Manuale di conservazione

REVISIONI DEL DOCUMENTO					
Data	**Versione**	**Elenco Modifiche**	**Compilato**	**Verificato**	**Validato**
2015-10-30	1.0	Prima emissione	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2015-12-18	2.0	Recepite osservazioni AGID del 24/11/2015	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2016-01-26	3.0	Recepite osservazioni AGID del 21/01/2016	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2016-02-08	3.1	Recepite osservazioni AGID del 05/02/2016	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2018-01-12	3.2	Cambio sito DR – cambio responsabile sicurezza-cambio hypertix con gestore TIX	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2018-03-02	3.3	Dettagli sui log	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Laura Castellani (RUP Regione Toscana)
2019-10-23	3.4	Precisazioni sui log come richiesto da ISO/IEC 27017 e 27018. Modifica del Responsabile trattamento dati personali e del Responsabile della Sicurezza	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Sergio Papiani (RUP Regione Toscana)

2022-01-01	4.0	Revisioni a seguito degli adeguamenti alle Linee Guida AgID	Andrea Panichi (Direttore Esecuzione Regione)	Anna Fuggi (Responsabile servizio DigiDoc)	Sergio Papiani (RUP Regione Toscana)

INDICE

INDICE DELLE FIGURE

1 Scopo e ambito del documento

Il presente documento costituisce il Manuale di Conservazione adottato da Regione Toscana per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento.

Il manuale comprende tutte le informazioni previste dall'Agenzia per l'Italia Digitale per quanto concerne le tipologie documentali oggetto di conservazione: all'ampliarsi e/o al variare di tali tipologie il manuale verrà aggiornato per recepire tutte le informazioni aggiornate relative al trattamento delle tipologie oggetto di conservazione.

Si precisa che, per garantire la protezione di informazioni riservate, i dettagli relativi a argomenti che riguardano aspetti delle specifiche forniture del servizio di conservazione, come anche alcune informazioni previste all'interno del manuale, non saranno inseriti nel presente manuale, ma saranno sviluppati in documenti specifici (ad es. "Proposta tecnica" o "Piano della Sicurezza"), depositati in sede di presentazione della domanda di accreditamento, per i quali non sussiste obbligo di pubblicazione.

Torna all' **INDICE**

2 Terminologia (glossario e acronimi)

Torna all' **INDICE**

2.1 ACRONIMI

ACRONIMO	DEFINIZIONE
ACL	Access Control List
AIP	Archival Information Package (ex OAIS), ovvero il pacchetto di archiviazione ex DPCM 3 Dicembre 2013
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale, ovvero D.lgs 7 marzo 2005, n.82 e successive modificazioni e integrazioni
CAdES	CMS (Cryptographic Message Syntax) Advanced Electronic Signatures

ACRONIMO	DEFINIZIONE
CNS	Carta Nazionale dei Servizi provvista almeno del certificato di autenticazione (recante il codice fiscale del titolare)
DB	Database
DIP	Dissemination Information Package (ex OAIS), ovvero il pacchetto di distribuzione DPCM 3 Dicembre 2013
eIDAS	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE
GDPR	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ("General Data Protection Regulation"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE
GUI	Graphical User Interface
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
HSM	Hardware Security Module
ORM	Object-relation Mapping
OAIS	Open Archival Information System, standard ISO 14721:2002
PAdES	PDF Advanced Electronic Signatures
PEC	Posta Elettronica Certificata
SdI	Sistema di Interscambio (per le fatture elettroniche destinate alle pubbliche amministrazioni)
SIP	Submission Information Package (ex OAIS), ovvero il pacchetto di versamento DPCM 3 Dicembre 2013
SSO	Single Sign On
TSA	TimeStamping Authority
UI	User Interface
UO	Unità organizzativa (cfr glossario)
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signatures

ACRONIMO	SIGNIFICATO
RT	Regione Toscana

Torna all' **INDICE**

2.2 Glossario

Obiettivo di questo glossario è quello di definire il significato con il quale alcuni termini "chiave" ricorrenti saranno utilizzati all'interno del presente documento. Le definizioni, nel rispetto della terminologia tecnica di riferimento e delle prescrizioni normative, sono quelle effettivamente utilizzate all'interno del sistema di conservazione.

TERMINE	DEFINIZIONE
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta
Aggregazione documentale informatica	Insieme di documenti informatici o insieme 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 dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche

TERMINE	DEFINIZIONE
Area organizzativa omogenea	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi
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 in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Base di dati	Collezione di dati registrati e correlati tra loro
CAD	Decreto legislativo 7 Marzo 2005, n. 82 e successive modificazioni e integrazioni
CAdES	CMS Advanced Electronic Signatures – Formato di firma che può essere apposto su qualsiasi tipo di file. Genera una busta genera una busta crittografica contenente il file originale. Si presenta come un file la cui estensione è p7m
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Certificato di firma	Certificato destinato alla generazione delle firme apposte ai documenti digitali.
Certificato di marcatura temporale	Certificato destinato alla generazione di marche temporali.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

TERMINE	DEFINIZIONE
Conservazione	Insieme delle attività finalizzate a definire ed 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
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DOI	Digital Object Identifier
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Vedi art. 1, comma 1, lett) i quinquies del CAD.
Esibizione	Operazione che consente di visualizzare un documento conservato
Estratto per riassunto di documento informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
Evidenza informatica	Sequenza di simboli binari, ossia di bit, che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento
Firme multiple	Firme digitali apposte da diversi sottoscrittori allo stesso documento.
Firme parallele	Firme apposte da differenti soggetti al medesimo documento digitale utilizzando una sola busta crittografica.

TERMINE	DEFINIZIONE
Firme verticali	Firme apposte da differenti soggetti, l'una ad un documento firmato in precedenza da un altro soggetto, creando delle buste crittografiche innestate l'una dentro l'altra.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o digest (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
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
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 crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica
Indice di conservazione	Evidenza informatica che elenca in forma strutturata – xml - le impronte, gli identificativi e le informazioni descrittive dei documenti digitali sottoposti insieme a processo di conservazione. Tale file è conforme al UNI 11386:2020 Standard SInCRO ed è firmato digitalmente dal responsabile del servizio di conservazione e marcato temporalmente.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

TERMINE	DEFINIZIONE
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
ISBN	International Standard Book Number
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
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	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
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	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione

TERMINE	DEFINIZIONE
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
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 logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione
PAdES	PDF Advanced Electronic Signatures– Formato di firma che può essere apposto esclusivamente sul tipo di file pdf.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a 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	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
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

TERMINE	DEFINIZIONE
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 e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Produttore dei PdV	Persona fisica o giuridica, di norma diversa dal soggetto che ha formato 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 individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare, ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
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

TERMINE	DEFINIZIONE
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia
Responsabile del servizio di conservazione	Soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
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
Responsabile dei sistemi informativi per la conservazione	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
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 definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
Scheda documento	Nel sistema DAX è un Aggregato logico costituito da uno o più documenti digitali e/o analogici che sono considerati come un tutto unico e come tali costituiscono l'oggetto di una singola descrizione: nel caso in cui sio formato da più documenti uno di essi si configura come "primario" e gli altri sono gli "allegati" che trovano il loro significato compiuto solo in relazione al primario. E' l'unità minima, concettualmente non divisibile, di cui è composto l'archivio.

TERMINE	DEFINIZIONE
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
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
Tag	Marcatori (etichette) per assegnare una semantica al testo nei file xml
Testo Unico	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modificazioni
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati
Unità di aggregazione	Nel sistema DAX è un aggregato logico di schede documento collegate tra loro che si forma nell'archivio corrente e che può costituire un'unità di versamento in conservazione. Il fascicolo che scaturisce da un procedimento amministrativo è il caso più comune di unità di aggregazione, altri esempi sono costituiti dalle serie tipologiche (delibere, contratti ecc).
Unità organizzativa	Qualsiasi articolazione di un'Area Organizzativa Omogenea, ovvero un nodo della struttura gerarchica – mappa organizzativa - in cui si organizza un'Amministrazione
URI	Uniform Resource Identifier
Utente abilitato	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

TERMINE	DEFINIZIONE
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce 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.

Torna all' **INDICE**

3 Normativa e standard di riferimento

Torna all' **INDICE**

3.1 Normativa di riferimento

Alla data l'elenco dei principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti, è costituito da:

[1] 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;

[2] 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;

[3] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

[4] Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;

[5] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

[6] Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;

[7] Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);

[8] Decreto del Presidente del Consiglio dei Ministri 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, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;

[9] Reg. UE 910/2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;

[10] Reg. UE 679/2016 (GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

[11] Linee Guida sulla formazione, gestione e conservazione dei documenti informatici adottate da AgID con determinazione n. 407/2020 e successivamente aggiornate e rilasciate con determinazione 37172021.

Torna all' **INDICE**

3.2 Standard di riferimento

Di seguito sono riportati gli standard ai quali si fa riferimento per il Manuale di Conservazione (si rimanda all'allegato 4 alle Linee guida AgID "Standard e specifiche tecniche"

- ISO 14721OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- UNI 11386Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- Moreq - Model Requirements for Electronic Records Management
- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine

Torna all' **INDICE**

4 Ruoli e responsabilità

Il Servizio di Conservazione gestito da Regione Toscana è basato su un modello organizzativo descritto nel successivo capitolo 5.

I ruoli che intervengono nella erogazione del servizio, con le pertinenti responsabilità, sono elencati nella tabella di seguito e assegnati a risorse che rispondono ai requisiti espressi da AgID, così come ufficializzati nel documento "Profili Professionali".

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile del servizio di conservazione	***Anna Fuggi***	• Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; • definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; • corretta erogazione del servizio di conservazione all'ente produttore; • gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione; • approvazione autorizzazioni al sistema.	Dal 20/10/2015	***Ivan Ricotti; Antonella Ghisaura; Laura Castellani (per approvazione modifiche sistema, dal 12/01/2018 al 09/06/2019); Andrea Panichi (per approvazione modifiche sistema, dal 12/01/2018), Angelo Marcotulli (per approvazione modifiche sistema, dal 10/06/2019)***
Responsabile Sicurezza dei sistemi per la conservazione	***Leonardo Borselli***	• Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; • segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	Dal 01/01/2022	***N/A***

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile funzione archivistica di conservazione	***Anna Fuggi***	• Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; • definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; • monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; • collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	Dal 20/10/2015	***Ivan Ricotti; Antonella Ghisaura.***
Responsabile trattamento dati personali	***Sergio Papiani***	• garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • garanzia che il trattamento dei dati affidati dagli Enti Produttori avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	Dal 23/09/2019	***N/A***
Responsabile sistemi informativi per la conservazione	***Andrea Panichi***	• Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; • monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; • segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; • pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; • controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	Dal 20/10/2015	***N/A***

RUOLO	NOMINATIVO	ATTIVITÀ DI COMPETENZA	PERIODO NEL RUOLO	EVENTUALI DELEGHE
Responsabile sviluppo e manutenzione del sistema di conservazione	***Rosario Graziano***	• Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; • pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; • monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; • interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; • gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Dal 01/01/2022	***N/A***

Alcuni ruoli sono cambiati nel tempo. Nominativi che hanno svolto in precedenza i ruoli indicati sono:

RUOLO	NOMINATIVO	PERIODO NEL RUOLO
Responsabile Sicurezza dei sistemi per la conservazione	***Sandro Piana***	Dal 20/10/2015 al 25/09/2017
Responsabile Sicurezza dei sistemi per la conservazione	***Marco Barbalinardo***	Dal 26/09/2017 al 2/10/2019
Responsabile Sicurezza dei sistemi per la conservazione	***Angelo Marcotulli***	Dal 3/10/2019 al 31/12/2021
Responsabile sviluppo e manutenzione del sistema di conservazione	***Valentina Martinucci***	Dal 20/10/2015 al 31.12.2021
Approvazione autorizzazioni al sistema	***Paola Collesei***	Dal 11/10/2016 al 10/01/2018
Delegato Responsabile del servizio di conservazione ***Delegato Responsabile funzione archivistica di conservazione***	***Marcello Serenetti***	Dal 20/10/2015 al 10/01/2018
Responsabile trattamento dati personali	***Laura Castellani***	Dal 20/10/2015 al 09/06/2019
Delegato Responsabile del servizio di conservazione	***Laura Castellani***	Dal 12/01/2018 al 9/06/2019
Responsabile trattamento dati personali	***Angelo Marcotulli***	Dal 10/06/2019 al 22/09/2019
Delegato Responsabile del servizio di conservazione	***Angelo Marcotulli***	Dal 10/06/2019 al 22/09/2019

Torna all' **INDICE**

4.1 Il Responsabile del servizio di conservazione

Nel presente paragrafo sono dettagliate le competenze del Responsabile del servizio di conservazione, affidate dal Responsabile della conservazione, interno al soggetto produttore, al Responsabile del servizio di conservazione che opera presso il soggetto conservatore secondo quanto previsto dal decreto [8].

- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento con sigillo qualificato con marcatura temporale, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata o sigillo qualificato, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della 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;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 decreto [8];
- 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 all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

- predispone il manuale di conservazione di cui all'art. 8 del decreto [8]e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
    1. descrizione del contenuto dell'insieme dei documenti;
    2. estremi identificativi del responsabile del servizio di conservazione;
    3. estremi identificativi delle persone eventualmente delegate dal responsabile del servizio di conservazione, con l'indicazione dei compiti alle stesse assegnati;
    4. indicazione delle copie di sicurezza;
- mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- verifica la corretta funzionalità del sistema e dei programmi in gestione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
- richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

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

Il responsabile del servizio di conservazione richiede l'intervento del Pubblico Ufficiale nei casi previsti, assicurando allo stesso l'assistenza e le risorse necessarie all'espletamento delle attività al medesimo attribuite.

