Manuale della conservazione

Sommario

Indice delle figure

1. INTRODUZIONE

1.1 Scopo del documento

Il presente documento costituisce il manuale della conservazione elaborato dalla divisione Document Management Outsourcing di Siav; descrive l'erogazione del servizio di conservazione degli archivi informatici nonché le modalità per lo svolgimento dello stesso progettato per i soggetti, sia pubblici che privati, che decidono di affidare il proprio archivio informatico a Siav.

1.2 Struttura del documento

Il presente manuale è suddiviso in 4 macro-unità articolate in capitoli:

- la prima unità (capitoli 1-2) ha l'obiettivo di fornire gli strumenti necessari per comprendere e contestualizzare quanto esposto nelle unità successive. Il 1° capitolo include lo scopo, la struttura del manuale e i riferimenti temporali delle precedenti versioni del manuale della conservazione; il 2° capitolo offre una panoramica sulla normativa inerente la gestione e conservazione di archivi informatici, gli standard cui si fa riferimento, le definizioni dei termini usati e una tavola degli acronimi;

- la seconda unità (capitolo 3) è dedicata ai soggetti coinvolti nel processo di conservazione;

- la terza unità (capitoli 4-5) descrive l'intero processo di conservazione, dalla formazione dei pacchetti alla procedura di scarto;

- la quarta unità (capitoli 6-9) descrive le procedure di controllo e le modalità per garantire la leggibilità dei documenti conservati, le componenti del sistema, l'interoperabilità tra sistemi e la procedura di change management.

Infine per alcune fasi del processo di conservazione si rimanda all'allegato "Specificità del contratto", documento strettamente riservato dato che contiene i dettagli tecnici e le soluzioni adottate dalla divisione Document Management Outsourcing di Siav.

1.3 Versioni del manuale della conservazione

Versione	Data di redazione	Periodo di validità
01	Aprile 2007	da redazione ad Aprile 2008
02	Aprile 2008	da redazione ad Aprile 2009
03	Aprile 2009	da redazione ad Aprile 2010
04	Aprile 2010	da redazione ad Aprile 2011
05	Aprile 2011	Da redazione a Settembre 2011
06	Settembre 2011	Da redazione a Dicembre 2011
07	Dicembre 2011	Da redazione a Dicembre 2012
08	Dicembre 2012	Da redazione a Marzo 2013
09	Marzo 2013	Da redazione a Aprile 2014
10	Aprile 2014	Da redazione a Luglio 2014
11	Luglio 2014	Da redazione a Ottobre 2014
12	Ottobre 2014	Ultima versione
13	Novembre 2014	Integrazione all'ultima versione

Di seguito i riferimenti della presente versione:

Redatto da	
Nicola Voltan	Responsabile del servizio di conservazione
Firma	

Verificato da	
Rosalia Telese	Responsabile della funzione archivistica di conservazione
Nicola Voltan	Responsabile del trattamento dei dati personali
Davide Mietto	Responsabile della sicurezza dei sistemi per la conservazione
Davide Mietto	Responsabile dei sistemi informativi per la conservazione
Morgan Rizzolo	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Daniela Perrone	Consulente per la conservazione

	digitale

Approvato da	
Nicola Voltan	Responsabile del servizio di conservazione
Firma	

2. NORMATIVA, TERMINOLOGIA E STANDARD DI RIFERIMENTO

2.1 Riferimenti normativi

Di seguito si elencano i principali testi normativi in tema di gestione documentale e conservazione a norma precisando che alcuni testi pur essendo stati in parte o completamente abrogati sono ancora validi per i sistemi di conservazione antecedenti all'emanazione del Dpcm 3 dicembre 2013.

- Codice Civile [Libro Quinto Del lavoro, Titolo II del lavoro nell'impresa, Capo III delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica

- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi

- Dpcm 31 ottobre 2000, Regole tecniche per il protocollo informatico di cui al Dpr 20 ottobre 1998, n. 428

- Dpr 28 dicembre 2000, n. 445, Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (d'ora innanzi Testo Unico)

- Circolare AIPA del 7 maggio 2001, n. 28

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

- Dpcm 13 gennaio 2004, Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici

- D.Lgs 22 gennaio 2004, n. 42, Codice dei beni culturali e del paesaggio

- Deliberazione Cnipa 19 febbraio 2004, n. 11, Regole tecniche per la riproduzione e conservazione di documenti su supporto idoneo a garantire la conformità dei documenti agli originali

- D.Lgs 20 febbraio 2004, n. 52, Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA

- D.Lgs 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (d'ora innanzi Codice), aggiornato dal D.Lgs 4 aprile 2006, n. 159, Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale

- Legge 244 del 24 dicembre 2007, Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge finanziaria 2008)

- Decreto 7 marzo 2008 del Ministero dell'economia e delle finanze, Individuazione del gestore del sistema di interscambio della fatturazione elettronica nonché delle relative attribuzioni e competenze

- D.Lgs 30 dicembre 2010, n. 235, Modifiche ed integrazioni al Decreto Legislativo 7 marzo 2005, n. 82

- Circolare dell'Agenzia per l'Italia digitale n. 60 del 23 gennaio 2013, Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni

- Dpcm 22 febbraio 2013, Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del Codice

- Dpcm 21 marzo 2013, "Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione, la loro conformità all'originale deve essere autenticata da un notaio o altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni"

- Decreto del Ministero dell'economia e delle finanze 3 aprile 2013, n. 55, Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre 2007, n. 244

- Dpcm 3 dicembre 2013, Regole tecniche per il protocollo informatico ai sensi degli articoli 40 bis, 41, 47, 57 bis e 71 del Codice

- Dpcm 3 dicembre 2013, 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

- Circolare AgID 10 aprile 2014, n. 65 (pubblicata in GU – serie generale n. 89 del 16 aprile 2014)

- 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 (art. 21, c. 5 del Codice).

2.2 Standard e raccomandazioni

Per l'elaborazione del presente documento, oltre agli standard e alle specifiche tecniche indicate nell'allegato 3 delle Regole tecniche in materia di sistema di conservazione, sono stati presi in considerazione gli standard di seguito elencati:

- ISAAR (cpf)- International Standard archival authority record for corporate bodies, persons and families

- ISAD (G) - General international standard archival description

- ISO 16363:2011 – Audit and certification of trustworthy digital repositories

- ISO 23081–1:2006 – Information and documentation – records management processes – metadata for records

- Iso/Iec 17021:2006 – Conformity assessment – Requirements for bodies provifing audit and certification of management system

- Mag – Metadati amministrativi e gestionali

- Mets - Metadata encoding & transmission standard

- Moreq - Model Requirements for Electronic Records Management

- Paimas – Iso 20652:2006 – Space data and information transfer system

- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine

- Rlg – Nara Task force on digital repository certification: *Audit checklist for certifying digital repositories*

2.3 Definizioni

Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Aggregazione documentale informatica	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
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del Testo Unico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del

	documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Ciclo di gestione	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	Decreto legislativo 7 Marzo 2005, n. 82 e successive modificazioni e integrazioni
Codice eseguibile	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'AgID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ad attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50, comma 4 del Testo Unico nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole tecniche per il sistema di conservazione
Dati giudiziari	Dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u), del Decreto del Presidente della

	Repubblica 313/2002[1] in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale[2]
Dati personali	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale[3]
Dati sensibili	Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale[4]
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
Documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Sequenza di simboli binari, ossia di bit, che può essere elaborata da una procedura informatica
Fascicolo informatico	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

[1] DPR n. 313 del 14 Novembre 2002, *Testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti*, art. 3.

[2] Cfr. DLgs n. 196 del 30 Giugno 2003, *Codice in materia di protezione dei dati personali*, art. 4, comma 1 – e.

[3] Cfr. DLgs n. 196 del 30 Giugno 2003, *Codice in materia di protezione dei dati personali*, art. 4, comma 1 – b.

[4] Cfr. DLgs n. 196 del 30 Giugno 2003, *Codice in materia di protezione dei dati personali*, art. 4, comma 1 – d.

	creato e gestito secondo le disposizioni stabilite dall'art. 41 del Codice
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
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
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[5]
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
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzionalità aggiuntive	Le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
Funzionalità interoperative	Le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'art. 60 del Testo Unico.
Funzionalità minima	La componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'art. 56 del Testo Unico
Funzione di hash	Una funzione matematica che genera, a partire

[5] Definizione introdotta dal DLgs n. 235 del 30 Dicembre 2010, *Modifiche ed integrazioni al decreto legislativo 7 Marzo 2005, n. 82, recante Codice dell'amministrazione digitale a norma dell'articolo 33 della legge 18 Giugno 2009, n. 69*, art. 1, comma q – bis.

	da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Generazione automatica di documento informatico	Formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immagine Iso	File immagine contenente l'intero contenuto di un archivio, può essere usato direttamente (tramite software di emulazione) oppure scritto su un supporto ottico tramite il processo di masterizzazione. L'estensione del file immagine è .iso (deriva dallo standard ISO 9660)
Immodificabilità	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
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione ad una sequenza informatica d'origine di un'opportuna funzione di hash
Indice di conservazione	È l'evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate; deve essere corredato da un riferimento temporale e dalla firma digitale o firma elettronica qualificata del soggetto che interviene nel processo di produzione del pacchetto di archiviazione
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 delle Regole tecniche, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano le qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici

	sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'art. 9 delle Regole tecniche del sistema di conservazione
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico DPCM 31 ottobre 2000 e successive modificazioni e integrazioni
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale. La marca temporale può essere solamente rilasciata da una *Time Stamping Authority*
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 delle Regole Tecniche del sistema di conservazione
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche solo i metadati riferiti agli oggetti da conservare
Piano della sicurezza del sistema di	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a

conservazione	proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'art. 68 del Testo Unico
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Posta elettronica certificata	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'art. 10 delle Regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha firmato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'art. 53, comma 5 del Testo Unico

Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del Testo Unico, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile del servizio di conservazione	Il Responsabile del servizio di conservazione definisce ed attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia; è responsabile dell'insieme delle attività elencate nell'art. 7 delle Regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	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
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di	Sistema di conservazione dei documenti

conservazione	informatici di cui all'art. 44 del Codice
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del Testo Unico; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	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
Supporto ottico	Mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser; sono supporti ottici, ad esempio, i CD, i dischi magneto-ottici, i DVD
Time stamping Authority	Enti certificatori abilitati a prestare il servizio di marcatura temporale
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati
Ufficio utente	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Versamento agli Archivi di Stato	Operazione con cui il Responsabile del servizio di conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali[6]

[6] Il termine dei 40 anni previsti dall'art. 41, c. 1 del D.Lgs. 42/2004, *Codice dei beni culturali e del paesaggio,* è stato modificato in 30 anni dalla Legge n. 106 del 29 luglio 2014, *Disposizioni urgenti per la tutela del patrimonio culturale, lo sviluppo della cultura e il rilancio del turismo,* art. 12, c. 4, l. b.

2.4 Acronimi

Di seguito si riporta la forma estesa degli acronimi utilizzati nel presente documento.

AGID	Agenzia per l'Italia digitale
AIPA	Autorità per l'informatica nella pubblica amministrazione
API	Application programming interface
ASCII	American standard code for information interchange
CA	Certification Authority
CD	Compact disc
CNIPA	Centro nazionale per l'informatica nella pubblica amministrazione
D.Lgs	Decreto Legislativo
DM	Decreto Ministeriale
DMO	Document Management Outsourcing
DPCM	Decreto del Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DPS	Documento programmatico della Sicurezza informatica
DVD	Digital versatile disc
FTP	File transfer protocol
GED	Sistema di Gestione Elettronica dei Documenti
HSM	Hardware security module
HTTPS	Hypertext transfert protocol over secure socket layer

ICR	Intelligent character recognition
IP	Internet protocol address
IPA	Indice pubblica amministrazione
ISO	International standard organization
JPEG	Joint photographic experts group
LDAP	Lightweight directory access protocol
NAS	Network attached storage
OCR	Optical character recognition
PA	Pubblica amministrazione
PdA	Pacchetto di archiviazione
PdD	Pacchetto di distribuzione
PDF	Portable document format
PDI	Preservation description information
PdV	Pacchetto di versamento
PEC	Posta elettronica certificata
SAN	Storage area network
SFTP	SSH (Secure SHell) File Transfer Protocol
SGML	Standard generalized markup language
SinCRO	Supporto all'interoperabilità nella conservazione e nel recupero degli oggetti digitali
SLA	Service Level Agreement
TIFF	Tagged image file format

TSA	Time Stamping Authority
UNI	Ente nazionale italiano di unificazione
URL	Uniform resource locator
USB	Universal serial bus
XML	Extensible markup language

3. SOGGETTI E RESPONSABILITÀ

3.1 Premessa

Nel processo di conservazione intervengono diversi soggetti aventi profili, compiti e responsabilità differenziate di seguito riportati:

- il responsabile del servizio di conservazione;
- il responsabile della funzione archivistica di conservazione;
- il responsabile del trattamento dei dati personali;
- il responsabile della sicurezza dei sistemi per la conservazione;
- il responsabile dei sistemi informativi per la conservazione;
- il responsabile dello sviluppo e della manutenzione del sistema.

Tali individui, presenti nella struttura organizzativa di Siav, svolgono attività specifiche nel processo di conservazione dei documenti informatici secondo quanto indicato nel presente documento.

Accanto ai responsabili collaborano anche i delegati dei responsabili, consulenti, tecnici, sviluppatori, sistemisti, ecc. che rientrano nell'organigramma Siav e partecipano al processo di conservazione condividendo la metodologia indicata dai diversi responsabili.

Il soggetto conservatore si impegna a monitorare tutte le fasi del processo al fine di migliorarle continuamente, ad assicurare lo sviluppo per sostenere la continuità del servizio di conservazione digitale e documentare i cambiamenti intervenuti nel repository con riferimento alle procedure, al software, all'hardware e in relazione alle strategie di conservazione adottate.

Il soggetto conservatore si interfaccia con molteplici comunità di riferimento ossia un gruppo ben individuato di potenziali utenti che dovrebbero essere in grado di comprendere un potenziale insieme di informazioni.

Il soggetto che decide di affidare il processo di conservazione a Siav può essere un soggetto pubblico (Comune, Università, ecc.) oppure un soggetto privato (azienda, associazione, fondazione, ecc.).

3.2 Il conservatore: Siav Spa DMO

Il conservatore Siav Spa – DMO (d'ora innanzi Siav) attua le politiche necessarie ai fini di poter garantire la conservazione dell'archivio informatico prodotto da un qualsiasi soggetto produttore, sia pubblico che privato, il quale decide di affidare il proprio patrimonio documentale digitalizzato al sistema di conservazione progettato da Siav.

Siav, in quanto soggetto conservatore e custode affidabile:

- si comporta come una terza parte neutrale, ossia dimostra di non aver nessun coinvolgimento nel contenuto dei documenti e nessun motivo per alterare i documenti che si trovano sotto la sua custodia e che non permetterà a nessuno di alterare in maniera accidentale o intenzionale gli oggetti digitali conservati;
- è dotato della conoscenza e delle abilità necessarie ad adempiere alle proprie responsabilità, tale elemento viene garantito dalla presenza di competenze specializzate nei settori tecnico-informatici, giuridici e archivistici;
- ha stabilito un processo di conservazione affidabile che sia capace di assicurare negli anni l'integrità e la leggibilità degli archivi conservati.

Siav è una società di programmazione software e di servizi informatici nata nel 1990 per dedicarsi principalmente allo sviluppo di procedure ICR. Nel corso degli anni l'azienda ha progressivamente ampliato la gamma delle proprie attività giungendo oggi ad occupare una posizione di rilievo nell'ambito dei prodotti e servizi offerti per la gestione documentale.

Infatti Siav ha ottenuto la certificazione UNI CEI ISO/IEC 27001:2006[7] per la progettazione e l'erogazione di servizi di dematerializzazione, gestione documentale e conservazione sostitutiva.

Siav garantisce la formazione e l'aggiornamento professionale in particolar modo ai responsabili coinvolti nel processo di conservazione digitale i quali periodicamente si interfacciano sulle tematiche con i membri della Fondazione Siav Academy[8].

Nella sede principale di Padova è presente la divisione Siav DMO che si occupa della gestione in outsourcing delle attività legate al trattamento dei flussi documentali; sono effettuati molteplici servizi, tra i quali:

- digitalizzazione di documenti in formato analogico e recupero archivi;
- termosigillatura, archiviazione e stoccaggio sicuro del cartaceo;
- elaborazione di documenti digitali e relativa gestione;
- fatturazione elettronica;
- postalizzazione massiva e multicanale;
- mail room, ossia domiciliazione della corrispondenza presso il centro servizi del DMO con scansione della posta in arrivo, indicizzazione ed elaborazione dei documenti;
- gestione documentale on-line, in modalità ASP e SaaS, ove i documenti possono essere inseriti come esito delle lavorazioni in outsourcing o direttamente dal soggetto produttore tramite una interfaccia web.

[7] Conforme allo standard ISO/IEC 27001:2005 "Requisiti di un ISMS (Information Security Management System)", indicato nell'all. 3 delle Regole tecniche sulla conservazione.

[8] http://www.fondazionesiavacademy.it/

3.3 Il Responsabile del servizio di conservazione

Il responsabile del servizio di conservazione, analizzando il processo di conservazione e le peculiarità del sistema progettato, ha predisposto il presente manuale della conservazione di cui si impegna a curare l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali e tecnologici rilevanti.

Il responsabile del servizio di conservazione per la gestione delle attività inerenti il processo di conservazione può delegare tutte o parte delle attività di sua competenza[9].

3.3.1 I profili dei responsabili

Il responsabile del servizio di conservazione opera d'intesa con i responsabili del trattamento dei dati personali, della sicurezza, dei sistemi informativi e della funzione archivistica di conservazione. Nelle tabelle che seguono sono riportati i nominativi di tutti i responsabili e le relative attività nel processo di conservazione.

