettare lo standard XML.

Elementi essenziali della segnatura di protocollo sono:

- denominazione / codice unico che individua pubblica amministrazione
- numero di protocollo
- data di registrazione nel registro di protocollo
- elementi per la gestione del documento (*records management*), in particolare, la classificazione che include metadati essenziali anche nella fase di conservazione: - anno - titolo - classe – fascicolo
- oggetto
- indicazione dell'Unità organizzativa responsabile (UOR)
- destinatario, in caso di documento in uscita

I documenti prodotti o ricevuti sono aggregati in fascicoli relativi a un procedimento amministrativo o oggetto specifico o organizzati cronologicamente in serie/repertori.

Quanto alla tipologia, si distinguono fascicoli relativi ad affari o procedimenti amministrativi e fascicoli relativi a persone fisiche o giuridiche.

Ciascun fascicolo è individuato dai seguenti elementi:

- ente titolare del procedimento
- amministrazioni partecipanti
- identificativo del fascicolo, costituito da
  - titolo e classe di appartenenza
  - anno di apertura (anno di inizio della pratica)
  - numero di repertorio, cioè un numero sequenziale (da 1 a n), attribuito con cadenza annuale, all'interno dell'ultimo grado divisionale del titolario (es. classe)
- oggetto, cioè una stringa di testo solitamente normalizzata per descrivere compiutamente un affare e/o un procedimento amministrativo.
- unità organizzativa responsabile
- Responsabile del procedimento amministrativo
- elenco dei documenti contenuti
- tempistiche di passaggio in conservazione
- tempistiche di scarto.

Accanto alla documentazione organizzata in fascicoli abbiamo serie di documenti e registri organizzati cronologicamente secondo la tipologia, quali:

- ordinanze, decreti, determine
- delibere, verbali
- contratti, convenzioni
- documenti contabili (mandati, reversali, ecc.)
- registri anagrafici, di stato civile

Per una corretta sedimentazione dei documenti nell'archivio e il rispetto del vincolo archivistico è essenziale che il soggetto produttore imposti correttamente già nelle prime fasi attività e procedure che assicurino, oltre ad un'efficiente gestione documentale, anche la possibilità di impostare una corretta attività di conservazione a norma.

È pertanto indispensabile:

1. individuare i settori della pubblica amministrazione in questione che producono e gestiscono documenti digitali;

2. individuare i procedimenti e le attività cui i documenti digitali prodotti e ricevuti si riferiscono;
3. descrivere i documenti prodotti e ricevuti per ciascun settore nell'ambito di ciascun procedimento e attività, esplicitandone i collegamenti;
4. elaborare l'elenco dei formati dei file dei documenti che afferiscono a ciascun procedimento; specificare gli identificativi dei documenti e delle aggregazioni documentali prodotte (metadati archivistici);
5. individuare i sistemi di produzione e gestione dei documenti;
6. definire le tempistiche di conservazione per ciascuna tipologia o aggregazione documentaria, distinguendo tra documentazione destinata a conservazione illimitata e documentazione soggetta a scarto secondo tempistiche definite;
7. ottenere una descrizione delle modalità di conservazione dei documenti informatici già adottate.

Il sistema di gestione dei flussi documentari – che cura la registrazione a protocollo e la classificazione dei documenti, l'assegnazione dei documenti alle unità organizzative responsabili (sulla scorta dell'organigramma dell'ente), la costituzione e la creazione del repertorio dei fascicoli, l'individuazione dei responsabili della conservazione dei documenti e dei fascicoli nella fase corrente - fa capo all'area organizzativa omogenea (AOO) ma vede l'intervento dei diversi settori dell'amministrazione.

Strumento fondamentale per l'individuazione di tipologie e aggregazioni documentarie è il piano di classificazione, c.d. titolario, allegato al manuale di gestione.

La classificazione dei documenti rappresenta l'attività di ordinamento di tutti i documenti (indipendentemente dallo stato di trasmissione e dal supporto) secondo un piano di classificazione predeterminato in base a principi funzionali che include, nel caso di documenti cartacei o di documenti informatici testuali, anche la fascicolazione dei documenti.

La classificazione è lo strumento per la formazione e l'ordinamento di tutti i documenti prodotti e acquisiti nello svolgimento dell'attività amministrativa ed ha la finalità di costruire un sistema integrato di informazioni sui documenti, basato sulla loro organizzazione funzionale in unità complesse stabili nel tempo (fascicoli, registri) che riflettono il concreto lavoro amministrativo, fiscale, legale, tecnico, giuridico ecc. di un soggetto pubblico produttore di documenti. La classificazione è obbligatoria per tutti i documenti che entrano a far parte dell'archivio dell'ente, anche i non protocollati.

Il titolario di classificazione è uno strumento dell'archivio corrente che serve per organizzare la documentazione prodotta o ricevuta dall'Amministrazione in settori e categorie,

schematizzando in maniera logica le sue competenze e funzioni. Esso guida la sedimentazione dei documenti in archivio e garantisce una crescita dello stesso ordinata e coerente.

Il titolario adottato rispecchia le funzioni dell'Amministrazione e in caso di archivi ibridi si applica all'archivio sia cartaceo che digitale; è adottato internamente con atto formale dell'organo deliberante. Il Responsabile della gestione documentale verifica periodicamente la rispondenza del titolario ai procedimenti amministrativi e agli affari in essere per l'eventuale aggiunta/eliminazione/modifica della voce.

Successivamente alla classificazione il documento deve essere fascicolato a cura del Responsabile del procedimento amministrativo e condiviso con gli utenti del proprio Ufficio. La fascicolazione è la creazione ordinata e funzionale di unità correlate al processo decisionale ed è strettamente correlata alla classificazione; la fascicolazione è un'attività sequenziale alla classificazione in quanto senza un titolario non è possibile aprire e gestire i fascicoli archivistici.

Le due attività si traducono nell'attribuzione a ciascun documento di un codice (indice di classificazione) desunto dal titolario di classificazione e di un ulteriore numero che identifica l'unità archivistica di base ovvero il fascicolo archivistico. In sintesi il titolario di classificazione racchiude tutto quello che può entrare a far parte del patrimonio documentario dell'ente mentre il piano di fascicolazione rappresenta gli affari, le attività e i procedimenti amministrativi che l'ente ha realmente gestito.

Il fascicolo è l'insieme organico e ordinato di documenti (originali e in copia; protocollati o meno) che si forma nel corso dell'attività amministrativa dell'ente riuniti insieme perché relativi allo stesso affare, può raccogliere un numero variabile di documenti relativi ad una determinata pratica sedimentati in maniera originaria e spontanea dal più vecchio al più recente. Il legame che unisce i documenti inseriti nello stesso fascicolo è il vincolo originario, il cosiddetto vincolo archivistico: legame naturale che si crea tra più documenti che riguardano lo stesso affare.

Il fascicolo garantisce non solo l'efficienza nella gestione dei workflow ma anche l'efficacia dell'azione amministrativa ed è obbligatorio per legge.

Quando la documentazione contenuta in un fascicolo raggiunge una mole consistente di documenti oppure il procedimento amministrativo risulta particolarmente complesso, oppure si sceglie di suddividere la documentazione per tempi di conservazione, un fascicolo può essere articolato in uno o più sotto-fascicoli.

Infine è possibile monitorare l'apertura dei fascicoli attraverso il repertorio dei fascicoli: l'elenco ordinato e aggiornato dei fascicoli istruiti all'interno di ciascuna classe del titolario. Il repertorio dei fascicoli costituisce uno strumento di gestione dell'archivio corrente in quanto

facilita il reperimento dei fascicoli ed è di supporto agli Uffici nell'apertura di fascicoli annuali standardizzati.

Le tipologie di fascicolo rappresentano dei modelli di fascicoli che possono essere utilizzati dagli utenti per la creazione dei fascicoli "reali" e hanno lo scopo di fornire il modello di riferimento del fascicolo dal quale l'utente in possesso di un apposito diritto creerà il fascicolo "reale" utilizzando apposite funzionalità.

Di seguito è riportato un esempio di fascicoli per l'Amministrazione universitaria:

- fascicolo generale: utilizzati per inserire tipologie documentali omogenee;
- fascicolo dello studente: fascicoli di persona fisica;
- fascicolo di affare: si tratta di fascicoli che vengono aperti con un provvedimento formale oppure relativi ad attività ripetitive e standardizzate (es. fascicoli delle Sedute del Consiglio di Amministrazione);
- fascicolo del dipendente: fascicoli di persona fisica;
- fascicolo di procedimento amministrativo: contengono documenti differenti quali atti formali, istanze, note ad es. un classico fascicolo di procedimento amministrativo è quello del concorso per il reclutamento del personale o per una gara.

Il manuale di gestione, proprio perché prevede le regole di gestione e conservazione dei documenti, può contenere anche una mappatura delle principali tipologie documentali gestite dal soggetto produttore e, in particolare, può riportare anche l'elenco delle serie di documenti che presentano caratteristiche intrinseche ed estrinseche omogenee più rappresentative e registrate in apposito repertorio o registro.

Ogni registrazione o documento a repertorio deve riportare:

- numero di repertorio progressivo e annuale (generato in modo non modificabile)
- dati identificativi di ciascun atto (autore, destinatario, oggetto, data: generati in modo non modificabile)
- dati di classificazione
- anche per le registrazioni e i documenti a repertorio è opportuno dare indicazione delle tempistiche di conservazione

L'attenzione alla fase della conservazione inizia già nel momento in cui si forma il documento e nella definizione e compilazione del corredo informativo costituito dai metadati.

Concettualmente, sia in ambito cartaceo che in ambito digitale, è opportuno distinguere la fase gestionale da quella conservativa del documento informatico, perché ognuna di esse richiede un'attenzione focalizzata su aspetti specifici: un rilievo particolare è conferito alla dimensione relazionale e procedurale nella fase gestionale; un rilievo viene posto invece alle integrità e autenticità delle informazioni da mantenere stabili e immodificabili nel tempo, nella fase conservativa. Di conseguenza il documento informatico può richiedere informazioni di corredo diverse in relazione ai due momenti in cui è considerato. Tuttavia gestione e conservazione sono fortemente correlate, come lo è la natura unica dell'archivio, in quanto corpus inscindibile: questa caratteristica non necessariamente entra in conflitto con la necessità di affidare subito al sistema di conservazione i documenti informatici appena formati in quanto realtà imposta dall'aggiornamento costante dei sistemi di gestione.

Pertanto è bene che i documenti rechino con sé, fin dalla formazione, tutti i metadati utili alle diverse fasi, con la possibilità di aggiungere altri set di corredo anche in un momento successivo, ad esempio dopo la chiusura del fascicolo/aggregato documentale informatico potrà essere aggiornato il dato relativo allo stato del fascicolo (aperto, chiuso) e dell'archivio di pertinenza (corrente, deposito, storico) secondo le tempistiche previste.

La documentazione da destinare alla conservazione, quindi, deve essere descritta in termini di:

- natura della documentazione (es. tipologia, classe);
- formato utilizzato;
- elenco e descrizione dei metadati;
- periodo di conservazione;
- tutte le informazioni ritenute utili per la conservazione.

La documentazione da trasferire nel sistema di conservazione viene esaminata dal conservatore con la collaborazione del produttore. Si procede dunque alla ricognizione puntuale delle tipologie documentali da trasferire nel sistema di conservazione partendo dall'analisi delle modalità di gestione delle stesse nel sistema di gestione documentale. A tal fine è fondamentale che il soggetto produttore invii in conservazione tutta la documentazione su cui si basa l'attività di gestione dei documenti come il manuale di gestione, il titolario, il registro di protocollo ed i repertori, il piano di conservazione, l'organigramma e le responsabilità.

La normativa italiana infatti ha da sempre differenziato il sistema di conservazione dal servizio di gestione documentale in quanto identificano fasi differenti della vita di un archivio:

- il servizio di gestione documentale permette la gestione dell'archivio corrente ovvero dei documenti utili alla trattazione dei procedimenti e degli affari in corso

- il sistema di conservazione garantisce, nel lungo termine, il valore legale dei documenti conservati e l'esibizione all'utente che rientrando nella *"comunità di riferimento"* ha diritto alla consultazione dei documenti conservati.

Il Responsabile della gestione documentale d'intesa con il Responsabile della conservazione e con il Responsabile del trattamento dati personali effettua l'analisi dei procedimenti amministrativi e una ricognizione delle tipologie documentali.