Il Responsabile del servizio di Conservazione non è responsabile del contenuto dei singoli documenti né degli indici (attributi) associati a ciascun Documento. La conformità dei documenti trasmessi ai corrispondenti originali è assicurata da formale autorizzazione alla Conservazione da parte del Produttore, eseguita mediante la sottoscrizione del contratto per la fornitura del servizio.

Il responsabile del servizio di conservazione è tenuto ad operare d'intesa con:

- il responsabile del trattamento dei dati personali
- il responsabile della sicurezza
- il responsabile dei sistemi informativi
- il coordinatore della gestione documentale, salvo che il ruolo sia ricoperto dallo stesso responsabile del servizio di conservazione
- i responsabili designati per ciascuno dei sistemi/applicativi abilitati a versare in conservazione la documentazione: per poter versare in conservazione ciascun sistema/applicativo deve essere a ciò abilitato attraverso apposita procedura che prevede di poter indicare il responsabile di riferimento del sistema/applicativo quale figura che il RdC può interpellare per qualsiasi problematica inerente la documentazione versata in conservazione dal sistema/applicativo stesso; qualora tale responsabile non sia designato il coordinatore della gestione documentale e il responsabile del cliente che ha versato la documentazione sono i soggetti tenuti a fornire al RdC tutte le informazioni richieste.

Torna all' **INDICE**

4.2 Formazione

Per il responsabile del servizio di conservazione è previsto uno piano di formazione allo scopo di adeguare il percorso formativo alle nuove eventuali esigenze di legge e di business. Tale percorso prevede la partecipazione ad eventuali corsi di aggiornamento e seminari periodici sul tema della conservazione digitale, corsi di formazione sulla sicurezza delle informazioni e sulla privacy.

Torna all' **INDICE**

5 Struttura organizzativa per il servizio di conservazione

Il servizio di Conservazione erogato dalla Regione Toscana si configura in armonia al seguente schema:

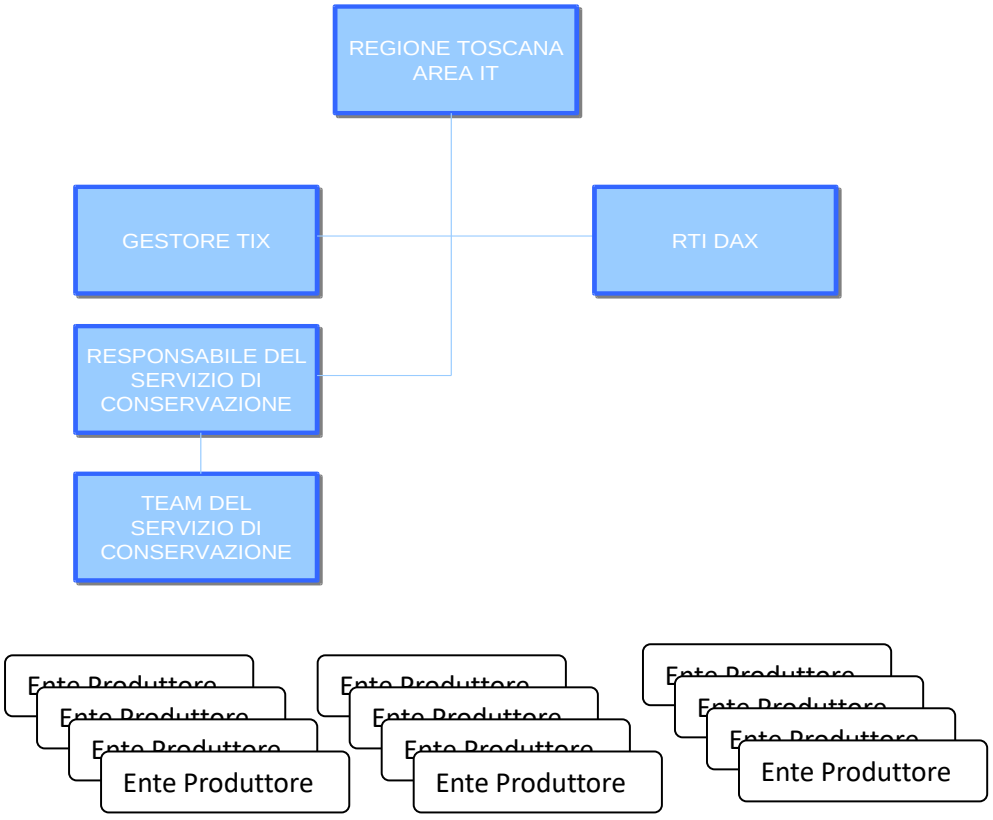

Figura 1 : La figura mostra l'organizzazione del servizio di Conservazione, in base ai ruoli svolti dai diversi soggetti coinvolti nella erogazione

Quanto sopra riportato dimostra la segregazione dei compiti all'interno del servizio di conservazione. In particolare:

- le figure di responsabilità descritte nel capitolo precedente sono ricoperte da persone distinte;
- le persone addette alla conduzione delle applicazioni e alla conduzione dei sistemi sono distinti;
- l'organizzazione dello sviluppo e manutenzione è in carico ad azienda certificata come conservatore, che pertanto garantisce le opportune separazioni tra sviluppatori, manutentori, tester e sistemisti.

Torna all' **INDICE**

5.1 Strutture organizzative

Torna all' **INDICE**

5.1.1 Regione Toscana

L'area IT di Regione Toscana, tra le altre responsabilità relative alle infrastrutture IT e alla gestione dei sistemi informativi in uso, si configura come Soggetto che coordina il Servizio di Conservazione che viene utilizzato sia all'interno della Regione stessa, sia dagli Enti Locali del territorio toscano che, poiché Regione Toscana svolge il ruolo di Centrale di committenza ai sensi dell'art. 33 del D.Lgs. 163/2006 e dell'art. 42 della L.R. 38/2007, possono aderire ai contratti regionali e quindi avvalersi della piattaforma Digidoc adottata dalla Regione per la Conservazione.

In tal senso, l'area IT della Regione Toscana ha le seguenti responsabilità:

- interfacciare gli Enti Locali, nelle fasi di adesione al contratto di servizio;
- Relazionarsi con gli outsourcer incaricati della gestione delle infrastrutture tecnologiche su cui si attesta il Servizio di Conservazione, per i diversi aspetti relativi alla gestione dell'infrastruttura fisica (in carico al Gestore TIX) e della piattaforma applicativa (in carico alla RTI DAX);
- Cooperare con il Responsabile della Conservazione, nelle diverse fasi di messa in piedi, erogazione ed eventuale dismissione del servizio stesso;
- Nominare ufficialmente le risorse che ricoprono i ruoli previsti dalla Normativa AgID per il Servizio di Conservazione.

Torna all' **INDICE**

5.1.2 Gestore del TIX

Il Gestore del TIX attualmente eroga presso il TIX (Tuscany Internet eXchange) servizi per conto di Regione Toscana o per altri Enti ed è incaricato da Regione Toscana stessa, con la stipula di un apposito contratto di Outsourcing, di gestire l'infrastruttura fisica (CED) su cui si attesta il servizio di Conservazione, in termini di:

- monitoraggio della disponibilità di sistemi e rete, secondo i Livelli di Servizio stabiliti contrattualmente con Regione Toscana;
- monitoraggio della connettività;
- gestione sistemistica di reti e sistemi (attività di Amministratore di Sistema);

- ricezione e gestione delle segnalazioni di malfunzionamenti riconducibili all'infrastruttura IT a perimetro, collaborando con le altre strutture organizzative coinvolte nel servizio di Conservazione per individuare e risolvere le cause di tali malfunzionamenti;
- gestione degli apparati di sicurezza in termini di:
    - Firewall;
    - Intrusion Detection System;
    - Gestione centralizzata log degli accessi ai sistemi ed agli apparati;
    - Bandwith management;
- gestione di:
    - sistemi di storage di classe enterprise;
    - virtual tape library per backup ed archiving.

Il Gestore TIX opera in via di San Piero a Quaracchi 250, Firenze.

Torna all' **INDICE**

5.1.3 RTI DAX

Il Raggruppamento di Imprese (RTI) DAX è incaricato da Regione Toscana, (attraverso la stipula di apposito contratto di outsourcing), della messa in opera e successiva manutenzione del sistema per la gestione di Archivio e di Conservazione. Il Raggruppamento è inoltre incaricato dalla Regione di fornire le risorse adeguate a gestire il Servizio di Conservazione in esercizio.

Le principali responsabilità in carico al Raggruppamento sono:

- assicurare la disponibilità delle licenze del Software DigiDoc, secondo quanto riportato nel Contratto di Outsourcing con Regione Toscana;
- supportare l'installazione e la manutenzione della piattaforma DigiDoc in ambiente di "staging" (collaudo) e successivamente in esercizio, secondo le modalità descritte nell'Accordo di Servizio tra Regione Toscana ed il fornitore della piattaforma DigiDoc;
- effettuare gli interventi di manutenzione ordinaria, correttiva e di adeguamento (per le applicazioni e i componenti di sistema, escluso l'hardware e lo strato di virtualizzazione), anche per quanto riguarda la sicurezza, in armonia a quanto previsto nell'Accordo di Servizio tra Regione Toscana e il fornitore della piattaforma DigiDoc;
- fornire a Regione Toscana la documentazione tecnica a corredo del software, sia in sede di prima installazione, sia in occasione di interventi di manutenzione (correttiva e/o adeguativa) come previsto dalle procedure di Regione Toscana e del fornitore della piattaforma DigiDoc;

- assicurare a Regione Toscana la disponibilità delle risorse adeguate a ricoprire i ruoli di cui al capitolo 5, le quali opereranno per conto della Regione Toscana, come definito nell'ambito del Contratto siglato tra Raggruppamento e Regione.

Torna all' **INDICE**

6 Oggetti sottoposti a conservazione

Torna all' **INDICE**

6.1 Oggetti conservati

Il servizio offerto da Regione Toscana permette potenzialmente il trattamento e la conservazione di

- documenti informatici e documenti amministrativi informatici
- aggregazioni documentali informatiche.

Il cliente che intende usufruirne, deciderà per quali oggetti digitali (rappresentati nel DAX come schede documento e unità di aggregazione) attivare il servizio di conservazione e, una volta comunicate a Regione Toscana, collaborerà con il team DigiDoc nelle operazioni di definizione del relativo trattamento.

Per ogni caso specifico, ossia per ogni Titolare i cui documenti vengano presi in carico, Regione Toscana individua le classi documentali e i dati o attributi specifici da associare a ciascuna di esse. In questa fase, con le cadenze da concordare; saranno ad esempio precisati i tempi di conservazione, la periodicità di invio dei documenti al sistema di conservazione, l'intervallo di tempo intercorrente tra la presa in carico e la chiusura del pacchetto di archiviazione.

La classe documentale racchiude tutte le caratteristiche comuni ad uno specifico tipo di documento da sottoporre a conservazione, definendone quindi le informazioni indispensabili per qualificarlo ed identificarne gli elementi distintivi. L'elenco e le caratteristiche delle classi documentali vengono precisate di caso in caso, in collaborazione con il Soggetto Produttore; a titolo esemplificativo, tuttavia, le classi più comunemente trattate sono documenti del ciclo attivo (Fatture Clienti, Libri e Registri, etc.), del ciclo passivo (Fatture di Acquisto, etc.) e documenti del lavoro (LUL) e dagli Atti amministrativi.

Il dettaglio delle informazioni sopra indicate, concordate con il soggetto produttore, viene riportato nella documentazione scambiata con il singolo Ente produttore.

Torna all' **INDICE**

6.2 Pacchetto di versamento

Il Pacchetto di versamento è il pacchetto informativo proveniente dal soggetto produttore e versato nel sistema di conservazione. Le modalità di versamento sono concordate e descritte nell'accordo di servizio.

Fra i diversi aspetti da concordare, i principali sono:

- le tipologie di documenti da conservare,
- metadati,
- eventuali informazioni extra,
- i formati da adottare per ogni classe/tipo di documento,
- le modalità e canali di trasferimento dei documenti nell'archivio (ws, ftp, http) ed ulteriori.

Il responsabile del servizio di conservazione coordina l'intero processo e si accerta del rispetto delle regole fissate negli specifici accordi di servizio. Sono conservati i seguenti oggetti: documenti informatici, documenti amministrativi informatici e fascicoli informatici e per ciascuno di queste tipologie di oggetti sono previsti determinati requisiti da rispettare per la corretta esecuzione della procedura di conservazione.

Con l'entrata in vigore delle nuove linee guida, a partire dal 1° gennaio 2022, il sistema di Conservazione della Regione Toscana DAX ha introdotto una serie modifiche in materia di formati documentali accettati (si rimanda all'allegato 2 Linee Guida AgID "Formati di file e riversamento") e metadati necessari per l'invio in conservazione (si rimanda all'allegato 5 Linee Guida "Metadati"), per il dettaglio dei quali si rimanda ai rispettivi paragrafi del presente manuale.