[9] Ai sensi dell'art. 6 delle Regole tecniche per la conservazione.

Nome e Cognome	Nicola Voltan
Carica	Responsabile del servizio di conservazione
Attività	Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione delle tipologie documentali; sottoscrive con firma digitale i pacchetti di archiviazione e distribuzione; effettua il monitoraggio per garantire la corretta funzionalità del sistema di conservazione; assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente; adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, ne ripristina la corretta funzionalità; adotta analoghe misure per affrontare l'obsolescenza dei formati; provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico; adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione; assicura la presenza di un Pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite; assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza; provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati presso l'Archivio centrale dello Stato e agli Archivi di Stato secondo quanto previsto dalle norme vigenti.
Modalità incarico	Nomina da parte del Consiglio di amministrazione
Data inizio incarico	28 settembre 2006
Data termine incarico	Fino a revoca

Nome e Cognome	Nicola Voltan
Carica	Responsabile del trattamento dei dati personali
Attività	Definisce la politica di sicurezza delle informazioni; recepisce le interpretazioni del Garante; monitora i sistemi informativi per stabilire e garantire i livelli di sicurezza e di riservatezza; definisce le strategie per un corretto salvataggio delle banche dati; definisce i profili e assegna le credenziali per l'accesso al sistema di conservazione.
Modalità incarico	Nomina da parte del Consiglio di amministrazione
Data inizio incarico	28 settembre 2006
Data termine incarico	Fino a revoca

Nome e Cognome	Rosalia Telese
Carica	Responsabile della funzione archivistica di conservazione
Attività	Definisce e gestisce il processo di conservazione, incluse le modalità di trasferimento da parte del soggetto produttore; descrive i documenti e le aggregazioni documentali trasferite nel sistema di conservazione e ne verifica l'integrità; monitora la fase di esibizione per garantire l'accesso e la fruizione del patrimonio documentario e informativo conservato; definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; mantiene traccia nel tempo delle modifiche effettuate al documento e ai fascicoli (versioning). Analizza lo sviluppo di nuove funzionalità archivistiche del sistema di conservazione; collabora con il soggetto produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali.
Modalità incarico	Incarico diretto da parte dell'Operations manager[10]
Data inizio incarico	1 ottobre 2014
Data termine incarico	Fino a revoca

[10] L'Operations manager risponde al Direttore generale di Siav.
Svolge principalmente le seguenti funzioni:
1) Responsabile dei Servizi informatici
2) Servizi professionali e consulenziali
3) Outsourcing
Su richiesta sarà fornito l'organigramma di Siav.

Nome e Cognome	Davide Mietto
Carica	Responsabile della sicurezza dei sistemi per la conservazione
Attività	Adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione dei documenti informatici; definisce le modalità per la generazione delle copie di sicurezza; aggiorna le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale, con particolare attenzione alla connessione alla Certification Authority; mantiene e rende accessibile un archivio del software dei programmi in gestione, nelle eventuali diverse versioni, aggiornando la lista del software di consultazione, garantendone la completezza in funzione della tipologia di documenti presenti in conservazione e la possibilità di istallarli sui sistemi operativi in uso presso Siav – DMO.
Modalità incarico	Incarico diretto da parte dell'Operations manager
Data inizio incarico	1 ottobre 2014
Data termine incarico	Fino a revoca

Nome e Cognome	Davide Mietto
Carica	Responsabile dei sistemi informativi per la conservazione
Attività	Verifica la corretta funzionalità del sistema e dei programmi in gestione, monitorando gli SLA applicativi appositamente definiti; attiva specifiche contromisure contro la minaccia di virus, malware, intrusioni non autorizzate e attacchi informatici; effettua periodicamente l'analisi dei rischi e gestisce le procedure di backup.
Modalità incarico	Incarico diretto da parte dell'Operations manager
Data inizio incarico	1 ottobre 2014
Data termine incarico	Fino a revoca

Nome e Cognome	Morgan Rizzolo
Carica	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
Attività	Analizza e valuta le funzionalità attuali per le future implementazioni del sistema di conservazione; valuta i cambiamenti ritenuti utili o necessari per i processi critici, che potrebbero potenzialmente impattare sul sistema di conservazione. Tali cambiamenti possono essere, ad esempio, relativi ai processi di versamento, archiviazione e distribuzione dei pacchetti, ai processi, alle modalità di gestione degli accessi, alla architettura infrastrutturale ed applicativa del processo, all'interazione con altri sistemi.
Modalità incarico	Incarico diretto da parte dell'Operations manager
Data inizio incarico	1 ottobre 2014
Data termine incarico	Fino a revoca

Nome e Cognome	Daniela Perrone
Carica	Consulente per la conservazione digitale
Ruolo nel processo	Consulente incaricato dal responsabile del servizio di conservazione per l'analisi di specifiche classi documentali e relativo processo di conservazione
Modalità incarico	Incarico diretto da parte dell'Operations manager
Data inizio incarico	3 novembre 2014
Data termine incarico	Fino a revoca

3.4 Il soggetto produttore

Il soggetto che fornisce le informazioni da conservare identifica il soggetto pubblico o privato, produttore di un archivio il quale decide di affidare la conservazione dei propri documenti a Siav.

Siav sottoscrive con il soggetto produttore gli accordi di servizio (SLA) che definiscono procedure e responsabilità dettagliate in base alla tipologia d'archivio.

Siav è responsabile in merito alle procedure adottate nel processo di conservazione mentre la responsabilità del contenuto dei documenti versati nel sistema di conservazione è in capo al responsabile della conservazione del soggetto produttore.

Al soggetto produttore spettano le seguenti attività:

- la redazione dei documenti e le relative attività di protocollazione, classificazione e fascicolazione;
- la registrazione in appositi registri per alcune tipologie documentali: es. documenti fiscali, contratti, ecc.;
- l'estrazione degli oggetti destinati alla conservazione dai propri sistemi (gestionali e specifici per la gestione documentale) e il versamento a Siav nei modi e nei tempi prestabiliti nel manuale della conservazione e negli accordi di servizio;
- in caso di documentazione rilevante ai fini fiscali, la corretta conservazione delle copie dei supporti ricevuti da Siav presso le proprie sedi, essendo queste ultime l'effettivo luogo "di tenuta e conservazione delle scritture" valido per le Agenzie competenti ai fini di eventuali verifiche.

In particolare, è importante evidenziare che:

- ricade sul soggetto produttore la responsabilità di inviare i documenti a Siav in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa e secondo quanto concordato negli accordi di servizio;
- qualora i documenti non fossero recapitati entro i tempi indicati, Siav provvederà a notificare al soggetto produttore la necessità di redigere una registrazione di non conformità: le specifiche relative a tale circostanza sono riportate negli accordi di servizio;
- il soggetto produttore trasmette i propri documenti al sistema di conservazione in forma stabile e non modificabile secondo gli accordi concordati e nel rispetto della normativa;
- il soggetto produttore risponde del contenuto dei documenti e di ogni responsabilità nei confronti delle Autorità preposte;

- il soggetto produttore concorda con l'Autorità preposta le modalità operative per la selezione e lo scarto di tipologie documentali; può ricevere supporto dal soggetto conservatore.

3.5 Il Pubblico ufficiale: modalità di intervento

Il responsabile del servizio di conservazione è obbligato, qualora fosse necessario, a contattare il Pubblico ufficiale e ad assicurare i diritti di accesso al sistema di conservazione per lo svolgimento delle attività per le quali è chiamato ad intervenire.

Per i documenti delle Pubbliche amministrazioni, la funzione di Pubblico ufficiale è svolta da un soggetto interno alla stessa amministrazione; tale ruolo non può sovrapporsi a quello di dirigente dell'Ufficio responsabile del servizio di conservazione dei documenti informatici.

Per i documenti provenienti da soggetti privati invece, il responsabile del servizio di conservazione, sulla base degli accordi di servizio, può eventualmente delegare a Siav il compito di convocare un Pubblico ufficiale.

Il Pubblico ufficiale interviene principalmente in fasi specifiche del processo quali:

- la verifica dei formati[11]
- la produzione di copie e duplicati[12].

3.6 I certificatori: Certification Authority e Time Stamping Authority

Tutte le firme digitali utilizzate da Siav vengono apposte tramite smart-card e sono supportate da un certificato emesso dalla Società Actalis, certificatore attivo presente nell'elenco pubblicato dall'AgID.

Anche il servizio di marcatura temporale del quale Siav Spa – DMO usufruisce è erogato dalla Società Actalis.

[11] Cfr. sotto-paragrafo 4.3.3 "Verifiche, eccezioni e rapporto di versamento".

[12] Cfr. paragrafo 6.2 "Produzione di copie e duplicati".

3.7 Utenti

L'utente è il ruolo svolto da soggetti (pubblici o privati) oppure da un sistema di gestione documentale, che interagiscono con i servizi del sistema di conservazione al fine di trovare e acquisire le informazioni di interesse. La *comunità di riferimento* è una classe speciale di utenti: è l'insieme degli utenti che dovrebbero essere in grado di comprendere l'informazione conservata.

Pertanto il soggetto produttore rappresenta la comunità di riferimento principale; ad essa si affiancano ulteriori soggetti che, nel rispetto della normativa vigente, accedono all'informazione. Le Autorità incaricate di effettuare i controlli quali l'Agenzia delle entrate, la Guardia di Finanza ecc. hanno diritto di accedere in qualsiasi momento al sistema di conservazione; inoltre godono dello stesso diritto anche le Autorità di controllo diversificate in base alla natura giuridica e alla mission del soggetto produttore.
L'AgID, in qualità di Autorità che ha rilasciato la certificazione dichiarando valido il sistema di conservazione, può effettuare l'accesso al sistema per espletare l'attività di controllo.

4. IL PROCESSO DI CONSERVAZIONE

4.1 Modello di conservazione

Il modello adottato da Siav per la conservazione digitale si ispira allo standard internazionale OAIS per la conservazione di oggetti digitali a lungo termine.

OAIS è un modello concettuale di rappresentazione degli oggetti, processi, strategie e tecniche finalizzati alla conservazione a lungo termine di un qualsiasi tipo di contenuto digitale.

Nasce inizialmente allo scopo di definire un modello di conservazione dei dati spaziali, dalla collaborazione tra il Comitato Consultivo per i Sistemi di Dati Spaziali (CCSDS) e l'ISO, elaborato come bozza nel 1997, diviene standard ISO nel 2003 noto come ISO 14721:2003.

Un sistema informativo aperto per l'archiviazione (OAIS) è «un archivio, inteso come struttura organizzata di persone e sistemi, che accetti la responsabilità di conservare l'informazione e renderla disponibile ad una comunità di riferimento»[13].

OAIS si propone di archiviare tutte le informazioni per l' "autoconsistenza" nell'interpretazione dell'oggetto digitale; quindi oltre all'informazione stessa viene inclusa anche una descrizione della struttura e del formato in cui l'informazione è archiviata.

Nel sistema di conservazione Siav, come già precedentemente indicato, operano tre soggetti (figura 1) aventi diversi ruoli e competenze:

- il produttore è il ruolo svolto dalle persone fisiche o giuridiche o dai sistemi che forniscono le informazioni da conservare;
- il responsabile è colui che definisce e attua le politiche complessive del sistema e ne governa la gestione con piena responsabilità e autonomia;
- l'utente è il ruolo svolto da persone o sistemi che interagiscono con il sistema di conservazione al fine di accedere e ricercare le informazioni di interesse.

Virgilio, il sistema di conservazione studiato e progettato da Siav, consente di gestire in modo semplice e sicuro la conservazione digitale di tutti di documenti e fascicoli informatici versati da un soggetto produttore attraverso un sofisticato sistema di monitoraggio e controllo.

Il mantenimento nel tempo del valore legale dei documenti e i processi di verifica/integrità dei supporti virtualizzati (LifeCycle) sono assicurati da una serie di servizi automatici di gestione e manutenzione dell'archivio digitale tra cui:

- gestione multi-azienda/multi-ente che permette di suddividere l'archivio digitale per azienda o ente; per ciascuno di essi è possibile attribuire diversi profili e ruoli per l'accesso ai dati e l'esecuzione delle attività di conservazione;

[13] G. Michetti, *Open archivial information system*, ICCU, 2007.

- gestione per ambiti che consente di organizzare logicamente l'archivio di Virgilio definendo ambiti documentali distinti relativi ad esempio alle diverse tipologie documentali;
- gestione per classi o tipologie documentali che permette di rintracciare in modo puntuale un documento tramite una serie di dati associati al medesimo.

Il sistema di conservazione Virgilio gestisce il workflow relativo a tutte le fasi del processo conservativo che vengono controllate e monitorate dai responsabili.

Il processo di conservazione descritto nel presente manuale verrà implementato sviluppando ulteriori funzionalità dell'applicativo e recependo i cambiamenti organizzativi e tecnologici; di pari passo verrà aggiornato anche il presente documento[14].

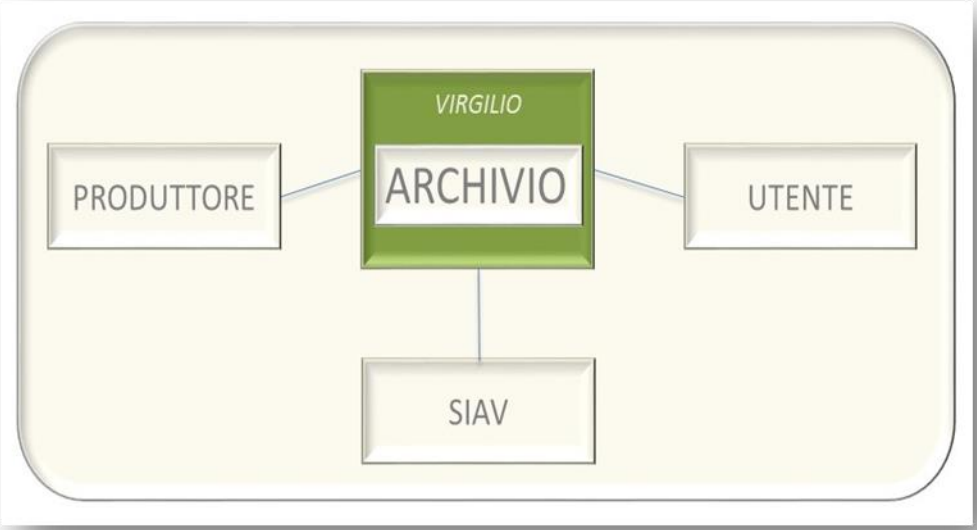

Figura 1: Virgilio - modello OAIS

[14] Nel modello OAIS tale adeguamento è definito come Preservation Planning (Pianificazione della conservazione) ossia la progettazione delle strategie di conservazione dell'archivio digitale in previsione ai cambiamenti tecnologici e organizzativi.

4.2 Composizione dei pacchetti

Gli oggetti conservati nel sistema di conservazione sono organizzati in pacchetti informativi, intesi come contenitori che racchiudono uno o più oggetti da trattare (documenti informatici, fascicoli informatici, aggregazioni informatiche oppure anche i soli metadati riferiti agli oggetti da conservare o conservati) comprensivi delle informazioni per la loro interpretazione e rappresentazione.

I pacchetti informativi quindi contengono non solo il documento e/o l'aggregazione (ciò che deve essere conservato) ma anche i metadati necessari a garantirne la conservazione e l'accesso nel lungo periodo.

Si tratta di una rappresentazione concettuale dell'informazione nelle sue fasi di vita:

- immissione in archivio;
- archiviazione e conservazione;
- distribuzione ed esibizione all'utenza.

I pacchetti informativi, a seconda della loro funzione, vengono distinti in tre tipologie:

- Pacchetto di versamento (PdV)
- Pacchetto di archiviazione (PdA)
- Pacchetto di distribuzione (PdD)

Nei successivi paragrafi verrà illustrato il processo di gestione e conservazione (come schematizzato nella figura 2) dal momento della trasmissione del PdV da parte del soggetto produttore fino alla creazione del PdD. Qualora intervenissero cambiamenti nel processo di conservazione sarà compito del responsabile del servizio di conservazione esplicitare le eventuali modifiche/integrazioni/correzioni inerenti il processo.

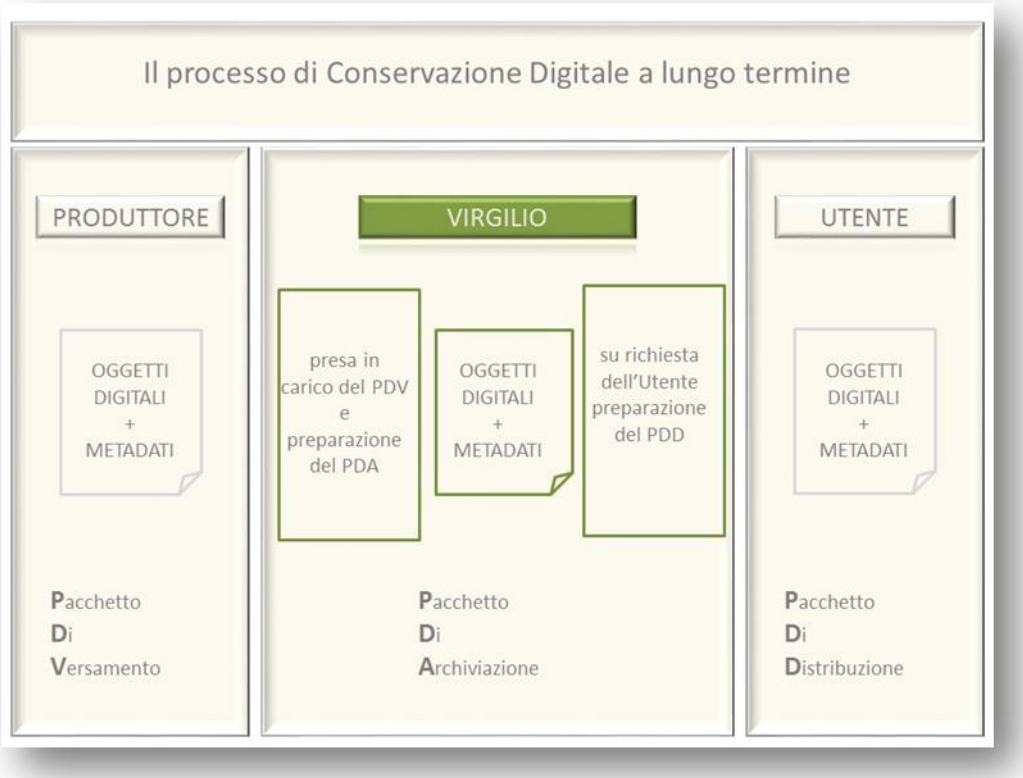

Figura 2: Schema del processo di conservazione

4.3 Creazione del pacchetto di versamento

Il PdV è il pacchetto informativo proveniente dal soggetto produttore e versato nel sistema di conservazione.