Questo lavoro di mappatura delle tipologie documentali prodotte e acquisite dal produttore risulta fondamentale almeno per i seguenti motivi:

- per l'analisi dei documenti protocollati e non protocollati;
- per l'analisi della classificazione apposta sui documenti;
- per l'analisi dei documenti antecedenti all'adozione del titolario e perciò non classificati ma ordinati secondo altro criterio;
- per l'elaborazione del massimario di selezione e scarto e quindi per la verifica dei tempi di scarto dei documenti;
- per verificare le incongruità tra i documenti solo analogici non inseriti nel fascicolo elettronico e viceversa: mappatura dei documenti nativi digitali che ai sensi della normativa vigente vanno conservati elettronicamente;
- mappatura dei documenti originali unici per i quali va garantita la conservazione dell'originale su supporto analogico;
- mappatura dei documenti rilevanti ai fini tributari (es. fatture) che rientrano nel registro di protocollo ufficiale o in altri registri;
- mappatura dei documenti (verbali, determine, contratti, ecc.) che rientrano in registri e repertori i quali seguono una numerazione differente da quella del registro di protocollo ufficiale;
- mappatura dei documenti che confluiscono nel servizio di gestione documentale da altri applicativi;
- analisi dell'archivio nella sua complessità e quindi l'identificazione di documenti ibridi (sia cartacei che digitali), quali invece sono solo cartacei e quali sono esclusivamente digitali;
- analisi dei formati utilizzati e definizione della tempistica di conservazione in base alla tipologia documentale.

Di seguito alcuni dei principali riferimenti normativi che insistono sulle diverse tipologie documentali:

- D.P.R. 26 ottobre 1972, n. 633 "Istituzione e disciplina dell'imposta sul valore aggiunto." (GU n.292 del 11 novembre 1972 - Suppl. Ordinario);
- D.P.R. 29 settembre 1973, n. 600 "Disposizioni comuni in materia di accertamento delle imposte sui redditi." (GU n .268 del 16 ottobre 1973 - Suppl. Ordinario);
- Codice Civile, articoli 2216, 2217, 2220, 2963;
- Circolare Agenzia delle Entrate 18/E, 2014;
- Circolare del Ministero della Sanità n. 900, 19 dicembre 1986;
- Decreto ministeriale del 9 luglio 2008.

A titolo meramente esemplificativo fare riferimento agli allegati B – Metadati del documento informatico, C – Metadati del fascicolo informatico e D – Elenco delle tipologie di documenti comuni da conservare per tipologia di amministrazione.

7.3 Predisposizione del manuale di conservazione

Il manuale della conservazione è il documento di riferimento in cui vengono descritte in modo dettagliato fasi di lavoro, strumenti e responsabilità che caratterizzano tutta l'attività di conservazione.

Lo scopo del manuale è quello di condividere il metodo tra produttore e conservatore e renderlo noto anche a chi ne abbia interesse; qualora il conservatore sia accreditato presso l' AgID il manuale è pubblicato in elenco all'indirizzo http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione/elenco-conservatori-attivi .

Le regole tecniche per la conservazione, adottate dal DPCM 3 dicembre 2013 all'art. 8, comma 2 tracciano una sorta di indice minimo degli argomenti che vanno trattati in questo manuale e cioè:

a) mantenere traccia dei soggetti che hanno assunto, nel tempo, la responsabilità del sistema di conservazione;
b) descrivere la struttura organizzativa, in cui sono chiari funzioni responsabilità e obblighi di chi interviene nel processo di conservazione sia nel ruolo di produttore che di conservatore;
c) descrivere gli oggetti che vengono conservati in termini di

- tipologia: registro di protocollo giornaliero, determinazioni di spesa, fattura elettronica[..] ;
- formato: indicare in quale formato vengono conservati i documenti per singola tipologia: pdf, jpg, xml e altri. In proposito è bene tener presente che l'art. 11 delle regole tecniche DPCM 3 dicembre 2013 limita le tipologie a quelle previste dal suo allegato 2 che viene periodicamente aggiornato. Alla data i formati indicati per la conservazione sono:
  - per i documenti e per gli allegati ai messaggi di posta: PDF, PDF/A, TIFF, JPG, office open XML (OOXML), ODF, XML, TXT;
  - per i messaggi di posta: RFC 2822/MIME.
- metadati: elencare cioè le informazioni che ne caratterizzano l'identificazione certa. Tali informazioni (metadati) sono organizzate in file xml, associate indissolubilmente al documento secondo quanto disposto dalle regole tecniche e devono necessariamente riferirsi almeno a:
  - (nel caso si tratti di un documento informatico)
    - identificativo;
    - data chiusura;
    - oggetto;
    - soggetto produttore;
    - destinatario;
  - (nel caso si tratti di un documento amministrativo informatico)
    - identificativo;
    - segnatura di protocollo ai sensi del D.P.R. 28 dicembre 2000, n. 445 art. 53 e delle regole tecniche per il protocollo informatico DPCM 3 dicembre 2013;
    - mittente;
    - destinatario.

d) descrivere il metodo di versamento in conservazione da parte del produttore, che, si ricorda, deve avvenire per gruppi di documenti - c.d. pacchetti – e che deve terminare con un rapporto di esito emesso dal conservatore; analogamente va descritto il metodo inverso, ossia quello c.d. di esibizione, quando cioè il produttore richiede al conservatore di recuperare ed esibire un documento precedentemente affidatogli per la conservazione;

e) descrivere il processo di conservazione ed il trattamento dei documenti nel sistema di conservazione; in tale sezione del manuale è necessario descrivere almeno quanto previsto dall'art.9 delle regole tecniche DPCM 3 dicembre 2013 ossia:

- metodo di acquisizione e presa in carico del pacchetto da parte del conservatore;
- tipo di verifiche effettuate sulla congruità del pacchetto da parte del conservatore e come viene gestito l'inevitabile rifiuto in caso di anomalie;
- metodo di produzione del rapporto di versamento di uno o più pacchetti che, ricordiamo, deve contenere anche un riferimento temporale (specificato con data e ora di riferimento internazionale, il c.d. UTC, tenendo conto dei periodi in cui è in vigore o meno l'ora legale. Vale a dire, ad esempio, che se deve riferire il giorno 10 luglio 2015 ore 12:30:29 a Roma, deve essere trascritto 10 luglio 2015 ore 10:30:29 mentre se deve riferire il giorno 8 novembre 2015 h 12:30:29 a Roma, deve essere trascritto 8 novembre 2015 h 11:30:29) ed una o più impronte calcolate sull'intero contenuto del pacchetto;
- metodo di calcolo delle impronte calcolate sull'intero contenuto del pacchetto;
- metodo di preparazione del pacchetto di archiviazione da parte del conservatore e validazione con firma digitale da parte del Responsabile della conservazione; si ricorda che la struttura di questo pacchetto deve essere conforme a quanto previsto dal DPCM 3 dicembre 2013 allegato 4;
- metodo di preparazione del pacchetto di distribuzione da parte del conservatore e validazione con firma digitale da parte del Responsabile della conservazione; tale evento è previsto quando l'utente chiede l'accesso ad un documento conservato e ne possiede titolo per accedere allo stesso;
- metodo di produzione di duplicati informatici e/o copie informatiche del documento conservato richieste dall'utente nel rispetto di quanto prescritto dal DPCM 13 novembre 2014, dall'effettivo diritto di accesso dell'utente medesimo al documento e da quanto previsto in tema di trattamento dei dati personali;
- metodo adottato per lo scarto del pacchetto di archiviazione nel rispetto delle disposizioni del MIBACT e della norma vigente in tal senso.

f) descrivere il sistema di conservazione negli aspetti prettamente tecnici: quali sono le componenti tecnologiche, fisiche e logiche utilizzate, quali le misure di sicurezza e come le stesse vengono gestite ed evolute nel tempo;

g) descrivere come viene svolto il monitoraggio sul corretto funzionamento del sistema di conservazione e sull'integrità dei documenti conservati. In questo ambito va evidenziato il comportamento che andrebbe ad adottarsi in caso anomalie;

h) descrivere il procedimento che consente ad un utente di richiedere l'esibizione di un documento conservato, su che base questa richiesta viene accolta o rifiutata, quali azioni ne conseguono e come vengono espletate (ad esempio: in caso di rifiuto, si riporta all'utente tale decisione con la motivazione oppure in caso di accettazione si risponde all'utente con copia del documento richiesto, ottenuta dal conservatore in forma di pacchetto di distribuzione), di conseguenza vanno anche descritte le modalità di produzione dei duplicati o copie del documento;

i) riportare, per tipologia, i tempi entro i quali i documenti debbano essere proposti allo scarto oppure avviati in conservazione facendo riferimento in tal senso al proprio manuale di gestione del protocollo informatico e gestione documentale;

j) indicare i procedimenti ed casi in cui interviene il pubblico ufficiale;

k) indicare le normative in vigore nei luoghi in cui vengono conservati i documenti.

Oggetto del manuale di conservazione	**Di competenza del produttore**	**Di competenza del conservatore**	**Di competenza di entrambi**
I dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa			X
La struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione			X

La descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni			X
La descrizione delle modalità di presa in carico di uno o più pacchetto di versamento comprensiva della predisposizione del rapporto di versamento		X	
La descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione		X	
La modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione			X
La descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime		X	
La descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie			X

La descrizione delle procedure per la produzione di duplicati o copie			X
I tempi entro i quali le diverse tipologie di documenti devono essere scartate ovvero trasferite in conservazione, ove, nel caso delle pubbliche amministrazioni, non già presenti nel manuale di gestione	X		
Le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento			X
Le normative in vigore nei luoghi dove sono conservati i documenti		X	

7.4 Definizione del modello applicativo di riferimento per il versamento dei documenti

I documenti informatici da avviare in conservazione devono essere preparati affinché, una volta inseriti nel sistema di conservazione, ne sia garantita l'autenticità, l'affidabilità, la leggibilità e la reperibilità. Il conferimento dei documenti nel sistema di conservazione si esplica nella produzione del pacchetto di versamento ossia nell'estrazione dei documenti/fascicoli/aggregazioni documentali e delle relative informazioni di contesto e metadati dalle varie applicazioni informatiche presenti nel sistema informativo dell'Amministrazione e successivo trasferimento al sistema di conservazione.

Le caratteristiche del pacchetto di versamento vanno concordate tra produttore e conservatore, con un livello di formalizzazione adeguato al modello organizzativo del processo di conservazione, in particolare se il conservatore è un soggetto giuridico esterno all'Amministrazione vi sarà necessariamente un contratto di servizi e le specifiche del pacchetto di versamento saranno disciplinate nei relativi accordi di servizio. Indipendentemente dal livello di formalizzazione degli compiti tra le parti, le caratteristiche del processo di versamento vanno documentate nel manuale di conservazione.

Nella definizione delle modalità applicative con cui realizzare il versamento si considerano:

- le caratteristiche del sistema informativo documentale della PA, quali il livello di eterogeneità/frammentazione delle varie applicazioni informatiche che lo compongono, le possibilità di estrazione native che offrono le varie applicazioni piuttosto che venga richiesto uno sviluppo *ad hoc* (es. *query database*, *webservices*...),
- la capacità dell'Amministrazione in termini di competenze informatiche, tramite personale interno o necessità più o meno spinta per l'ente di contattare i fornitori delle varie applicazioni per "adattarsi" all'interfaccia e i relativi costi;
- la disponibilità del conservatore di offrire interfacce differenti di versamento.

Tale preparazione consiste nel:

- assicurarsi che il documento informatico sia in formato accettato dal sistema di conservazione; in tal senso, si segnala che il DPCM 3 dicembre 2013 individuano idonei per la conservazione i seguenti formati perché assicurano leggibilità e reperibilità del documento.
- assicurarsi che al documento siano collegate, in maniera indissolubile, informazioni (metadati) necessarie a qualificarlo ed identificarlo univocamente; è buona prassi ragionare per classe documentale a cui associare il documento informatico da conservare e convenire con il conservatore quali informazioni utilizzare ai fini della sua identificazione e riconducibilità. Nel definire tale convenzione con il conservatore va tenuto presente che l'allegato 5 del DPCM 3 dicembre 2013 impone un set minimo di metadati.

- inserire il documento in un file "contenitore" (pacchetto) che a sua volta è associato in maniera indissolubile ad un file di indice che descrive il contenuto ed i dati relativi alla richiesta di versamento in conservazione;
- apporre la firma qualificata o digitale del Responsabile della conservazione sul pacchetto così confezionato.

A questo punto il produttore consegna il pacchetto, su cui può essere apposta la firma digitale, al sistema di conservazione; quest'ultimo effettua subito una verifica sul fatto che il pacchetto ed i documenti in esso contenuti siano stati preparati nel rispetto di quanto previsto dalle regole condivise e descritte dal manuale di conservazione. Se tutto è a posto, il produttore riceve dal sistema un rapporto di versamento ed il sistema procede al suo interno a produrre, in forma analoga a quanto ha fatto il produttore, il pacchetto di archiviazione e quindi a depositare in conservazione il pacchetto ricevuto dal produttore. Se qualcosa non va, il sistema segnala la problematica al produttore e rimane in attesa di istruzioni per superarla (istruzioni che possono essere la sostituzione del pacchetto, l'integrazione oppure il benestare a procedere nonostante l'anomalia quando la sua gravità non è tale da compromettere la rintracciabilità e la leggibilità del documento).