Il pacchetto di versamento è corredato dal un file xml - SIPManifest.xml, il cui schema è fornito nell'allegato *Allegato1 – SIPManifest.v.2.0.pdf* - che contiene sia le descrizioni della documentazione che i puntatori e le impronte dei file che compongono la documentazione digitale da inviare in conservazione. In caso di documentazione già inviata in conservazione e di cui si devono solo aggiornare dati e/o file, per le unità di descrizione - schede documento, unità di aggregazione di documenti ecc - e i documenti digitali da aggiornare si rimanda al documento di Specifiche tecniche.

La responsabilità del produttore è quella di provvedere e monitorare il corretto funzionamento dell'integrazione tra i sistemi producer e il sistema di conservazione.

E' altresì a cura del produttore fare quanto necessario per assicurarsi che:

- tutta la documentazione venga inviata in conservazione correttamente "tipizzata" nel pacchetto di versamento secondo quanto specificato nell'accordo di servizio, cosicché dalla

tipologia specificata il sistema di conservazione sia in grado di impostare correttamente sia il termine entro cui obbligatoriamente deve essere effettuato il processo di conservazione che il termine fino cui decorre l'obbligo di conservazione della documentazione;

- tutta la documentazione sia inviata al sistema di conservazione in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa vigente e secondo quanto concordato negli accordi di servizio;

- la documentazione venga inviata in conservazione corredata almeno dei metadati obbligatori previsti dal profilo specifico della tipologia documentale specificata;

Per quanto concerne gli allegati delle fatture

- nel caso delle fatture attive in base alle nuove regole tecniche della fatturazione elettronica gli eventuali allegati, recanti ad esempio il dettaglio di ciò che viene fatturato, sono inglobati all'interno della fatturaPA (*embedded* in base 64 nell'xml della fattura stessa), e dato che la fattura è firmata digitalmente sono inviati in conservazione come parte integrante del documento xml principale della fattura (esattamente come ricevuti dal SdI); tuttavia per garantire una maggior leggibilità vengono anche versati in conservazione come documenti distinti (allegati) della scheda documento della fattura, "estraendoli" dall'xml firmato in cui sono inglobati;

- nel caso delle fatture attive è previsto che eventuali allegati a corredo della fattura siano descritti nel pacchetto di versamento come documenti allegati della scheda documento di cui la fattura è il documento principale

Per quanto concerne eventuali ricevute/notifiche provenienti o inviate al SdI a fronte di una data fattura passiva o lotto di fatture ricevuto, esse vengono versate in conservazione come schede documento distinte dalla fattura o lotto a cui fanno riferimento, creando una relazione con la scheda documento della fatturaPA cui sono relative (attraverso gli appositi tag di relazione tra schede documento previsti dal tracciato xsd del pacchetto di versamento).

Torna all' **INDICE**

6.3 Pacchetto di archiviazione

L'elaborazione del pacchetto di versamento verifica dati e file dei documenti versati al fine di stabilire quali dei documenti del pacchetto possano esser presi in carico da DigiDoc e quali vadano rifiutati (vi può essere anche una presa in carico parziale). Al termine di questa elaborazione i risultati e i dettagli dei controlli effettuati su tutti i documenti del pacchetto, sia quelli accettati che

quelli rifiutati, sono riportati nel rapporto di versamento (SIPResult.xml, il cui schema è fornito nell'allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*) che viene restituito al versatore e al tempo stesso diviene esso stesso oggetto di conservazione in DigiDoc.

Il Pacchetto di Archiviazione (PdA) o Archival Information Package (AIP) secondo la terminologia OAIS, viene generato dal sistema a conclusione del processo di verifica e presa in carico degli item – schede documento e unità di aggregazione – del PdV e si ottiene dalla trasformazione di uno o più pacchetti di versamento. Esso contiene:

- I documenti conservati nel formato utilizzato all'atto del versamento;
- Il file indice IPdA firmato e marcato temporalmente: esso è un file XML formato secondo le regole tecniche definite nella norma UNI 11386:2020 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; nella sezione MoreInfo prevista dallo standard contiene per ciascun documento del PdA:
  - il corrispondente tag *Item* del SIPManifest.xml con cui il documento è stato versato in conservazione (per dettagli si rimanda all'allegato *Allegato1 – SIPManifest.v.2.0.pdf*);
  - il corrispondente tag del *Item* del SIPResult.xml, ovvero il rapporto di versamento, contenente l'esito dei controlli effettuati sul documento (per dettagli si rimanda all'allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*).

Torna all' **INDICE**

6.4 Pacchetto di Distribuzione

Il Pacchetto di distribuzione (PdD) o Dissemination Information Package (DIP) secondo la terminologia OAIS, consente di rispettare l'obbligo di esibizione dei documenti conservati; esso viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli Utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione. Un pacchetto di distribuzione può coincidere con un pacchetto di archiviazione, ma è possibile gestire la produzione di pacchetti di distribuzione specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il Pacchetto di distribuzione può essere generato al momento della richiesta da parte di un Utente e non conservato nel Sistema.

Torna all' **INDICE**

6.5 Formati

L'allegato 2 alle Linee Guida "Formati di file e riversamento" presenta un elenco dettagliato dei formati dei file con cui vengono rappresentati i documenti informatici, specificando, per ciascuno di questi, se è idoneo o meno per la conservazione nel lungo periodo.

L'adeguamento del sistema DAX su questo tema ha previsto:

- l'introduzione di nuovi formati o nuove estensioni e mimetype a formati già presenti in configurazione;
- l'accettazione di quei formati considerati da AgID non più idonei alla conservazione. In questo caso specifico, nel rapporto di versamento sarà incluso un messaggio di warning che indicherà il conferimento di formato documentale escluso da AgId in ambito di conservazione.

Negli accordi di servizio con ogni ente sarà definito l'elenco dei formati dei documenti che il soggetto produttore vuole conservare nell'archivio digitale.

L'elenco dei principali formati che saranno accettati dal DAX, a partire dal 1° gennaio 2022 e l'elenco dei formati esclusi da AgID per la conservazione, ma che continueranno ad essere accettati dal sistema DAX, sono stati riportati nell' *Allegato5 - ElencoFormatiDigitali.v.1.0.pdf*).

Torna all' **INDICE**

6.6 Metadati conservati

Il sistema di conservazione consente di gestire tutti i metadati obbligatori previsti dalla normativa vigente ai quali vanno aggiunti quelli presenti negli accordi specifici.

In particolare, tutti i metadati definiti nel nuovo allegato 5 alle Linee guida AgId vengono inclusi all'interno del descrittore del pacchetto di versamento (SIPManifest.xml); la loro definizione è quella di AgID sia nella sintassi che nella semantica. Vengono ridefinite le tipologie documentali attualmente accettate dal DAX e le relative schede tecniche sono state adeguate.

Le versioni attuali delle tipologie documentali continueranno ad essere accettate: in caso di conferimento di documenti afferenti a tali versioni di tipologie, nel rapporto di versamento sarà incluso un messaggio di warning che segnalerà il conferimento in deroga alla normativa AgId.

Saranno definiti, sempre nel rapporto di versamento, nuovi messaggi di warning in caso di:

- Documento dichiarato firmato dall'Ente versatore (tramite apposito metadato obbligatorio definito da AgId) ma che non risulti firmato o il caso inverso;

- Formato del documento dichiarato dall'Ente versatore (tramite apposito metadato obbligatorio definito da AgId) non conforme al reale formato del documento.

Per entrambi i casi d'uso precedenti, il conferimento della documentazione avrà sempre esito positivo, salvo che non siano presenti altri errori.

Torna all' **INDICE**

6.7 Tempi di conservazione

Il sistema di conservazione consente di gestire i tempi entro cui è necessario mettere in conservazione e quelli per cui è necessario conservare i documenti. Tali informazioni sono fornite dal produttore all'atto del versamento e indicate nelle schede anagrafiche per ogni tipologia documentale.

La permanenza in conservazione è specificata nei "Piani di conservazione", che indicano, tipologia per tipologia, i tempi (p.e. le delibere sono mantenute per sempre).

I tempi di conservazione sono un metadato della tipologia documentale. Per ogni PdV l'ente produttore specifica, tra i metadati, il tempo di conservazione. Pertanto, le eventuali modifiche di politica sono in carico al produttore.

Ciò detto è responsabilità fondamentale del produttore indicare correttamente la tipologia documentale: in caso di mancata o errata attribuzione della tipologia il sistema di conservazione non potrà procedere all'avvio e mantenimento della conservazione secondo le corrette tempistiche.

Il tempo di conservazione di tutte le tipologie documentali dei cicli attivo e passivo di fatturazione è configurato a 10 anni.

Torna all' **INDICE**

7 IL PROCESSO DI CONSERVAZIONE

DigiDoc adotta lo standard ISO 14721:2003, comunemente noto come OAIS (Open Archival Information System), che costituisce lo standard di riferimento per qualsiasi sistema si occupi di digital preservation.

La soluzione, nel pieno rispetto della normativa in materia e degli standard internazionali di riferimento, assicura la gestione di tutti i processi inerenti alla conservazione quali:

- Processo di Amministrazione: preparazione dell'ambiente, intendendo con ciò la messa a punto del contesto operativo, finalizzata alla predisposizione degli elementi necessari alla creazione, gestione, archiviazione e conservazione dei documenti (massimario di scarto, formati, metadati associati ai documenti …);
- Processo di Invio in Conservazione: trasferimento del documento al Sistema di Conservazione.
- Processo di Controllo: verifica che il documento abbia i requisiti per essere accettato dal sistema di conservazione
- Processo di Conservazione e fruizione della memoria digitale.
- Processo di Consultazione: ricerca della documentazione conservata da parte di soggetti abilitati.

Le funzionalità gestite dal sistema permettono di garantire:

- l'identificazione certa del soggetto che ha formato il documento e dell'AOO di riferimento
- l'integrità del documento
- la leggibilità e l'agevole reperibilità dei documenti e dei relativi metadati
- il rispetto della normativa nazionale sulla conservazione, con adeguamento alla variazione delle norme
- la prevenzione della obsolescenza hw e sw, attraverso adeguamenti continui dell'HW e del SW e attraverso riversamenti sostitutivi dei documenti digitali;
- il rispetto del trattamento dei dati e della tutela dei dati tramite la registrazione e conservazione in un sistema di audit unico in grado di restituire dati di sintesi, ma interrogabili a più livelli di dettaglio;
- il tracciamento di ogni accesso, variazione e intervento sul sistema: accessi, modifiche tecnologiche, aggiornamenti dei metadati e dei documenti digitali.
- l'ampliamento e l'aggiornamento della lista dei formati digitali ammessi;
- la ricezione, il mantenimento, l'aggiornamento e la conservazione di tutti i metadati relativi alla documentazione dell'archivio.

Torna all' **INDICE**

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Il processo di invio in conservazione inizia con l'invocazione da parte di un sistema/applicativo del soggetto produttore del web service di receiveSIP esposto da DigiDoc.

Tale servizio prevede l'invio in conservazione di una collezione di uno o più documenti o aggregati di documenti attraverso un attachment, il Submission Information Package (SIP) di OAIS, che è un file compresso – zip o tar.gz – contenente:

- un file xml *SIPManifest.xml* che contiene sia i metadati del/i documenti e loro aggregati (fascicoli, serie ecc) da inviare in conservazione, sia le impronte e gli URI (percorsi relativi all'interno del file archivio) dei file associati ai documenti;
- i file che compongono i documenti digitali da inviare in conservazione (che possono essere o meno firmati digitalmente).

Per ogni item – i.e. documento o aggregato di documenti – presente nel SIP il sistema del produttore deve specificare nel SIPManifest.xml un identificativo univoco attraverso cui può richiederne in seguito degli aggiornamenti o l'esibizione. Infatti, lo stesso servizio di receiveSIP consente anche di inviare ad DigiDoc solo degli aggiornamenti dei metadati e/o l'aggiunta di allegati della documentazione già inviata in conservazione. In questo caso l'attachment contiene solo il SIPManifest.xml, se si devono rettificare, aggiornare o versionare solo dei metadati, ed eventualmente anche i file da rettificare o versionare. Peraltro, l'identificativo che il soggetto produttore deve specificare per ogni item (univoco solo limitatamente a quelli degli item inviati dal dato sistema) serve anche affinché DigiDoc possa controllare se un dato sistema ha già inviato un dato item in modo da non accettarlo in conservazione qualora quel soggetto produttore lo stia inviando una seconda volta (senza indicare che si tratta di un aggiornamento).

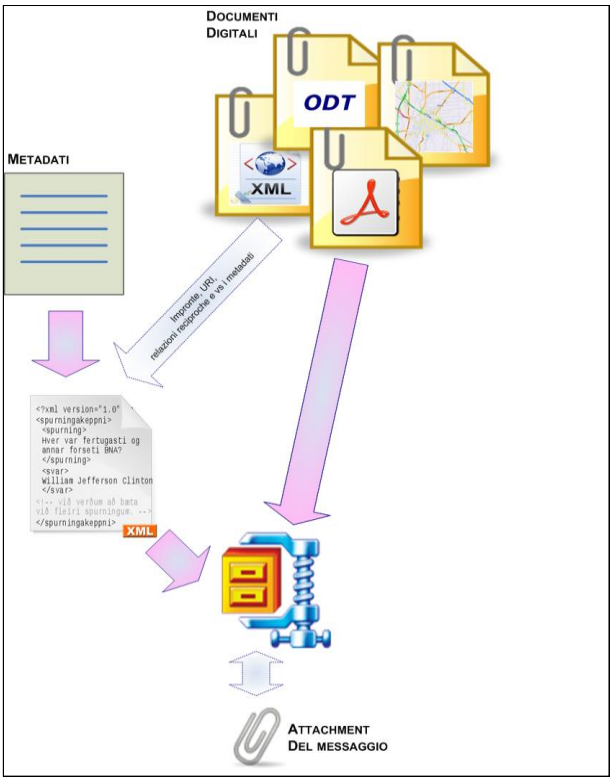

Figura 2: La figura rappresenta il flusso con cui un documento viene versamento del documento nel sistema di conservazione

Gli estremi di ciascun SIP ricevuto, tra cui il produttore e l'identificativo univoco assegnatogli dal produttore, sono memorizzati insieme al numero di registrazione, in apposito registro dei SIP, assegnatogli da DigiDoc stesso. Associato a questo record viene archiviato e avviato alla conservazione il corrispondente SIPManifest.xml.