Il processo di acquisizione individua l'insieme delle attività finalizzate all'accettazione delle risorse digitali versate dal soggetto produttore e alla loro preparazione per l'inserimento nell'archivio[15].

Le condizioni di versamento sono concordate a monte con il soggetto produttore; il responsabile del servizio di conservazione, d'intesa con il responsabile della funzione archivistica, coordinano l'intero processo monitorando le attività. Viene verificata la presenza dei metadati minimi che il soggetto produttore deve associare alle tipologie/aggregazioni documentali informatiche che si accinge a versare nel sistema; se presente si procede alla lavorazione del PdV altrimenti viene effettuata una pre-lavorazione per attribuire i metadati al documento[16].

Il metadato oltre ad essere un dato è un'informazione che descrive un insieme di dati.

I metadati minimi per il documento informatico sono:

- identificativo

[15] Il modello funzionale OAIS identifica tali attività nelle operazioni di ingest.

[16] Per la descrizione dettagliata si rimanda al sotto-paragrafo 4.3.1 (4° caso).

- data di chiusura
- oggetto (sintesi del contenuto di un documento)
- soggetto produttore
- destinatario

I metadati minimi per il documento amministrativo informatico sono:

- codice identificativo dell'amministrazione (codice IPA)
- codice identificativo dell'area organizzativa omogenea (codice IPA)
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo

I metadati minimi per i fascicoli e le aggregazioni documentali sono:

- identificativo
- amministrazione titolare
- amministrazione partecipante
- oggetto
- responsabile del procedimento
- elenco dei documenti contenuti nel fascicolo

I documenti digitali vengono trasferiti in Virgilio tramite protocollo di tipo FTP, SFTP e HTTPS, sistemi criptati per garantire la sicurezza dei dati. Il soggetto produttore trasferisce i propri documenti nell'area dedicata di presa in carico; i file da elaborare vengono suddivisi per tipologia documentale e scaricati in cartelle appositamente predisposte. Il responsabile del servizio di conservazione allestisce un'area specifica dedicata al trasferimento dei file da elaborare e comunica al soggetto produttore i dati per il collegamento: indirizzo, nome utente, password[17].

Il responsabile della funzione archivistica verifica la presenza di ulteriori metadati inerenti il contesto e l'integrità degli oggetti/aggregazioni documentali versati nel sistema; si tratta di informazioni che nel modello OAIS corrispondono al PDI[18], informazioni descrittive per la conservazione a lungo termine dei PdA.

L'invio avviene sotto forma di lotti, che devono rispondere a precise caratteristiche quali l'essere in formato zip e recare un nome file senza spazi né caratteri speciali[19]. Ciascun lotto deve contenere i file documento e un file indice, che contiene la lista di tutti i documenti inviati e tutti i metadati obbligatori previsti dalla normativa vigente e dalla tipologia documentale interessata.

Ad ogni documento versato in conservazione il sistema associa automaticamente una serie di metadati di processo[20]; tra questi assume particolare importanza il codice alfanumerico identificativo univoco (d'ora

[17] Tali dati sono indicati negli accordi di servizio.

[18] I dettagli sul PDI sono descritti nel paragrafo 4.4.

[19] Ulteriori dettagli, inerenti l'intero processo conservativo, saranno di volta in volta concordati con il soggetto produttore negli accordi di servizio.

[20] Metadati utili alla gestione delle tipologie documentali/aggregazioni informatiche versate nel sistema di conservazione.

innanzi ID univoco) del soggetto produttore assegnato ad ogni oggetto/aggregazione documentale informatica.

L'ID univoco ha una duplice funzione:

- segna la tracciabilità del documento durante l'intero processo di conservazione;
- identifica in modo univoco il soggetto produttore.

L'ID univoco è un codice di 20 caratteri alfanumerici (es. figura 3): i primi 6 caratteri identificano il soggetto produttore e sono comuni a tutti gli oggetti documentali versati nel sistema da parte del medesimo produttore. I restanti 14 caratteri sono univoci per ogni documento versato nel sistema.

L'identificativo del soggetto produttore coincide con il codice IPA per quanto riguarda le Pubbliche amministrazioni, mentre per le Aziende private verrà fornito dal responsabile del servizio di conservazione. Il codice identificativo del soggetto produttore è riportato negli accordi di servizio.

Figura 3: Esempio di ID univoco

Il soggetto produttore, dopo aver trasferito il PdV nell'area di presa in carico, invia l'impronta dei documenti inserendola tra i metadati. Il responsabile del servizio di conservazione di Siav richiede infatti che tra i metadati di ogni documento sia presente il campo "impronta" che riporta l'hash del documento. Al momento della presa in carico del PdV il sistema automaticamente ricalcola l'impronta di ogni documento e la confronta con quella indicata nei metadati. In questo modo viene garantita l'integrità dei documenti in quanto si ha la sicurezza che non siano intervenute perdite di dati durante le fasi di lavorazione.

4.3.1 Pre - lavorazioni antecedenti alla conservazione

Siav offre alcuni servizi aggiuntivi di pre-lavorazione al fine di predisporre correttamente il PdV. Tali attività, opportunamente indicate negli accordi di servizio, prevedono innanzitutto l'analisi dei supporti e dei formati sui quali sono stati memorizzati i dati.

Di seguito si riportano quattro casi frequenti per i quali Siav interviene effettuando la pre-lavorazione. Si precisa che per ogni pre-lavorazione effettuata viene elaborata documentazione esemplificativa a supporto delle procedure tecniche e metodologiche garantendo in questo modo la tracciabilità delle operazioni svolte.

1° caso: Pre-lavorazione di documenti cartacei

I documenti in formato cartaceo giungono presso la divisione DMO o tramite corriere, scelto ed inviato dal soggetto produttore, oppure in seguito al ritiro da parte di un incaricato di Siav direttamente presso la sede del soggetto produttore.

Giunto a destinazione, il materiale documentale viene estratto dai contenitori di trasporto, liberato da eventuali punti metallici e sottoposto ad ogni trattamento necessario al fine di predisporlo per la digitalizzazione. Quest'ultima avviene scansionando i documenti con l'utilizzo del software Vincent[21]. A partire dalle immagini ottenute, il personale addetto procede all'indicizzazione dei dati minimi fondamentali per la descrizione e la conservazione. Terminata questa fase i documenti digitalizzati vengono gestiti nei fascicoli elettronici ed eventualmente riversati in Archiflow, il software progettato da Siav per la gestione documentale.

Il cartaceo, a seconda degli accordi presi con il soggetto produttore e della natura dei documenti in questione, può percorrere diverse strade[22]:

- viene restituito al soggetto produttore, che si assume la responsabilità di deciderne collocazione, destinazione e utilizzo;
- viene preso in carico da Siav e quindi collocato in deposito;
- destinato al macero secondo le modalità concordate con il soggetto produttore e ai sensi della normativa vigente.

2° caso: Pre-lavorazione di documenti digitali

Altre tipologie di lavorazione possono comportare la migrazione in formato PDF di documenti inviati dal soggetto produttore sotto forma di spool di stampa, rispettandone le informazioni di fincatura; oppure la separazione in singoli file di documenti giunti raggruppati in un unico PDF.

Ove contemplato negli accordi di servizio, una volta ultimati i controlli di continuità, gli operatori del DMO procedono per conto del soggetto produttore, all'apposizione della firma per l'emissione dei documenti elettronici, rendendoli così validi ai fini fiscali. In altri casi, i documenti consolidati vengono messi nuovamente a disposizione del soggetto produttore affinché li sottoscriva; collegandosi all'apposito portale, il soggetto produttore ha l'opportunità di operare un controllo sui documenti e di riscontrare l'esito del trattamento ad essi applicato.

[21] Vincent è la soluzione OCR-ICR-OMR barcode progettata da Siav per l'acquisizione automatica dei dati e delle immagini dei documenti.

[22] Per un ulteriore approfondimento si rimanda al documento "Piano per la sicurezza".

3° caso: Pre-lavorazione di documenti digitali in formato non idoneo alla conservazione a lungo termine

Spesso il soggetto produttore si trova ad avere la necessità di conservare documenti in formati che non presentano le caratteristiche adatte alla conservazione a lungo termine; in questo caso Siav offre un servizio di conversione dei formati che prevede la scelta, per un determinato file, del formato più adatto in termini di mantenimento della forma e dei contenuti tra quelli prescritti dalla normativa e dalle raccomandazioni internazionali in materia di conservazione a lungo termine[23].

4° caso: Associazione dei metadati ai documenti

Alcuni soggetti produttori potrebbero non avere la possibilità di creare un file xml che riporti i metadati minimi da associare al documento informatico; in questi casi Siav interviene offrendo un servizio di associazione dei metadati ai documenti.

Il soggetto produttore invia a Siav, per ogni documento, un file txt/csv contenente gli attributi utili alla popolazione dei metadati obbligatori ed eventualmente aggiuntivi. Siav procederà quindi alla creazione di un file nel quale verranno riportati i metadati definiti dal soggetto produttore. Per alcune tipologie documentali, che presentino un layout standardizzato[24] sarà altresì possibile un rilevamento automatico dei metadati ad opera del sistema.

[23] In particolare si fa riferimento a Pronom, registro internazionale sui formati che viene periodicamente consultato per l'aggiornamento sui formati idonei alla conservazione a lungo termine.

[24] Ad esempio lotti di fatture o verbali di ordine del giorno.

4.3.2 Fase di versamento

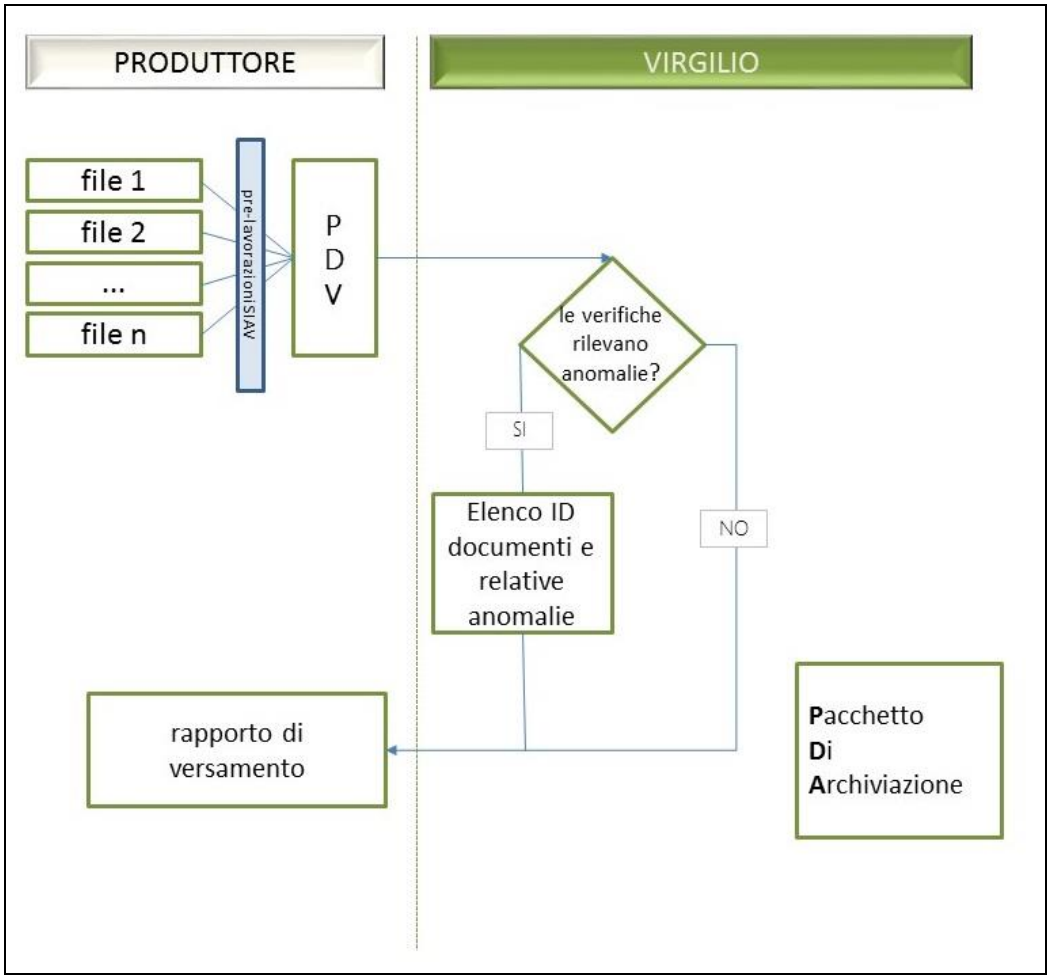

Figura 4: Fase di versamento

La figura 4 illustra il flusso di lavoro dell'intera fase di versamento, dal trasferimento dei documenti/aggregazioni informatiche da parte del soggetto produttore fino alla formazione del PdA.

Il soggetto produttore ha la possibilità di monitorare tutte le fasi del processo di conservazione attraverso l'interfaccia web predisposta dal sistema (figura 5).

L'intero processo di versamento viene tracciato dai log generati automaticamente dal sistema, salvati e conservati nel database Oracle.

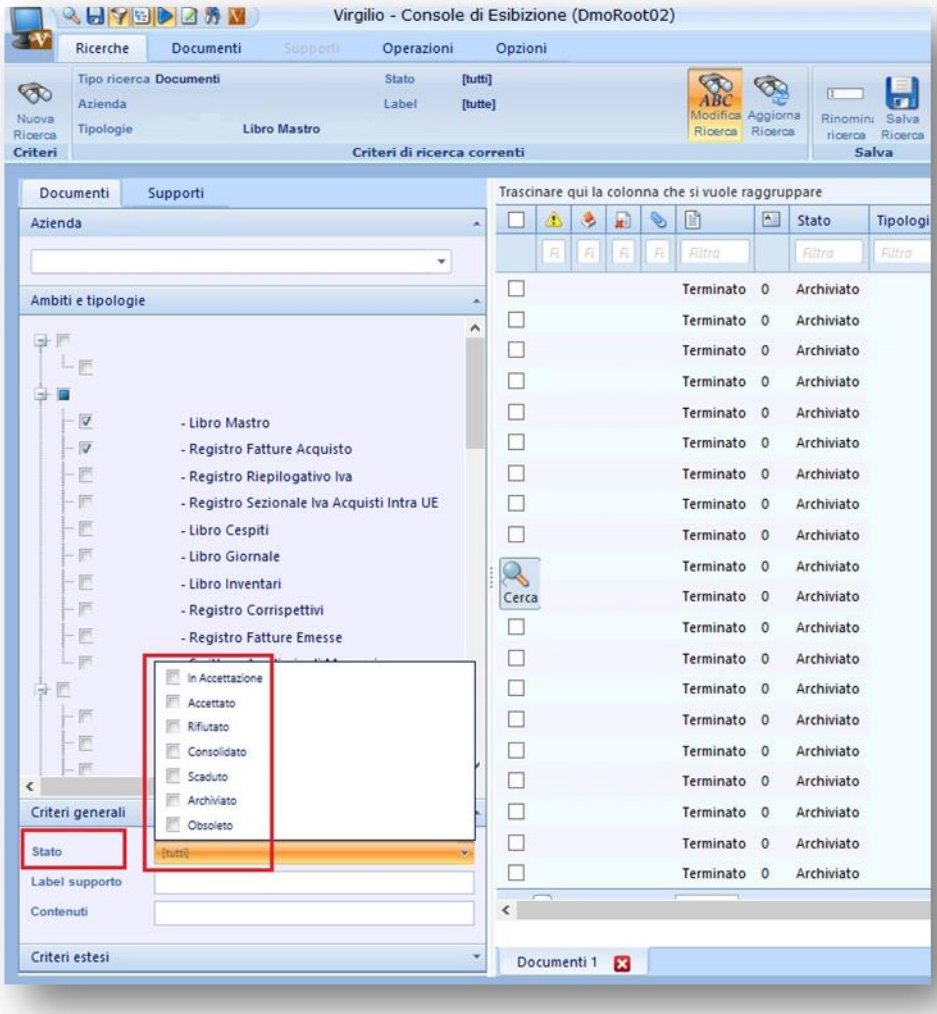

Figura 5: Console di esibizione di Virgilio

4.3.3 Verifiche, eccezioni e rapporto di versamento

L'acquisizione dei PdV nel sistema di conservazione avviene a cadenza programmata, concordata con il soggetto produttore sulla base delle proprie esigenze e della natura dei documenti trasferiti.