Quando invece il produttore voglia recuperare un documento conservato deve farne richiesta al sistema di conservazione fornendo dati utili all'individuazione del documento; con queste informazioni il sistema è in grado di rintracciare il documento, del quale ne confeziona copia con regole del tutto similari a quelle usate per produrre il pacchetto di versamento o il pacchetto di distribuzione, e che consegna in forma di pacchetto di esibizione al produttore che ne ha fatto richiesta.

Il produttore ed il conservatore devono interagire rispetto alla gestione dello scarto, in base a quanto definito con il Ministero dei beni e delle attività culturali e del turismo, e del riversamento dei documenti conservati per garantire la conservazione dei documenti a norma nel tempo.

Questa interazione tra produttore e conservatore, rappresentata dalla Figura 6 - Rappresentazione dei flussi di interazione tra produttore e conservatore, va tenuta in alta considerazione nella progettazione del modello applicativo che s'intende adottare.

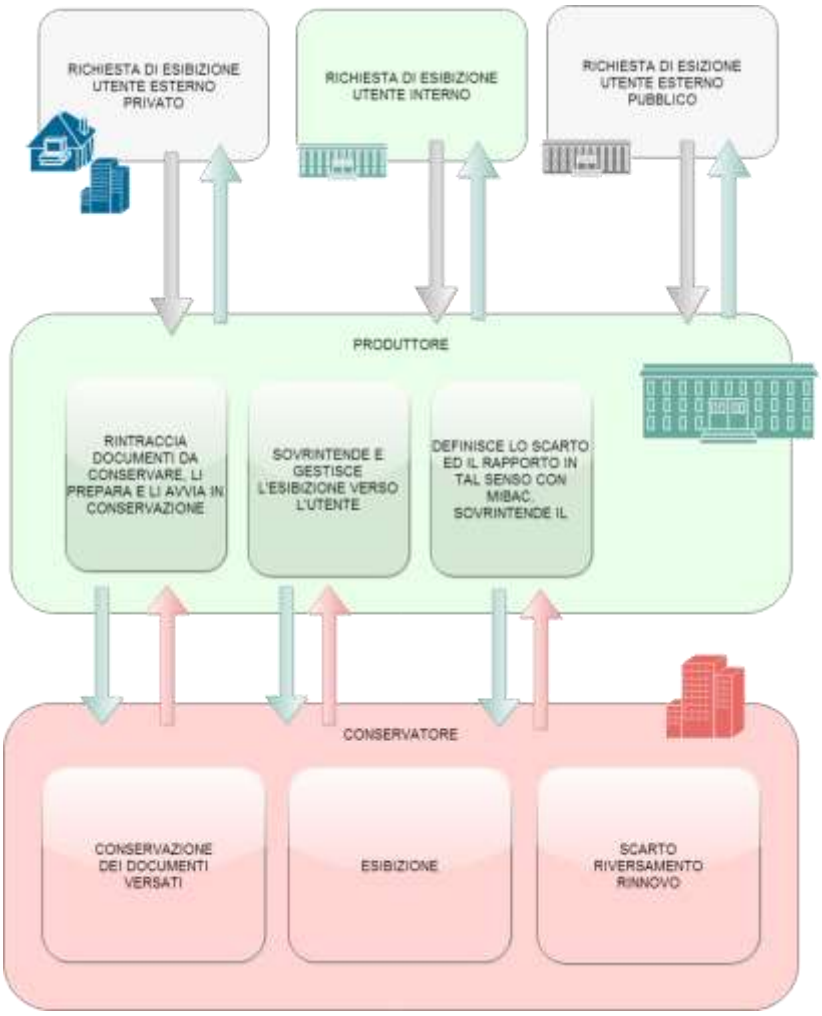

Figura 6 - Rappresentazione dei flussi di interazione tra produttore e conservatore

Emergono infatti evidenti due livelli di interazione:

- ad elevata integrazione, tra il sistema di gestione documentale del produttore (tipicamente integrato e condiviso nel sistema di gestione applicativa del produttore) ed il sistema di conservazione; questo livello è garantito ricorrendo all'uso di *web services* che garantiscono la cooperazione applicativa tra i due sistemi.
- a media integrazione, tra il sistema di gestione documentale e gli utenti esterni, che siano essi pubblici o privati; in tale contesto è sicuramente importante abilitare un livello di interazione tra il sistema di gestione documentale, il sistema di conservazione ed il sistema di servizi online di cui possono far uso gli utenti esterni.

Nella scelta del modello applicativo da adottare è quindi importante tener conto di:

- quale livello di interazione tra sistema di gestione documentale e sistema di conservazione si intende usufruire;

- quali opportunità di comunicazione si intende avere a disposizione per scambiare dati e documenti tra il sistema di gestione documentale ed il sistema di conservazione.

Il modello più performante è quello che elimina la quasi totalità delle fasi manuali affidandole quanto più possibile ad automatismi di cooperazione applicativa tra il sistema usato dal produttore per produrre i documenti informatici ed il sistema usato dal conservatore per conservarli.

In particolare, il produttore dovrebbe essere in grado di produrre in autonomia i pacchetti di versamento, nell'ambito del proprio ambiente gestionale o direttamente con il sistema del conservatore a cui accede in modalità *cloud computing*. Tale condizione dovrà essere disciplinata nella procedura di acquisto.

7.5 Acquisizione del servizio di conservazione da soggetti privati tramite gara d'appalto

La scelta di affidare a terzi il servizio di conservazione per una Pubblica Amministrazione, ex art. 5 comma 2 lett. b) delle regole tecniche DPCM 3 dicembre 2013, è possibile se il produttore affida il servizio ad un soggetto privato accreditato presso l'Agenzia per l'Italia Digitale ai sensi dell'art. 44-bis del CAD; a fronte della corresponsione di un importo per il servizio reso, il produttore ha la certezza che il suo archivio è conservato secondo tecnologia e sicurezza idonei a garantire la sua integrità, leggibilità ed accessibilità. Affidare i propri documenti ad un soggetto accreditato implica inoltre anche la scelta di avvalersi di un servizio rispondente pienamente alle regole tecniche DPCM 3 dicembre 2013 sul piano tecnologico, sulla cooperazione applicativa e sulla sicurezza.

Il conservatore deve garantire:

- la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale;
- un accesso ai dati al produttore.

Oltre all'osservanza delle regole tecniche, sussistono però anche fattori importanti a rendere "pratica" l'attività di conservazione; infatti, è importante puntare quanto più possibile ad evitare che il produttore debba preoccuparsi di trovare il modo di rintracciare i documenti, costruire i pacchetti di versamento in autonomia (ma nel rispetto del DPCM 3 dicembre 2013) e trovare il modo di trasmetterli al conservatore ma dovrebbe avere, in tal senso, supporto dal conservatore con strumenti informatici idonei a supportare anche tale attività contenendo al massimo la spesa.

In tale ottica, sarebbe molto importante avere almeno l'opportunità di fruire in *cloud* del servizio in modo che:

1. accolga i documenti, li predisponga per la conservazione e li conservi;

2. dia la possibilità di monitorare il proprio archivio in conservazione;
3. accolga le richieste di esibizione e le esegua.

Fondamentale a tal fine appare l'attivazione di una cooperazione applicativa, tramite *web services,* tra il sistema di gestione documentale del produttore ed il sistema di conservazione.

Infine, va prestata molta attenzione su come governare la conclusione del contratto in caso di recesso o scadenza. Devono essere garantita la predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori. Deve essere prevista la possibilità di riversare tutti i documenti informatici conservati, completi dei file a corredo per la loro corretta tenuta in archivio, nel nuovo sistema di conservazione indicato dal produttore tramite funzioni conformi allo standard UNI SinCRo su canali di comunicazione sicuri.

7.6 Acquisizione del servizio di conservazione da soggetti pubblici tramite convenzione

La conservazione dei documenti rappresenta per le pubbliche amministrazioni una funzione di carattere istituzionale. Esse infatti, come già ricordato, sono tenute per legge a conservare i propri documenti e archivi sia come testimonianza diretta delle loro azioni al servizio della collettività che come memoria storica.

Le regole tecniche sulla conservazione prevedono la possibilità di affidare, mediante contratto o convenzione di servizio, la conservazione a soggetti esterni pubblici o privati che offrano idonee garanzie organizzative e tecnologiche, accreditati come conversatori presso l'Agenzia per l'Italia Digitale. L'affidamento a soggetto esterno può essere effettuato a tali condizioni, fatte salve le competenze del MIBACT che mantiene la competenza in materia di tutela dei sistemi di conservazione degli archivi pubblici o degli archivi privati che rivestono interesse storico particolarmente importante.

Oltre a forme contrattuali simili a quelle con i privati, le pubbliche amministrazioni possono concludere tra loro specifici accordi per lo svolgimento in collaborazione di attività di interesse comune.

Nel caso della conservazione l'interesse comune tra produttore e soggetto conservatore si può identificare nel reciproco interesse alla corretta conservazione del patrimonio documentale pubblico: obbligo di legge per l'ente produttore e funzione specifica di un conservatore pubblico. Inoltre può contribuire a raggiungere l'obiettivo di creare un circuito virtuoso che permetta a tutte le Pubbliche Amministrazioni di muoversi in maniera condivisa per costituire forme sempre più strette di accordo, collaborazione e cooperazione istituzionale tra i soggetti che operano in ambito archivistico per la conservazione, tutela e valorizzazione della documentazione archivistica, dal momento della sua formazione sino alla fase di conservazione permanente a fini di memoria storica.

La legge 7 agosto 1990, n. 241 e s.m.i. recante *"Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"* stabilisce espressamente all'art. 15 che: *"le amministrazioni pubbliche possono sempre concludere tra loro accordi per disciplinare lo svolgimento in collaborazione di attività di interesse comune".*

L'art. 2, comma 1 del CAD stabilisce che: "*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".*

Lo sviluppo della amministrazione digitale, normata dal CAD, è ampiamente improntata a logiche di collaborazione e cooperazione attiva tra le Amministrazioni, attuabili con la promozione di intese ed accordi, al fine di promuovere azioni tese principalmente a realizzare un processo di digitalizzazione dell'azione amministrativa a garanzia di un migliore servizio al cittadino e alle imprese ed attuare il trasferimento delle soluzioni tecniche ed organizzative per prevenire il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.[43]

La determinazione dell'Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture n. 7 del 21 Ottobre 2010 su *"Questioni interpretative concernenti la disciplina dell'articolo 34 del d.lgs. 163/2006 relativa ai soggetti a cui possono essere affidati i contratti pubblici"*, conformemente a quanto in precedenza affermato dalla giurisprudenza comunitaria, ha ribadito la legittimità del ricorso a forme di cooperazione pubblico-pubblico attraverso cui più amministrazioni assumono impegni reciproci, realizzando congiuntamente le finalità istituzionali affidate loro, purché vengano rispettati una serie di presupposti. I presupposti richiesti ai fini della legittimità dell'impiego dello strumento convenzionale sono stati individuati nei seguenti punti:

a) l'accordo deve regolare la realizzazione di un interesse pubblico, effettivamente comune ai partecipanti, che le Parti hanno l'obbligo di perseguire come compito principale, da valutarsi alla luce delle finalità istituzionali degli Enti coinvolti;
b) alla base dell'accordo deve esserci una reale divisione di compiti e responsabilità;

43 Cfr. art 14 CAD, in particolare commi 2, 2-bis, e 3 che recitano rispettivamente: "2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi... per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso... . 2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali . 3. Lo Stato … promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diverse dimensioni e collocazione territoriale.".

c) i movimenti finanziari tra i soggetti che sottoscrivono l'accordo devono configurarsi solo come ristoro delle spese sostenute, essendo escluso il pagamento di un vero e proprio corrispettivo, comprensivo di un margine di guadagno;
d) il ricorso all'accordo non può interferire con il perseguimento dell'obiettivo principale delle norme comunitarie in tema di appalti pubblici, ossia la libera circolazione dei servizi e l'apertura alla concorrenza non falsata negli Stati membri.

Tale considerazione è stata recentemente ribadita da un recente parere del Consiglio di Stato:

"In linea di principio, non sono soggetti alle direttive appalti e sono dunque legittimi, gli accordi tra pubbliche amministrazioni, anche se appartenenti ad ordinamenti autonomi e/o in rapporto di reciproca indipendenza, finalizzati alla cooperazione cd. non istituzionalizzata/orizzontale" purché il trasferimento di risorse resti "entro i ristretti limiti del riconoscimento di un corrispettivo forfettario a copertura delle spese vive sostenute".[44]

Inoltre singole Regioni hanno espressamente legiferato in tema di conservazione digitale anche a supporto degli enti del territorio.

