

Manuale della Conservazione

di DocFlow Italia S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>	10/03/2018	Alessandro De Pasquale	Legal Local Compliance
<i>Verifica</i>	11/03/2018	Maria Elena Medina	Resp. Servizio Conservazione
<i>Controllo</i>	13/03/2018	Francesca Di Bella	Resp. Sicurezza informazioni
<i>Approvazione</i>	16/04/2018	Carlo Petti	Amministratore delegato

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1	18/05/2015	Versione iniziale	
2	4/02/2016	Correzione errori	
2.1	19/05/2016	Riorganizzazione indice	
2.2	20/05/2016	Correzione definizioni, eliminazione refusi, precisazioni relative al processo di conservazione, ridefinizione organigramma, riformulazione cap. 8 e 9	
2.3	26/09/2016	Aggiornamento ruoli e incarichi, aggiornamento riferimenti normativi aggiunto nuovo formato, correzione refusi.	
2.4	23/01/2017	Correzione refusi	
2.5	16/04/2018	Aggiunto tipo documenti Aggiornamento procedure Correzione refusi	

INDICE DEL DOCUMENTO

1	SCOPO, AMBITO E RIFERIMENTI DEL DOCUMENTO	7
1.1	Scopo del Manuale	7
1.2	Contesto di riferimento.....	8
1.2.1	<i>Comunità di riferimento.....</i>	8
1.3	Applicabilità.....	8
1.4	Processo di nomina del Responsabile della Conservazione e	8
1.5	Riferimenti a documentazione di dettaglio	8
2	TERMINOLOGIA (GLOSSARIO E ACRONIMI)	10
2.1	Glossario.....	10
2.2	Acronimi	14
3	NORMATIVA E STANDARD DI RIFERIMENTO.....	16
3.1	Normativa di riferimento.....	16
3.2	Standard di riferimento	17
4	RUOLI E RESPONSABILITÀ.....	18
4.1	Responsabile della conservazione.....	21
4.2	Modello organizzativo.....	22
5	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE.....	23
5.1	Organigramma.....	23
5.2	Strutture organizzative.....	24
6	OGGETTI SOTTOPOSTI A CONSERVAZIONE.....	26
6.1	Documenti conservati.....	26
6.2	Pacchetto di versamento.....	27
6.3	Pacchetto di archiviazione.....	30
6.4	Pacchetto di distribuzione.....	38
7	II PROCESSO DI CONSERVAZIONE	41
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	42
7.1.1	<i>Ricezione documenti via WEB.....</i>	44
7.1.2	<i>Ricezione documenti via FTP/SFTP.....</i>	44
7.1.3	<i>Ricezione documenti ERP.....</i>	44
7.1.4	<i>Ricezione documenti E-mail/PEC.....</i>	44
7.2	Verifiche effettuate sui pacchetti di versamento e generazione del rapporto di versamento e presa in carico.....	45
7.2.1	<i>Verifica segnalazione di errore.....</i>	45
7.2.2	<i>Risoluzione anomalia.....</i>	45

7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico.....	45
7.4	Rifiuto/Acettazione del pacchetto di versamento.....	46
7.5	Preparazione e gestione del pacchetto di archiviazione.....	47
7.5.1	Generazione del pacchetto di archiviazione.....	47
7.5.1.1	Notifica pacchetto in attesa di firma digitale non automatica	48
7.5.2	Firma digitale.....	48
7.5.2.1	Gestione del pacchetto di archiviazione	48
7.5.3	Notifica conservazione	48
7.6	Preparazione e gestione dei pacchetti di distribuzione	48
7.6.1	Definizione del pacchetto di distribuzione.....	49
7.6.2	Creazione del pacchetto di distribuzione.....	49
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del Pubblico Ufficiale nei casi previsti	49
7.7.1	Intervento del Pubblico Ufficiale	50
7.8	Scarto dei pacchetti di conservazione	51
7.8.1	Chiusura del servizio di conservazione.....	51
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori.....	52
7.10	Attività proprie di gestione dei sistemi informativi:	52
7.10.1	conduzione e manutenzione del sistema di conservazione.....	52
7.10.2	monitoraggio del sistema di conservazione.....	52
7.10.3	change management.....	53
7.10.4	verifica periodica di conformità a normativa e standard di riferimento.....	53
8	IL SISTEMA DI CONSERVAZIONE	54
8.1	Componenti Logiche	54
8.2	Componenti Tecnologiche.....	55
8.3	Componenti Fisiche.....	56
8.4	Procedure di Gestione e di evoluzione.....	57
8.4.1	Start up del servizio	57
8.4.1.1	Gestione apertura commessa in SaaS.....	57
8.4.1.2	Apertura commessa Servizi.....	57
8.4.1.3	Organizzazione del servizio	57
8.4.1.4	Richiesta attivazione del canale di comunicazione.....	58
8.4.1.5	Approvazione dell'attività di attivazione del canale di comunicazione.....	58
8.4.1.6	Attivazione del canale di comunicazione.....	58
8.4.1.7	Configurare servizi di conservazione.....	58