Per ogni pacchetto ricevuto, il sistema verifica che il contenuto sia rispondente a quanto definito negli accordi di servizio (formato dei file, presenza di metadati, eventuali verifiche sulla validità della firma, ecc.).
Virgilio effettua automaticamente le seguenti verifiche sulla documentazione trasmessa dal soggetto produttore:

- la validità delle firme, eseguita rispetto alla data indicata nel metadato "data di chiusura del documento" riportato dal soggetto produttore;
- la verifica di integrità, eseguita confrontando l'impronta nuova del documento con quella inviata dal soggetto produttore tra i metadati: il sistema ricalcola l'impronta del documento e la confronta con quella

iniziale presente tra i metadati del documento dal suo ingresso nel sistema.

I controlli fiscali, invece, vengono effettuati al momento della formazione del PdA.

Qualora venissero rilevate eventuali anomalie il sistema provvederà a notificarle al responsabile del servizio di conservazione; quest'ultimo procede a concordare con il soggetto produttore le modalità di risoluzione.

Negli accordi di servizio viene definito l'elenco dei formati dei documenti che il soggetto produttore vuole conservare nell'archivio digitale. Il responsabile del servizio di conservazione effettua periodicamente i controlli sui documenti e sulle aggregazioni documentali presenti nel sistema, in modo da identificare eventuali anomalie. Per il soggetto produttore sarà ovviamente possibile modificare/integrare l'elenco, stabilendo anche, in accordo con il responsabile del servizio di conservazione, eventuali eccezioni.

Le eccezioni fanno riferimento alla necessità, da parte del soggetto produttore, di conservare i documenti in formati non compatibili con la conservazione a lungo termine e sui quali non sia possibile effettuare una conversione di formato senza alterarne la leggibilità e la forma. In questo caso il responsabile del servizio di conservazione ammette tali documenti nel sistema di conservazione specificando però che, su queste eccezioni, non sarà possibile assicurare l'integrità e la leggibilità per la conservazione a lungo termine. In casi particolari, in cui risulti necessario effettuare trasformazioni sui documenti versati in formato non ammesso, potrebbe essere necessario l'intervento di un Pubblico ufficiale che attesti la correttezza del processo e l'integrità del contenuto e della forma del documento modificato rispetto all'originale.

I controlli effettuati da Virgilio sui documenti e sulle aggregazioni informatiche versate dal soggetto produttore comprendono anche le verifiche volte ad indentificare il formato dei file. Comunemente il formato di un file è riconosciuto attraverso la sua estensione; ai fini di una corretta identificazione questo non è però sufficiente in quanto l'estensione di un file può essere modificata, volontariamente o involontariamente, ad esempio a causa di una ridenominazione accidentale o per l'intervento di un virus. In ogni caso, anche se eseguita correttamente, l'identificazione del file tramite l'estensione permette di riconoscere solo la famiglia di formati cui appartiene e non la specifica versione, utile ai fini di una corretta rappresentazione del file.

Per la verifica dei formati all'interno di Virgilio, si utilizzano dei tool di riconoscimento basati sull'identificazione dei magic number, particolari sequenze di byte, composte in modo variabile da 2 a 10 byte, che si trovano in specifiche posizioni del file (comunemente all'inizio).

Di seguito vengono indicati alcuni esempi di magic number: i file PDF iniziano con la sequenza "%PDF" (0x25504446, in notazione esadecimale); i file PostScript cominciano con la stringa "%!" (0x2521); le immagini GIF sono identificate dalla stringa ASCII "GIF87a" (0x474946383761) o "GIF89a" (0x474946383961), a seconda della versione; le immagini JPG (o JPEG) cominciano con la stringa esadecimale 0xFFD8FF; le immagini JPEG/JFIF contengono la stringa 0x4A464946 (equivalente a "JFIF" in ASCII); le immagini JPEG/EXIF contengono la stringa 0x45786966 (equivalente a 'Exif' in

ASCII) collocata a partire dal sesto byte e seguita dai metadati riguardanti il file; le immagini TIFF cominciano con la stringa ASCII "II" o "MM" a seconda del byte order utilizzato (II per Intel, o little endian, MM per Motorola, o big endian), seguita dal numero "42" ("0x2A00" o "0x002A" in notazione esadecimale, rispettivamente nella convenzione little endian o big endian)[25].

Effettuate tali verifiche il sistema genera automaticamente il rapporto di versamento che contiene un riferimento temporale e viene inviato al soggetto produttore con PEC o anche condiviso in area SFTP cui il soggetto produttore accede tramite username e password fornite dal responsabile del trattamento dei dati personali.
I rapporti di versamento vengono salvati dal sistema e versati in conservazione; Virgilio raggruppa la tipologia documentale "rapporto" la quale, per ogni soggetto produttore, include tutti i rapporti di versamento.

4.3.4 Rifiuto del pacchetto di versamento

Le verifiche sopra indicate possono dare anche esito negativo e quindi il sistema segnala la presenza di un'anomalia. Si hanno documenti anomali quando è avvenuta una corruzione o perdita di dati, ad esempio i dati sono memorizzati su formati non compatibili, sono presenti fatture discontinue, metadati mancanti, documenti con firma scaduta, ecc. In questi casi il sistema procede a "rifiutare" i documenti su cui sono state riscontrate le anomalie; Virgilio all'interno del rapporto di versamento segnala i documenti anomali contenuti nel PdV e il responsabile del servizio di conservazione carica il rapporto di rifiuto nell'area SFTP dedicata inviando una PEC al soggetto produttore con l'elenco delle anomalie riscontrate e la richiesta di un nuovo invio.
Il soggetto produttore, supportato dai responsabili del conservatore, procede alla risoluzione dell'anomalia e alla rielaborazione e al successivo invio di un nuovo PdV[26].

4.4 Pacchetto di archiviazione

Il pacchetto di archiviazione (PdA) è il pacchetto di informazioni destinato alla conservazione a lungo termine; è un'aggregazione di quattro tipi di oggetti informativi[27]:

- il contenuto informativo (content information – CI), include i dati di interesse primario ossia le informazioni destinate alla conservazione e le

[25] S. Allegrezza, *Requisiti e standard dei formati elettronici per la produzione di documenti informatici*, Eum, 2008.

[26] Per ulteriori dettagli sulle anomalie e relativa comunicazione si rimanda al paragrafo 4.4 del documento allegato "Specificità del contratto"; si precisa che l'assistenza e gli interventi aggiuntivi forniti da Siav nelle fasi del processo di conservazione saranno di volta in volta concordati con il soggetto produttore in base alle diverse esigenze e criticità.

[27] Cfr. M. Guercio, *Conservare il digitale. Principi, metodi e procedure per la conservazione a lungo termine di documenti digitali*, Laterza, 2013, pp. 65-66.

informazioni di rappresentazione associate, ad es. uno specifico documento xml e lo schema xml relativo;
- le informazioni descrittive per la conservazione (PDI), includono le informazioni di identificazione dell'oggetto digitale, di contesto, provenienza e integrità;
- le informazioni sull'impacchettamento (packaging information – PI), le informazioni sulla composizione del pacchetto informativo (al fine di collegare l'oggetto digitale e i metadati associati);
- le informazioni descrittive, finalizzate a sostenere l'accesso alle risorse/contenuto informativo mediante strumenti di ricerca o di recupero.

Il PdA si ottiene dalla trasformazione di uno o più PdV; il responsabile della conservazione, supportato dal suo team, effettua le operazioni di *archivial storage* relative all'immagazzinamento a lungo termine delle risorse digitali affidate a Virgilio. Più specificamente, le funzioni di *archival storage* prevedono attività volte a garantire l'affidabilità e la funzionalità dei sistemi di immagazzinamento (storage); l'integrità e la fruibilità a lungo termine delle sequenze di bit (bit stream) che compongono i dati conservati.

Il responsabile della sicurezza dei sistemi informativi effettua periodicamente l'aggiornamento dei supporti di archiviazione (refresh) e la migrazione dei formati. Inoltre d'accordo con il responsabile del servizio di conservazione aggiorna le politiche di recupero da disastro (disaster recovery) per mitigare gli effetti di eventi catastrofici[28].

Infine, la componente *archival storage* recupera i documenti/fascicoli nel momento in cui si ha la necessità di consultarli; la richiesta può pervenire dal soggetto produttore o da altri utenti[29].

Il PdA (figura 6) prevede una specifica articolazione per mezzo del linguaggio formale xml, per la cui applicazione pratica si rimanda allo standard UNI SinCRO. Tale standard definisce, nel rispetto del modello OAIS, una struttura di dati xml che consente di predisporre sia le informazioni identificative minime (previste dal legislatore) che una infrastruttura generale in grado di gestire tutte le informazioni archivistiche necessarie al processo di formazione e tenuta dei documenti informatici in modo da assicurare l'interoperabilità tra sistemi e la conservazione a lungo termine.

Le informazioni PDI costituiscono metadati fondamentali per la conservazione a lungo termine dei documenti; tali informazioni sono articolate in 5 aree:

- **Provenance** (provenienza) sono le informazioni relative alla provenienza del contenuto informativo ovvero dati sulla natura giuridica, organigramma e funzionigramma del soggetto produttore e la tracciabilità dei cambiamenti avvenuti;
- **Reference** (identificazione) sono le informazioni che identificano in maniera univoca gli oggetti digitali (ad es. data e numero di protocollo);
- **Fixity** (integrità) sono informazioni sulla verifica della firma e impronta dell'autore del documento/aggregazione informatica;

[28] Per un approfondimento si rimanda al documento "Piano per la sicurezza".

[29] Procedura specificata nel paragrafo 4.5 dedicato all'esibizione.

- **Context** (contesto) sono le informazioni di contesto (es. l'ID del documento, il titolario, il repertorio dei fascicoli);
- **Right** (diritti) sono le informazioni sui diritti di accesso al contenuto informativo.

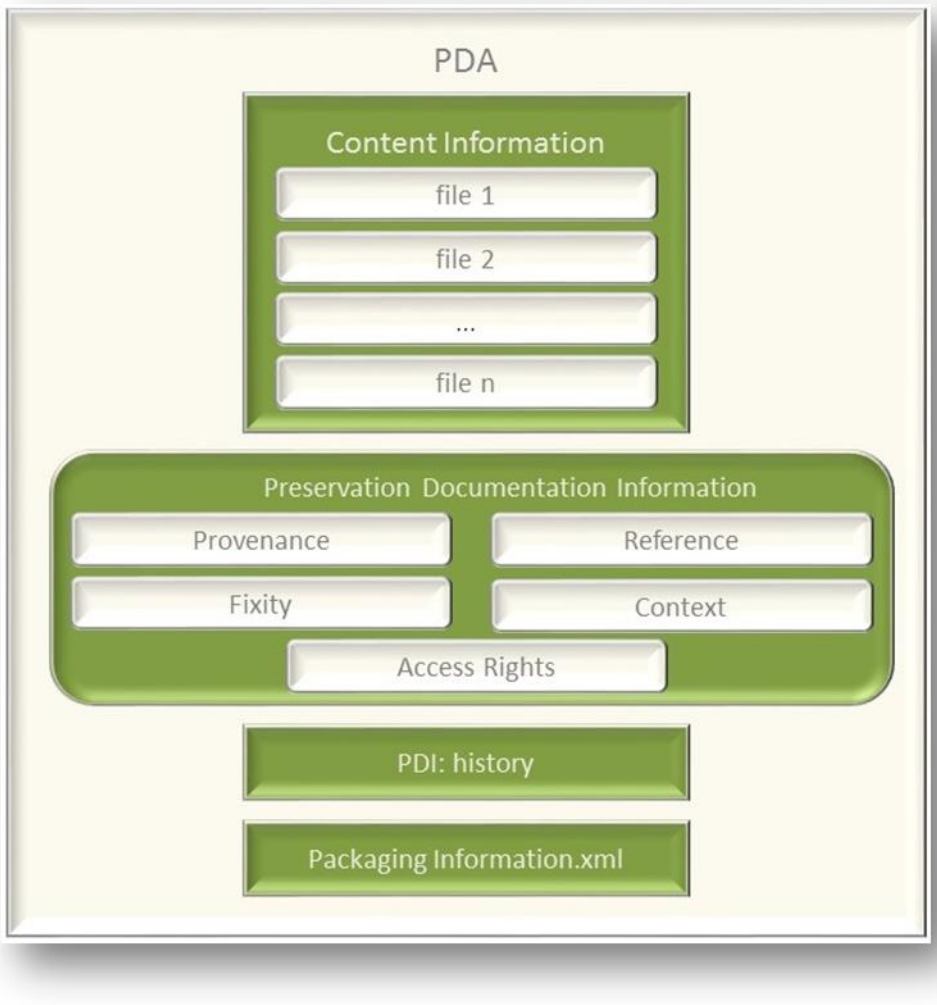

Figura 6: Schema del PdA

4.4.1 Creazione e struttura

Il sistema di conservazione gestisce esclusivamente PdA omogenei: i PdA sono formati accorpando documenti informatici della stessa tipologia.
Virgilio scompatta i PdV suddividendo i documenti in base alla tipologia documentale cui appartengono; per ogni tipologia documentale viene formato un PdA (es. figura 7).
Se nel PdV sono presenti documenti fiscali su cui vanno effettuati i controlli di continuità (ad esempio fatture), il sistema procede ad accorpare i documenti afferenti la stessa tipologia documentale e ad ordinarli, procedendo successivamente ad effettuare i controlli sulla numerazione dei documenti. Se

vengono riscontrate anomalie, il sistema provvede automaticamente a bloccare la formazione del PdA e a segnalare il problema al responsabile del servizio di conservazione. L'anomalia viene segnalata anche al soggetto produttore cui viene richiesto un nuovo invio. Il sistema sospende il processo per quello specifico PdA fino all'invio del documento rettificato. Dopo il nuovo invio vengono effettuati ex novo i controlli di continuità e, in caso di esito positivo, si può procedere alla formazione del PdA.

Una volta formato, il PdA viene firmato digitalmente dal responsabile del servizio di conservazione e viene apposta una marca temporale.
La procedura si conclude con la notifica al soggetto produttore dell'avvenuta formazione e certificazione del PdA tramite PEC trasmessa dal responsabile del servizio di conservazione.

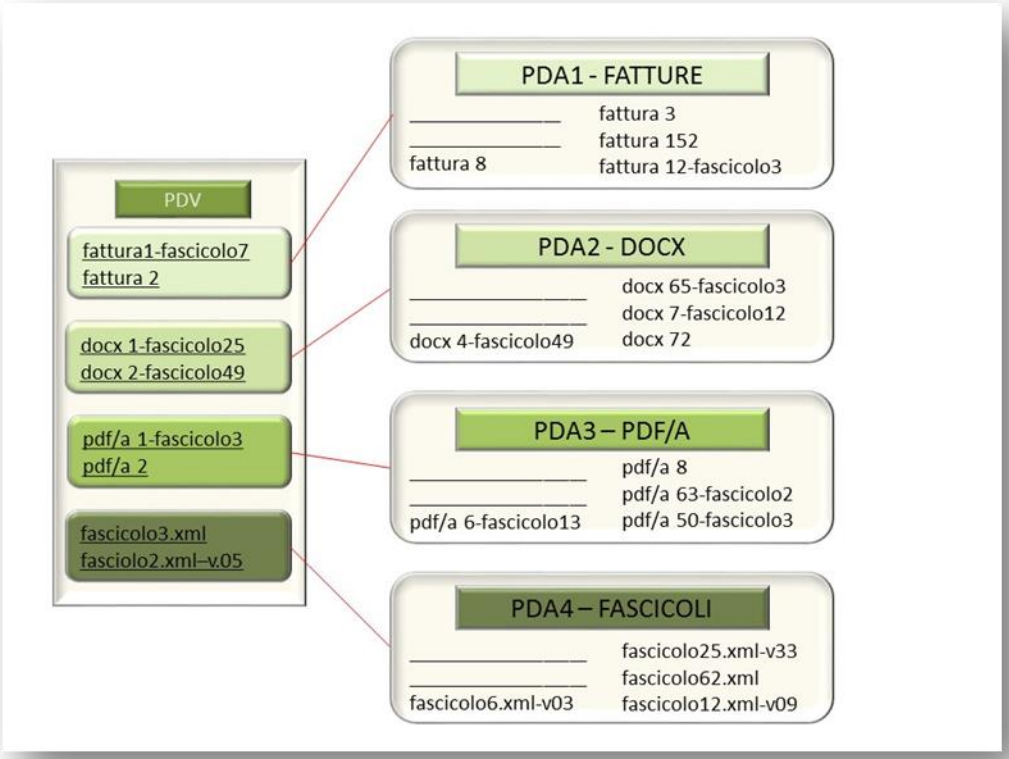

Figura 7: Formazione dei PdA

4.4.2 La gestione del fascicolo informatico in Virgilio

Il fascicolo informatico è un insieme di documenti prodotti da un soggetto nell'espletamento delle proprie funzioni relative alla stessa attività, affare, procedimento amministrativo.

I fascicoli di un soggetto, sia pubblico che privato, si differenziano in base all'argomento trattato dai documenti; sono collegati al titolario e la durata è molto variabile.

L'aggregazione documentale informatica è un raggruppamento di documenti o fascicoli riuniti per caratteristiche omogenee, in relazione alla natura giuridica (sentenze, libri mastri, ecc.) o alla forma dei documenti (verbali, decreti, contratti) o ancora in relazione all'oggetto e alla materia trattata[30].

Il PdA può contenere singoli documenti oppure aggregazioni documentali informatiche omogenee in relazione alla natura e alla forma dei documenti.

Sono previsti due differenti scenari attraverso cui il fascicolo informatico può entrare a fare parte del sistema di conservazione.