Ad esempio la L. R. dell'Emilia-Romagna del 24 maggio 2004, n. 11 e s.m.i. (recante "Sviluppo regionale della società dell'informazione") con la modifica introdotta dalla L. R. 24 ottobre 2013, n.17 stabilisce all'art. 2, comma 4-bis, che: *"La Regione, anche in collaborazione con le altre pubbliche amministrazioni interessate, favorisce altresì lo sviluppo integrato della conservazione digitale dei documenti informatici e, nel rispetto dei principi di efficacia, efficienza ed economicità, svolge le funzioni di archiviazione e conservazione digitale dei documenti informatici..."*.

Più in dettaglio la normativa della Regione Emilia-Romagna prevede che sia l'Istituto per i beni artistici culturali e naturali (IBACN), che su mandato della Regione stessa: *"svolge le funzioni di archiviazione e conservazione digitale dei documenti informatici anche a rilevanza fiscale, con le modalità previste dalle disposizioni vigenti, prodotti o ricevuti dalla Regione e dagli altri soggetti di cui all'articolo 19, comma 5, lettera a) della legge regionale 24 maggio 2004, n. 11 nonché, mediante apposita convenzione, dei documenti informatici prodotti o ricevuti dai soggetti di cui all'articolo 19, comma 5, lettera b) della medesima legge e da altri soggetti pubblici"*[45].

I soggetti indicati al citato articolo 19 sono rispettivamente:

44 È questo in sintesi il principio sancito nel parere reso dalla Seconda Sezione del Consiglio di Stato, Adunanza di Sezione del 22.4.2015, n. 1178. Cfr: http://www.ilquotidianodellapa.it/_contents/news/2015/aprile/1429736919882.html e https://www.giustiziaamministrativa.it/cdsintra/cdsintra/AmministrazionePortale/DocumentViewer/index.html?ddocname=GTNTIBYCJIRJ3BX7RNLA7O4EGU&q=costi.

45 Articolo 2, comma 1 lettera f-bis della L.R. 29/1995, così come modificato dalla L. R. 17/2013

a) la Regione, gli enti e gli organismi regionali, le loro associazioni e consorzi, quali le agenzie, le aziende egli istituti, anche autonomi, nonché gli enti e le aziende del Servizio sanitario regionale, ed inoltre gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria dai soggetti precedenti

b) gli Enti locali, i loro enti e organismi, le loro associazioni, unioni e consorzi, quali le aziende e gli istituti, anche autonomi, le istituzioni, gli organismi di diritto pubblico e le società strumentali partecipate in misura totalitaria o maggioritaria da tali soggetti, ed inoltre gli istituti di istruzione scolastica e universitaria presenti e operanti nel territorio regionale

I soggetti elencati al punto a), ai sensi del comma 3 dell'art. 16 della L.R. 11/2004 sono "obbligati" ad utilizzare le funzioni di archiviazione e conservazione digitale dei documenti informatici svolte da IBACN. Invece quelli elencati al punto b) hanno la facoltà di utilizzare le funzioni di conservazione svolte da IBACN, approvando e sottoscrivendo una apposita convenzione, secondo lo schema definito dall'IBACN stesso per gli enti del territorio della regione Emilia-Romagna, pubblicata nel sito specifico del Servizio Polo archivistico (Parer).[46]

Si può quindi dire che l'apparato legislativo della Regione Emilia-Romagna individua uno specifico soggetto pubblico che svolge le funzioni di archiviazione e conservazione digitale per la Regione e gli altri enti sopracitati, in particolare gli enti e le aziende del Servizio sanitario regionale, nella logica di sviluppo integrato della conservazione digitale dei documenti informatici nel rispetto dei principi di efficacia, efficienza ed economicità. Infatti per garantire risparmi ed efficienza si concentra in un soggetto specializzato una funzione complessa come quella della conservazione degli oggetti digitali.

Anche la recente legge regionale della Regione Marche 16 febbraio 2015, n. 3 concernente "Legge di innovazione e semplificazione amministrativa" all'art. 15 (Polo di conservazione Marche DigiP) stabilisce che:

1. *Gli atti della Regione sono prodotti e conservati in originale informatico e firmati digitalmente.*
2. *Per le finalità indicate al comma 1, la Regione utilizza un sistema di conservazione dei documenti digitali che garantisce il mantenimento nel tempo dei requisiti di integrità, autenticità e intellegibilità dei documenti informativi denominato "Polo di conservazione Marche DigiP".*

46 http://parer.ibc.regione.emilia-romagna.it/conservazione/enti-emilia-romagna.

3. I servizi indicati al comma 2 possono essere utilizzati anche dagli enti strumentali, dagli enti locali e dagli enti del servizio sanitario regionale previa stipulazione di appositi accordi.[47]

Si può ricordare inoltre la legge della Regione Toscana 05 ottobre 2009, n. 54 *"Istituzione del sistema informativo e del sistema statistico regionale. Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell'informazione e della conoscenza, che prevede all'articolo 10 Attività documentale"* che:

1. Nel rispetto del d.lgs. 82/2005, la Regione intraprende le azioni necessarie per la dematerializzazione dei documenti amministrativi, incentivandone l'archiviazione in formato digitale con modalità che ne consentono la conservazione e la fruibilità nel tempo.

2. La Giunta regionale predispone e mantiene una piattaforma tecnologica e servizi digitali per la conservazione dei documenti informatici, che consente di gestire in modo unitario i documenti in formato cartaceo e digitale e di validare e certificare i processi di archiviazione documentale che hanno come presupposto la gestione informatica dei flussi documentali.

3. La Regione rende la piattaforma tecnologica e i servizi digitali di cui al comma 2 disponibili ai soggetti pubblici che ne vogliono usufruire.

Anche altri enti come la Provincia Autonoma di Trento hanno stabilito per legge la costruzione di poli archivistici. In particolare la L.P. 27 luglio 2012, n. 16 ("Disposizioni per la promozione della società dell'informazione e dell'amministrazione digitale e per la diffusione del software libero e dei formati di dati aperti") ha istituito il sistema informativo elettronico trentino (SINET) quale complesso dei dati e delle informazioni a supporto delle attività di tutte le pubbliche amministrazioni del Trentino in un'ottica di cooperazione e collaborazione, anche per l'attuazione delle norme sull'archiviazione e conservazione digitale. Nello specifico, l'art. 13 della legge provinciale 27 luglio 2012, n. 16, rubricato "Istituzione del polo archivistico digitale territoriale del Trentino", stabilisce che *"Per le finalità individuate dall'articolo 1 e per gli obiettivi definiti dall'articolo 2, nell'ambito del SINET può essere istituito il polo archivistico digitale territoriale del Trentino, per promuovere la cultura ed erogare i servizi per la dematerializzazione dei procedimenti amministrativi e l'archiviazione digitale dei documenti",* precisando al secondo comma che: *"Il polo eroga i propri servizi alle organizzazioni del settore pubblico trentino e, ove consentito dalla vigente normativa, alle*

47 Già in precedenza con la deliberazione della Giunta Regione Marche n. 265 del 10/03/2014 ad oggetto: "Schema di convenzione tra la Regione medesima e gli Enti locali delle Marche e le loro forme associate, per l'avvio dei servizi di conservazione dei patrimoni documentali informatici da questi ultimi prodotti e mantenuti", in accordo con gli orientamenti nazionali in materia di dematerializzazione dei documenti, si era dato avvio ai servizi del polo di conservazione digitale Marche Digip.

organizzazioni private", secondo un progetto di fattibilità approvato con deliberazione della Giunta provinciale.

Tale previsione si è recentemente concretizzata nella produzione di una serie di documenti e di atti amministrativi finalizzati a definire gli strumenti necessari per gli adempimenti di tipo giuridico-formale e operativo relativi all'attivazione e alla gestione del processo di conservazione digitale predisposti dall'Ufficio Beni archivistici, librari e Archivio provinciale a supporto degli enti vigilati di competenza della Provincia autonoma di Trento, indirizzati quindi alla pubbliche amministrazioni del Trentino.[48]

Sulla base di tali esperienze si può quindi concludere che, nel rispetto della normativa vigente, è pienamente legittimo il ricorso ad accordi tra enti pubblici per lo svolgimento di attività di conservazione.

Diversi modelli di convenzione possono essere reperiti nei siti dei conservatori pubblici accreditati o possono essere opportunamente sviluppati in riferimento a casistiche particolari.

È infine da ricordare che gli accordi ai sensi dell'art. 15 della Legge 7 agosto 1990, n. 241 a fare data dal 30 giugno 2014 debbono obbligatoriamente essere sottoscritti con firma digitale, o con firma elettronica avanzata o qualificata, a pena di nullità.

7.7 Acquisizione del servizio per la progettazione e realizzazione del sistema interno di conservazione (gara d'appalto)

Questa modalità di attivazione del servizio di conservazione pone il produttore nella condizione di affrontare considerevoli investimenti diretti per mantenere il suo sistema nel rispetto delle regole tecniche del DPCM 3 dicembre 2013, ivi compresi gli obblighi sul *disaster recovery* e continuità operativa, e quelli conseguenti ad eventuali ulteriori interventi normativi.

Sussistono però condizioni che giustificano tale scelta in funzione dell'autonomia e della creazione di un sistema veramente integrato ed a misura dell'Ente: è il caso, ad esempio, di enti che trattano documenti protetti da codici di segretezza che ne vietano l'affidamento a soggetti esterni al produttore per ragioni di tutela e sicurezza nazionale.

In tale contesto, è consigliabile bandire una gara per la progettazione e la realizzazione del sistema interno di conservazione con:

1. Requisiti tecnici pienamente rispondenti al DPCM 3 dicembre 2013 ed alla circolare dell'Agenzia per l'Italia Digitale del 15 gennaio 2014 n. 64; in tal senso si faccia riferimento anche a quanto disposto:

48 Cfr. la documentazione pubblicata nel sito Trentino Cultura: https://www.cultura.trentino.it/Il-Dipartimento/Soprintendenza-per-i-beni-culturali/Ufficio-beni-archivistici-librari-e-Archivio-provinciale/Strumenti/2-Strumenti-per-la-conservazione-dei-documenti-informatici.

- nel precedente paragrafo,
- nello schema di manuale di conservazione reso disponibile dall'AgID;
- nello schema di piano di sicurezza reso disponibile dall'AgID.

2. Clausola contrattuale sulla proprietà del prodotto software sviluppato e dei prodotti in genere; è bene prevedere che il produttore acquisisca il diritto di proprietà e, quindi, di utilizzazione e sfruttamento economico, di tutto quanto realizzato dalla Ditta aggiudicataria in esecuzione del contratto, dei relativi materiali e documentazione creati, inventati, predisposti o realizzati dalla Ditta aggiudicataria o dai suoi dipendenti nell'ambito o in occasione dell'esecuzione del contratto. Prevedere inoltre che il produttore possa, senza alcuna restrizione, utilizzare, pubblicare, diffondere, duplicare o cedere anche solo parzialmente detti materiali ed opere dell'ingegno; questi diritti devono intendersi acquisiti dal produttore in modo perpetuo, illimitato ed irrevocabile. La ditta aggiudicataria deve essere obbligata a fornire al produttore tutta la documentazione ed il materiale necessario all'effettivo sfruttamento di detti diritti di titolarità esclusiva, nonché a sottoscrivere tutti i documenti necessari all'eventuale trascrizione di detti diritti a favore del produttore in eventuali registri od elenchi pubblici.
3. Clausola contrattuale sulla riservatezza del progetto: tutta la documentazione creata o predisposta dalla Ditta aggiudicataria nell'esecuzione del contratto deve essere protetta dalla diffusione a terzi, senza la preventiva approvazione espressa da parte del produttore; in caso di, fermo restando il diritto al risarcimento del danno, il produttore deve avere facoltà di dichiarare risolto il contratto.

8. Attività del soggetto produttore nel caso di affidamento del servizio di conservazione

8.1 Predisposizione, invio e gestione dei pacchetti di versamento

Il processo di conservazione dei documenti informatici inizia con la presa in carico del documento da parte del sistema di conservazione ma, al fine di consentire la corretta conservazione di tale documento, risulta di fondamentale importanza già la fase di sua formazione del pacchetto di versamento presso il soggetto produttore, il quale produce oppure acquisisce i documenti durante l'espletamento delle funzioni che gli sono proprie.

I contenuti dei pacchetti e i tempi di invio al sistema di conservazione devono essere preventivamente definiti e concordati con il Soggetto produttore il quale veicola al Responsabile del servizio di conservazione, al Responsabile per il trattamento dei dati personali e al Responsabile della funzione archivistica la richiesta di attivazione del servizio per la trasmissione dei pacchetti di versamento. Una valutazione della domanda di acquisizione,

effettuata dalle figure responsabili sopracitate, avrà il fine di accertare che i requisiti del Soggetto produttore siano compatibili con le *policy* aziendali.

I dati inseriti sono strutturati in modo tale da consentire al sistema di conservazione di identificare e comprendere la struttura organizzativa e gli uffici che hanno emesso la documentazione.

Ad ogni documento da conservare, vengono opportunamente associati i metadati descrittivi del contesto di produzione del singolo documento e quelli atti a rappresentare i nessi logici di questo con il fascicolo che lo conserva ciascun pacchetto di versamento è dunque composto da uno o più file e dai relativi metadati descrittivi.