Sia i file che le strutture dati dei SIP sono oggetto delle procedure di back-up adottate per tutti i dati e i file archiviati in DigiDoc.

Una volta che il pacchetto di versamento è stato preso in carico dal Sistema di Conservazione, il sistema produttore riceve un ticket attraverso cui può in seguito richiedere l'esito dell'invio di quel SIP, vale a dire il rapporto di versamento: stato di trasmissione/elaborazione e dettaglio dell'elaborazione, ovvero cosa è stato accettato in conservazione e cosa no e perché. Infatti, il processo di invio in conservazione della documentazione nel suo complesso prevede una modalità di interazione che è asincrona, dato che i documenti inviati in un unico SIP possono essere molti o di dimensioni ragguardevoli e che la verifica del SIP da parte del Sistema di Conservazione può richiedere un certo tempo di elaborazione.

Torna all' **INDICE**

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Quando la documentazione inviata in conservazione arriva al modulo di elaborazione dei pacchetti di versamento, il modulo si occupa per prima cosa di effettuare i controlli dei metadati e dei file del SIP pervenuto: la documentazione che non supera i controlli "bloccanti" non può essere ammessa in conservazione. Il sistema DigiDoc compie le seguenti classi di controlli dettagliati nei seguenti paragrafi:

- Controllo dell'identità del soggetto produttore del pacchetto;
- Controllo delle Firme Digitali;
- Controlli dei Formati digitali;
- Controllo della Presenza di Macro e Codice Eseguibile;
- Controllo dei Metadati;
- Controllo impronta.

Torna all' **INDICE**

7.2.1 Controllo impronta del pacchetto di versamento

Per evitare eventuali alterazioni, al produttore del pacchetto di versamento viene richiesto di inserire l'impronta. Il sistema DigiDoc, all'atto del versamento, calcola l'impronta e la confronta con quella inserita dal produttore. Se le due stringhe non coincidono, il pacchetto viene rifiutato.

Torna all' **INDICE**

7.2.2 Controllo dell'identità del soggetto produttore del pacchetto

Il versamento di un pacchetto può avvenire solo fornendo una coppia di credenziali – userid e password – che vanno specificate nell'header del messaggio con cui il pacchetto viene inviato a DigiDoc: tali credenziali sono state precedentemente generate e memorizzate da DigiDoc associandole ai dati anagrafici – denominazione, codice fiscale, partita IVA, codice IPA se trattasi di PA ecc - del Titolare degli oggetti di conservazione a cui sono state rilasciate. Inoltre, nel SIPManifest.xml sono previsti come dati obbligatori – si veda *Allegato1- SIPManifest.v2.0.pdf* (Indice di Versamento) per maggiori dettagli – i dati identificativi del soggetto che ha prodotto il pacchetto. Quando riceve un pacchetto di versamento il primo controllo effettuato da DigiDoc è quello relativo alle credenziali di autenticazione inviate e subito dopo quello che il soggetto produttore specificato nel SIPManifest.xml sia quello corrispondente alle credenziali verificate.

Torna all' **INDICE**

7.2.3 Controllo delle Firme Digitali

I controlli sulla/e firme digitali e sulle relative marche temporali, sono i seguenti:

- la firma non deve precludere la leggibilità del documento, per cui se il documento firmato è una busta crittografica quale una busta p7m o CAdES, la busta deve poter essere aperta: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- le eventuali marche temporali associate alle firme devono essere valide, ovvero: integre, di formato ammesso dalla normativa, emesse da una TSA accreditata da AgID, firmate da un certificato valido e non revocato né sospeso alla data della marca, non ancora scadute: qualora alcuni di questi controlli non siano superati ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- la busta crittografica deve essere in uno dei formati ammessi dalla normativa italiana (quella in vigore alla data del riferimento temporale associato al documento firmato - una marca temporale o una data, quale la data di protocollo del documento, associata al documento digitale nel SIPManifest – ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo) e deve risultare integra: il mancato superamento di tale controllo impedisce l'accettazione in conservazione;
- i certificati di firma devono essere attendibili, ovvero emessi da CA accreditate da AgID: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare scaduti alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento;
- i certificati di firma non devono risultare revocati o sospesi alla data del riferimento temporale associato al documento firmato ovvero, in assenza di questo riferimento temporale, alla data di esecuzione del controllo: qualora il controllo non sia superato ciò non preclude l'accettazione in conservazione ma dà solo luogo a degli avvertimenti restituiti nel rapporto di versamento.

Il Sistema di Conservazione è in grado di verificare tutti i tipi e i formati di firme digitali e marche temporali ammessi dalla normativa italiana, e si adegua nel tempo ad ogni cambio normativo in materia di firma digitale.

Dunque, ad oggi è in grado di verificare:

- controfirme, firme parallele e firme multiple
- le buste crittografiche: p7m (PKCS#7 e CAdES); PDF (PAdES); XML (XAdES)
- le modalità di imbustamento (enveloped, enveloping, detached)
- le eventuali marche temporali associate alle firme, di qualunque dei formati ammessi (tsr, tsd, tst), sia detached che embedded nella busta crittografica.

Trattandosi di un sistema pensato per la conservazione a lungo termine, e che quindi ha un'attesa di vita molto lunga, è progettato per poter effettuare controlli diversi sui tipi e i formati di firme e marche accettati, a seconda del riferimento temporale dei documenti: in questo modo tiene conto del fatto che ciò che è stato validamente firmato secondo la normativa vigente quando la firma è stata apposta, può non essere conforme alla norma vigente al momento del suo invio in conservazione.

Il sistema traccia tutti i controlli effettuati e i relativi esiti (corredandoli del timestamp in cui li ha effettuati). In particolare, dato che il servizio di verifica firma restituisce tutti i dati ottenuti dall'analisi della busta crittografica - superamento o meno dei vari gradi di validità; estremi degli intestatari dei certificati di firma e delle CA che li hanno emessi; timestamp delle eventuali marche temporali associate; tipo di busta crittografica ecc – tutti questi dati vengono memorizzati nel pacchetto di archiviazione del documento.

Da notare in particolare che il servizio di verifica delle firme digitali:

- consente di specificare un riferimento temporale – quale una data di registrazione a protocollo – rispetto al quale deve essere effettuata la verifica della firma: in questo modo viene soddisfatto il requisito di legge che prevede di considerare altri riferimenti temporali, oltre alle marche, come riferimenti temporali opponibili a terzi;
- quando la verifica della firma viene fatta rispetto ad una data passata, indicata da una marca temporale o da un altro riferimento temporale, il sistema valuta la validità del formato della busta crittografica rispetto a quella data (ad esempio una busta p7m non CAdES che utilizza ancora l'algoritmo SHA-1 per il calcolo dell'impronta può risultare comunque valida purché riferita ad una data antecedente 30/6/2010);
- anche il periodo di validità delle marche temporali viene valutato rispetto alla loro data di emissione (la norma ha cambiato nel tempo il periodo di validità minimo richiesto alle TSA);
- grazie ad un archivio storico di CRL che viene man mano incrementato – ogni qual volta, nel verificare una firma, si scarica o si aggiorna una CRL – è in grado di verificare lo stato di revoca e sospensione di un certificato di firma a cui sia associato un riferimento temporale così addietro nel tempo che la relativa CRL non è più pubblicata (la norma impone alle CA di

mantenere le CRL solo fino allo scadere dei certificati con cui sono stato firmati i certificati di firma che rimandano alle CRL).

Torna all' **INDICE**

7.2.4 Controllo dei Formati digitali

Su ciascun documento digitale inviato in conservazione il sistema di conservazione effettua il controllo del formato: se il formato non è riconosciuto o non è tra quelli ammessi l'intera scheda documento cui appartiene il documento digitale non viene accettata in conservazione. Tale controllo si basa sul contenuto del file e non sull'estensione del nome file (che potrebbe non essere indicata o peggio essere discordante rispetto al formato effettivo del file). In particolare, nel caso di documenti che sono buste crittografiche - p7m, tsd, m7m - il formato che viene riconosciuto è quello del documento con il contenuto informativo depurato dellae eventuali buste crittografiche: il sistema prima procede allo "sbustamento" (se necessario anche ricorsivamente) ed una volta che è arrivato ad un file che non è più una busta crittografica procede al riconoscimento del formato di quel file.

Il servizio di verifica formati del Sistema di Conservazione è ad oggi in grado di riconoscere con un buon grado di affidabilità i seguenti formati:

- PDF e PDF/A;
- tutti i formati della suite MS Office (inclusi Power Point, Visio e Project);
- tutti i formati della suite Open Office;
- I formati immagine più diffusi;
- xml, ascii (txt, csv, ecc);
- i formati audio e video più diffusi;
- gli archivi compressi;
- mail in formato eml.

Il formato eml di fatto è un formato archivio/busta che a loro volta contengono delle parti con dei loro formati. Quindi quando vengono verificati, come nel caso delle buste crittografiche, il servizio di verifica formato va a verificare anche i contenuti del file archivio e delle parti della busta eml (attachment e body): se questi sono riconosciuti e ammessi il file archivio o eml è ammissibile in conservazione, altrimenti no. È anche gestita la verifica ricorsiva dei formati dei file contenuti se nel

file archivio/eml vi sono dei file/attachment che sono a loro volta file archivio o e-mail. Il fatto che il servizio di verifica formato sia in grado di riconoscere e verificare il contenuto di questi formati "contenitore", anche nel caso di annidamenti di buste, mette il Sistema di Conservazione nella condizione di poter accettare in conservazione:

- e-mail firmate;
- ricevute PEC, ovvero e-mail che in genere contengono a loro volta, come attachment, l'e-mail di cui sono la ricevuta: possono essere documenti che è importante conservare in quanto a norma di legge costituiscono un riferimento temporale opponibile a terzi (riferimento utilizzabile, per esempio. per il documento firmato che è stato inviato in uscita tramite PEC e il cui invio ha dato luogo a quella ricevuta);
- archivi compressi per i quali esiste solo una descrizione complessiva, come documento semplice, e non quelle singoli file componenti.

Una volta che il formato di un documento inviato in conservazione è stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto: attraverso tale analisi il Sistema di Conservazione può determinare la versione del formato, laddove prevista e altre utili informazioni, che andranno ad arricchire i metadati dell'AIP del documento (in particolare la sezione delle informazioni di stabilità, come definite da OAIS).

Tenuto conto che i formati ad oggi riconosciuti dal Sistema di Conservazione, in un'ottica di conservazione a lungo termine, non sono tutti ugualmente idonei alla conservazione, i formati che effettivamente il sistema di conservazione accetterà e che saranno indicati negli accordi di servizio seguiranno formati caratterizzati dai seguenti aspetti:

- aperti;
- ben documentati;
- standard, possibilmente de-jure;
- non proprietari;
- largamente diffusi;
- indipendenti dalla piattaforma;
- che permettono di includere nei file l'insieme di metadati - self-documentation - che ne descrivono il contenuto e il processo di produzione, fornendo anche i dettagli tecnici per la loro rappresentazione negli ambienti tecnologici del futuro;
- che non possano contenere macroistruzioni o per i quali siano disponibili strumenti efficaci per rilevare con sufficiente sicurezza la presenza di macroistruzioni;

- che non prevedano meccanismi tecnici di protezione e di limitazione sull'utilizzo;
- accessibili e robusti;
- caratterizzati da un'elevata stabilità (backward e forward compatibility).

È buona norma considerare che i formati per cui siano disponibili viewer o reader solo per una o poche piattaforme, anche se non vietati e quindi inseribili nel set dei formati ammessi, andranno comunque evitati quanto più possibile, perché utilizzarli corrisponderebbe a creare una limitazione forte sulla capacità dei sistemi e client fruitori di riprodurre i documenti, e di conseguenza sulla capacità del sistema di conservarli.

Infine, si è stabilito che tra i formati che non devono comunque essere accettati in conservazione, vi siano quelli per i quali, sui registri internazionali di formati – quali UDFR e PRONOM – sia indicata una data di obsolescenza o di prevista/avvenuta cessazione di supporto. È responsabilità del RdSC ed eventuali suoi delegati verificare gli aggiornamenti dei formati in suddetti registri al fine di configurare correttamente il set di formati ammessi in conservazione, procedere ad eventuali procedure di riversamento di quanto già conservato in quel formato nonché dare indicazioni ai produttori e in particolare al coordinatore della gestione documentale in merito a quali formati abbandonare perché a rischio di obsolescenza.

Una volta che il formato di un documento inviato in conservazione sia stato riconosciuto viene sottoposto ad un filtro ulteriore che analizza il formato utilizzando detector diversi e specifici a seconda del formato riconosciuto.

Nel dettaglio del formato sono inoltre presenti:

- tutti i dati previsti per la descrizione dei formati nei registri internazionali quali PRONOM e UDFR;
- l'identificativo – obbligatorio - assegnato al formato in uno dei registri appena menzionati.