Nel primo caso il soggetto produttore ha la necessità di conservare un documento afferente ad un fascicolo corrente ovvero un'unità archivistica che raccoglie documentazione relativa a procedimenti/affari/attività in corso. Questa eventualità è gestita da Virgilio inviando in conservazione, insieme al documento in questione, anche il relativo fascicolo informatico. Il campo "Relation" dei metadati del documento informatico[31] è popolato con l'identificativo univoco del fascicolo informatico cui appartiene; questo permetterà la conservazione del vincolo archivistico fondamentale per garantire la correlazione tra i documenti informatici conservati. Il soggetto produttore ha la possibilità, tramite Virgilio, di conservare anche gli strumenti di gestione dell'archivio corrente ossia il piano di classificazione e il piano di fascicolazione; Virgilio conserva in un PdA tutti gli strumenti di gestione che il soggetto produttore procederà a versare man mano nel sistema di conservazione (es. un nuovo titolario, il manuale di gestione, il piano di conservazione, ecc.).

Il vincolo archivistico è rafforzato anche attraverso la valorizzazione dei metadati dell'oggetto digitale fascicolo che riporta, tra gli attributi obbligatori anche i riferimenti ai documenti che vi afferiscono.

Nel momento in cui il documento informatico viene inserito all'interno del PdA, il sistema forma parallelamente un ulteriore PdA-fascicolo che contiene il file xml del relativo fascicolo informatico.

Quando il fascicolo verrà nel tempo modificato (documenti aggiunti, modificati o rimossi) sarà attivata manualmente un'operazione di versioning del fascicolo: sarà formato un ulteriore file xml, collegato al precedente attraverso il popolamento dell'elemento "Source" con l'ID univoco del fascicolo originario, che riporta i dati originari del fascicolo, aggiungendo ulteriori elementi "Documento" in cui saranno riportati i dati dei documenti aggiunti, i dati dei versioning dei documenti modificati e i dati relativi ai documenti eliminati. Questa operazione di versioning può essere ripetuta *n* volte; l'ultimo versioning del fascicolo riporta la chiusura dello stesso e i riferimenti afferenti a tutti i documenti del fascicolo. Nel momento in cui l'utente richiede l'esibizione del fascicolo il sistema automaticamente seleziona l'ultimo versioning rilevato identificandolo attraverso la data riportata nell'IPdA. I PdA contenenti i versioning precedenti all'ultimo saranno scartati, in quanto l'ultimo versioning riporterà anche i dati relativi a tutte le modifiche apportate al fascicolo nel corso del tempo, comprensivi delle informazioni utili a richiamare i log di sistema salvati e conservati nel database Oracle. Tali log sono fondamentali per poter ricostruire il percorso del PdA all'interno di Virgilio.

[30] Per un approfondimento si rimanda al documento allegato "Specificità del contratto".

[31] Si fa riferimento al set di metadati Dublin Core.

Nel secondo caso il soggetto produttore ha la necessità di conservare un fascicolo chiuso ovvero un'unità archivistica contenente documentazione relativa a procedimenti/affari conclusi. In questo caso il soggetto produttore trasmette a Virgilio, secondo le modalità indicate nel paragrafo 4.3.2 *"Fase di versamento"*, il PdV contenente il fascicolo e tutti i documenti che lo compongono. Dopo i normali controlli sui documenti versati, il sistema provvede a suddividere i diversi documenti sulla base delle relative tipologie documentali e a formare *n* PdA contenenti le *n* tipologie documentali rilevate. Le relazioni tra i documenti e il fascicolo saranno mantenute grazie ai metadati dei documenti/fascicoli informatici.

4.4.3 L'indice del pacchetto di archiviazione

Il responsabile della funzione archivistica di conservazione procede alla verifica delle informazioni archivistiche necessarie al processo di tenuta dei documenti/aggregazioni informatiche e obbligatorie per assicurare le garanzie di affidabilità, integrità e autenticità nel lungo periodo.

Il lotto di documenti sottoposti a conservazione viene riepilogato in un file di chiusura, il cosiddetto Indice del Pacchetto di archiviazione (IPdA), il quale costituisce l'evidenza informatica associata ad ogni PdA contenente un insieme di informazioni articolate come descritto di seguito e illustrato nella figura 8.

Le informazioni archivistiche obbligatorie racchiuse in un IPdA sono:

- descrizione generale, comprende l'identificativo univoco dell'IPdA e le informazioni relative all'applicazione che lo ha generato (nome e versione dell'applicativo e produttore del software). Possono eventualmente essere inclusi i riferimenti per collegare l'IPdA ad altri precedenti IPdA presenti all'interno del sistema di conservazione;
- attributi del PdA cui l'IPdA è associato, comprendono l'identificativo univoco del PdA ed, eventualmente, i riferimenti che permettono di collegare tale PdA ad altri PdA presenti all'interno del sistema di conservazione;
- file gruppo, questo campo permette di aggregare più oggetti documentali presenti all'interno del PdA indicandone l'identificativo univoco e l'impronta. Tale attributo consente di formare degli insiemi di oggetti sulla base di criteri funzionali;
- processo, attraverso questo attributo vengono inserite le informazioni riguardanti il processo di conservazione dello specifico PdA cui l'IPdA fa riferimento. Sono riportati i dati dei soggetti intervenuti durante il processo di formazione del PdA, le informazioni relative a data e ora di produzione dell'IPdA sotto forma di riferimento e marca temporale; infine è previsto un campo Extrainfo in cui il sistema riporta le informazioni utili a richiamare i log di sistema salvati e conservati nel database Oracle.

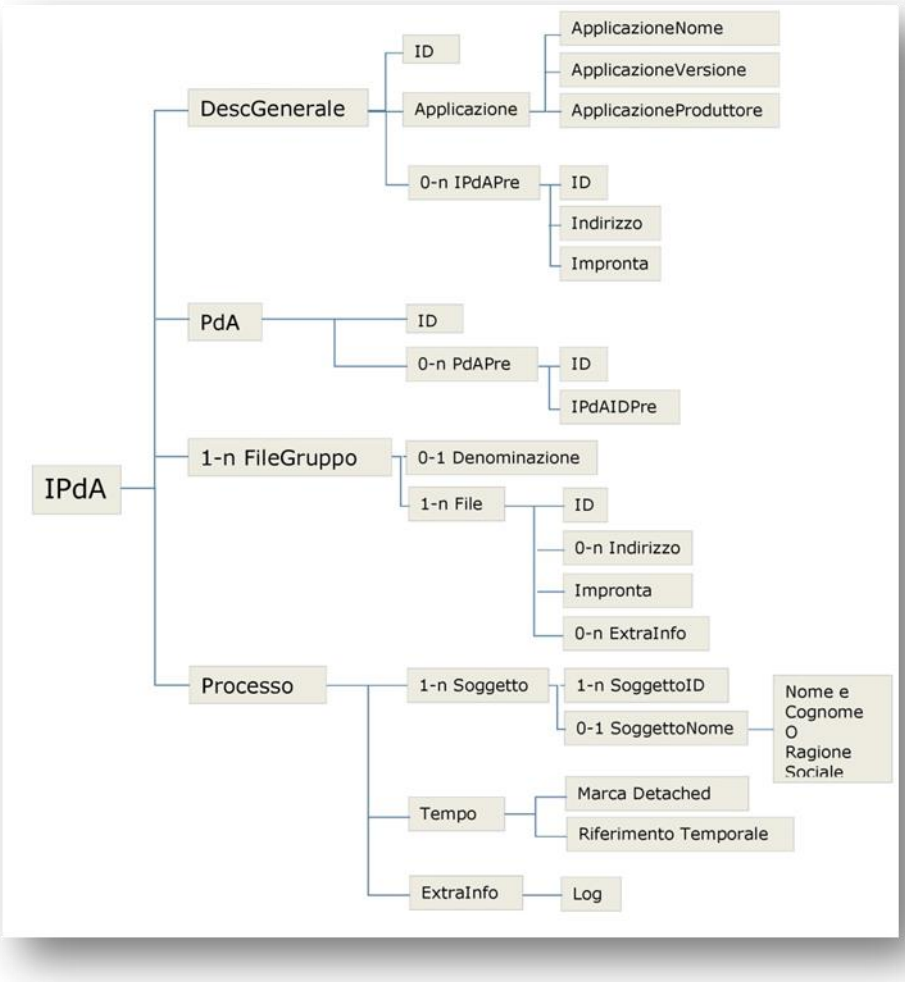

Figura 8: Struttura dell'IPdA

4.5 Richiesta di esibizione e diritti d'accesso

L'utente è il ruolo svolto da persone o sistemi che interagiscono con il sistema di conservazione al fine di accedere e ricercare le informazioni di interesse.

Il documento conservato deve essere leggibile in qualunque momento presso il sistema di conservazione e disponibile su richiesta anche su supporto ottico e/o analogico.

La richiesta di esibizione può essere inoltrata dal soggetto produttore o dai soggetti autorizzati tramite due modalità:

- i soggetti inviano una PEC allegando alla richiesta di consultazione l'elenco dei documenti/aggregazioni informatiche di cui richiedono l'esibizione. Il conservatore individua tali documenti attraverso l'ID univoco e li predispone per l'esibizione creando il PdD;

- i soggetti effettuano il login con username e password[32] forniti dal conservatore ed effettuano l'accesso alla console web di esibizione di Virgilio; il firewall del sistema riconosce l'indirizzo IP da cui viene effettuata la richiesta di esibizione e la concede solo se l'indirizzo è tra quelli dichiarati dal soggetto produttore negli accordi di servizio. Attraverso la console di esibizione il soggetto produttore procede alla ricerca e alla selezione dei documenti di cui richiede l'esibizione.

Il soggetto produttore stabilisce i livelli di accesso e di consultabilità della propria documentazione affidata al conservatore.

Il responsabile della conservazione del soggetto produttore è l'unico che può richiedere e ricevere i documenti; i livelli di accesso e di riservatezza sono forniti esclusivamente da parte del soggetto produttore. Quest'ultimo comunica tempestivamente eventuali variazioni circa i dati personali del soggetto avente account per l'accesso al sistema di conservazione in modo che il responsabile del trattamento dei dati personali, d'accordo con il responsabile della sicurezza, possa procedere a fornire un nuovo username e password. Il responsabile del servizio di conservazione per ogni soggetto produttore tiene traccia dell'elenco storico delle credenziali di accesso assegnate.

Nel documento "Piano per la sicurezza" di Siav sono definite le politiche di gestione degli accessi, riviste periodicamente, che assicurano la disponibilità delle informazioni al solo personale autorizzato sulle base di specifiche richieste. Dunque il responsabile della sicurezza verifica periodicamente le credenziali di accesso al sistema di conservazione, sulla base della periodicità di consultazione indicata nella richiesta, proprio per accertare che la necessità di accesso sia ancora valida. La documentazione e i log di analisi e verifica sono accessibili al solo personale strettamente autorizzato.

Il reparto Software Development di Siav sta lavorando alla gestione degli attributi di riservatezza a livello di documento informatico. Questa implementazione permetterà di differenziare e ampliare i profili relativi all'esibizione dei documenti conservati, permettendo al soggetto produttore di assegnare un determinato livello di riservatezza ad ogni documento versato nel sistema di conservazione ed eventualmente di modificarlo nel corso del tempo. Sarà possibile pertanto fornire l'esibizione dei documenti non solo a coloro che possiedono i diritti di visualizzazione sull'intero archivio conservato, ma anche ad ulteriori utenti che potranno avere accesso ai documenti afferenti la tipologia di riservatezza consona al livello di accesso loro assegnato dal soggetto produttore.

[32] Le modalità di accesso e le indicazioni degli indirizzi IP da cui è possibile effettuare l'accesso al sistema sono indicati negli accordi di servizio.

4.5.1 Creazione ed esibizione del pacchetto di distribuzione

Al fine di rendere disponibile l'informazione (*dissemination*) e rispettare così l'obbligo di esibizione dei documenti conservati, il sistema deve restituire in qualsiasi momento la documentazione richiesta dall'utente assicurandone l'autenticità rispetto all'originale.

In base agli ID univoci forniti dal soggetto produttore al momento della richiesta, il sistema localizza i documenti conservati nei diversi PdA ed effettua un duplicato.

I duplicati dei documenti informatici richiesti sono inseriti all'interno di un unico PdD che viene firmato digitalmente dal responsabile del servizio di conservazione e salvato nel formato di file immagine .iso; a questo punto il sistema procede ad esibire il PdD all'utente attraverso due modalità:

- se la richiesta è pervenuta tramite console web Virgilio automaticamente restituisce un messaggio di avvenuta presa in carico in cui viene indicato il link del canale FTP o FTPS dal quale il soggetto produttore può procedere a scaricare il file immagine .iso del PdD. Se la richiesta è invece pervenuta via PEC il responsabile del servizio di conservazione, nella PEC di risposta, indica il link da cui il soggetto produttore può scaricare l'.iso del PdD;
- su richiesta dei soggetti il file immagine .iso può essere masterizzato su un supporto ottico DVD ed inviato al responsabile della conservazione del soggetto produttore[33].

La materializzazione dei supporti certificati avviene attraverso la produzione automatica di una loro copia ISO che risiede sul server stesso del sistema di conservazione.

Altre modalità di esibizione sono stabilite, di volta in volta, negli accordi di servizio concordati con il soggetto produttore.

[33] Le modalità di consegna sono descritte nel documento "Piano per la sicurezza".

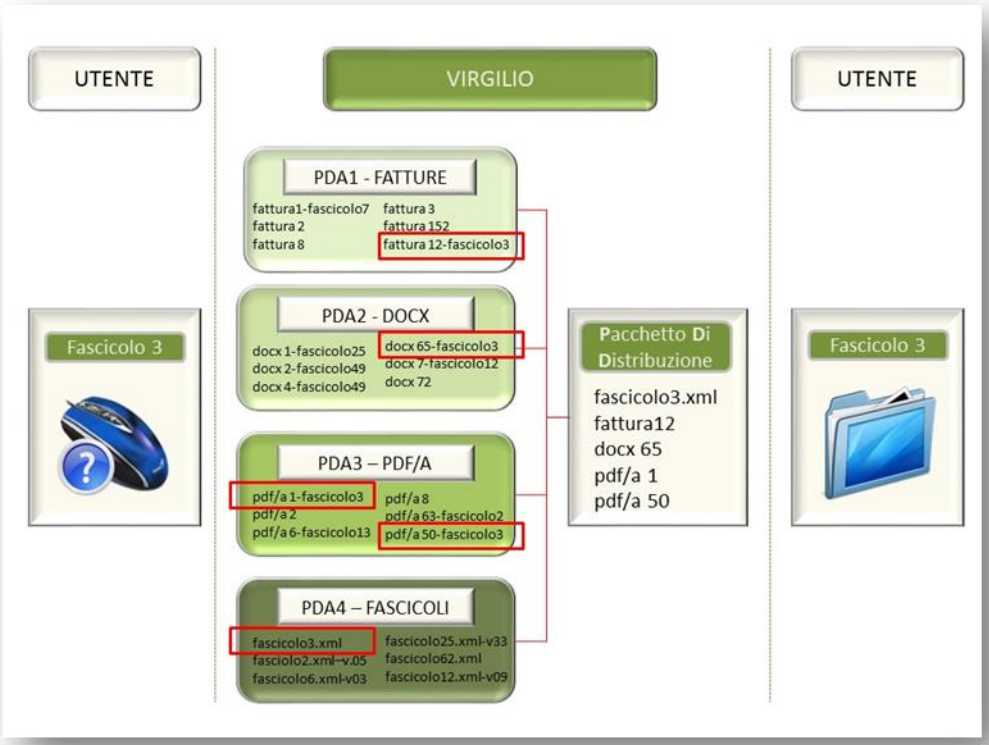

Figura 9: Schema del processo di esibizione

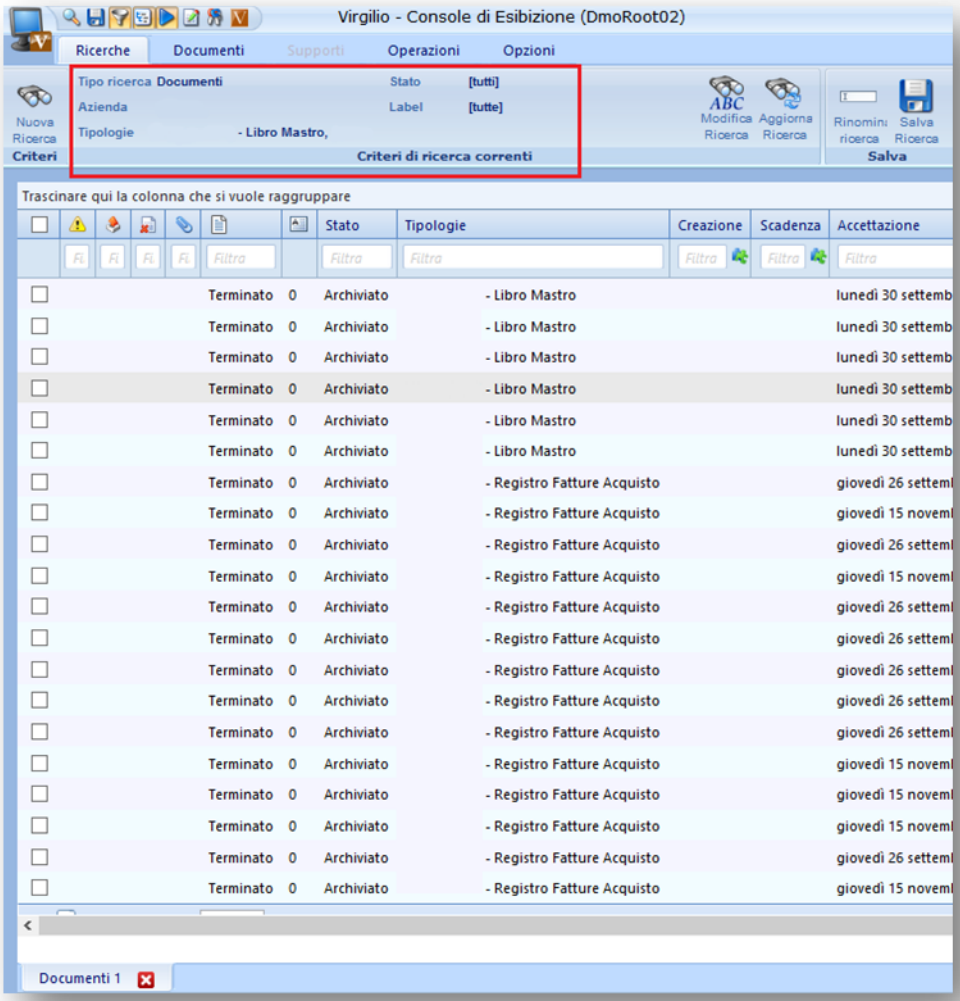

Figura 10: Console di esibizione - Virgilio

Nella figura 10 si riporta uno screenshot relativo alla console di esibizione di Virgilio in cui vengono mostrati i documenti ricercati dall'utente nel sistema di conservazione.