I metadati minimi del pacchetto di versamento posso essere così sintetizzati:

- Identificativo univoco e persistente del pacchetto di versamento;
- Riferimento temporale valido, attestante la data e l'ora di creazione del pacchetto;
- Denominazione del Responsabile della produzione del pacchetto;
- Impronta del pacchetto di versamento;
- Numero dei documenti compresi nel pacchetto.

I metadati del fascicolo informatico e dei documenti informatici e amministrativi informatici riportano le indicazioni già fornite nella fase di formazione e gestione del documento, oltre alle informazioni utili ai fini della verifica dell'autenticità, dell'integrità e dell'immodificabilità dei *file*:

I metadati minimi associati al fascicolo informatico sono i seguenti:

- Denominazione dell'amministrazione titolare del procedimento e delle amministrazioni partecipanti
- Estremi cronologici
- Oggetto dell'affare o del procedimento amministrativo
- Identificativo del fascicolo
- Formato dei *file*
- Impronta dei documenti.

I metadati minimi associati al documento informatico sono i seguenti:

- Identificativo univoco e persistente
- Denominazione del soggetto produttore (per le persone fisiche: nome, cognome e codice fiscale del rappresentante legale; denominazione dell'organizzazione e codice fiscale o partita IVA in caso di persona giuridica)
- Data di versamento del pacchetto nel sistema di conservazione
- Eventuale data di sottoscrizione del documento
- Oggetto del documento
- Indice di classificazione, ove presente
- Formato del file
- Impronta del documento

I metadati minimi da associare al documento amministrativo informatico sono i seguenti:

- Codice IPA dell'amministrazione titolare;
- Codice IPA delle eventuali amministrazioni partecipanti all'iter procedimentale;
- Ufficio o amministrazione titolare dell'affare;
- Data di sottoscrizione del documento;
- Data di versamento del pacchetto nel sistema di conservazione;
- Oggetto del documento;
- Nome, cognome e codice fiscale del Responsabile del procedimento;
- Indice di classificazione;
- Formato del file;
- Impronta del documento.

Il manuale di gestione dei documenti informatici, il titolario di classificazione, il repertorio dei fascicoli, il piano di conservazione, il registro di protocollo e i registri dei documenti soggetti a registrazione particolare, prodotti da pubbliche amministrazioni e enti pubblici, sono anch'essi da sottoporre al processo di conservazione a norma, unitamente al resto della documentazione.

Prima dell'invio al sistema di conservazione, sul pacchetto può essere apposta una firma digitale da parte del produttore: attraverso l'apposizione di tale firma si avrà la garanzia dell'integrità del pacchetto di versamento specialmente nei casi di sua trasmissione telematica.

Al fine di garantire una corretta gestione del trattamento dei dati, la fase iniziale dell'attivazione del servizio prevede la dichiarazione mediante un apposito modulo con le seguenti informazioni:

- ragione sociale;
- indirizzo;
- partita iva;
- e-mail;
- oggetti documentali gestiti;
- interoperabilità tra sistema del Soggetto produttore e sistema di conservazione;
- tipo di protocollo da utilizzare per lo scambio dei Pacchetti.

Inoltre per ogni pacchetto di versamento dichiarato dal soggetto produttore, sono richiesti:

- i volumi in termini di numero documenti annui previsti da gestire e spazio di occupazione previsto per i dati da conservare (GB);
- la dimensione massima del pacchetto di versamento;
- la frequenza di invio dei pacchetti;
- l'eventuale richiesta di invio di supporti ottici (CD,DVD) di conservazione con la definizione della relativa frequenza.

Il Responsabile del servizio di conservazione e il Responsabile della funzione archivistica una volta ricevuta la richiesta, si impegnano a valutarne l'impatto stimando la data di evasione e fornendo al Soggetto produttore una pianificazione delle fasi successive.

L'esito positivo delle verifiche effettuate sui pacchetti di versamento viene registrato in un rapporto di versamento di presa in carico. Il rapporto conterrà un'impronta del file originale comprensivo di algoritmo con la quale tale impronta viene calcolata (*hash)* e un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del rapporto collegato all'istante indicato.

Il rapporto di versamento attesta la corretta esecuzione del processo di immissione dei pacchetti, ha la funzione di raccogliere evidenze indirette di tutti i documenti del pacchetto e garantisce due principali funzioni:

- la possibilità di provare l'integrità dei dati di ogni file contenuto nel pacchetto,
- di permettere il controllo dell'integrità per ogni file in modo separato, senza creare un'interdipendenza tra i file ai fini dell'esibizione e del controllo.

Il rapporto di versamento è un file in formato XML che riporta, per ognuno dei file inclusi nel pacchetto, alcune informazioni tra cui un "URN" (*uniform resource name*)[49] e un "hash". L'URN è una stringa univoca che identifica l'oggetto digitale, mentre l'*hash* è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale (in modo pratico possiamo dire di avere la garanzia che a due file differenti corrispondono sempre due impronte distinte).

La modalità di conservazione mediante rapporto di versamento permette di verificare l'integrità di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso pacchetto. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo URN identificativo per poter eseguire la funzione di *hash* e confrontare l'impronta ricalcolata con la stringa riportata nel rapporto.

In questa fase vengono associate all'indice tutte le evidenze di autenticità delle firme digitali che verranno verificate all'istante del riferimento temporale:

- i certificati di firma di tutte le firme presenti nel pacchetto di versamento;
- tutti i certificati appartenenti alle catene di certificazione (*trusting chain*);
- le liste di revoca dei singoli certificati (CRL).

Il rapporto di versamento viene conservato all'interno del sistema garantendone l'ininterrotta custodia e la non modificabilità.

Le verifiche effettuate sui pacchetti di versamento possono risultare negative. Nei casi in cui anche solo su uno dei controlli sopraindicati indicati si dovesse riscontrare una mancanza o non corrispondenza di informazioni viene generato un file di comunicazione delle anomalie che verrà comunicato mediante un file di esito al soggetto produttore. Tale comunicazione comprenderà i dettagli delle verifiche eseguite sui pacchetti di versamento comprensive delle precisazioni sulle anomalie. Le anomalie possono essere identificate nella mancata corrispondenza di ciò che viene versato a quanto dichiarato dal soggetto produttore nel modulo in termini di firma digitale, formati e metadati.

Sulla comunicazione delle anomalie verrà apposto un riferimento temporale e conservata così come viene conservato il rapporto di versamento.

49 Un *Uniform Resource Name* o URN è un URI che identifica una risorsa all'interno di un *namespace*, ma, a differenza del URL, non permette l'identificazione della locazione della risorsa stessa. Un esempio di URN è il codice ISBN: questi identifica univocamente un libro, ma non ci dà alcuna informazione sulla locazione dello stesso.

A titolo meramente esemplificativo, fare riferimento all'allegato E – Generazione del pacchetto di versamento.

8.2 Controlli e monitoraggio del servizio di conservazione

I contenuti del pacchetto di versamento formato sono sottoposti a verifica da parte del produttore prima dell'invio al sistema di conservazione.

I controlli effettuati dal produttore dovrebbero essere orientati al fine di permettere al sistema di conservazione di poter garantire l'autenticità, l'integrità, l'immodificabilità e la leggibilità dei documenti conservati e gli stessi controlli possono riguardare:

- la validità dei certificati di firme digitali dei documenti sottoscritti;
- la validità delle marche temporali;
- il formato del file, che dovrà garantire l'interoperabilità tra il sistema di gestione e il sistema di conservazione e la consultabilità e reperibilità nel lungo periodo;
- la corrispondenza tra i dati e l'impronta calcolata sui documenti.

I pacchetti di versamento che risultano adeguatamente formati e corrispondenti alle caratteristiche attese nella forma e nel contenuto, sono inviati tempestivamente al sistema di conservazione, attraverso canali sicuri di trasmissione.

Le modalità di invio possono essere individuate tramite una delle seguenti possibili soluzioni tecnologiche:

- *Web services*;
- Collegamento SFTP[50], accessibile su *server* previa autenticazione tramite *username* e *password*;
- Via posta elettronica anche certificata (PEC);
- Supporti rimovibili (Hard-Disk, CD, DVD).

L'attività di monitoraggio e controllo è finalizzata alla rilevazione di eventi di sicurezza, identificabili come stati che indicano il mancato rispetto delle politiche di sicurezza, che possano costituire una possibile fonte di rischio per il sistema di conservazione. Nello specifico gli obiettivi delle attività di monitoraggio sono la valutazione del livello del rischio associato agli eventi di sicurezza e la gestione di tali eventi, mediante strumenti come i report dei controlli, agendo per il contenimento e/o eliminazione delle cause.

50 SSH *File Transfer Protocol* o SFTP è un protocollo di rete che prevede il trasferimento dei dati e funzionalità di manipolazione. È tipicamente usato con il protocollo SSH-2 che utilizza un trasferimento dei *file* sicuro, anche se è utilizzabile con un qualsiasi altro protocollo.

Gli eventi di sicurezza sono monitorati tramite il sistema di *log* che consente la registrazione degli accessi e degli eventi (operazioni). Vi sono:

- i log del sistema operativo atto ad identificare ingressi, anomalie ed errori,
- i log del Data Base atti ad identificare ingressi, anomalie ed errori, i log dei sistemi di rete (firewall e router) atti ad identificare ingressi, anomalie ed errori ed infine i log delle applicazioni software utilizzate (realizzati con vista a livello di singolo utente) atti ad identificare ingressi, principali attività svolte dagli utenti, sequenze del processo, accessi ai dati.

I log file degli applicativi contengono almeno le seguenti informazioni:

- utente che ha eseguito l'operazione;
- data e ora dell'operazione;
- operazione eseguita.

I file di log non sono modificabili o eliminabili da parte degli utenti che usano il sistema (che non dispongono dei diritti di accesso), sono analizzati da parte dei sistemisti qualora si rendesse necessaria un'indagine a seguito di un malfunzionamento del sistema e vengono successivamente inviati in conservazione per mantenere traccia delle comunicazioni tra soggetto produttore e sistema di conservazione.

Il sistema di conservazione deve gestire un sistema di tracciatura nel quale vengono registrati tutti i singoli eventi che riguardano sia la gestione dei pacchetti, dalla fase di versamento a quella di distribuzione, sia i singoli documenti. Questa tracciatura prevede la registrazione di informazioni relative alle diverse funzioni del processo di conservazione in tutte le fasi sia per la reportistica relativa al processo di conservazione, sia per la reportistica del servizio di supporto utente (*Service Desk*).

La reportistica di servizio, con periodicità mensile e/o semestrale, può essere di due tipologie:

- reportistica relativa al processo di conservazione, vengono prodotti periodicamente i seguenti report:
  - *report* consuntivo pacchetti di archiviazione;
  - *report* excel che fornisce la lista dei pacchetti di archiviazione e che comprende questo set minimo di informazioni:
    - ragione sociale cliente;

    - numero documenti conservati e spazio occupato nel periodo totali e per tipologia di documento;
    - numero documenti conservati e spazio occupato totali e per tipologia di documento.
  - generazione del rapporto di versamento sia per pacchetti di versamento accettati che rifiutati. Tale documento contenente un *file* di esito deve essere obbligatoriamente comunicato e messo a disposizione del soggetto produttore (si veda la descrizione fornita al punto 1).

- reportistica del servizio di supporto utente (*service desk*), viene prodotto un report di servizio che fornirà le seguenti evidenze:
  - numero *incident* segnalati;
  - media tempo di presa in carico *incident*;
  - media tempo di chiusura *incident*;
  - numero *service request*;
  - media tempo di presa in carico *service request*;
  - media tempo di chiusura *service request*.

Le suddette funzioni garantiscono la gestione di tutte le anomalie relative al servizio di conservazione assicurando due tipologie di interventi, interventi reattivi a fronte delle segnalazioni degli utenti ed interventi proattivi a fronte di generazioni spontanee di eventi e segnalazioni generati dai sistemi di monitoraggio infrastrutturale e applicativo.

8.3 Gestione degli scarti da comunicare al conservatore

La normativa in materia di archivi e documenti pubblici, come ricordato nel capitolo 2, è stata sempre ispirata al principio della salvaguardia della documentazione prodotta dalla Pubblica Amministrazione, tutelata come bene culturale e individuata come rappresentativa di atti o fatti giuridicamente rilevanti. L'obbligo di conservazione dei documenti d'archivio è inteso a salvaguardare diritti soggettivi, interessi legittimi, il diritto d'accesso[51], la ricerca a fini storici,

51 Disciplinato dall'art. 22 e ss. della Legge 241/1990 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" (GU n.192 del 18-8-1990).

culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico.