Torna all' **INDICE**

7.2.4.1 Funzionalità di configurazione

Il sistema consente di configurare per ciascun formato ammesso i seguenti dati di dettaglio:

- nome ed eventuale versione del formato: è questa la coppia che lo identifica univocamente tra tutti gli altri formati censiti;
- estensione principale dei file del dato formato: tale estensione sarà quella che verrà aggiunta in automatico ai nomi dei file accettati in conservazione qualora i nomi originali

specificati nel tracciato di versamento/trasferimento non abbiano estensione o ne abbiano una ma non congruente con quella/e previste per il formato effettivo dei file;

- lista dei viewer/reader che sono utilizzabili per il rendering dei file del dato formato.

Torna all' **INDICE**

7.2.5 Controllo della Presenza di Macro e Codice Eseguibile

Sui documenti digitali inviati in conservazione sono effettuati i controlli per verificare la presenza di parti variabili – macro – e codice eseguibile/dinamico; infatti questi elementi, qualora presenti, non solo danno luogo a sottoscrizione non valida se il file è firmato digitalmente, ma rendono comunque il documento non ammissibile in conservazione in quanto perde le sue caratteristiche di documento così come sancito dalla norma: non è un documento un oggetto che non si presenta sempre uguale nel tempo. Inoltre, le macro e il codice eseguibile/dinamico sono i principali veicoli di virus e altri elementi potenzialmente nocivi, se non per il sistema di conservazione in sé, quantomeno per i client che dovessero richiedere l'esibizione di documentazione contenente malware.

Il controllo della presenza di macro viene effettuato su tutti i formati MS Office e Open Office che sono quelli che contemplano tale rischio, mentre la presenza di parti di codice eseguibile o dinamico (ad esempio javascript) viene verificata sul formato pdf che la consente (salvo se PDF/A).

Torna all' **INDICE**

7.2.6 Controllo dei Metadati

Per garantire la qualità dei metadati contenuti nel SIPManifest, il sitema di conservazione è in grado di effettuare sui metadati di ogni item tutti i seguenti tipi di controlli:

- di obbligatorietà: verifica la presenza di taluni metadati (o loro combinazioni) in assenza dei quali l'item non può essere accettato in conservazione;
- di correttezza sintattica: effettua controlli formali – di tipo e formato, di appartenenza ad un certo range/set predefinito di valori ecc – su tutti i metadati;
- di unicità: il sistema è in grado di verificare, sulla base di alcuni dati del SIPManifest che fanno parte delle informazioni di identificazione di OAIS, se un certo documento o unità di aggregazione di documenti è già stato inviato in conservazione o risulta descritto più volte nello stesso SIPManifest (nel qual caso può dar luogo ad un errore bloccante o solo ad un avvertimento).

Il nucleo base dei controlli sui metadati è prestabilito per tutti gli Enti che utilizzano DigiDoc: si tratta dei controlli che sono indispensabili a garantire la corretta conservazione della documentazione, così come regolata dalle norme e intesa e realizzata dal sistema. A questo nucleo base di controlli ogni Ente può aggiungerne altri, anche specializzati per le diverse tipologie documentali, in modo da rafforzare e modulare il filtro di ciò che DigiDoc può prendere in carico.

Le obbligatorietà/vincoli del nucleo base di controlli sui metadati sono i seguenti:

- è obbligatorio specificare un identificativo (univoco per il sistema che invia) per ogni documento o aggregato di documenti;
- è obbligatorio specificare un'etichetta/segnatura per ogni documento o aggregato di documenti (nel caso di documento protocollato potrebbero essere gli estremi di protocollo, nel caso di un fascicolo archivistico la sua segnatura basata sulla classifica e l'anno di apertura);
- è obbligatorio specificare un'intitolazione ovvero una descrizione/oggetto per ogni aggregato di documenti o singolo documento;
- è obbligatorio specificare almeno un riferimento cronologico (data di acquisizione/produzione/registrazione a protocollo; data/anno di apertura o chiusura del fascicolo, ecc.) per ogni documento o aggregato di documenti;
- è obbligatorio specificare la tipologia documentale e il tempo o termine di conservazione se non desumibile da nessuno degli elementi precedenti. Se il tempo è specificato sul documento o aggregato inviato, non può essere inferiore ma solo superiore a quello stabilito da eventuali regole del massimario di selezione e scarto applicabili a quel documento o aggregato.

Torna all' **INDICE**

7.2.7 Controllo Impronta

Il sistema calcola l'impronta dei file e la confronta con quella dichiarata nel SipManifest.xml. Se le due stringhe non coincidono, viene segnalato nel rapporto di versamento.

Torna all' **INDICE**

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Gli audit dei controlli effettuati, con dettaglio di esiti ed eventuali risultati (ad esempio nel caso della verifica della validità delle firme, tra i risultati vi sono i dati dei certificati di firma) vengono memorizzati per tutti gli item del SIP, sia quelli accettabili che quelli rifiutati, andando a costituire il "rapporto di versamento" SIPResult.xml, il cui schema è fornito nell'allegato *Allegato2 – SIPResult (Rapporto di Versamento).pdf*. Il rapporto di versamento, rilasciato dunque dal sistema di conservazione come esito del conferimento del pacchetto di versamento e sottoscritto con sigillo qualificato, viene esso stesso archiviato e avviato alla conservazione per tempo illimitato. Come detto in precedenza anche il SIPManifest.xml viene archiviato e avviato alla conservazione, il tutto al fine di attestare nel tempo il flusso di tutto ciò che è arrivato in conservazione e come tale flusso è stato trattato. Più precisamente il rapporto di versamento SIPResult.xml viene archiviato collegandolo al relativo pacchetto di versamento attraverso l'inserimento della sua impronta, data e ora di generazione e URI nella stessa tabella di archiviazione dei dati dei SIP.

E' a cura del sistema produttore che ha inviato il SIP richiedere, attraverso polling, il rapporto di versamento di ciascuno dei SIP inviati fintantoché essi non risultino disponibili, ed è altresì responsabilità del RdSC e suoi delegati accertarsi della corretta e tempestiva (compatibilmente con il carico di lavoro del sistema di conservazione) produzione dei rapporti di versamento di ogni SIP ricevuto nonché della loro messa in conservazione unitamente al SIPManifest.xml.

DigiDoc esegue appositi controlli sui documenti versati propedeutici all'accettazione del documento in conservazione di seguito descritti.

Torna all' **INDICE**

7.3.1 Rinnovo marche temporali in scadenza

DigiDoc prevede un controllo periodico dei paccchetti per verificare se le marche temporali apposte sugli Indici di Conservazione firmati vanno rinnovate perché prossime alla naturale scadenza.

A valle di questa verifica per ogni Indice di Conservazione la cui marca temporale è in scadenza DigiDoc può:

a) rinnovare la marcatura in modo automatico, richiedendo una nuova marca ad una delle TSA accreditate: la marca viene apposta sull'Indice di Conservazione già firmato e marcato, in modo da garantire la non soluzione di continuità del processo di conservazione;

b) far rifirmare e marcare l'Indice già firmato e marcato

Nello scenario b) apposita GUI pone i volumi da rimarcare, previa nuova firma, all'evidenza dell'RdSC.

Torna all' **INDICE**

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Se un pacchetto di versamento non supera uno dei controlli previsti, viene rifiutato e non viene caricato nel sistema. I seguenti controlli, se non vengono superati, generano uno scarto del pacchetto:

- Verifica impronta (hash) del pacchetto;
- Apertura della busta crittografica dei file firmati;
- Conformità del formato della busta crittografica dei file firmati alla normativa italiana;
- Formati dei documenti digitali;
- Incompletezza o assenza dei metadati.

Viene prodotto un report dello scarto in cui viene riportato il timestamping in cui è avvenuto il controllo ed un dettaglio dei controlli effettuati ed il loro esito.

Non esistono meccanismi di correzione automatica degli errori.

Torna all' **INDICE**

7.5 Preparazione e gestione del pacchetto di archiviazione

I documenti contenuti nel SIP che superano tutti i controlli (salvo quelli eventualmente "elusi" dal Soggetto Produttore) entrano nel sistema di conservazione.

Per facilitare la verifica, il contenuto degli elenchi è presentato nelle seguenti sezioni distinte:

- Unità archivistiche;
- "documenti sciolti": unità documentarie non versate all'interno di un'unità archivistica in esso contenuti

I documenti digitali accettati vengono consolidati attraverso l'aggregazione dei documenti stessi in insiemi logici chiamati pacchetti in consolidamento (ovvero pacchetti non ancora chiusi, vedi §

successivo). Già al momento dell'accettazione in conservazione per ogni scheda documento e ogni unità di aggregazione sia tutti i dati presenti nel SIPManifest.xml che quelli frutto dei controlli vengono "impacchettati" in xml, a formare i pacchetti di archiviazione, e in questa forma archiviati sullo storage del sistema di conservazione. Sul database relazionale vengono memorizzati i puntatori ai pacchetti di archiviazione conservati su storage. Al tempo stesso i dati di descrizione di ciascun item versato e accettato vengono inseriti nella banca dati relazionale del Sistema di Conservazione.

E' possibile configurare:

- sia i trigger di innesco automatico della creazione degli Indici di Conservazione, quali i seguenti:
  - quando sono stati accumulati un determinato numero o una determinata dimensione di documenti;
  - con una certa cadenza temporale, ad esempio settimanale o mensile;
- sia i vincoli da rispettare nella creazione dei pacchetti quali:
  - Aggregazione per classe documentale;
  - Aggregazione per formato digitale;
  - Aggregazione per applicazione.

Quando c'è un nuovo documento "da consolidare" il sistema verifica se c'è un pacchetto ancora in consolidamento in cui quel documento può essere inserito tenuto conto dei vari criteri di formazione dei pacchetti: se non c'è, ne istanzia uno nuovo e vi inserisce il documento. In questo processo di consolidamento, se nei metadati del documento è specificata, in apposito tag del SIPManifest, l'appartenenza ad un aggregato, ad esempio un fascicolo, il sistema di conservazione cerca di mantenerlo "unito" nella formazione dei pacchetti, cercando di mettere nello stesso pacchetto tutti i documenti relativi allo stesso aggregato (compatibilmente con gli altri criteri di creazione pacchetto configurati). Lo stesso fa per i documenti relativi alla medesima scheda documento (es file principale di una registrazione di protocollo e suoi allegati).

Torna all' **INDICE**

7.5.1 Creazione Indice di Conservazione

L'attività di creazione degli Indici di Conservazione conformi al UNI 11386:2020 Standard SInCRO, è svolta per lo più in modo automatico, ma se necessario, in rari casi, può essere forzata manualmente dal RdSC o suo delegato.

Quando viene predisposto l'Indice di Conservazione, il pacchetto cambia stato da "in consolidamento" (aperto) a "chiuso": non vi si possono più aggiungere documenti e il file xml dell'Indice, una volta completato, è disponibile in apposita interfaccia WEB per essere firmato e marcato temporalmente dal RdSC o suo delegato.

La chiusura manuale di un pacchetto può comunque essere fatta in qualsiasi momento dal RdSC o suo delegato; egli dispone di un'apposita GUI attraverso cui non solo vede e può chiudere manualmente tutti i pacchetti in consolidamento ma può anche procedere a mano a modificare la composizione – i documenti – dei pacchetti in consolidamento o a creare nuovi pacchetti.

Negli indici di conservazione, oltre alle impronte e ai dati identificativi dei documenti digitali vengono riportati:

- gli URI che puntano allo stream dei componenti digitali di ciascun documento sullo storage del sistema: l'URI permette il reperimento certo dei file ma non è un path assoluto, cosicché qualora i file dovessero essere riversati (riversamento diretto) su altro storage l'URI può non cambiare, il che costringerebbe a riformare e certificare nuovamente i pacchetti contenenti quei documenti;

- nel tracciato dell'Indice per ogni documento viene riportato l'XML che costituisce il pacchetto di archiviazione della scheda documento di appartenenza (quello anche archiviato su storage): in questo modo, attraverso la firma e marcatura, viene anche congelata la situazione dei dati del documento alla data di inizio della conservazione. Qualora i dati di un documento fossero aggiornati a seguito dell'invio di un SIP con aggiornamento dei dati del documento, i dati aggiornati verranno riportati nella banca dati relazionale e nell'AIP conservato su storage, mentre l'Indice di Conservazione attraverso cui è conservato il documento resterà invariato, quale fotografia dello stato del documento al momento dell'avvio della conservazione.

Torna all' **INDICE**

7.5.2 Certificazione pacchetto (firma e apposizione riferimento temporale)

La fase di certificazione del pacchetto ha come scopo quello di completare il processo di conservazione, perfezionando l'Indice di Conservazione attraverso l'apposizione della firma digitale del RdSC e l'apposizione di un riferimento temporale.

Le attività di certificazione dei pacchetti avviene tramite l'individuazione da parte del Sistema di Conservazione dei pacchetti chiusi che devono essere firmati.

Una volta che il Responsabile del servizio di conservazione o suo delegato ha firmato il pacchetto, se il pacchetto, in base alla normativa vigente, prevede una seconda firma dell'Indice di Conservazione

(da parte di un notaio o di un pubblico ufficiale), il Sistema di Conservazione gestisce anche questa casistica e inserisce il pacchetto che manca della seconda firma in un apposito elenco di pacchetti in attesa della seconda firma.