4.6 Struttura dati per gli oggetti digitali e per i metadati

La gestione dei metadati nel sistema di conservazione è definibile per ogni tipologia di oggetto digitale che dovrà essere sottoposta al processo di conservazione. Ogni oggetto digitale (documento e fascicolo) è caratterizzato dal set di metadati minimi obbligatori e da quelli aggiuntivi che vengono concordati con il soggetto produttore[34].
I metadati di ciascuna tipologia sono descritti e definiti attraverso un sistema di configurazione. Nel sistema di conservazione, i metadati di ogni oggetto sono rappresentati attraverso una struttura xml:

```
<metadata>
  <metadata nome="Data documento" tipo="xs:date">2014-08-12T12:00:00</metadata>
  <metadata nome="Numero Protocollo" tipo="xs:string">Registro Ufficiale</metadata>
  <metadata nome="Classe" tipo="xs:string">1</metadata>
  <metadata nome="Sottoclasse" tipo="xs:string">1</metadata>
  <metadata nome="Titolo" tipo="xs:string">VII</metadata>
  <metadata nome="Data Protocollo Mittente" tipo="xs:datetime">2011-10-06T00:00:00Z</metadata>
  <metadata nome="Mittente" tipo="xs:string">Servizio ORG</metadata>
  <metadata nome="Formato" tipo="xs:string">FIRMA DIGITALE (PER POSTEL)</metadata>
  <metadata nome="Tipo Comunicazione" tipo="xs:string">COMUNICAZIONI ESTERNE</metadata>
  <metadata nome="Copie Cartacee" tipo="xs:string">NO</metadata>
  <metadata nome="Procedimento Amministrativo" tipo="xs:string">PROVVEDIMENTO TEST</metadata>
  <metadata nome="Oggetto" tipo="xs:string">Oggetto Test</metadata>
  <metadata nome="Protocollo Mittente" tipo="xs:string">BANCA</metadata>
</metadata>
```

Figura 11: File xml

Il file xml è memorizzato all'interno della base dati per ciascun documento e viene utilizzato per la rappresentazione in fase di esibizione e per comporre l'IPdA nel formato UNI SInCRO per ogni singolo documento.

Nei capitoli 3 e 4 del documento "Specificità del contratto" (allegato al presente manuale) sono descritte sia le strutture dati delle tipologie e delle aggregazioni documentali contenute nei PdV e nei PdA che le strutture dati dei pacchetti e del rapporto di versamento. Si precisa che il contenuto delle strutture dati è variabile in base alla tipologia di documenti e fascicoli gestiti dal soggetto produttore per cui ulteriori dettagli saranno man mano concordati negli accordi di servizio.

Nella figura 12 si può vedere, in un estratto del PdA, come vengono rappresentati i metadati per una specifica tipologia documentale.

[34] Esempi di metadati aggiuntivi sono indicati nel capitolo 2 del documento allegato "Specificità del contratto".

```
<IdC xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" d1p1:version="1.0'
  <d1p1:SelfDescription>
    <d1p1:ID>D6E61E76-E304-4531-9476-E7CB59D00785</d1p1:ID>
    <d1p1:CreatingApplication>
      <d1p1:Name>Siav Virgilio 2012 R2</d1p1:Name>
      <d1p1:Version>4.4.14.12</d1p1:Version>
      <d1p1:Producer>Siav S.p.A.</d1p1:Producer>
    </d1p1:CreatingApplication>
  </d1p1:SelfDescription>
  <d1p1:VdC>
    <d1p1:ID>Document Type ID</d1p1:ID>
    <d1p1:VdCGroup>
      <d1p1:Label>Registro Ufficiale</d1p1:Label>
      <d1p1:ID>ID PdA</d1p1:ID>
      <d1p1:Description>Registro Ufficiale</d1p1:Description>
    </d1p1:VdCGroup>
    <d1p1:MoreInfo d1p1:XMLScheme="file:///VGLMediaMetadataScheme.xsd">
      <d1p1:EmbeddedMetadata>
        <mediainfo xmlns="">
          <company>Company</company>
          <documentspath>17164FEE-0D3F-4749-B999-9CD321379178.xml</documentspath>
          <media>Company Registro Ufficiale 3</media>
        </mediainfo>
      </d1p1:EmbeddedMetadata>
    </d1p1:MoreInfo>
  </d1p1:VdC>
  <d1p1:FileGroup>
    <d1p1:File d1p1:extension=".pdf" d1p1:format="application/octet-stream">
      <d1p1:ID>document id</d1p1:ID>
      <d1p1:Hash d1p1:function="Sha256">4e712d200cb7910bf074eed65af4fd949bdcaff413ba9f93e7e3a20d25ce435f</d1p1:Hash>
      <d1p1:MoreInfo d1p1:XMLScheme="file:///VGLDocumentMetadataScheme.xsd">
        <d1p1:EmbeddedMetadata>
          <document documentpath="document.pdf" >
            <metadata>
              <metadata nome="ID" tipo="xs:string">document id</metadata>
              <metadata nome="Numero Protocollo" tipo="xs:string">Registro Ufficiale</metadata>
              <metadata nome="Classe" tipo="xs:string">1</metadata>
              <metadata nome="Sottoclasse" tipo="xs:string">1</metadata>
              <metadata nome="Titolo" tipo="xs:string">VII</metadata>
              <metadata nome="Data Protocollo Mittente" tipo="xs:datetime">2011-10-06T00:00:00Z</metadata>
              <metadata nome="Mittente" tipo="xs:string">Servizio ORG</metadata>
              <metadata nome="Formato" tipo="xs:string">FIRMA DIGITALE (PER POSTEL)</metadata>
              <metadata nome="Tipo Comunicazione" tipo="xs:string">COMUNICAZIONI ESTERNE</metadata>
              <metadata nome="Copie Cartacee" tipo="xs:string">NO</metadata>
              <metadata nome="Procedimento Amministrativo" tipo="xs:string">PROVVEDIMENTO TEST</metadata>
              <metadata nome="Oggetto" tipo="xs:string">Oggetto Test</metadata>
              <metadata nome="Protocollo Mittente" tipo="xs:string">BANCA</metadata>
            </metadata>
          </document>
```

Figura 12: Esempio di rappresentazione dei metadati della tipologia documentale "Registro ufficiale"

Ogni documento digitale viene mantenuto nel sistema di conservazione in un repository dedicato. Le modalità di gestione di questo repository sono definite negli accordi di servizio. Il repository è poi indicizzato all'interno della base dati mantenendo tutte le informazioni necessarie per raggiungere l'oggetto in questione oltre all'impronta del documento stesso; questo per poter verificare in ogni momento che quanto registrato nella base dati corrisponda con ciò che è presente nel repository. L'archiviazione nel repository del documento digitale avviene in una struttura di cartelle la cui definizione è basata su un algoritmo che prende in considerazione il soggetto produttore e la data e l'ora del versamento. Nel pacchetto di distribuzione la struttura di memorizzazione su file system dei documenti digitali è differente rispetto a quella del repository, comunque attraverso la lettura dell'IPdA UNI SInCRO è possibile reperire le informazioni per visualizzare l'oggetto digitale interessato. Utilizzando il visualizzatore fornito con il PdD l'associazione tra documento e oggetto digitale è effettuata in modo trasparente dall'applicazione; è infatti possibile ricercare uno specifico documento attraverso i suoi metadati e ciò permette di individuarlo e visualizzarlo in maniera univoca. Nel caso non si utilizzasse il

visualizzatore fornito con il PdD, gli oggetti digitali saranno raggiungibili consultando direttamente l'IPdA ed il file, specificato nella sezione "documentspath" inserita in "mediainfo". L'accesso agli oggetti digitali avverrà utilizzando come chiave di accesso l'indice del documento, specificato per ogni file, e la posizione nel repository del PdD, posizione che sarà estratta dal file indicato in "*documentspath*".

```
<pathdocumenti>
  <document ID="id documento 1" FileName="1.pdf.p7m" FilePath=".\.\DATABASE\IMAGE\0" />
  <document ID="id documento 1" FileName="2.pdf.p7m" FilePath=".\.\DATABASE\IMAGE\0" />
<pathdocumenti>
```

5. IL PROCESSO DI SELEZIONE E SCARTO

Il processo di selezione e scarto include gli interventi finalizzati da una parte alla selezione e conservazione della documentazione avente valore giuridicamente e storicamente rilevante e dall'altra alla distruzione di parte della documentazione giudicata irrilevante.

Tale eliminazione è necessaria per ottenere una ordinata tenuta dell'archivio e per evitare l'accumulo di masse ingenti di documentazione che ha esaurito la propria validità giuridica e/o amministrativa e che può essere scartata.

Ogni soggetto pubblico deve dotarsi del piano di conservazione, definito anche massimario di selezione e scarto[35]. Tale strumento, in stretta relazione con il sistema di classificazione, indica per quanto tempo devono essere conservati i documenti e i fascicoli prodotti dall'ente[36].

Il piano di conservazione viene approvato dalla Soprintendenza archivistica competente territorialmente, le PA infatti per ogni intervento di scarto sono obbligate a richiedere l'autorizzazione alla Soprintendenza archivistica competente territorialmente trasmettendo l'elenco di scarto che riporta la tipologia dei documenti proposti per lo scarto, la quantità, la classificazione, gli estremi cronologici, la motivazione, il peso, i metri lineari e la firma del responsabile della gestione documentale.

Solo dopo aver ottenuto l'autorizzazione della Soprintendenza archivistica, il soggetto produttore può procedere allo scarto consegnando la documentazione da eliminare alla Croce rossa italiana o ad altra organizzazione no-profit di volontariato. Quest'ultima è obbligata a comunicare l'avvenuta distruzione della documentazione alla Soprintendenza e al soggetto produttore.

Ai sensi del Codice, al pari di un archivio cartaceo anche l'archivio digitale conservato in Virgilio deve essere sottoposto ad uno o più interventi di scarto; il procedimento parte dalla richiesta formale di scarto trasmessa con PEC dal soggetto produttore al responsabile del servizio di conservazione. La richiesta, firmata digitalmente dal responsabile della conservazione del soggetto produttore e marcata temporalmente, include un allegato che riporta l'elenco degli ID univoci dei documenti e/o dei fascicoli da scartare.

Il responsabile della funzione archivistica prende in carico la richiesta di scarto, verifica che ci siano le autorizzazioni delle Autorità preposte e gli elenchi di scarto completi in tutte le parti. Nel caso venissero rilevate delle anomalie il responsabile del servizio di conservazione notifica il problema inviando una PEC al soggetto produttore richiedendo la correzione dei problemi rilevati e l'invio di un nuova richiesta di scarto; in caso di esito positivo delle verifiche il soggetto produttore avvia il processo di scarto tramite la console web Virgilio localizzando i documenti in base agli ID univoci.

Nel caso in cui il processo di scarto coinvolga tutti i documenti contenuti in un unico PdA il sistema provvede a cancellare fisicamente l'intero PdA

[35] Art. 68 del Testo Unico.

[36] Alcuni esempi di massimari di scarto per archivi comunali, archivi scolastici e archivi sanitari sono disponibili sul sito della Direzione generale degli archivi, servizio II Tutela e conservazione.

dall'archivio[37]. In questa eventualità nel rapporto di scarto viene riportato anche l'ID del PdA oltre a quello dei documenti ivi contenuti.

Virgilio applica un filtro che impedisce la visualizzazione e la modifica dei documenti scartati e crea il rapporto di scarto in cui vengono riportati gli ID univoci dei documenti sottoposti alla procedura di scarto e le informazioni utili a richiamare i log di sistema relativi all'intero processo[38].

Il rapporto di scarto viene trasmesso con PEC; il responsabile del servizio di conservazione d'accordo con il responsabile della funzione archivistica mantiene traccia delle operazioni di scarto conservando le ricevute della PEC e i rapporti di scarto per ogni soggetto produttore; tali rapporti costituiscono una specifica tipologia documentale e pertanto sono sottoposti al processo di conservazione.

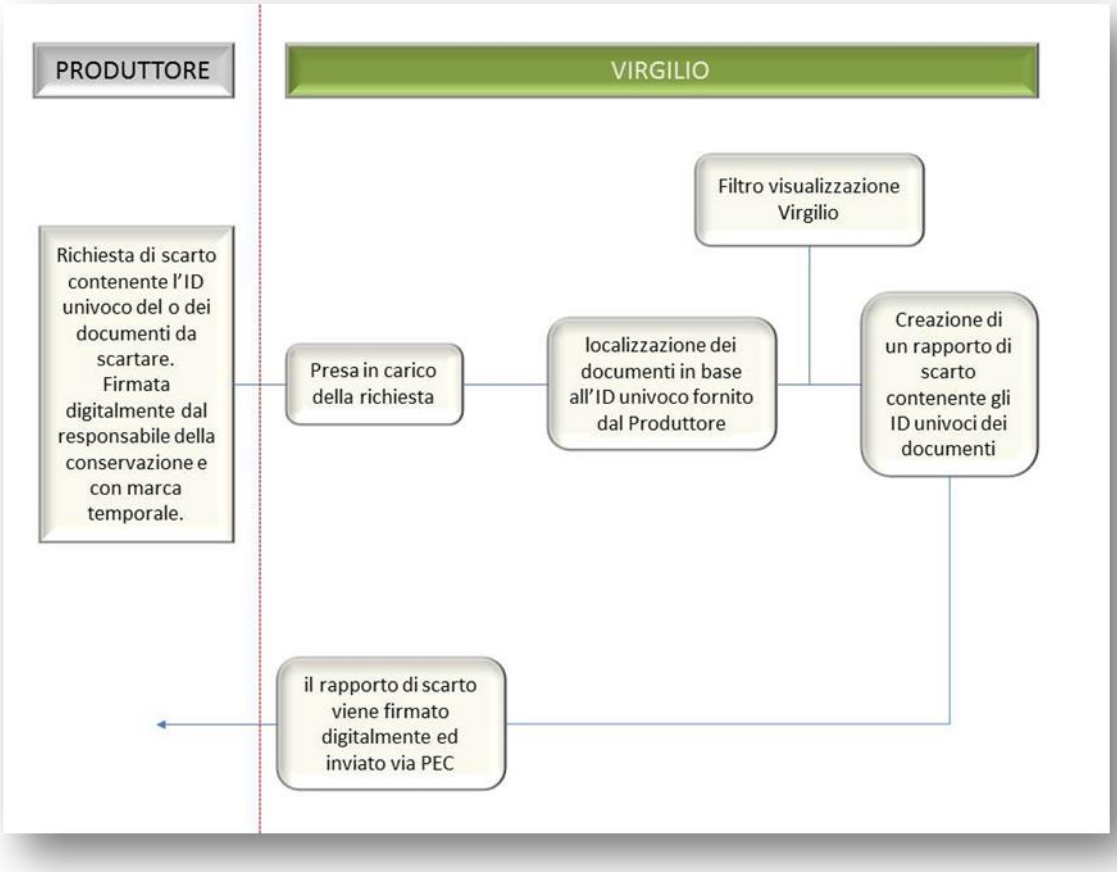

Figura 13: Schema del processo di scarto

[37] Si ha uno scarto progressivo del PdA nel momento in cui il soggetto produttore effettua le operazioni di scarto sulla base delle tempistiche indicate nel piano di conservazione adottato.

[38] I log di sistema sono salvati e conservati nel database Oracle.

6. SICUREZZA LOGICA E FISICA DEI DOCUMENTI CONSERVATI

6.1 Controlli sulla leggibilità

Conservare un contenuto informativo digitale significa mantenere nel tempo la capacità di riprodurlo con il contenuto e la forma originaria. In altre parole, significa mantenere, attraverso il sistema di conservazione, la capacità di leggere la relativa sequenza binaria nella sua interezza, di interpretarla con le regole del formato elettronico, di visualizzare, a video, a stampa o su un altro dispositivo di output, il documento risultante.

Per mantenere nel lungo periodo l'autenticità, l'integrità e la leggibilità di tutti i documenti conservati nel sistema, il responsabile del servizio di conservazione ha predisposto e attua un piano della sicurezza[39] volto ad individuare e correggere tempestivamente eventuali processi di corruzione dei documenti e dei supporti.

Il responsabile del servizio di conservazione, d'intesa con gli altri responsabili, pianifica la tempistica e le attività inerenti i controlli per la verifica dei documenti conservati. Alcune verifiche vengono effettuate automaticamente dal sistema che seleziona un campione casuale di documenti sull'intero archivio di ogni soggetto produttore, calcola l'impronta di ogni documento e la confronta con quella rilevata al momento dell'acquisizione del documento stesso da parte del sistema di conservazione e memorizzata tra i metadati del documento. Se l'impronta risulta valida significa che la stringa di bit che forma il documento informatico è rimasta invariata, e non sono occorse nel tempo delle corruzioni, volontarie o involontarie, che possano aver cambiato la forma e/o il contenuto del documento. Attraverso il confronto delle impronte è possibile verificare, oltre all'integrità, anche l'autenticità del documento. Infatti la modifica o la rimozione delle firme digitali e delle marche/riferimenti temporali apposte al documento andrebbe a modificare la stringa di byte che lo compone causando la generazione di un'impronta differente.