La produzione documentaria attuale ha però raggiunto dimensioni quantitative tali che è impensabile conservarla tutta. Da un punto di vista teorico l'idea che più documenti equivalgano a maggiore conoscenza del passato è stata ormai abbandonata e si è arrivati a ritenere che l'eccesso di documenti e informazioni possa costituire una sorta di ostacolo alla ricerca e tendere ad occultare più che rilevare.

Quindi è ormai accettato il principio che parte di documentazione debba essere eliminata. L'eliminazione deve essere realizzata tramite le procedure definite di scarto.

Come scrive Paola Carucci: "L'operazione con la quale si distrugge una parte della documentazione si chiama scarto"[52].

Sostanzialmente per scarto s'intende la distruzione, previa selezione, del materiale documentario ritenuto non necessario per la ricerca storica e inutile o superfluo ai bisogni ordinari dell'amministrazione, avendo perso, col decorrere del tempo, rilevanza giuridica ed amministrativa.

Lo scarto dei documenti negli enti pubblici è ora regolato dall'art. 21 comma 1 lettera d) del Codice dei beni culturali, che stabilisce che lo scarto di documenti degli archivi di enti pubblici e degli archivi privati di notevole interesse storico è subordinato ad autorizzazione del MIBACT nella figura del Soprintendente archivistico. La distruzione non autorizzata di documenti d'archivio, anche informatici è punibile con l'arresto da sei mesi a un anno e con l'ammenda da euro 775 ad euro 38.374,50 (art. 169, comma 1 del Codice dei beni culturali).

Scartare è considerata ormai una operazione necessaria ed inevitabile, ma per farlo bisogna individuare criteri oggettivi che permettano di operare una corretta selezione sottraendola all'arbitrarietà. La definizione di tali criteri è comunque legata a una valutazione contingente, condizionata da un determinato momento storico e sociale e dal clima culturale coevo.

Per definire tali criteri e agevolare le operazioni di selezione si sono elaborati alcuni "strumenti di tipo pratico"[53] i massimari di scarto, una sorta di elenco di massima, indicativo e non tassativo, di tipologie documentarie da eliminare a scadenze prefissate.

52 CARUCCI Paola, Le fonti archivistiche: ordinamento e conservazione, I ed. Roma, La Nuova Italia Scientifica, 1983 (più volte ripubblicato), p. 50. Il termine 'scarto', nella dottrina archivistica, può anche significare la "scelta delle carte destinate alla eliminazione".

53 ZANNI ROSIELLO Isabella, "Spurghi e distruzioni di carte d'archivio" in L'archivista sul confine. Scritti di Isabella Zanni Rosiello, a cura di C. Binchi e T. Di Zio, Roma, Ministero per i beni culturali e ambientali, Ufficio centrale per i beni archivistici, 2000, pp. 273-303 (originariamente edito in "Quaderni Storici", XVIII (1983), 54, pp. 985-1017), p. 296.

L'elaborazione di massimari di scarto dovrebbe essere realizzata in collaborazione tra le amministrazioni e il MIBACT, basandosi su criteri metodologici sostanzialmente condivisi:

- analisi del quadro di classificazione in relazione alle funzioni dell'ente;
- analisi della tipologia dei documenti e delle modalità di formazione dei fascicoli;
- analisi delle relazioni tra le serie;
- rispetto dei tempi di prescrizione e delle esigenze amministrative dell'ente;
- verifica della presenza o meno di documentazione riassuntiva.

Le finalità dei massimari di scarto è quella di elencare tipologie di serie e di documenti che, superati i tempi di conservazione indicati (in media cinque o dieci anni) possono essere eliminati con una certa automaticità, previa sempre opportuna valutazione ed approvazione da parte della competente Soprintendenza archivistica.

Le procedure di scarto, almeno in Italia, sono state fino ad ora finalizzate alla eliminazione di documentazione cartacea, ma il fondamento scientifico della selezione della documentazione permane e per alcuni casi si accentua anche nella gestione di documenti informatici, per i quali la conservazione non può essere una funzione passiva, né da un punto di vista teorico né negli aspetti operativi e pratici.

L'utilizzo delle memorie digitali permette per certi aspetti il superamento delle limitazioni fisiche e quantitative dei documenti conservati, ma non elimina il problema della "selezione" dell'informazione. Ciò che consente di "leggere" un archivio e di ripercorrere le vicende dell'organizzazione che lo ha posto in essere, non è la mole di documenti e di informazioni conservate, ma la qualità delle relazioni tra i documenti, la loro stabilità, il mantenimento delle informazioni di contesto, la presenza di strumenti di corredo, cioè di una serie di misure e di strumenti pianificati in fase attiva.

In tale logica in ambiente digitale bisogna operare misure di salvaguardia dell'efficacia e dell'efficienza della ricerca e della coerenza dei complessi documentari conservati, che consentano di privilegiare la qualità sulla quantità delle informazioni gestite e conservate dal sistema informativo documentario.

I recenti mutamenti legislativi, e ancor di più quelli tecnologici hanno fatto della selezione una delle funzioni più qualificanti della professione archivistica, chiamata ad organizzare sistemi per la conservazione permanente della documentazione informatica.

La pianificazione delle procedure di selezione e la definizione dei tempi di trasferimento nel sistema di conservazione dovrebbero essere ricompresi nel piano di conservazione, che deve diventare non un semplice massimario, ma uno strumento che permetta di programmare il

trasferimento dei documenti dal sistema di gestione documentale al sistema di conservazione anche in funzione delle logiche di selezione e scarto e di gestirli in modo efficiente e sicuro.

L'elaborazione e l'aggiornamento del piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione permanente dei documenti nel rispetto delle disposizioni in materia di tutela dei beni culturali rientra tra i compiti del servizio per la gestione dei flussi documentali e degli archivi previsto dall'art. 61 del D.P.R. 28 dicembre 2000, n. 445 (art. 68 del D.P.R. 28 dicembre 2000, n. 445).

Rientra anche nella documentazione collegata al manuale di gestione. Infatti l'art. 5 del DPCM 3 dicembre 2013 relativo alle regole per il protocollo informatico dedicato al manuale di gestione indica alla lettera m) tra i contenuti del manuale di gestione: *"il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto".* Si tratta in questo caso della visione del piano di conservazione partendo dal sistema di classificazione, mentre nell'art. precedentemente citato era invertita la prospettiva.

Si può comunque ritenere che possa identificarsi in un unico strumento essenziale per la corretta formazione e tenuta della documentazione e degli archivi.

Anche nel caso della documentazione informatica è necessario applicare criteri di selezione improntati a valutazioni elaborate dalla disciplina archivistica, che tende sempre più a definirli in base al grado di rilevanza dei documenti in rapporto all'attività dell'ente produttore e ad inserirli in un contesto di economicità di scelte.

In ambiente digitale vi potranno essere inoltre delle differenze e delle peculiarità rispetto alle procedure di eliminazione di documenti cartacei. Ad esempio se in ambiente cartaceo proliferano copie di documenti, in ambiente digitale bisognerà prestare la massima attenzione ai diversi legami che un unico documento può avere ed evitare procedure di selezione che eliminino documenti vitali perché magari in connessione con una voce di titolario e un fascicolo indicato come passibile di scarto.

Ovviamente non si procederà nelle modalità tradizionali di distruzione dei documenti che prevedevano la consegna alla Croce Rossa per avviare i documenti al macero, ma bisognerà ugualmente prestare attenzione alla completa distruzione dei documenti e dei dati destinati allo scarto anche nel rispetto della normativa sulla tutela dei dati personali.

Il massimario o piano di conservazione in ambiente digitale deve essere collegato con il sistema di gestione documentale tramite una tabella collegata alla classificazione che assegna e definisce il tempo di conservazione dei documenti in ciascuna registrazione, e che può

diventare modello anche per la redazione degli elenchi di scarto. Si possono ipotizzare come campi della tabella il seguente tracciato:

- titolario di classificazione: codice classificazione;
- tipologia documentaria (descrizione);
- tempo di conservazione;
- motivazione;
- note con riferimenti normativi di supporto alla motivazione.

A questi si possono aggiungere legami con le tabelle dei procedimenti e le unità organizzative responsabili.

Tali informazioni devono essere trasferite al sistema di conservazione che dovrà poi operare materialmente le operazioni di scarto.

Nel caso comunque di procedure di scarto è necessario prevedere l'eliminazione dei documenti sottoposti a scarto oltre che nel sistema di conservazione anche in tutti i sistemi gestiti dal produttore, che eventualmente avessero ancora memorizzato i documenti da scartare.

Bisogna ricordare che i tempi di conservazione è buona regola calcolarli dalla data di chiusura dell'affare o procedimento e non dalla data dei singoli documenti. Quindi le procedure di scarto vanno applicate a fascicoli chiusi relativi a pratiche cessate o a serie annuali complete.

Operativamente si può valutare che in base ai tempi di conservazione risultanti dai massimari di scarto dei produttori, definiti a livello di piano di classificazione, di unità archivistica o di unità documentaria in appositi metadati, il sistema di conservazione produca annualmente, o su richiesta, un elenco di scarto per ogni produttore, cioè un elenco delle unità archivistiche o unità documentarie che hanno superato il tempo minimo di conservazione e possono essere sottoposte a procedure di scarto.

Tale elenco di scarto, dopo una verifica da parte del Responsabile del servizio di conservazione, viene comunicato al Responsabile della gestione documentale che, utilizzando apposite funzionalità del sistema di conservazione, può rifiutarlo (perché non intende procedere allo scarto) o validarlo (eventualmente dopo averlo opportunamente modificato).

L'elenco di scarto così validato nel caso degli archivi pubblici o privati che rivestono particolare interesse storico viene trasmesso dal produttore all'Autorità di vigilanza (Soprintendenza archivistica competente) che, in base alle norme vigenti, deve fornire l'autorizzazione e il nullaosta per lo scarto.

Il produttore, una volta ricevuto il nullaosta (che può essere concesso anche solo su una parte dell'elenco proposto), provvede ad adeguare, se necessario, l'elenco di scarto presente sul sistema di conservazione alle decisioni dell'autorità. Una volta che l'elenco di scarto definitivo

viene predisposto, il produttore lo valida e trasmette al sistema di conservazione la richiesta di procedere allo scarto.

Il Responsabile del servizio di conservazione effettua un ulteriore controllo sulla congruenza dell'elenco di scarto definitivo con quello autorizzato dall'autorità e, in caso riscontrasse anomalie, provvede alla correzione e sottopone nuovamente l'elenco alla validazione del produttore.

Nel caso il controllo sull'elenco di scarto dia esito positivo, il Responsabile del servizio di conservazione procede, previa notifica al produttore che, contestualmente nel caso di archivi pubblici, emana apposito e motivato provvedimento di eliminazione dei documenti e di loro sdemanializzazione alla cancellazione dei pacchetti di archiviazione contenuti nell'elenco. L'operazione di scarto viene tracciata sul sistema mediante la produzione di metadati che descrivono le informazioni essenziali sullo scarto, inclusi gli estremi delle richiesta di nullaosta allo scarto e al conseguente provvedimento autorizzatorio e la traccia del passaggio del pacchetto di archiviazione scartato nell'archivio di conservazione.

Le modalità di deliberazione (o determinazione) dello scarto da parte dell'Ente produttore sono fissate dal medesimo, nell'ambito della sua potestà di autoregolamentazione.

Al termine delle operazioni di eliminazione logica dal sistema di conservazione dei documenti informatici scartati il Responsabile del servizio di conservazione fornirà opportuna informativa al produttore.

È però prevedibile che la materiale distruzione dei documenti informatici verrà resa effettiva solo alla momento della eliminazione dei supporti di conservazione. In una prima fase si tratterà solo di una eliminazione logica. Anche tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di *backup* del sistema.

In quest'ottica la produzione della proposta di scarto potrà essere una operazione di reporting periodico del software di gestione dei documenti o del sistema di conservazione, che dovrà essere comunque attentamente vagliata e validata dal Responsabile del servizio archivistico, prima di essere sottoposta all'autorizzazione della competente Soprintendenza archivistica. Anche in questo caso non si possono prevedere automatismi nelle procedure di scarto, ma solo ausili nella complessa opera di selezione.

La documentazione non sottoposta a scarto e destinata alla conservazione permanente viene a costituire l'archivio storico. Nel caso degli organi giudiziari ed amministrativi dello Stato a tal fine versano all'Archivio Centrale dello Stato e agli Archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni (art. 41, comma 1 del Codice dei bene culturali). Le Regioni e gli altri enti pubblici hanno invece l'obbligo di istituire in sezioni separate i propri archivi

storici, costituiti dai documenti relativi ad affari esauriti da oltre quaranta anni (art. 30, comma 4 del Codice dei bene culturali).

Anche l'art. 69 del D.P.R. 28 dicembre 2000, n. 445 stabilisce che *"i documenti selezionati per la conservazione permanente sono trasferiti, contestualmente agli strumenti che ne garantiscono l'accesso, negli Archivi di Stato competenti per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali"*.