Quando sull'Indice di Conservazione viene apposta una delle firme previste nella busta crittografica viene inserito il riferimento temporale – signing time – che attesta quando è stata effettuata la firma. Il tipo di firma che viene apposta è CadES-BES con profilo specifico della conservazione a lungo termine.

A questo punto il processo di conservazione è concluso ai sensi di quanto previsto dalla norma.

Torna all' **INDICE**

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

7.6.1 Funzionalità di ricerca

Le GUI del portale DigiDoc consentono di ricercare la documentazione presa in carico da DigiDoc attraverso tutti i dati specificati nel pacchetto di versamento nonché attraverso i dati acquisiti dai documenti durante il loro ciclo di vita in DigiDoc (data di versamento in conservazione, data di accettazione in conservazione, data inizio conservazione ecc).

Le GUI di ricerca sono progettate e realizzate per offrire un accesso:

- sicuro;
- semplice;
- guidato;
- adeguato alle esigenze.

La sicurezza dell'accesso è garantita attraverso:

- accesso autenticato alle GUI del portale;
- gestione delle richieste di accesso alla documentazione e del relativo iter;
- gestione di diversi livelli di sicurezza sulla documentazione.

Attraverso questi meccanismi il sistema garantisce che ognuno acceda solo alla documentazione e alle informazioni cui è autorizzato.

La semplicità dell'accesso è principalmente ottenuta attraverso l'adozione del motore di indicizzazione con cui vengono indicizzati i documenti digitali che alcuni metadati generali contenuti

nel SIPManifest.xml. Al tempo stesso DigiDoc permette di adeguare la modalità di accesso alle esigenze di chi ricerca: infatti consente di impostare filtri di ricerca "strutturati" – con operatori di uguaglianza, somiglianza, maggiore, minore, compreso tra, valorizzato e non valorizzato su alcuni metadati della documentazione conservata, inclusi quelli specifici di certe tipologie documentali.

Dalla lista dei risultati che rispondono ai criteri di ricerca impostati, è possibile accedere al dettaglio dei singoli documenti visualizzando:

- il/i file che compongono il documento;
- i principali metadati trasmessi dal versatore (Oggetto del documento/Intitolazione/ Tipologia Documentale/Identificativo);
- metadati espressi dal sistema in fase di versamento (Data invio in conservazione/Identificativo associato dal sistema di conservazione e trasmesso via rapporto di versamento);
- l'esito dei singoli controlli eseguiti;
- le informazioni del pacchetto di appartenenza del documento (stato del pacchetto, descrizione, data creazione, ecc.).

L'accesso ai documenti è riservato agli utenti autorizzati, secondo le regole impostate nel sistema.

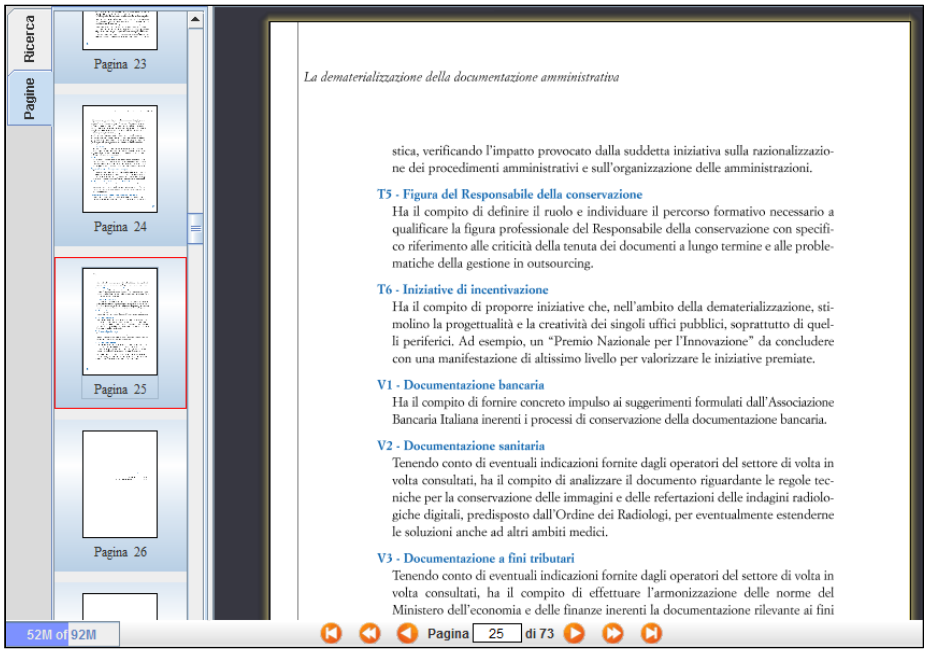

Figura 3: la figura rappresenta la modalità di visualizzazione di un documento, a seguito di ricerca nel sistema di conservazione

Torna all' **INDICE**

7.6.2 Funzionalità di esibizione

Per l'esibizione dei documenti conservati nelle forme prescritte dalla norma il sistema di conservazione ad oggi provvede:

- in cooperazione applicativa, dei web service che in modo completamente automatizzato consentono di recuperare uno o più documenti conservati da parte del sistema/applicativo che li ha versati in conservazione o altri applicativi con opportuni diritti di accesso, unitamente, se richiesti, alle prove di conservazione (Indica di Conservazione firmato e marcato) e/o all'attestato di conformità all'originale conservato;

- attraverso le web GUI con cui RdSC e suoi delegati nonché personale abilitato dei soggetti produttori possono visionare la documentazione conservata.

Per entrambe le modalità, al pacchetto di distribuzione sarà apposto il sigillo qualificato.

Torna all' **INDICE**

7.6.2.1 Esibizione in cooperazione applicativa

Si tratta della modalità tramite cui i sistemi o applicativi che hanno inviato in conservazione i loro documenti possono ottenere dal Sistema di Conservazione, in cooperazione applicativa, l'esibizione di uno o più documenti conservati.

Tale modalità di esibizione viene implementata attraverso servizi – web services – in cui i DIP restituiti sono realizzati ancora una volta come dei file archivio – zip o tar.gz – che contengono:

- un file manifest.xml con i metadati del documento e i puntamenti ai suoi componenti digitali;

- i componenti digitali del documento.

L'esibizione tramite cooperazione applicativa prevede di poter specificare le seguenti opzioni:

- indicazione se è richiesto anche l'Indice di Conservazione attestante che il documento è conservato secondo norma.

L'esibizione tramite cooperazione applicativa può essere eseguita per più documenti con un'unica invocazione del servizio. Infatti nella richiesta di esibizione si può indicare anche:

- una lista di documenti;

- uno o più aggregati di documenti (fascicoli, cartelle, serie, ecc.).

Per l'esibizione in cooperazione applicativa è prevista una duplice modalità di interazione per il sistema/applicativo che sottomette la richiesta:

- sincrona, quando il richiedente resta in attesa della risposta contenente il DIP. Consente l'esibizione di un solo documento alla volta, ed è ammessa solo per documenti di dimensione inferiore ad una soglia prestabilita; qualora la dimensione del documento richiesto superi il valore soglia la richiesta viene respinta;

- asincrona, quando a fronte dell'invocazione del servizio il richiedente ottiene solo un ticket di richiesta con il quale, in un momento successivo, va a richiedere lo stato della sua richiesta e l'eventuale risultato – il DIP – qualora la richiesta sia stata evasa.

L'xml di richiesta delle due modalità, con le possibili opzioni previste, sono rispettivamente i tag RequestEsibizioneSync e RequestEsibizioneAsync dell'xsd RequesteEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato3 - RequestEsibizione.pdf*.

L'xml di risposta nelle due modalità nonché quello del manifest del DIP (nel caso di esibizione asincrona), sono rispettivamente descritti dai tag ResponseEsibizioneSync, ResponseEsibizioneAsync, ResponseGetDIP e DIP dell'xsd ResponseEsibizione.xsd la cui documentazione di dettaglio è nell'allegato *Allegato4 - ResponseEsibizione.pdf*.

Torna all' **INDICE**

7.6.2.2 Esibizione on-line

Questa modalità di esibizione prevede che dalle GUI web di DigiDoc si visualizzi il documento direttamente all'interno della pagina web. Tale modalità di esibizione è disponibile solo per i documenti in formati pdf o formati Office e ascii convertibili in PDF: infatti prevede la conversione in pdf effettuata a carico del sistema di conservazione.

Se il documento è firmato digitalmente e in particolare se si tratta di una busta crittografica di tipo p7m o tsd o m7m, il sistema esibisce il contenuto della busta depurato della/e firme digitali: di ciò viene data evidenza all'utente che a fianco dell'area in cui visualizza il documento vede le informazioni sulle firme ad esso associate: stato di validità (con dettaglio relativo ai vari livelli di controllo della validità); estremi dei certificati di firma; date ed estremi delle eventuali marche temporali presenti nella busta. Peraltro le informazioni sulle firme e sulle marche temporali apposte sul documento vengono mostrate anche in caso di buste crittografiche pdf (PadES) e xml (XAdES) come pure in caso di firma e/o marche detached.

Questa modalità di esibizione è pensata per allargare la fruibilità dei documenti nei casi in cui:

- per il client non vi sia un viewer/reader in grado di restituirgli il documento nel formato originale;

- l'utente che chiede la visualizzazione non voglia o non possa installare sul proprio client il viewer o reader necessario alla restituzione del documento digitale nel formato originale in cui è conservato.

Quando viene utilizzata questa modalità di visualizzazione, se il formato di conservazione del file non è pdf, il sistema dà evidenza del fatto che si tratta di una copia non conforme all'originale conservato e riporta tutte le informazioni del formato originale di conservazione (mimetype, eventuale versione ecc.).

Torna all' **INDICE**

7.6.2.3 Esibizione tramite download da web GUI

Questa modalità di esibizione viene attivata dalla stessa interfaccia web da cui che consente l'esibizione on-line del documento (illustrata nel § precedente). In questo caso però il documento digitale non viene visualizzato all'interno di una pagina web, bensì previo scarico – download – del/i file che lo compongono: dopo di che il client che li ha scaricati può visualizzarli off-line.

Torna all' **INDICE**

7.6.2.4 Esibizione di singolo documento

Laddove viene reso disponibile il download del/dei file del documento vengono date le seguenti possibilità/opzioni:

- in caso di documento firmato digitalmente che sia una busta crittografica p7m, tsd o m7m, vengono forniti due link, uno per scaricare la busta e uno per scaricarne il contenuto depurato delle firme (il file "sbustato");
- scelta se scaricare o meno anche il file xml "Indice di Conservazione", firmato dal Responsabile del servizio di conservazione (o suo delegato) e marcato temporalmente, attestante la conservazione del documento;
- il sistema consente di scaricare la ricevuta di "conformità all'originale conservato" del documento, ovvero un PDF/A che contiene: i riferimenti dell'Ente produttore; gli estremi e i principali dati descrittivi del documento; un timbro digitale – codice a barre bidimensionale - contenente le impronte del/dei componenti digitali del documento.

Torna all' **INDICE**

7.6.2.5 Esibizione tramite Stampa

Anche questa modalità di esibizione è messa a disposizione dalle GUI web di DigiDoc: laddove sono rese disponibili l'esibizione online e il download del/dei file del documento (esibizione tramite

download) è data anche una funzione per effettuarne la stampa: selezionandola il sistema attiva la stampa dei file sul client – purché questo sia già dotato dei programmi necessari ad aprire e mandare in stampa quei file – ed eventualmente, se richiesto, la fa seguire dalla stampa della ricevuta di conformità.

L'esibizione tramite stampa, come quella tramite download, può essere effettuata anche contestualmente per più documenti: una volta effettuata la selezione dei documenti di interesse, con un'unica operazione, si può richiedere la stampa su carta di tutti i documenti selezionati (e delle relative ricevute di conformità).

Torna all' **INDICE**

7.6.2.6 Esibizione di copia conforme all'originale conservato a norma

Il rilascio di copia conforme di un documento conservato viene realizzata da DigiDoc attraverso la produzione della "ricevuta di conformità all'originale conservato", ovvero un PDF/A recante, oltre che la dichiarazione di conformità all'originale conservato, anche un timbro digitale contenente la/le impronte dei file che compongono il documento. Tale timbro è realizzato come codice a barre bidimensionale: sono disponibili SW freeware che consentono di interpretare il contenuto di questi codici a barre (anche da un'immagine che è la scansione della ricevuta stampata su carta) e quindi di recuperare le impronte del documento riportate nel timbro al fine di verificare che coincidano con le impronte calcolate sulla copia del documento che è stata rilasciata.

Se la ricevuta viene firmata, digitalmente o su carta (una volta stampata), questo vale a fornire quella garanzia di autenticità della stessa che consente di realizzare un rilascio di copia conforme ai sensi di quanto previsto dalla legge.

La firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.1. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

Torna all' **INDICE**

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Dalle web GUI che DigiDoc mette a disposizione è possibile selezionare uno o più documenti e aggregati di documenti al fine di richiedere un pacchetto di distribuzione contenente tutta la

documentazione selezionata. Una volta acquisita la richiesta DigiDoc attiva in modo asincrono l'elaborazione del DIP richiesto e quando questo è pronto rende scaricabile il DIP da apposita GUI in cui il richiedente consulta lo stato delle richieste di esibizione effettuate. Il DIP è un archivio compresso che oltre ai documenti richiesti contiene un file indice conforme allo schema documentato in *Allegato4 - ResponseEsibizione.pdf*.

Nei casi previsti dalla normativa, la firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.1. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

Torna all' **INDICE**

7.8 Scarto dei pacchetti di archiviazione

Un obiettivo importante per il sistema è quello di dare supporto, oltre che alla conservazione, anche al processo di selezione e scarto di ciò che non deve più essere conservato perché sono trascorsi i tempi di conservazione stabiliti.