La leggibilità dei documenti conservati è assicurata da una parte attraverso il confronto dell'impronta, in quanto la corruzione della stringa di bit che compone il documento provocherebbe la visualizzazione a schermo in maniera distorta[40]. In parte, invece, dipende dalla possibilità di reperire strumenti software e hardware in grado di riprodurre a schermo il formato in cui il documento è salvato.

Si parla in questo caso di obsolescenza tecnologica, un processo causato dalla velocità del progresso tecnologico che, a seguito dell'introduzione sul mercato di tecnologie sempre più avanzate, causa il disuso di formati e supporti. Il responsabile del servizio di conservazione si tiene aggiornato sullo stato dei formati e dei supporti utilizzati all'interno del sistema di conservazione e, nel

[39] Si rimanda al documento "Piano per la sicurezza".

[40] Il grado di perdita di leggibilità dipende dal livello di corruzione intervenuto e dalla solidità del formato in cui il documento è salvato.

caso venisse prospettato un caso di obsolescenza tecnologica, attua tempestivamente il piano di riversamento.

6.2 Produzione di copie e duplicati

Il responsabile del servizio di conservazione impartisce istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. Inoltre gestisce periodicamente le procedure per la produzione di copie e duplicati dei PdA e PdD.

Le copie informatiche dei documenti contenuti in un PdA sono identiche a ai documenti originari; le operazioni per la realizzazione delle copie sono coordinate dal responsabile del servizio di conservazione d'intesa con il responsabile della funzione archivistica e descritte negli accordi di servizio.

La copia conforme al documento informatico originale viene prodotta su richiesta del soggetto produttore e nei casi in cui Siav debba esibire un documento per costituirsi in giudizio; il Pubblico ufficiale, con una dichiarazione formale, attesta la conformità della copia prodotta all'originale.

Il duplicato informatico è il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della stessa sequenza di valori binari del documento originario. Siav produce i duplicati informatici per la formazione dei PdD.

Le copie di sicurezza dei PdA vengono prodotte nel momento in cui il PdA viene generato e sono memorizzate automaticamente sui server.

Solitamente sono generate quattro copie di sicurezza: due vengono consegnate al soggetto produttore, la terza è memorizzata in Virgilio e la quarta è salvata su un disco esterno nel formato di file immagine .iso.

È possibile, su richiesta del soggetto produttore o in situazioni particolari, generare le copie anche su supporti fisici come CD e DVD; ogni copia ISO è corredata di un numero progressivo del PdA e dalla tipologia di documenti che contiene.

Le etichette (label) poste sul singolo DVD contengono:

- identificativo/nome/ragione sociale del soggetto produttore;
- data di masterizzazione e numero della copia;
- informazioni sul PdA conservato (indicazioni sugli oggetti e sulla tipologia di documenti/fascicoli archiviati nel supporto);
- la data di prima certificazione della copia ISO che contiene;
- gli estremi cronologici di ogni copia ISO ivi contenuta.

6.3 Verifiche, riversamento e monitoraggio

Il responsabile del servizio di conservazione effettua continue verifiche circa l'integrità e la leggibilità dei dati, la robustezza dei supporti e in caso di obsolescenza degli stessi può procedere alla generazione di copie e al riversamento.

Il riversamento è il processo attraverso il quale si riproducono i documenti affidati a dispositivi di memorizzazione digitali. Le tipologie di riversamento sono due: diretto e sostitutivo e si differenziano per il tipo di risultato che producono.

Nel corso di un periodo di conservazione dei documenti, può ritenersi necessario trasferire il contenuto di un supporto di memorizzazione a un altro. Tale esigenza può presentarsi, ad esempio, nel caso in cui sia necessario creare copie di backup o in caso di obsolescenza tecnologica dei supporti.

L'operazione deve essere effettuata dal responsabile del servizio di conservazione, o da un suo delegato, e assume il nome tecnico di "processo di riversamento diretto".

Anche se il riversamento diretto non prevede particolari iter formali da seguire, la norma prescrive che le informazioni riportate sul nuovo supporto non devono subire alcuna modifica. Per certificare che questo accada, il sistema calcola automaticamente un'impronta dei documenti registrati sul supporto prima del trasferimento e la confronta con l'impronta calcolata dopo il riversamento diretto.

Periodicamente viene garantita la conformità degli archivi digitali conservati attraverso i seguenti interventi:

- controlli di processo, per lo più automatizzati dal sistema, sulle fasi operative del processo di conservazione e sulla gestione delle anomalie[41];
- controlli periodici pianificati preventivamente dai responsabili della conservazione e dei sistemi informativi;
- controlli e manutenzione delle strutture hardware e software.

Il responsabile della sicurezza e dei sistemi informativi effettua e monitora le procedure di backup[42]; inoltre d'intesa con il responsabile del servizio di conservazione coordina anche le attività previste per il piano di gestione di continuità operativa[43] e del risk assessment[44].

Il sistema effettua diverse forme di monitoraggio:

- tracciamento e monitoraggio di tutte le attività del processo di conservazione e di gestione dei supporti, notificando gli esiti delle diverse attività svolte, così come eventuali problemi, anomalie e criticità;

[41] Per un approfondimento si rimanda al documento allegato "Specificità del contratto".

[42] Indicata nel documento "Piano per la sicurezza".

[43] Indicato nel documento "Piano per la sicurezza".

[44] Indicata nel documento "Piano per la sicurezza".

- per ogni documento conservato viene verificato lo stato, la leggibilità, l'integrità, il valore legale e il livello di obsolescenza del formato;
- rinnovo automatico del periodo di validità dei certificati e delle marche temporali dei documenti (mediante accesso alla CA e alla TSA utilizzate), tracciando e segnalando gli esiti;
- tutti gli esiti delle operazioni svolte, incluse le anomalie e le situazioni critiche o potenzialmente rischiose evidenziate dal sistema di conservazione sono visualizzabili sui report disponibili online attraverso la console di gestione. Sono inoltre inviate via e-mail all'amministratore (il responsabile dei sistemi informativi) e al responsabile del servizio di conservazione le notifiche di errori o anomalie riscontrati durante lo svolgimento delle varie fasi del processo[45].

[45] Per il dettaglio sulle procedure inerenti il monitoraggio delle funzionalità del sistema di conservazione, delle verifiche effettuate sugli archivi conservati e sulla modalità di comunicazione dell'anomalia si rimanda al capitolo 8 del documento allegato "Specificità del contratto".

7. LE COMPONENTI DEL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione Virgilio è basato su un'architettura modulare service-based pensata per soddisfare la gestione delle procedure di conservazione a norma degli archivi digitali.

Virgilio può gestire archivi di più soggetti produttori, applicando ad essi regole gestionali diverse. Per ogni azienda possono, infatti, essere definiti ambiti di gestione diversi (ad esempio l'ambito dei documenti fiscali); per ogni ambito sono definite varie tipologie documentali con gli attributi appropriati[46].

L'architettura del sistema di conservazione Virgilio può essere suddivisa in tre livelli (three-tier architecture - figura 14), dedicati rispettivamente all'interfaccia utente (Presentation layer), alla logica funzionale (System Services) e alla gestione dei dati e dei documenti (Repository).

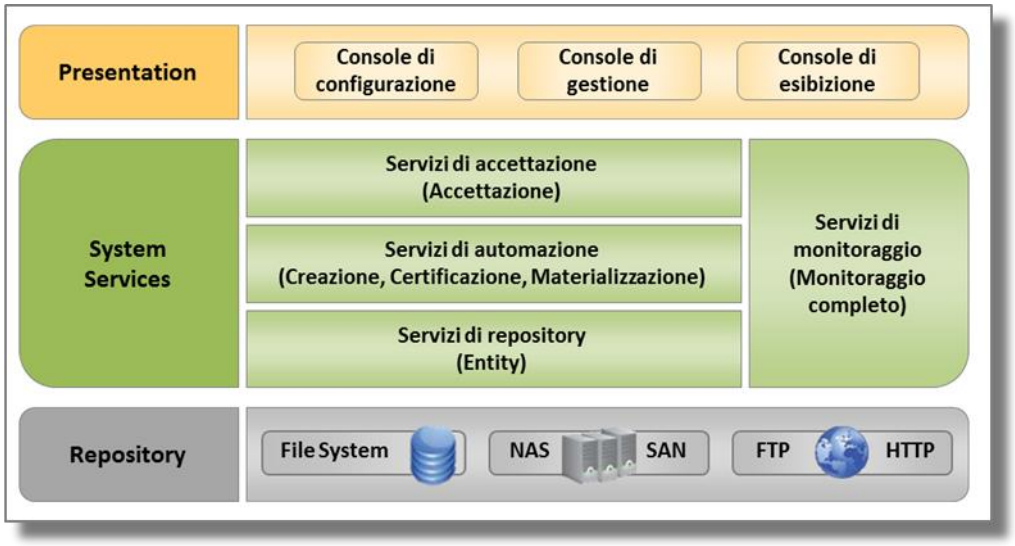

Figura 14: Architettura three-tier

Lo strato di Presentation è costituito dalle interfacce di gestione e di utilizzo del sistema (console) accessibili solo da parte degli utenti autorizzati via client Windows e/o via web (ad esempio per esibire un documento a prescindere dal luogo fisico di conservazione). In particolare, Virgilio supporta diverse interfacce che permettono ai responsabili e agli utenti abilitati di amministrare e monitorare opportunamente il processo di conservazione:

- la console di configurazione (disponibile solo sul client Windows), utilizzata dai responsabili del sistema per accedere a tutte le funzionalità di amministrazione;
- la console di esibizione (disponibile via web), per la ricerca e la visualizzazione, la verifica di validità e di integrità e la materializzazione dei

[46] Per il dettaglio sulle tipologie di oggetti digitali conservati si rimanda al capitolo 2 del documento allegato "Specificità del contratto".

documenti e dei supporti presenti nell'archivio di conservazione e, più in generale, per effettuare le verifiche sul processo di conservazione a norma;

- la console di gestione (disponibile via web), specificatamente predisposta per il responsabile del servizio di conservazione, che, oltre a includere tutte le funzionalità disponibili nella console di esibizione, permette sia di gestire i supporti logici di conservazione (creazione, certificazione, materializzazione) sia di monitorare lo stato di avanzamento del processo di conservazione e lo stato fisico e logico di tutto l'archivio.

Lo strato System Services è costituito da un insieme di servizi che supportano il sistema nello svolgimento di tutte le fasi del processo di conservazione, presidiando controlli e automatizzando alcune attività, così come nel monitoraggio dello stato dei documenti e dei supporti utilizzati. In generale opera su tre diverse console:

- console di Accettazione e Consolidamento (disponibile anche nella versione WEB), permette la firma digitale, dove richiesta, sui documenti da importare in Virgilio;
- console di import supporti, permette di caricare supporti di conservazione generati con sistemi diversi da Virgilio e di inserirli nel ciclo di controllo del sistema;
- console correzione di anomalie e supporti: permette di gestire le eventuali anomalie nel processo di conservazione.

Lo strato di Repository infine, sotto il controllo del servizio Entity, gestisce la consistenza dell'archivio del sistema di conservazione a norma, sfruttando le risorse storage a disposizione (File System, NAS, SAN ed eventuali sistemi remoti accessibili via FTP e HTTP).

Virgilio si propone come sistema dedicato alla conservazione che può operare in modalità stand-alone o connesso ad un sistema di gestione documentale (ad esempio Archiflow). In entrambi i casi è Virgilio che si occupa di verificare che le operazioni necessarie alla conservazione siano eseguite e che nel tempo sia verificata la validità dei documenti. La differenza che esiste fra un sistema stand-alone ed un sistema interconnesso è che lo storage dei documenti conservati sarà Virgilio piuttosto che il sistema GED utilizzato.

Le modalità di comunicazione con il sistema di gestione documentale dovranno naturalmente essere valutate, verificate ed eventualmente realizzate volta per volta.

La conservazione degli oggetti digitali nel sistema Virgilio è riassumibile nelle seguenti fasi di processo:

- definizione delle regole di conservazione che il documento deve osservare (generalmente dipendono dalla tipologia documentale a cui è associato);
- verifica delle regole di conservazione ed esecuzione delle eventuali operazioni necessarie (firma, marca) in base alla tipologia documentale di appartenenza del documento;
- acquisizione (intesa come inserimento) del documento nel sistema Virgilio;
- verifica delle scadenze e dell'integrità dei documenti;

- archiviazione del documento in un supporto (creazione del supporto virtuale);
- certificazione del supporto virtuale in base al modello associato alla tipologia documentale;
- creazione delle copie del supporto virtuale (copie automatiche di backup);
- verifica delle scadenze e dell'integrità dei supporti e del loro contenuto.

L'intero processo di conservazione è quindi basato sulla tipologia documentale: ad essa, infatti, si collegano tutti i modelli necessari nell'esecuzione delle operazioni sia automatizzate che manuali.

7.1 Funzionalità del sistema

I servizi Windows servono per effettuare le operazioni di conservazione (creazione supporti, ecc.) e per le normali attività di Virgilio (monitoraggio, ecc.). I servizi sono gestiti attraverso la console di configurazione del sistema e sono:

1. Accettazione — Servizio usato per inserire nuovi documenti in Virgilio: come sistemi di input può utilizzare dei file di testo (stile CSV con separatore o a lunghezza fissa) e può interfacciarsi direttamente a Svaol.
2. Creazione supporti — Servizio per la creazione dei supporti in base ai modelli definiti.
3. Certificazione — Servizio per la certificazione automatica di firma e marca.
4. Materializzazione — Creazione delle copie fisiche dei supporti virtuali in base alle regole impostate.
5. Monitoraggio — Servizio di monitoraggio dell'archivio digitale: viene pianificato periodicamente dal responsabile del servizio di conservazione d'accordo con il responsabile dei sistemi informativi e prevede la verifica della consistenza e coerenza dei documenti e degli indici di conservazione.
6. Operazioni generiche — Servizio per la gestione delle operazioni generiche quali ad esempio la cancellazione, le richieste effettuate dal web, ecc.
7. WCF per il Web — Servizi WCF per il web e viene definito una volta sola per tutto l'impianto.
8. WCF di amministrazione — I servizi WCF di amministrazione mettono a disposizione una serie di funzionalità per la creazione di Aziende, tipi documenti, ecc.; può essere definito una volta sola per tutto l'impianto.
9. WCF per i Gadget — Espone i servizi per l'utilizzo dei Gadget di Virgilio; può essere definito una volta sola per tutto l'impianto.

10. Agenzia delle Entrate	Servizio per gestire le operazioni di invio delle impronte; può essere definito una volta sola per tutto l'impianto.
11. FTP HHTP	Non è un servizio Windows; serve a Virgilio per identificare la modalità di trasporto delle copie ISO sul server web e utilizza il protocollo HTTP.
12. FTP Standard	Non è un servizio Windows; serve a Virgilio per identificare la modalità di trasporto delle copie ISO sul server web e utilizza il protocollo FTP.
13. Entity Server	Questo servizio è utilizzato per gestire i volumi in modalità FTP.
14. Gestione Volumi	Questo servizio gestisce la storicizzazione dei volumi correnti delle immagini.

Alcuni di questi servizi, in un ambiente che utilizza più server, possono essere definiti più volte in modo da parallelizzare le operazioni su entità differenti.

Le funzionalità che caratterizzano il sistema Virgilio e rese disponibili, sono di seguito sintetizzate:

- verifica dei documenti in termini di leggibilità, integrità, ecc.[47];
- gestione dei supporti di documenti (supporti logici di conservazione);
- certificazione dei supporti;
- materializzazione dei supporti certificati;
- ricerca ed esibizione dei documenti;
- monitoraggio sullo stato logico e fisico del sistema;
- amministrazione e configurazione del sistema.

È importante sottolineare che il sistema Virgilio permette di attivare anche manualmente tutte queste funzionalità ma che per l'impostazione del processo di conservazione progettato da Siav la maggior parte di queste vengono attivate automaticamente.

[47] Sistemi automatizzati di allerta permettono la periodicità di tali verifiche.

7.2 Service - Orientation e integrabilità

Nell'architettura di Virgilio, i servizi caratterizzanti sono interoperabili secondo una definizione formale indipendente dalla piattaforma e dalle tecnologie di sviluppo (come Java, .NET, ecc.) dato che viene applicata una logica comunemente conosciuta come Service-Oriented Architecture (SOA). Ciò significa che ogni servizio può essere richiamato per eseguire i propri compiti senza avere conoscenza dell'applicazione chiamante e senza che l'applicazione, a sua volta, abbia conoscenza del servizio che effettivamente esegue l'operazione.

Il SOA funziona attraverso l'uso di una componente di orchestrazione, secondo il modello dell'Enterprise Service Bus, che opera nel rispetto dei principi di cooperazione applicativa basati sullo standard xml.

L'implicazione principale di un tale approccio, grazie anche alla possibilità di modificare in maniera semplice le modalità di interazione tra i servizi e in generale la loro combinazione (per soddisfare le esigenze dei processi che implementano), è che la logica di business è svincolata dalla tecnologia utilizzata, per cui è possibile realizzare la separazione tra "cosa un'applicazione fa" da "come lo fa".

Un ulteriore vantaggio di un'architettura a servizi è l'integrazione immediata con altri applicativi via web services; in sintesi altri applicativi, indipendentemente dal linguaggio di programmazione in cui sono stati scritti e dalla piattaforma su cui sono implementati, possono utilizzare i servizi messi a disposizione attraverso l'invio via HTTP di messaggi in formato xml.