Le regole tecniche sulla conservazione (DPCM 3 dicembre 2013) ricordano opportunamente (art. 8, comma 1 lettera l) che il Responsabile della conservazione, per gli organi giudiziari e amministrativi dello Stato, alla scadenza dei termini sopra indicati e previa operazioni di selezione e scarto deve provvedere al versamento dei documenti conservati all'Archivio Centrale dello Stato o ai competenti Archivi di Stato.

Allo stato attuale però non sono disponibili indicazioni sulle possibili modalità operative di tali versamenti, come non sono chiare le modalità di versamento negli archivi storici degli altri enti.

È questo un punto cruciale del tema della conservazione permanente dei documenti informatici che non ha ancora trovata una precisa risposta né in norme generali né in specifiche regole tecniche.

Sarà necessario riflettere approfonditamente su tali temi per individuare soluzioni che permettano di coniugare le norme sulla conservazione dei documenti informatici con le norme sui beni culturali e con le tradizionali funzione di conservazione e valorizzazione degli istituti culturali a tal fine preposti.

L'art. 101 del D.Lgs 22 gennaio 2004, n.42 definisce in particolare tra gli istituti e luoghi della cultura come "Archivio" una struttura permanente che raccoglie, inventaria e conserva documenti originali di interesse storico e ne assicura la consultazione per finalità di studio e di ricerca. Tali istituti che appartengono a soggetti pubblici sono destinati alla pubblica fruizione ed espletano un servizio pubblico.

8.4 Gestione della cancellazione, presso il soggetto produttore, dei documenti inviati in conservazione

Come abbiamo visto nel precedente paragrafo le norme prevedono ad un certo punto (30 o 40 anni) per la documentazione destinata a conservazione permanente un completo trasferimento della documentazione in archivi storici, definito in termini tecnico-archivistici versamento.

Nel caso di documenti originali analogici questo azione prevede obbligatoriamente un trasferimento fisico della documentazione, che, quindi, naturalmente, non sarà più presente negli archivi correnti e di deposito degli enti produttori.

Nel caso della documentazione informatica abbiamo visto che il trasferimento al sistema di conservazione può o, in certi casi, deve avvenire in modo molto anticipato in un momento in cui i documenti non hanno perso la loro rilevanza amministrativa e quindi coincidente con la fase corrente. Il trasferimento in questo caso però non comporta l'immediata eliminazione nei sistemi correnti, che possono mantenere in forma di duplicato i documenti stessi, anche in un momento successivo al trasferimento al sistema di conservazione.

Comunque è opportuno prevedere che nel momento in cui i documenti non si ritengano più necessari per la trattazione degli affari correnti o a seguito di procedure di scarto i documenti vengano eliminati dai sistemi di gestione documentale corrente.

Operativamente si pongono gli stessi problemi della eliminazione dei documenti nei sistemi di conservazione precedentemente descritti.

Nel caso in cui si tratti di documenti destinati alla conservazione permanente, o per una eliminazione nel sistema corrente in tempi anticipati rispetto ai temi di conservazione, tale eliminazione può avvenire solo nel caso in cui si abbia piena certezza del completo e corretto trasferimento al sistema di conservazione.

Prima di procedere alla eliminazione dei documenti nel sistema corrente è opportuno valutare le effettive necessità di rapido recupero di tali documenti ed attivare approfondite procedure di verifica di completezza dei versamenti nel sistema di conservazione, che, dopo la distruzione dei duplicati nei sistemi correnti, diviene l'unico custode di tali documenti. Tali procedure debbono concentrarsi più che sui singoli documenti sulle aggregazioni documentali verificandone la loro completezza e integrità. Bisogna inoltre avere la certezza del completo trasferimento ed aggiornamento dei metadati ritenuti significativi e rilevanti per il recupero dei documenti dal sistema di conservazione.

Infine è da valutare anche l'opportunità del mantenimento in forma di metadati di informazioni relative ai documenti eliminati.

8.5 Gestione degli accessi dell'utenza (privacy, profili di autorizzazione)

Innanzitutto è necessario conoscere quali siano le categorie di utenti, interni o esterni, che usufruiranno dell'archivio in questione, la c.d. comunità designata secondo lo standard OAIS. Bisogna tenere conto degli interessi (a fini gestionali, giuridico-amministrativi o storico culturali) che muoveranno gli utenti ad accedere, di cosa potrebbero cercare, di cosa possono consultare e a cosa invece posso accedere per ottenerne copia. Esistono utenti interni, a cui per diritto o responsabilità, bisogna garantire l'accesso di tutto o almeno di parte dell'archivio: l'amministratore, il Responsabile della conservazione, gli operatori sia del polo di conservazione che del soggetto produttore, la Sovraintendenza archivistica, gli organi giudiziari e le forze dell'ordine. I soggetti esterni invece possono essere: dipendenti di

un'Amministrazione diversa dal soggetto produttore che ha necessità di accedere esclusivamente a fini istituzionali su documentazione su cui abbia comunque un interesse o cittadini, a fini amministrativi o a fini storici. Infine non bisogna dimenticare gli utenti automatici cioè quelli che operano in regime di interoperabilità.

Gli utenti da abilitare per l'accesso al sistema di conservazione vengono comunicati al conservatore attraverso un documento aziendale, che il soggetto produttore deve predisporre con l'indicazione dei referenti/utenti da abilitare/abilitati ad accedere al sistema di conservazione. Il conservatore invia tramite canale sicuro, al momento dell'attivazione del soggetto produttore al servizio di conservazione, le credenziali di accesso ai diretti interessati. Gli utenti possono collegarsi all'indirizzo comunicatogli, autenticandosi tramite username e una *password* generica modificabile al primo accesso. I profili di autorizzazione previsti per l'accesso, vengono individuati per ogni utente a seconda delle esigenze e della mansione dell'utenza all'interno del soggetto produttore., non è sufficiente una distinzione fra abilitati e non. I profili applicati posso essere filtrati in base a:

- autorizzazioni di operatività dell'utente, ad esempio dalla semplice visualizzazione e/o ricerca dei documenti conservati all'invio/gestione degli stessi.
- per tipologia documentale che contraddistingue ogni utente su vari livelli di autorizzazione all'accesso.

8.6 Gestione del transitorio per l'avvicendamento dei conservatori

Il processo di conservazione deve adottare il modello standard ISO 14721:2012 OAIS – Open Archival Information System che definisce concetti e funzionalità degli archivi digitali. Il soggetto produttore invia il pacchetto di versamento, di cui ha piena responsabilità, al Soggetto conservatore il quale provvede a trasformarlo in pacchetto di archiviazione. Ai fini dell'esibizione e della distribuzione richiesti dalla comunità di riferimento, il Soggetto conservatore provvederà a creare i pacchetti di distribuzione così che venga garantita la corretta visualizzazione di questi. È necessario adottare strutture dei dati e standard idonei a garantire l'interoperabilità e la trasferibilità tra i sistemi di conservazione.

9. Allegati

Allegato A - Modello di autorizzazione al trasferimento per la conservazione di documenti informatici.

Al Ministero dei Beni e delle Attività Culturali e del Turismo

Soprintendenza Archivistica territorialmente competente

Oggetto: richiesta di autorizzazione al trasferimento per la conservazione di documenti informatici.

Lo scrivente Ente intende sottoscrivere un contratto/convenzione con il conservatore accreditato

---

Ai fini della conservazione dei documenti informatici su piattaforma digitale. Si prevede quindi che i documenti da conservare saranno trasferiti nel sistema di conservazione del citato conservatore accreditato.

Si riporta nella tabella allegata l'indicazione delle tipologie di documenti informatici che si intende trasferire con indicazione degli estremi cronologici ed una stima quantitativa.

Si chiede pertanto di conoscere l'eventuale sussistenza di motivi ostativi alla stipula del sopraindicato Contratto/convenzione (il cui schema è allegato alla presente) e, così come previsto dall'art. 21 comma 1 lettera e) del D. Lgs. 22 gennaio 2004, n. 42 e s.m.i., recante il "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137", si richiede l'autorizzazione al trasferimento dei documenti informatici da conservare.

Ci si impegna a rispettare le indicazioni di codesta Soprintendenza.

Distinti saluti

Firma rappresentate Ente

TABELLA (MODELLO PER DOCUMENTAZIONE AMMINISTRATIVA NON SANITARIA)

Informazioni sui documenti digitali da trasferire al sistema di conservazione

Tipologie documentarie da inviare in conservazione

Tipologie documentarie	Estremi cronologici: anno iniziale	Stima numero documenti per anno	Software per la gestione dei documenti *(specificare se possibile fornitore, denominazione prodotto)*
Documenti registrati a protocollo			
Determinazioni e altri atti monocratici			
Deliberazioni			
Contratti			
Scritture private			
Registri di protocollo (giornaliero, annuale)			
Registri di repertorio			
Ordinativi (OIL): mandati e reversali			
Fatture			
CUD/CU			
Cedolini stipendiali			
Modelli 770			
Modelli F24			

Libri giornale			
Altro:			
Altro:			
Altro:			

Strumenti per la gestione documentale

Strumenti	**Data ed estremi atto di adozione**	**Note descrittive e/o riferimenti alla pubblicazione**
Manuale di gestione		
Titolario di classificazione		
Piano di conservazione o massimario di selezione e scarto		

Allegato B - Metadati del documento informatico

- Metadati obbligatori e aggiuntivi del documento informatico (documento non protocollato)

  - ID univoco e persistente
  - Codice identificativo dell'amministrazione titolare (codice iPA)
  - Codice AOO
  - Data del documento
  - Soggetto produttore valorizzato con Ufficio di competenza e/o RPA
  - Destinatario valorizzato con Soggetto giuridico/Ufficio di competenza e/o RPA
  - Oggetto
  - Classificazione e fascicolazione

- Metadati obbligatori e aggiuntivi del documento amministrativo informatico (documento protocollato)

  - Codice AOO
  - Numero di protocollo
  - Data di protocollo
  - Soggetto produttore valorizzato con Ufficio di competenza e/o RPA
  - Destinatario (in caso di documento in uscita) valorizzato con Soggetto giuridico/Ufficio di competenza e/o RPA
    Mittente (in caso di documento in entrata) valorizzato con Soggetto giuridico/Ufficio di competenza e/o RPA Protocollo Mittente
  - Oggetto
  - Classificazione e fascicolazione

- Metadati del registro giornaliero di protocollo

- Data di generazione del registro giornaliero di protocollo
- Soggetto produttore valorizzato con Ufficio di competenza oppure Nome e cognome
- Oggetto del documento
- Classificazione e fascicolazione

➢ Metadati del documento amministrativo informatico

versione XML	**<?xml version=1.0" encoding="ISO-8859-1" ?>**		
schema XML	**<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema>**		
tipo oggetto	**documento amministrativo informatico**		
nome oggetto			
tempo di conservazione			
metadati obbligatori			
informazione	**valori ammessi**	**tipo dato**	**Xsd**
identificativo	**come da sistema di identificazione formalmente definito**	**alfanumerico 20 caratteri**	**<xs:attribute name="IDDocumento" type="xs:string" use="required"/>**
amministrazione titolare	**vedi specifiche codice IPA**	**codice IPA**	
AOO titolare	**vedi specifiche codice IPA**	**codice IPA**	
numero di protocollo del documento	**da 1 a 9.999.999**		
data di registrazione di	**data**	**gg/mm/aaaa**	

protocollo			
mittente	**soggetto che ha autorità e competenza a spedire il documento informatico**		
destinatario	**soggetto che ha autorità e competenza a ricevere il documento informatico**		
Oggetto del documento	**breve riassunto del contenuto o natura del documento**	**alfanumerico 100 caratteri**	**<xs:element name="oggettodocumento" type="xs:string" use="required"/>**
l'impronta del documento informatico	**SHA-256 del documento informatico**		
ulteriori metadati			
informazione	**valori ammessi**	**tipo dato**	**Xsd**

Per quanto riguarda i metadati obbligatori il conservatore deve dare indicazioni da riportare nelle celle a sfondo rosa.

Per quanto riguarda i metadati ulteriori, il produttore ed il conservatore individuano congiuntamente eventuali ulteriori dati da registrare (celle a sfondo azzurro) ed il conservatore nel stabilisce le caratteristiche tecniche (celle a sfondo rosa).