Salvo casi particolari in cui il tempo di conservazione è esplicitato sul singolo documento o aggregazione di documenti al momento dell'invio in conservazione, in generale il tempo di conservazione della documentazione non è esplicitato e viene determinato dal sistema sulla base del massimario di selezione e scarto che stabilisce le regole e i tempi di conservazione agganciandoli ad uno o più dei seguenti dati di definizione del contesto:

- tipologie dei documenti e loro aggregati;
- voci del piano di classificazione;
- tipologie dei procedimenti da cui scaturiscono i fascicoli.

Da notare che laddove non specificato e non ricavabile dalle regole configurate il tempo di conservazione della documentazione viene considerato implicitamente "per tempo illimitato".

Così determinato il tempo di conservazione, DigiDoc è in grado di fornire una proposta di scarto che può essere modulata opportunamente istruendo DigiDoc in merito alla "granularità" dello scarto che si vuole effettuare:

- intere unità di aggregazione (fascicoli o serie);
- singoli documenti.

A partire dalla proposta predisposta in automatico da DigiDoc e trasmessa al Soggetto produttore, quest'ultimo redige la proposta di scarto definitiva e la sottomette alla Sovrintendenza competente

per territorio per autorizzazione. La Sovrintendenza verifica la documentazione contenuta nella proposta e seleziona quella di cui autorizzare lo scarto.

Nel caso la documentazione candidata allo scarto sia di particolare interesse culturale, DigiDoc prevede di poter richiedere ed acquisire un'ulteriore autorizzazione allo scarto da parte del Ministro dei Beni e delle attività culturali e del turismo.

Quando viene acquisita l'autorizzazione allo scarto, gli AIP e i documenti digitali corrispondenti alla documentazione scartata vengono rimossi dallo storage; quanto ai metadati della documentazione scartata memorizzati su RDBMS essi vengono spostati in aree logiche – i.e. tabelle – dedicate alla documentazione scartata e

- perdono le informazioni di stabilità e di pacchetto (diventano inutili dal momento che i documenti digitali vengono fisicamente eliminati), e nelle informazioni di pacchetto vengono aggiunte le informazioni relative all'autorizzazione allo scarto;
- perdono le informazioni di rappresentazione (ormai inutili, a fronte dell'eliminazione fisica dei documenti);
- acquisiscono delle nuove informazioni, quelle relative allo scarto (data, autorizzato da chi).

Torna all' **INDICE**

7.8.1 Cancellazione di pacchetti di archiviazione inviati per errore

Nel caso in cui il produttore abbia versato dei documenti errati e voglia richiederne la cancellazione, dovrà inviare formale richiesta, trasmessa via PEC, all'indirizzo regionetoscana@postacert.toscana.it indicando nella comunicazione:

- l'elenco degli indici dei pacchetti da eliminare,
- la motivazione della cancellazione.

L'intervento effettuato viene annotato nel sistema e la richiesta di intervento verrà archiviata nel DAX.

Torna all' **INDICE**

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Il sistema DigiDoc rispetta lo standard OAIS e lo standard UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; pertanto è in grado di esportare secondo lo schema documentato in *Allegato4 - ResponseEsibizione.pdf* i pacchetti di archiviazione conservati in pacchetti seguendo le regole che permettono la loro importazione in un altro sistema aderente allo standard OAIS.

Allo stesso modo il sistema DigiDoc è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi aderente allo standard OAIS.

L'esportazione dei pacchetti di conservazione (pacchetti di archiviazione) può essere effettuata su supporto elettronico in formato ZIP. Il cliente può scaricare i pacchetti utilizzando un'interfaccia WEB messa a disposizione dal sistema DigiDoc.

Torna all' **INDICE**

7.10 Riversamento

Il riversamento è la procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione Cfr. Allegato 1 Linee Guida AgiD).

DigiDoc prevede le funzionalità di riversamento necessarie a garantire la conservazione della documentazione anche nel medio e lungo termine e che sono implementate secondo quanto previsto dalle normative in vigore.

Tali procedure possono essere avviate su precisa iniziativa del Responsabile del servizio di conservazione, o su richiesta di un soggetto produttore e la loro realizzazione avverrà in conformità alle indicazioni previste dall'allegato 2 alle Linee Guida AgID "Formati di file e riversamento", soprattutto per ciò che riguarda la scelta dei formati di arrivo. Nella scelta dei nuovi formati di file, così come nella scelta metodologica circa l'esecuzione del riversamento, saranno prese in considerazione le peculiarità tecniche del formato sorgente e di quello riversato, con particolare riferimento sia alla perdita di dati e metadati, sia alla diversa qualità o rappresentazione tecnica dei medesimi.

Tutte le informazioni relative ai riversamenti che un documento ha subito durante la sua conservazione in DigiDoc vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento (oltre che essere memorizzate negli audit trail generali del sistema): in particolare, nel caso di sostituzioni con nuovi formati, vengono memorizzati nell'AIP i formati originale e di destinazione e gli eventuali dettagli sul formato originale (versione, rischi connessi, ecc.).

Ogni procedura di riversamento vedrà inoltre il coinvolgimento del pubblico ufficiale per il rilascio dell'attestazione di conformità sottoscritta con firma digitale o altra firma elettronica qualificata, così come stabilito ai sensi dell'art. 23-bis del CAD.

Torna all' **INDICE**

8 Il sistema di conservazione

Le componenti del sistema di conservazione di seguito descritte sono intese sia per gli ambienti di collaudo che per quelli di produzione che sono separati e indipendenti.

Torna all' **INDICE**

8.1 Componenti Logiche

I processi sopra illustrati corrispondono ad altrettanti gruppi di **servizi applicativi** previsti dalla soluzione DigiDoc:

- DigiDocWePo (versamento): permettono l'invio della documentazione, sia singoli documenti che loro eventuali aggregazioni, al sistema di conservazione nonché l'aggiornamento di quanto già inviato in precedenza;
- DigiDocCtrl: svolgono i controlli sulla documentazione inviata in conservazione, necessari per l'accettazione da parte del sistema di conservazione. Sono controlli sia sui dati di descrizione che sui componenti digitali (file) da conservare, in particolare sui loro formati e su eventuali firme digitali e marche temporali;
- DigiDocConS: comprendono le funzionalità espressamente richieste dalla normativa italiana per la Conservazione dei documenti;
- DigiDocWeCS: consentono le ricerche su tutto il materiale conservato nel sistema, sfruttando tutti i dati di descrizione della documentazione conservata come chiavi di ricerca;
- DigiDocMoEs: permettono di verificare la corretta funzionalità del sistema in tutti i suoi aspetti e componenti, consentendo al Responsabile del servizio di Conservazione ed eventuali autorità di vigilanza di assolvere ai propri compiti di verifica ordinaria e straordinaria;
- DigiDocAdmi: trasversali a tutto il sistema, consentono di aggiornare e storicizzare strumenti e dati di definizione del contesto che sono funzionali alla descrizione degli archivi (es.

organigrammi, piani di classificazione, tipologie documentali, massimari di selezione e scarto)

L'architettura applicativa di DigiDoc, coerentemente con il modello di sviluppo a servizi (SOA), si compone di moduli separati, seppur interdipendenti, che a loro volta composti da servizi e funzionalità applicative, permettono di gestire i processi identificati. Questa separazione consente di installare le varie componenti su sistemi fisici differenti.

Torna all' **INDICE**

8.2 Componenti Tecnologiche

Schema e descrizione delle componenti tecnologiche (strumenti informatici a supporto delle funzionalità del sistema di conservazione) che implementano il sistema di conservazione.

Torna all' **INDICE**

8.2.1 Software di base

- http Server:
  - CentOS 6.5/7.0;
  - Apache HTTP Server;
  - Java Runtime;
  - JDK e JRE Compatibility level;
- Application Server:
  - CentOS 6.5/7.0;
  - Apache Tomcat;
  - Java Runtime;
  - JDK e JRE Compatibility level;
- Batch Server:
  - CentOS 6.5/7.0;
  - Java Runtime;
  - JDK e JRE Compatibility level;
- DB Server:
  - CentOS 6.5 staging;

- Oracle Linux 6.6;
- Java Runtime.

Torna all' **INDICE**

8.2.2 Framework di sviluppo utilizzati

NOME	UTLIZZO
JAX-WS (Java API for XML Web Services)	Per realizzare web-service – SOAP e REST – e client che utilizzano XML per comunicare.
Jersey	Per realizzare web-service REST e i relativi client (è l'implementazione di riferimento della specifica JAX-RS).
Smart GWT	Framework di base per la realizzazione delle web UI: si occupa del rendering del framework ajax GWT appoggiandosi alle librerie Smartclient.
Spring	Per realizzare i componenti come applicazioni java enterprise facilmente configurabili e altamente riusabili.
Hibernate	ORM utilizzato per l'accesso al database.

Torna all' **INDICE**

8.3 Componenti Fisiche

Le componenti fisiche del servizio di conservazione sono localizzate in:

- sito primario, situato presso la struttura del TIX, via San Piero a Quaracchi 250, Firenze;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR), presso il data centre di Cesano Maderno (MB) di Telecom Italia;
- sito secondario, avente almeno le stesse caratteristiche di sicurezza di quello primario, per la replica dei documenti, presso il data centre di di Engineering Informatica, in Viale Carlo Viola 76, a Pont-Saint-Martin (AO).

Gli impianti tecnologici del TIX sono all'interno del perimetro recintato della sede e sono alloggiati sia all'interno che all'esterno dell'edificio che ospita i CED; ad essi si accede attraverso porte chiuse a chiave e/o sistemi di controllo accessi con badge.

Le sale CED sono comunque separate fisicamente dalle sale dell'edificio che ospitano gli impianti di alimentazione elettrica.

L'accesso agli impianti tecnologici è consentito soltanto alle persone addette alla conduzione e manutenzione degli impianti stessi.

Gli impianti sono presidiati in orario esteso da personale qualificato e con servizio di reperibilità h24.

Il sistema di monitoraggio, controllato H24 dagli operatori del NOC, consente di verificare a distanza lo stato degli apparati e di attivare il personale di manutenzione o la reperibilità. Per garantire il supporto di secondo livello le console del sistema di monitoraggio sono accessibili in occasione dell'attivazione del piano di continuità.

Il sito è dotato di impianti per:

- rilevazione incendi: i locali del DC e alcuni dei locali Impianti sono dotati di un impianto centralizzato di rilevazione incendi, i cui allarmi sono riportati nella cabina di Vigilanza e nel NOC;
- estinzione incendi: i locali del DC e i locali Impianti sono dotati di un sistema automatico di estinzione incendi, compartimentato e pilotato dal sistema di rilevazione; in tutti questi locali l'impianto agisce nello spazio libero dell'ambiente e nel sottopavimento; nelle Sale energia sono presenti anche degli erogatori a scarica automatica (non pilotati dall'impianto di rilevazione) posti all'interno dei quadri elettrici di potenza e degli armadi batterie; in tutti i locali, compresi gli spazi di servizio e di transito, è presente un numero adeguato di estintori della tipologia adatta alle specifiche circostanze,
- impianto elettrico: la continuità dell'alimentazione delle macchine è garantita da un impianto elettrico così composto:
    - cabina di media tensione (15.000 V), situata all'esterno dell'edificio principale, (cabina di consegna) alimentata da una linea fornita da ENEL;
    - due linee di trasformazione di alimentazione indipendenti, alimentate dalla cabina di consegna, ognuna composta da:
        - un trasformatore 15.000/400 V che assicura l'alimentazione in bassa tensione alla linea di appartenenza, installato in una cabina di trasformazione situata all'esterno dell'edificio principale;
        - un gruppo elettrogeno, che garantisce l'alimentazione preferenziale in caso di prolungata interruzione di energia da parte dell'ente erogatore, con inserzione automatica in caso di mancanza rete. L'autonomia è di 24 ore a pieno carico senza rifornimento; il gruppo è posizionato su una struttura metallica sopraelevata di tre metri rispetto al piano stradale, al fine di garantire il funzionamento degli apparati anche a fronte di eventuali

allagamenti dell'area su cui insiste la sede; è un'installazione a cielo aperto, monitorata a distanza e sorvegliata dalle telecamere a circuito chiuso.

- UPS che garantisce la continuità di alimentazione in caso di breve interruzione di energia elettrica (autonomia di circa 10 minuti a pieno carico). L'UPS, insieme agli armadi batterie e ai quadri elettrici della distribuzione primaria, è installato in una Sala energia situata all'interno dell'edificio principale e separata dalle sale CED. Gli UPS hanno ridondanza N+1.

- doppia alimentazione elettrica indipendente (un'alimentazione da ciascuna linea) su ogni rack ospitante gli apparati IT;
- Sistema STS di interconnessione tra le sale energia in grado garantire la doppia alimentazione alle sale CED anche con una sola sala energia operativa.