L'organizzazione in servizi, interagenti tra loro e attivabili in funzione delle esigenze, permette di massimizzare anche la modularità e l'estensibilità della soluzione, ottimizzando da una parte il carico di lavoro e soddisfacendo dall'altra tutte le esigenze di amministrazione delle attività di conservazione a norma degli archivi digitali.

In particolare in Virgilio sono attivi i seguenti moduli:

- accettazione
- creazione
- certificazione
- materializzazione
- monitoraggio completo
- entity

Si riporta la descrizione dettagliata degli stessi:

- il modulo di accettazione gestisce l'importazione dei documenti versati, normalizzando i documenti in ingresso con la creazione e la gestione di metadati associati e procedendo alle verifiche formali sui documenti e, nel caso siano firmati digitalmente, alle verifiche sulla validità della firma;

- il modulo di creazione dei supporti gestisce la trasformazione del PdV in PdA conservazione, supportando la creazione di supporti differenti in funzione della tipologia di documenti che dovranno contenere e inserendo i documenti accettati dal sistema nei supporti di riferimento;
- il modulo di certificazione gestisce l'attività di chiusura del PdA dei supporti, avvisando il responsabile del servizio di conservazione della presenza di nuovi supporti logici da certificare, permettendo a quest'ultimo di monitorare il processo e di firmare digitalmente i supporti, e, se opportunamente configurato, di procedere automaticamente all'apposizione del riferimento o della marca temporale;
- il modulo di materializzazione gestisce l'attività di materializzazione dei supporti virtuali in modalità istantanea o schedulata e, interfacciandosi con i più comuni masterizzatori, di procedere in modalità semi-automatica alla creazione delle copie su supporti ottici di varia natura (CD/DVD, periferiche di archiviazione usb, hardware specialistico per la masterizzazione massiva di CD/DVD, ecc.) e permette la creazione di PdD;
- il modulo di monitoraggio completo controlla gli stati di ogni singolo servizio, catturandone gli eventi e gestendone tutte le eccezioni, verifica l'integrità e la fruibilità dei documenti e dei supporti, notificando al responsabile del servizio di conservazione l'esistenza di supporti logici scaduti e gestendo completamente in automatico l'eventuale loro rinnovo;
- il modulo di entity serve invece per la gestione dei dati e dei volumi e in particolare dei flussi di informazioni che da Virgilio spostano o copiano i supporti (e quindi i documenti ivi contenuti) verso gli storage (file system, FTP/HTTP Server, SAN, NAS, ecc.).

7.3 Scalabilità e affidabilità

L'architettura di Virgilio è stata progettata per gestire in modo ottimale le performance dei processi di conservazione e di esibizione applicando un approccio multi-server e tecniche di bilanciamento intelligente del carico di lavoro.

In particolare essa garantisce:

- l'estensibilità della soluzione, grazie alla possibilità di attivare solo i moduli necessari per la specifica implementazione;
- l'alta affidabilità, grazie alla possibilità di distribuire i moduli su server indipendenti e di clusterizzare tutti i suoi componenti;
- la scalabilità, grazie alla possibilità di distribuire i vari moduli su più server al crescere del carico di lavoro e di sfruttare la piena compatibilità con i più diffusi e affidabili sistemi NAS e SAN per la gestione dello storage.

Segue un esempio generico dell'architettura base di Virgilio; si precisa che la soluzione è scalabile in base alle esigenze del soggetto produttore e pertanto viene dettagliata di volta in volta negli accordi di servizio.

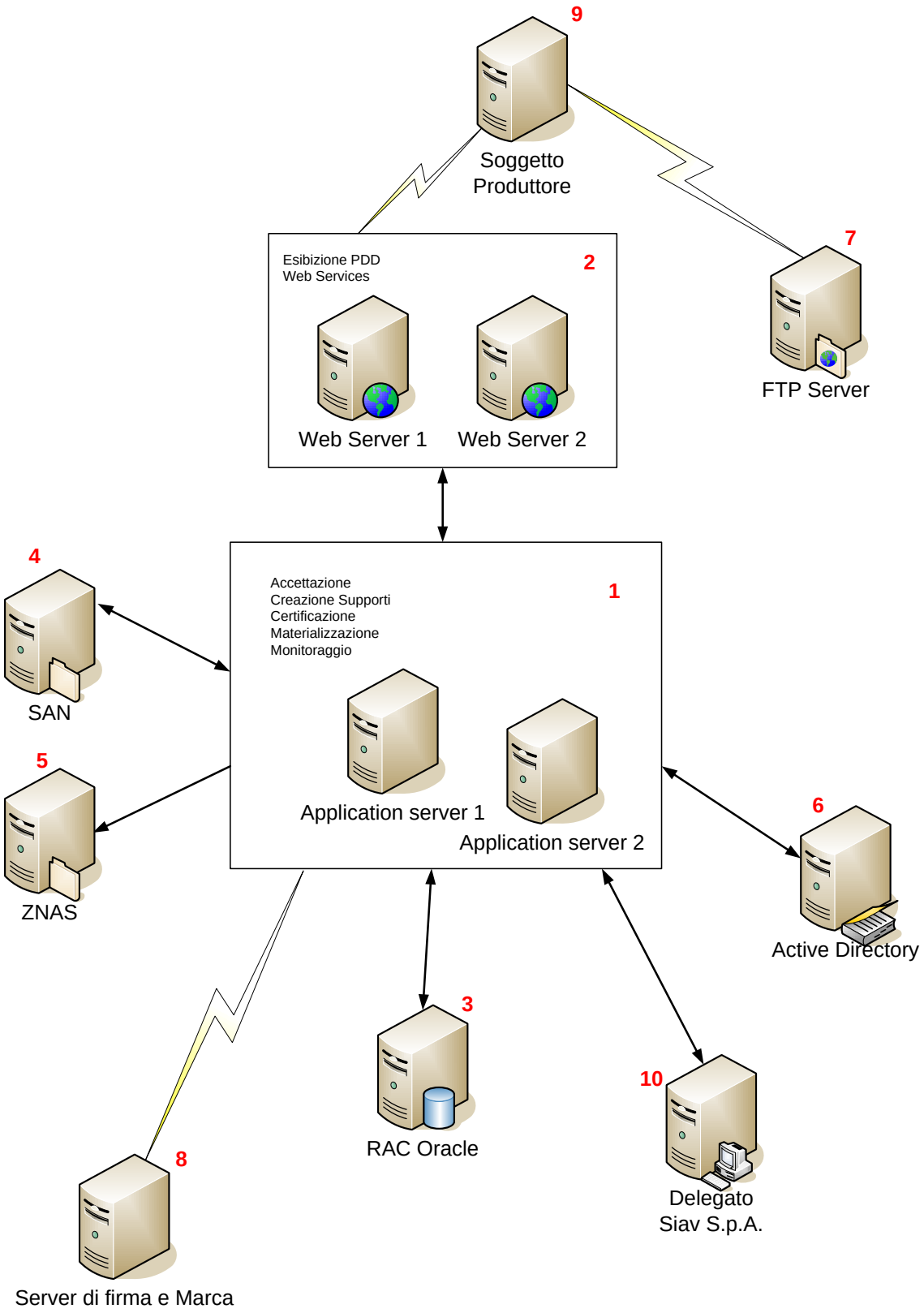

Figura 15: Architettura base di Virgilio

1. i servizi di Virgilio sono installati su due diversi Application Server che lavorano in parallelo;
2. il servizio di esibizione del PdD e i web services, accessibili dal soggetto produttore (9), operano attraverso due web server che lavorano in parallelo;
3. sul cluster Oracle risiedono i metadati, i dati, i log di sistema e le path utili a collegare i metadati ai relativi documenti;
4. area di storage in cui vengono salvati i documenti;
5. area di storage dove risiedono le immagini storicizzate dei documenti;
6. attraverso il protocollo LDAP, l'active directory è utilizzata come base dati per memorizzare in forma centralizzata tutte le informazioni del dominio di rete relativamente all'autenticazione e all'accesso degli utenti;
7. il server FTP permette di accettare le connessioni in entrata e di comunicare con un client attraverso protocollo FTP/FTP-S/SFTP;
8. il sistema si collega ad un server esterno per i controlli di validità delle firme digitali e delle marche temporali. Lo stesso server è utilizzato dal responsabile del servizio di conservazione e dai suoi delegati (10) per apporre la propria firma digitale attraverso un HSM remoto.

7.4 Profilazione degli utenti

Il sistema permette di definire diversi gruppi di utenti al fine di assegnare loro le corrette autorizzazioni di accesso alle funzionalità disponibili. Di base sono previsti almeno cinque profili:

- amministratore del sistema (il responsabile dei sistemi informativi), per lo svolgimento di tutte le funzionalità di amministrazione (disponibili nell'interfaccia "console di configurazione") quali le modalità di impostazione dei servizi e delle funzionalità da attivare, l'impostazione dei volumi fisici atti a contenere i documenti e i supporti, il monitoraggio del processo di conservazione e la configurazione delle tipologie di documenti con i relativi metadati, l'impostazione delle regole di conservazione e la definizione dei profili e degli utenti, ecc.;
- responsabile del servizio di conservazione, attraverso l'interfaccia "console di gestione", effettua il monitoraggio dello stato d'avanzamento del processo di conservazione e dello stato fisico e logico di tutto l'archivio, per la gestione dei lotti e lo svolgimento di tutte le funzionalità di ricerca, visualizzazione, verifica della validità e dell'integrità dei documenti e materializzazione dei lotti;

- utente di consultazione, attraverso l'interfaccia "console di esibizione", richiede la consultazione di documenti e/o fascicoli;
- i delegati dei responsabili della conservazione e dei sistemi informativi;
- gli operatori dei delegati, effettuano gli interventi di competenza dei delegati.

8. INTERAZIONE CON ALTRI SISTEMI

"Un nodo cruciale è infine la capacità di assicurare la trasferibilità delle informazioni tra i sistemi nel tempo e nello spazio, ovvero la capacità di comunicare ed elaborare con efficienza le informazioni digitali anche nel caso di dispositivi e ambienti eterogenei senza che sia necessario riprogrammare o modificare l'esistente. L'interoperabilità ha necessità in primo luogo di elementi e attributi che descrivano con sufficiente dettaglio le fonti informative da trattare al fine di consentirne la leggibilità e l'intelligibilità da parte degli utenti"[48].

Di seguito viene descritto il workflow relativo sia all'esportazione che all'importazione di un archivio informatico.

8.1 Esportazione di un archivio informatico

In caso di interruzione degli accordi del servizio di conservazione con il soggetto produttore, il responsabile del servizio di conservazione procede alla restituzione dell'archivio secondo la seguente modalità operativa:

- ricezione via PEC delle modalità di trasferimento e relative coordinate;
- il responsabile del servizio di conservazione incarica un operatore all'estrazione dell'archivio digitale da restituire secondo le modalità richieste;
- l'operatore del centro servizi accedendo alla console del sistema di conservazione individua l'elenco dei Pacchetti di archiviazione certificati che compongono l'archivio ed esegue una procedura di materializzazione su supporto ottico (DVD) o storage;
- generazione di un report che contiene l'elenco di tutti i PdA con i relativi estremi di certificazione;
- nel caso di restituzione di archivi memorizzati su supporti ottici il servizio avviene attraverso spedizione all'indirizzo specificato via PEC dal soggetto produttore;
- nel caso di trasmissione telematica i PdA sono caricati nell'area FTP riservata; viene inviata una PEC con il report dell'avvenuto deposito nell'area di download.

In alcuni casi, il soggetto produttore può richiedere a Siav una relazione archivistica inerente l'archivio digitale restituito. Tale relazione, redatta dal responsabile della funzione archivistica di conservazione, contiene il dettaglio di tutte le informazioni utili per la comprensione e gestione dell'archivio: indicazione delle informazioni PDI presenti nel PdV e nel PdA, della struttura delle serie archivistiche, degli estremi cronologici, dei soggetti intervenuti nel processo di conservazione e degli interventi effettuati.

Il soggetto produttore può richiedere un formato accessorio e procedure specifiche in grado di agevolare il recepimento dell'archivio digitale nel sistema di conservazione di destinazione.

[48] Cfr. M. Guercio, *Conservare il digitale. Principi, metodi e procedure per la conservazione a lungo termine di documenti digitali,* cit., p. 92.

Tali ed ulteriori eccezioni sono concordate di volta in volta negli accordi di servizio.

8.2 Importazione di un archivio informatico

La richiesta di importazione di un archivio informatico nel sistema di conservazione prevede una serie di controlli effettuati a monte dal responsabile della funzione archivistica quali:

- l'analisi preventiva dell'archivio per la rilevazione delle criticità;
- la redazione di un'analisi tecnica dettagliata sulle modalità di importazione;
- la definizione e configurazione dell'archivio nel sistema di conservazione;
- la verifica della presenza delle informazioni PDI nei PdV e PdA;
- il monitoraggio della procedura di versamento dei PdA nel sistema di conservazione effettuando verifiche sull'integrità fisica e logica dei documenti/fascicoli in essi contenuti;
- l'analisi della consistenza e completezza degli oggetti digitali costituenti l'archivio da importare;
- l'approvazione dell'importazione e la redazione di una relazione di accettazione che descrive il contenuto e le criticità di quanto acquisito.

8.3 Interoperabilità applicativa tra i sistemi

Il sistema di conservazione ed in particolare le sue componenti applicative, mettono a disposizione un insieme di API esposte sotto forma di web services. Tramite questi web services è possibile costruire integrazioni che permettono ad altri sistemi di accedere da remoto all'intero archivio oppure a porzioni di esso.

9. PROCEDURA DI CHANGE MANAGEMENT

Il presente capitolo descrive le modalità attuate da Siav per la gestione dei cambiamenti al sistema informatico a supporto del sistema di conservazione.

Il responsabile del servizio di conservazione autorizza la procedura del change management che solitamente viene gestita dai responsabili del sistema informativo e dello sviluppo e manutenzione del sistema di conservazione.

Il sistema informatico cambia principalmente per due motivi:

- correzione di malfunzionamenti riscontrati;
- evoluzioni/miglioramenti/adeguamenti normativi.

Le principali componenti informatiche oggetto del cambiamento sono:

- sistemi operativi;
- software applicativi a supporto del processo di gestione e conservazione dell'archivio digitale.

L'aggiornamento dei sistemi server side avviene sfruttando l'infrastruttura di virtualizzazione ed il relativo sistema di Business Continuity.
Tutti i sistemi e le componenti sono duplicate su due nodi distribuiti su due macchine fisiche differenti.

9.1 Aggiornamento dei sistemi operativi

Il responsabile dei sistemi informativi per la conservazione, con il proprio team, procede come di seguito:

- aggiornamento del nodo passivo;
- promozione del nodo passivo a nodo attivo;
- esecuzione di uno specifico piano di test;
- nel caso in cui non siano rilevati errori, avviene l'aggiornamento del nodo passivo;
- in caso di problemi il nodo passivo ritorna attivo abortendo di fatto l'aggiornamento e ripristinando la precedente versione;
- redazione di un resoconto e invio al responsabile del servizio di conservazione e al responsabile dello sviluppo e della manutenzione del sistema di conservazione.

9.2 Aggiornamento applicativo

L'aggiornamento applicativo è di tre tipologie:

- manutenzione correttiva
- manutenzione adattiva
- manutenzione evolutiva

La manutenzione del sistema include tutti gli interventi finalizzati al miglioramento e quindi all'evoluzione del software ed è di tre tipi:

- la manutenzione correttiva, che comprende la diagnosi e la rimozione delle cause e degli effetti dei malfunzionamenti delle procedure e dei programmi;
- la manutenzione adattiva, che comprende l'attività di manutenzione volta ad assicurare la costante aderenza delle procedure e dei programmi all' evoluzione dell'ambiente tecnologico del sistema informativo e al cambiamento dei requisiti (organizzativi, normativi, ecc.);
- la manutenzione evolutiva, che prevede il miglioramento della soluzione a fronte di nuovi processi e quindi include l'introduzione di nuove funzionalità e/o il miglioramento di quelle esistenti e in alcuni casi anche la rimozione.

Il responsabile dello sviluppo e della manutenzione del sistema di conservazione, coinvolgendo una o più risorse del settore dei Professional Services, procede ad effettuare l'aggiornamento del sistema[49].

Le componenti da modificare possono essere più o meno estese ma generalmente la procedura è la seguente:

- aggiornamento dell'ambiente di test dell'applicativo;
- esecuzione di un piano di test estratto dal piano di test generato in funzione delle componenti da aggiornare;
- in caso di fallimento viene redatto un verbale con i problemi riscontrati e viene terminata la procedura;
- individuazione della finestra temporale di minor impatto, tipicamente durante il fine settimana per gli aggiornamenti più corposi;
- backup a caldo differenziale della base di dati;
- aggiornamento del nodo passivo;
- promozione del nodo passivo a nodo attivo;
- esecuzione di uno piano di test relativo alle sole funzioni critiche impattate dall'aggiornamento;
- in caso di fallimento viene redatto il verbale contenente l'elenco dei problemi riscontrati, termine della procedura e ripristino dal backup della macchina virtuale;
- nel caso in cui non siano rilevati errori, viene effettuato l'aggiornamento del nodo passivo (precedentemente attivo);
- aggiornamento del registro delle versioni installate nei vari ambienti;
- monitoraggio del funzionamento del sistema per 48-72 ore successive all'aggiornamento.

[49] Per un approfondimento si rimanda al capitolo 7 del documento allegato "Specificità del contratto".

Periodicamente il responsabile dello sviluppo e della manutenzione del sistema di conservazione esegue un aggiornamento della base dati del sistema di test per adeguarlo alle nuove esigenze. La periodicità standard è di 12 mesi salvo situazioni particolari.

Esistono casi specifici nei quali il processo di aggiornamento applicativo richiede l'intervento diretto dell'intero reparto di Sviluppo Software di Siav.