8.4.1.8	<i>Collaudo e validazione</i>	59
8.4.2	<i>Modifiche al sistema</i>	59
8.5	Gestione e conservazione dei log	60
9	MONITORAGGIO E CONTROLLI	61
9.1	Procedure di monitoraggio	61
9.2	Controlli	62
9.2.1	<i>Mantenimento della leggibilità nel tempo</i>	62
9.2.2	<i>Controlli di processo</i>	62
9.2.3	<i>Controlli di sistema</i>	63
9.2.3.1	<i>Riesame del servizio</i>	63
9.2.3.2	<i>Auditing generale del servizio</i>	64
9.3	Soluzioni adottate in caso di anomalia	65
9.3.1	<i>Incident management</i>	65

INDICE DELLE FIGURE

Figura 1 - Organigramma 23

Figura 2 - Componenti logiche 54

Figura 3 - Componenti tecnologiche..... 55

Figura 4 - Componenti fisiche..... 56

1 SCOPO, AMBITO E RIFERIMENTI DEL DOCUMENTO

1.1 Scopo del Manuale

In questo Manuale si descrive il sistema di conservazione di DocFlow Italia. S.p.A. (di seguito DocFlow) denominato AipaDoc, con evidenza dell'organizzazione, dei soggetti coinvolti e i ruoli svolti dagli stessi, del modello di funzionamento. Vengono riportate la descrizione del processo, delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento del sistema di conservazione.

Il Manuale della Conservazione costituisce requisito imprescindibile per la procedura di accreditamento come conservatore presso l'Agenzia per l'Italia Digitale, quindi per il riconoscimento del possesso dei requisiti di più alto livello, in termini di qualità e sicurezza del Servizio erogato da DocFlow. Il Manuale di Conservazione è lo strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle del DPCM del 3 dicembre 2013 (di seguito "Regole Tecniche") del sistema di conservazione.

In particolare sono descritte le procedure operative adottate da DocFlow per il procedimento di conservazione elettronica conforme alle vigenti leggi e realizzato attraverso l'apposito Servizio in outsourcing per ciascun cliente.

Il documento descrive le procedure adottate da DocFlow secondo quanto definito dal contratto stipulato tra le parti e nei relativi Allegati, in conformità alle normative e prassi in materia.

Il presente Manuale descrive in line generale il sistema messo a disposizione da DocFlow. I dettagli relativi alle Specificità di Contratto relativi agli accordi stipulati con ogni singolo Cliente.

Il servizio è erogato attraverso una piattaforma di servizio specializzata, ospitata nella server farm di DocFlow e con adeguato supporto sistemistico per garantire l'integrità dei dati e per mantenere la piattaforma applicativa al massimo livello di disponibilità ed efficienza.

Conformemente a quanto previsto dalle Regole Tecniche all'art. 5 comma 2, lett. B, il servizio viene proposto da DocFlow in qualità di soggetto affidatario privato che offre idonee garanzie organizzative e tecnologiche e consente la conservazione elettronica in conformità alle leggi di documenti elettronici e/o analogici, in outsourcing.