- impianto di condizionamento: il DC è dotato di un sistema di condizionamento misto differenziato in funzione degli ambienti da climatizzare. In particolare:
  - CDZ ad espansione diretta di tipo under; la ridondanza N+1 è garantita dal dimensionamento di progetto) dal collegamento elettrico alle linee preferenziali di alimentazione, e dalla possibilità di commutare l'alimentazione del CDZ centrale tra le due linee;
  - Il CED AD è un ambiente progettato per l'alta densità e quindi è stato dotato di un raffreddamento di precisione costituito da condizionatori inseriti nelle file di rack; i rack sono a loro volta assemblati in due linee parallele, con il retro contrapposto e chiuso in modo da segregare l'aria calda generata dal raffreddamento degli apparati IT. Il vettore termico è l'acqua refrigerata, prodotta da una coppia di chiller e trasportata da due linee di raffreddamento indipendenti e interscambiabili.
    I due chiller sono macchine della capacità di 155 KWf ciascuno, collegati ognuno ad una linea di alimentazione diversa. Sono posti all'esterno del primo piano dell'edificio su una piattaforma a cielo aperto non accessibile e sorvegliata con telecamere a circuito chiuso e sono monitorati a distanza.
    La ridondanza di alimentazione elettrica dei chiller, la duplicazione delle linee di distribuzione acqua (ognuna con una coppia di pompe per la circolazione del refrigerante), il serbatoio di accumulo del refrigerante e la distribuzione a matrice delle alimentazioni elettriche e idrauliche sui CDZ InRow permettono di garantire il condizionamento del CED in qualsiasi condizione tranne quella di un evento disastroso.
    Le due Sale energia e la Sala TLC sono dotate di CDZ ad espansione diretta di tipo under. Il condizionamento di questi ambienti presenta un livello di ridondanza 2N.

Criteri costruttivi: la dislocazione del Data Center e l'infrastruttura che lo compone rappresentano una garanzia rispetto a fenomeni di allagamento per inondazione; la risposta progettuale a questa

tipologia di rischio è la collocazione al di sopra del livello di allagamento dei gruppi elettrogeni e delle Sale energia (UPS e distribuzione elettrica primaria), oltre che ovviamente tutti i locali CED.

Torna all' **INDICE**

8.3.1 Componenti HW

L'infrastruttura fisica dei sistemi è costituita da apparati con tecnologia CICSCO UCS che garantisce elevata potenza elaborativa, ridondanza delle connessioni LAN e SAN, capacità di sostituzione di un componente HW guasto attraverso componente spare e configurazione SW.

I sistemi sono server virtuali realizzati su tecnologia VMWARE ESX.

In caso di fault dei sistemi la ripartenza è garantita sfruttando la HA VMWARE.

Tutte le componenti HW utilizzate dal servizio (chassis, lame, storage, SAN, LAN, firewall) sono ridondate ed in configurazione di alta affidabilità.

Torna all' **INDICE**

8.4 Procedure di gestione e di evoluzione

- Conduzione e manutenzione applicativa del sistema di conservazione (manutenzione adeguativa e correttiva): si seguirà quanto riportato nell'accordo di servizio siglato tra Regione Toscana e il fornitore della piattaforma Digidoc, nonché quanto previsto dalle procedure del Sistema per la Gestione della Qualità di quest'ultimo;
- monitoraggio delle componenti fisiche e applicative del sistema di conservazione: cfr. capitolo 9;
- conduzione e manutenzione dell'infrastruttura hardware (manutenzione evolutiva e correttiva): vedere paragrafo successivo
- gestione e conservazione dei log (anche in accordo con l'ente Produttore)): vedere paragrafo successivo
- verifica periodica di conformità a normativa e standard di riferimento: sono svolti audit periodici da parte di Regione Toscana, sia per verificare che siano seguite le procedure, sia per verificare che le procedure siano allineate con la normativa e gli standard applicabili e aggiornati (procedure interne "Gestione degli audit" e "Gestione dei riesami del SGSI").

Torna all' **INDICE**

8.4.1 Procedure per la conduzione e manutenzione dell'infrastruttura hardware (manutenzione evolutiva e correttiva)

L'esercizio dell'infrastruttura HW e SW utilizzata per l'erogazione dei servizi del TIX si basa sul modello ITIL.

Sono quindi adottate procedure documentate che coprono:

- La gestione degli incident, con particolare attenzione agli aspetti legati alla sicurezza fisica e logica.
- Il Service Desk, come unico punto di contatto per tutti gli aspetti legati all'infrastruttura HW e SW;
- L'event management per il monitoraggio e la gestione delle procedure schedulate;
- Il change management; i change sono valutati in base a diversi parametri, quali ad esempio:
    - l'entità dell'impatto sia sull'operatività del servizio erogato, sia sui componenti HW e SW implicati;
    - la tipologia dell'intervento, espresso in termini di manutenzione correttiva, evolutiva, adeguativa;
    - l'urgenza degli interventi, pianificabili o meno (es. interventi per i quali è necessario un fermo del sistema che può essere programmato o accidentale, a seconda delle cause che lo determinano).

Sulla base dell'analisi dell'impatto si provvede alla pianificazione del change, tenendo in considerazione le modalità operative per un eventuale ritorno all'indietro.

I sistemi HW e SW sono monitorati H24 con strumenti in grado di rilevare dati sulla situazione corrente e per avere un controllo sull'andamento delle risorse, anche ai fini del processo di capacity.

La gestione degli incident del TIX è descritta nel documento TIX-ITIL-PRO-001-Incident Management e al paragrafo 9.4.

Il processo di cambiamento dei servizi del TIX è attuato in conformità a quanto definito nel documento TIX-ITIL-PRO-008 Change Management.

Torna all' **INDICE**

8.4.2 Procedure per la gestione e conservazione dei log (anche in accordo con il Titolare degli oggetti di conservazione)

I log di sistema sono considerati parte integrante del patrimonio informativo. Per tale motivo sono definite le politiche relative alla gestione dei log sulla base delle prescrizioni di legge e degli impegni contrattuali.

I log applicativi permettono di tracciare le azioni svolte sul sistema, in modo da ricostruirle in caso di necessità.

I log sono raccolti attraverso strumenti centralizzati che garantiscono prestazioni nella raccolta (numero di eventi al secondo) e forniscono adeguati strumenti di analisi e di protezione. La protezione è assicurata dallo strumento di log collection, usato per conservare i log.

I log di sistema sono relativi ad eventi di sistema, di operazioni autorizzative, di anomalie, inviati da apparti di rete e sistemi.

Verifica periodica di conformità a normativa e standard di riferimento: sono svolti audit periodici da parte di Regione Toscana, sia per verificare che siano seguite le procedure, sia per verificare che le procedure siano allineate con la normativa e gli standard applicabili e aggiornati (procedure interne “Gestione degli audit” e “Gestione dei riesami del SGSI”).

I log applicativi sono conservati per almeno un anno e sono oggetto di controllo accessi e backup per assicurarne l’integrità.

Torna all’ **INDICE**

8.4.2.1 Riesame dei log

I log sono riesaminati in caso di eventi particolari che possono essere stati originati da azioni che necessitano approfondimenti.

Torna all’ **INDICE**

8.4.2.2 Clock di sistema

L'NTP è erogato da due server presso il TIX, a loro volta sincronizzati con un pool di server riconosciuto come affidabile a livello di comunità Internet. Il controllo di affidabilità è effettuato ad ogni sincronizzazione. I sistemi presso il TIX, per assicurare il livello di sicurezza, non si possono collegare autonomamente a NTP server esterni.

Torna all’ **INDICE**

9 Monitoraggio e controlli

9.1 Procedure di monitoraggio

Il servizio è strutturato per fornire servizi continuativi con operatività H24 presidiata, garantendo:

- Implementazione dei sistemi di monitoraggio e relativo aggiornamento;
- Rilevazione degli eventi di allarme;
- Tracciamento su Sistema di Ticketing;
- Applicazione dell'opportuna procedura di fixing o innesco della Procedura di Escalation Operativa / Informativa;
- Follow-up del problema in caso di escalation;
- Valutazione dell'utilizzo di risorse rispetto all'andamento passato e futuro del servizio (Capacity planning);
- andamento del servizio, rispetto agli SLA di disponibilità, affidabilità ed esecuzione richieste di servizio.

A supporto delle attività di Monitoring è stato sviluppato un apposito Sistema Informativo ad esclusivo uso del personale tecnico dove sono mantenute e costantemente aggiornate le informazioni riguardanti ogni singolo apparato/sistema monitorato e le procedure da attuare in caso di evento la cui azione correttiva è stata predefinita.

Il monitoraggio dei sistemi viene effettuato con le seguenti modalità:

- monitoraggio istantaneo; vengono utilizzati strumenti per una rapida ed efficace gestione degli eventi; un evento anomalo può essere classificato per l'ambito in cui accade (hardware, software, rete), per il contesto (servizio online, eccezione in un'esecuzione batch, back-up, ecc.) e per la gravità (impatto totale, parziale o nullo sul servizio, ecc.). Una dashboard consente al presidio sistemistico di avere visibilità h24 dell'insorgere di situazioni anomale. Il sistema è realizzato integrando diversi strumenti SW come XYmon, Openms. Il SW di monitoraggio utilizza sia agent (ad es. sui server, sia agentless, ad es. per apparati di rete. Il SW di monitoraggio è configurato anche per controllare il superamento di soglie associate agli indicatori di utilizzo risorse (ad es. CPU, disco, Java VM, etc.).

  Oltre ai servizi e sistemi il monitoraggio è in grado di rilevare anomale sulla Rete Telematica Regione Toscana (RTRT) e sugli impianti tecnologici del CED (alimentazione elettrica, condizionamento, temperatura e umidità relativa attraverso il SW StruXureWare della APC.

  Attraverso il monitoraggio istantaneo sono tenute sotto controllo le procedure ricorrenti (ad es. backup).
- monitoraggio andamentale; vengono utilizzati strumenti che permettono una raccolta storica dei dati di monitoraggio, effettuandone delle aggregazioni secondo opportune configurazioni; oltre a permettere una verifica della disponibilità del servizio (SLA),

permettono un'efficace presa visione dell'andamento delle risorse ai fini di un corretto Capacity Planning.

Infatti, il SW conserva la storia di tutti i cambiamenti di stato e l'andamento delle risorse per almeno un anno.

Attraverso i dati del Sistema di monitoraggio e dei Ticket (incident, richieste di servizio) viene predisposta la reportistica sull'andamento del servizio, prodotta trimestralmente ma con aggregato base mensile, per riscontro rispetto agli SLA.

Il servizio di Monitoraggio viene erogato attraverso una Control Room dislocata presso il TIX situata in ambiente protetto (guardiana armata, sistemi autonomi di riscaldamento e condizionamento) e dotata di sistemi di supporto video dedicati (maxi schermi, postazioni audio-video; il presidio TIX opera in modalità H24; gli operatori tengono sotto controllo lo stato dei sistemi e dei servizi; l'obiettivo è il Monitoring Proattivo per rilevare condizioni di criticità e porvi rimedio prima che l'insorgenza del problema generi un disservizio percepibile all'utente.

La procedura prevede che all'insorgere di una anomalia o di un allarme gli operatori, traccino l'evento sul sistema di Ticketing ed utilizzando una "Knowledge Base" mettano in atto le azioni previste (esecuzione di procedure di recovery, dispatching a team sistemistici specializzati on site o remoti ovvero al team responsabile della conduzione del servizio).

A supporto di queste procedure vi sono il sistema di Trouble Ticketing, basato su OTRS, ed il sistema per la documentazione di esercizio, basato su Alfresco.

Tutti gli strumenti utilizzati per monitoraggio e gestione sono oggetto del servizio di Disaster Recovery e quindi operativi anche in caso di switch del servizio sul sito DR.

Torna all' **INDICE**

9.2 Procedure di monitoraggio per il cliente

Gli SLA sono forniti ai clienti con report trimestrali che possono essere richiesti a Regione Toscana.

Torna all' **INDICE**

9.3 Verifica dell'integrità degli archivi

La verifica dell'integrità dei dati è effettuata mediante l'esecuzione di una procedura schedulabile che può essere configurata per scegliere la profondità di osservazione (file analizzati da oltre un determinato periodo) ed agisce sui pacchetti che rispettano il criterio impostato.

Per ogni file contenuto nell'indice viene verificata la sua presenza e viene controllata la corrispondenza della sua impronta con quella indicata nell'indice. Per ogni elaborazione viene prodotto un report in formato xml, riportante l'esito della verifica per ogni indice e per ogni documento contenuto al suo interno.

La procedura sarà schedulata per essere eseguita con frequenza tale da garantire che:

- il tempo di esecuzione sia inferiore alla periodicità di schedulazione;
- sia possibile effettuare il restore dei dati a partire dai backup effettuati con la cadenza prestabilita (ovvero la periodicità della schedulazione deve essere minore del tempo di retention dei backup).
- I backup seguono le seguenti regole:
    - Frequenza almeno ogni 24 ore (con anche alternanza di backup full settimanali e incrementali giornalieri) per macchine virtuali, database, log.
    - conservazione almeno di 15 giorni.

Torna all' **INDICE**

9.4 Soluzioni adottate in caso di anomalie

La procedura applicabile è "Gestione degli incidenti del TIX", che specifica le modalità di contatto tra utenti, l'help desk, la conduzione sistemistica e la conduzione applicativa. In particolare, ogni entità (help desk, conduzione sistemistica e conduzione applicativa) contatta le altre attraverso sistemi di ticketing tra loro interfacciati.

Ogni anomalia è risolta dall'entità più adeguata, che predispone anche un rapporto di incidente.

Le anomalie possono essere riscontrate attraverso:

- strumenti di monitoraggio delle funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi, presso la conduzione applicativa;
- strumenti di monitoraggio delle prestazioni dei sistemi e della rete presso la conduzione sistemistica;
- chiamate degli utenti all'help desk (come specificato nella documentazione che descrive il servizio erogato al singolo Ente Produttore.

Torna all' **INDICE**