Esempio di compilazione

versione XML	**<?xml version=1.0" encoding="ISO-8859-1" ?>**		
schema XML	**<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema>**		
tipo oggetto	**documento amministrativo informatico**		
nome oggetto	**documento protocollato**		
tempo di conservazione	**perpetuo**		
metadati obbligatori			
informazione	**valori ammessi**	**tipo dato**	**Xsd**
identificativo	**qualsiasi**	**alfanumerico 20 caratteri**	**<xs:attribute name="IDDocumento" type="xs:string" use="required"/>**
amministrazione titolare	**codice IPA**	**alfanumerico**	**<xs:element name="AMMtitolare" type="xs:string" use="required"/>**
AOO titolare	**codice IPA**	**alfanumerico**	**<xs:element name="AOOtitolare" type="xs:string" use="required"/>**
numero di protocollo del documento	**da 1 a 9.999.999**	**numerico di almeno 7 cifre**	**<xs:element name="numprotocollo"**

			type=”xs:string” use=”required”/>
data di registrazione di protocollo	data	gg/mm/aaaa	<xs:element name=”dataprotocollo” type=”xs:date” use=”required”/>
mittente	soggetto che ha autorità e competenza a spedire il documento informatico	alfanumerico 100 caratteri	<xs:element name=”mittente” type=”xs:string” use=”required”/>
destinatario	soggetto che ha autorità e competenza a ricevere il documento informatico	alfanumerico 100 caratteri	<xs:element name=”destinatario” type=”xs:string” use=”required”/>
Oggetto del documento	breve riassunto del contenuto o natura del documento	alfanumerico 100 caratteri	<xs:element name=”oggettodocumento” type=”xs:string” use=”required”/>
l'impronta del documento informatico	SHA-256 del documento informatico	alfanumerico 256 caratteri	<xs:element name=”docprint” type=”xs:string” use=”required”/>
ulteriori metadati			
informazione	valori ammessi	tipo dato	Xsd
entrata/uscita	entrata, uscita	alfanumerico 7 caratteri	<xs:element name=”tiporegistro” type=”xs:date” />

data di protocollo del documento ricevuto	**data**	**gg/mm/aaaa**	**<xs:element name="dataprotmitt" type="xs:date"/>**
numero di protocollo del documento ricevuto	**qualsiasi**	**alfanumerico 20 caratteri**	**<xs:element name="numprotmitt" type="xs:string"/>**

Allegato C - Metadati del fascicolo informatico

- Metadati obbligatori e aggiuntivi del fascicolo informatico:

  - Amministrazione titolare (almeno codice iPA)
  - Amministrazione partecipante (almeno codice iPA)
  - Anno di apertura del fascicolo
  - Codice identificativo: Titolo, Classe e numero progressivo del fascicolo
  - ID univoco: restituito dal Sistema
  - Oggetto: testo sintetico che descrive puntualmente l'affare cui si riferisce
  - Segnatura archivistica
  - Descrizione: sintesi di ciò che è possibile classificare su quella specifica voce di titolario
  - RPA (Responsabile del procedimento amministrativo)
  - UOR (Unità organizzativa Responsabile)
  - Anni di conservazione nell'archivio corrente
  - Anni di conservazione nell'archivio di deposito
  - Data apertura
  - Data chiusura
  - Totale dei documenti contenuti nel fascicolo
  - Totale dei sotto fascicoli contenuti nel fascicolo
  - numero di protocollo del primo documento inserito nel fasc.
  - numero di protocollo dell'ultimo documento inserito nel fasc.
  - Tipo fascicolo
  - Indicazione del procedimento amministrativo

versione XML	**<?xml version=1.0" encoding="ISO-8859-1" ?>**		
schema XML	**<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema>**		
tipo oggetto	**fascicolo informatico**		
nome oggetto			
tempo di conservazione			
metadati obbligatori			
informazione	**valori ammessi**	**tipo dato**	**Xsd**
identificativo	**come da sistema di identificazione formalmente definito**	**alfanumerico 20 caratteri**	**<xs:attribute name="IDFascicolo" type="xs:string" use="required"/>**
amministrazione titolare	**vedi specifiche codice IPA**	**codice IPA**	**<xs:element name="IPAtitolare" type="xs:string" maxOccurs="1"/>**
amministrazioni partecipanti	**vedi specifiche codice IPA**	**codice IPA**	**<xs:element name="IPApartecipante" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>**
Responsabile del procedimento	**nome: testo libero**	**alfanumerico 40 caratteri**	**<xs:element name="responsabile"> <xs:complexType> <xs:sequence> <xs:element name="nome" type="xs:string"/> <xs:element**
	cognome: testo libero	**alfanumerico 40 caratteri**	
	codice fiscale: testo libero	**alfanumerico 16 caratteri**	

			name="cognome" **type="xs:string"/>** **<xs:element name="codicefiscale"** **type="xs:string"/>** **</xs:sequence>** **</xs:complexType>** **</xs:element>**
Oggetto del documento	**testo libero**	**alfanumerico 100 caratteri**	**<xs:element name="oggettofascicolo"** **type="xs:string"**
documento	**identificativo del documento formalmente definito**	**alfanumerico 20 caratteri**	**<xs:element name="documento"** **type="xs:string"** **maxOccurs="unbounded"/>**
ulteriori metadati			
informazione	**valori ammessi**	**tipo dato**	**Xsd**

Per quanto riguarda i metadati obbligatori il conservatore deve dare indicazioni da riportare nelle celle a sfondo rosa.

Per quanto riguarda i metadati ulteriori, il produttore ed il conservatore individuano congiuntamente eventuali ulteriori dati da registrare (celle a sfondo azzurro) ed il conservatore nel stabilisce le caratteristiche tecniche (celle a sfondo rosa).

L'elenco minimale dei metadati da memorizzare da parte di ciascun sistema regionale, sia che essi siano relativi a documenti o dati memorizzati nel dominio regionale a cui il sistema fa riferimento, sia che essi siano memorizzati in altri domini regionali, è indicato in Tabella, in conformità con quanto stabilito nel paragrafo 6.2 del disciplinare tecnico allegato al DPCM attuativo.

Tipo metadato	**Descrizione**
Tipologia	Indica il tipo di dato/documento (referto di laboratorio, profilo sanitario sintetico, ecc.) ed è rappresentato da un codice LOINC.
Stato	Indica lo stato corrente del dato/documento (approvato, obsoleto, aggiornato, ecc.).
Identificativo documento o dato aggiornato	Elemento da memorizzare solo nel caso in cui il documento/dato a cui i metadati fanno riferimento aggiorna un precedente documento/dato presente nel FSE. In tal caso, l'elemento deve contenere il riferimento al documento o dato aggiornato, secondo la struttura presentata all'ultima riga.
Data	Indica la data di creazione del dato/documento.
Identificativo del paziente	Rappresenta il codice fiscale del paziente a cui il dato/documento fa riferimento.
Fonte	Indica se il dato/documento è stato caricato nel FSE da un professionista sanitario o del sociale oppure dall'assistito (nel taccuino personale).
Riferimento	Rappresenta un puntatore al dato/documento ed è suddiviso in: • Identificativo regionale – codice per l'identificazione della Regione o Provincia Autonoma contenente il dato/documento. • Identificativo della struttura sanitaria – codice per l'identificazione della struttura sanitaria contenente il dato/documento. • Identificativo del dato/documento – identificativo unico e persistente.

Allegato D - elenco delle tipologie di documenti comuni da conservare per tipologia di amministrazione

Segue un esempio di tipologie documentali con i periodi normativi di riferimento per la conservazione e il formato idoneo alla conservazione nel lungo periodo.

L'Amministrazione cui si fa riferimento sono i Comuni.

Il periodo di riferimento è individuato sulla base delle scelte organizzative dell'ente entro eventuali scadenze previste dalla normativa di settore (es, un anno per le fatture)

Tipologia documentale	**Periodo di riferimento dei documenti con cui si avvia la conservazione digitale**	**Durata di conservazione prevista dal massimario di scarto dei Comuni**	**Formato del file**
Registro di protocollo	**Giornaliero** **(DPCM 3/12/2013, art. 7 c. 5)**	**Illimitata come da massimario di scarto dei Comuni italiani approvato dalla DGA**	**PDF/A; l'immodificabilità del documento è garantita dalla memorizzazione nel SgD e dal trasferimento nel SdC**
Contratti	**Trimestrale**	**Illimitata come da massimario di scarto dei Comuni italiani approvato dalla DGA**	**PDF/A,**
Deliberazioni	**Trimestrale**	**Illimitata come da massimario di scarto dei Comuni italiani approvato dalla DGA**	**PDF/A,**

Determine	**Trimestrale**	**Illimitata come da massimario di scarto dei Comuni italiani approvato dalla DGA**	**PDF/A**
Fatture elettroniche	**Mensile**	**Illimitata come da massimario di scarto dei Comuni italiani approvato dalla DGA**	**XML**

Segue un esempio delle tipologie di fascicolo con i periodi normativi di riferimento per la conservazione. L'Amministrazione cui si fa riferimento sono i Comuni.

Tipologia di fascicolo	**Periodo di riferimento dei fascicoli con cui si avvia la conservazione digitale**	**Durata di conservazione del fascicolo prevista dalla normativa**
Fascicolo di procedimento amministrativo	**Annuale**	**Variabile in base ai documenti contenuti; il tempo di conservazione del fascicolo eredita il tempo dei documenti con durata di conservazione più lungo**
Fascicolo di affare	**Annuale**	**Solitamente 5/10 anni**

Fascicolo di persona fisica	**Annuale con aggiornamenti**	**Scarto selettivo per tipologia documentale**

AMMINISTRAZIONE PUBBLICA	
Amministrazione	**Tipologia/Serie/Aggregato documentale**
Azienda Sanitaria e Azienda Ospedaliera	**Deliberazioni**
	Determinazioni dei Dirigenti
	Bilanci
	Cartella clinica (varie tipologie)
	Cartella sanitaria (varie tipologie)
	Verbale di Pronto Soccorso
	Referti (varie tipologie)
	Registri vaccinazioni
	Registro giornaliero di protocollo
Comune	**Deliberazioni del Consiglio comunale**
	Deliberazioni della Giunta comunale
	Determinazioni dei Dirigenti
	Verbali degli organi collegiali
	Bilanci
	Registro giornaliero di protocollo
	Fatture elettroniche passive
Ministero	**Deliberazioni**
	Bilanci
	Decreti
	Determinazioni dei Dirigenti
	Registro giornaliero di protocollo

AMMINISTRAZIONE PRIVATA	
Amministrazione	**Tipologia/Serie/Aggregato documentale**
Assicurazione	**Registri Assicurativi**
	Polizza
	Allegati Polizza
	etc…

AMMINISTRAZIONE PRIVATA	
Amministrazione	**Tipologia/Serie/Aggregato documentale**
Assicurazione	**Registri Assicurativi**
	Polizza
	Allegati Polizza
	etc…

Allegato E - Generazione del pacchetto di versamento

I pacchetti di versamento si dividono normalizzati e non normalizzati.

I pacchetti di versamento normalizzati sono gli unici accettati direttamente dal sistema e sono versati utilizzando i servizi di versamento sincroni descritti. Devono rispettare una determinata struttura dati valida per tutte le tipologie documentarie e sono composti da due elementi:

- Indice Sip**:** un documento XML che contiene le informazioni descrittive dell'oggetto versato (metadati di identificazione, metadati di struttura, metadati di profilo archivistico, metadati di profilo generali, metadati di profilo specifici) e i parametri di versamento;
- Oggetto-Dati: una sequenze di bit (tipicamente in forma di *file*) da sottoporre a conservazione.

I pacchetti di versamento non normalizzati sono trasmessi dal produttore al sistema quando, per ragioni tecniche od organizzative, non è in grado di produrre e versare pacchetto di versamento normalizzati. Questi, le cui strutture dati possono differire molto tra loro e per questo devono essere concordate di volta in volta con il produttore, per essere versati nel sistema devono essere rielaborati per essere trasformati in pacchetti di versamento normalizzati. Tale processo di rielaborazione è chiamato normalizzazione ed è eseguito durante la fase di preacquisizione del processo di conservazione, tali pacchetti di versamento sono versati utilizzando i servizi di versamento asincroni.

Sia per i pacchetti di versamento normalizzati che per quelli non normalizzati, sono previsti diversi modelli di pacchetto di versamento, definiti in base agli oggetti da portare in conservazione, alle caratteristiche dei sistemi del produttore che li gestiscono e alle modalità di versamento utilizzate.

Modelli di pacchetti di versamento normalizzata seconda dell'oggetto contenuto, sono i seguenti:

- SIP di Unità Documentaria;
- SIP di Documento;
- SIP di Metadati;
- SIP di Unità Archivistica.

Il sistema di conservazione è in grado di accettare qualsiasi tipologia documentale precedentemente dichiarata nel modulo di attivazione. Di conseguenza è possibile ricevere diverse topologie di pacchetto di versamento. Nel caso specifico è permesso un duplice iter per la ricezione dei pacchetti di versamento:

- ricezione dei file tramite canale *File Transfert Protocol*
- ricezione tramite sistema *Web service*.

La ricezione mediante *File Transfert Protocol* prevede l'*upload* del Pacchetto di versamento composto da un file indice e da un insieme di file, in formato .zip.

La ricezione tramite Sistema *Web Service* è possibile da qualsiasi piattaforma che permetta di eseguire e ricevere chiamate *Web Service* conformi allo standard WS-I Basic Profile 1.0. Con questo servizio il sistema di conservazione riceve singoli documenti ed eventuali allegati, ne verifica la firma digitale se presente e ne gestisce la conservazione autentica.