Il manuale riassume i compiti che sono descritti dalle Regole Tecniche e dal Codice dell'Amministrazione Digitale, si seguito anche "CAD" (Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni).

Il presente Manuale è prodotto in formato digitale da parte di DocFlow, pubblicato in apposito repository del Servizio ad uso interno DocFlow e fornito al Cliente.

Nel caso di eventuali aggiornamenti e adeguamenti viene inviata copia al Responsabile di progetto del Cliente o DocFlow.

[Torna al sommario](#)

1.2 Contesto di riferimento

Il Servizio di conservazione è erogato in modalità di Full Outsourcing è conforme ai dettami dell'articolo 44 del CAD in base al quale la conservazione può essere svolta affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale.

[Torna al sommario](#)

1.2.1 Comunità di riferimento

DocFlow opera al momento, per quanto riguarda la conservazione dei documenti, esclusivamente nell'ambito del settore privato e tratta documenti indicati agli articoli da 2214 a 2220 del codice civile.

In particolare sono trattati i documenti relativi all'area amministrativa/contabile.

[Torna al sommario](#)

1.3 Applicabilità

Il manuale si riferisce al Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione che prevede, all'art 14, la possibilità di adeguare i sistemi esistenti all'entrata in vigore del citato decreto, entro 36 mesi.

Il documento "Piano di migrazione dei sistemi di conservazione in SaaS" specifica i tempi e i modo di migrazione dei singoli clienti alle nuove regole. Per ciascun cliente sono state applicate le regole previste dalla precedente normativa fino al termine del processo di migrazione.

[Torna al sommario](#)

1.4 Processo di nomina del Responsabile della Conservazione

Il responsabile della conservazione è la persona fisica interna all'organizzazione del soggetto Titolare dei documenti.

In ogni caso la nomina è fatta dall'ente/persona del titolare dei documenti che abbia i poteri opportuni per tale compito.

[Torna al sommario](#)

1.5 Riferimenti a documentazione di dettaglio

Nel presente documento sono parzialmente descritti aspetti architetturali e processi in essere.

Per un maggior dettaglio tecnico/funzionale si rimanda ai seguenti documenti:

- Documento di dettaglio del processo – Specificità di contratto
 - o Specificità di contratto, contenute nel Contratto di servizio, per gli aspetti attinenti le implementazioni tecniche della Conservazione, non allegato al presente Manuale, predisposto sulla base dello specifico contesto progettuale del Cliente;
 - o Responsabile della conservazione;

- o Ruoli, dati anagrafici e di contatto;
- o Descrizione particolarità del processo;
- o Tabelle e indicazioni tecniche per il trasferimento e l'identificazione dei documenti;
- o Descrizione dei pacchetti informativi qualora differiscano da quelli standard.

[Torna al sommario](#)

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

2.1 Glossario

Le definizioni di seguito elencate, utilizzate nell'ambito del presente Manuale, fanno riferimento a quanto riportato in Allegato 1 al DPCM 3 dicembre 2013.

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
AipaDocs	Servizio di conservazione di DocFlow, erogato in modalità di outsourcing
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Cliente	Società Cliente ed eventualmente, le società del gruppo che hanno sottoscritto le opportune contratti per l'affidamento del Servizio di Conservazione.
Codice o CAD	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici

conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall’Agenzia per l’Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall’Agenzia per l’Italia digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell’articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DocFlow	Società DocFlow Italia. S.p.A. (anche DocFlow)
uplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l’estensione del file
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l’evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all’aggregazione documentale informatica, in modo da consentirne l’individuazione
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	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l’applicazione alla prima di una opportuna funzione di hash
insieme minimo di metadati del documento informatico integrità	complesso dei metadati, la cui struttura è descritta nell’allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l’intero ciclo di gestione dei documenti

log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM 3/12/2013
pacchetto di archiviazione	Detto anche PdA, pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
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
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
produttore	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 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
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali

responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
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
titolare dei documenti	Persona fisica o giuridica titolata a disporre dei documenti. Solitamente coincide con Cliente
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse

[Torna al sommario](#)

2.2 Acronimi

Di seguito i principali acronimi utilizzati nel documento e relative definizioni:

TERMINE	DEFINIZIONE
AgID	Agenzia per l'Italia Digitale
CA	Certification Authority, cioè ente accreditato per l'emissione e la gestione di certificati di firma qualificata
CAD	Codice dell'amministrazione digitale, Decreto Legislativo 7 marzo 2005, n. 82 e successive modifiche/integrazioni
CADES-T	Cryptographic Message Syntax Advanced Electronic Signature, formato standard di firma che genera una busta crittografica (file con estensione. p7m), con informazioni aggiuntive rispetto al formato base (CADES-BES) per includere la marca temporale
<Cliente>	Società Cliente ed eventualmente, le società del gruppo che hanno sottoscritto le opportune contratti per l'affidamento del Servizio di Conservazione.
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate revocation list, liste di certificati digitali revocati
DigitPA	In precedenza Centro nazionale per l'informatica nella pubblica amministrazione
DL	Decreto legge
DLgs	Decreto legislativo
DM	Decreto ministeriale
DMEF	Decreto Ministero dell'Economia e delle Finanze
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
HASH	Impronta informatica di un documento ottenuta applicando una "funzione di hash" e costituita da una sequenza di simboli binari.
HSM	Hardware Security Module, dispositivo che consente di ospitare diverse chiavi di firma e in grado di garantire elevatissimi livelli di sicurezza, affidabilità e performance in termini di velocità di esecuzione delle operazioni.
http	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
https	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
IPdA	Indice del Pacchetto di Archiviazione – evidenza informatica associata ad ogni pacchetto di archiviazione contenente un insieme di informazioni articolate secondo lo standard SInCRO
L	Legge
NAS	Network Attached Storage, dispositivi ad alta capacità, sicurezza ed affidabilità per la memorizzazione dei dati
PADES-T	PDF Advanced Electronic Signature, formato standard di firma su PDF, con informazioni aggiuntive rispetto al formato base (PADES-BES) per includere la marca temporale
PdA	Pacchetto di archiviazione

PDF	Portable Document Format
PKCS#7	Standard della sintassi dei messaggi crittografici, usato per firmare o criptare messaggi in una infrastruttura a chiave pubblica (PKI).
PKI	Public Key Infrastructure, cioè l'infrastruttura che crea e gestisce i certificati (qualificati) di firma elettronica basati su crittografia a chiave pubblica
Piano della Sicurezza DocFlow	Piano della sicurezza del sistema di conservazione
PO	Process Owner
RDC	Responsabile della Conservazione
SinCRO	Supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI11386:2010) - Standard nazionale in linguaggio xml, riguardante la struttura dell'insieme di dati a supporto del processo di conservazione
STS	Signature Time stamping, marca temporale apposta alla Firma mediante richiesta al servizio centralizzato di Time Stamping Server della Certification Authority DocFlow per l'oggetto Firma
Synergy / Synergy for service	Piattaforma tecnologica utilizzata dal Servizio di conservazione in outsourcing di DocFlow
TSA	Time Stamping Authority, infrastruttura necessaria a realizzare e svolgere la funzione di timbratura temporale.
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee –CCIR)
Web	World Wide Web - principale servizio di Internet che permette di navigare e usufruire di un vasto insieme di contenuti

[Torna al sommario](#)

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- 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;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- 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, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Deliberazione Cnipa 21 maggio 2009, n. 45 (come modificata dalla determinazione dirigenziale DigitPA n. 69/2010) – Regole per la creazione dei certificati di firma e di marca che quelle per il loro utilizzo, riconoscimento e verifica;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82;
- Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni;
Decreto del Ministro dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
- Regolamento (ue) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- Decreto Legislativo del 26 agosto 2016, n. 179 - Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.

[Torna al sommario](#)

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° marzo 2015.

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

[Torna al sommario](#)

4 RUOLI E RESPONSABILITÀ

Di seguito sono indicati le attività svolte e i nominativi delle persone che ricoprono i ruoli principali – come specificati nel documento “Profili professionali” reso disponibile da AgID – all'interno dell'organizzazione deputata alla gestione del sistema di conservazione realizzato da DocFlow.

Ruolo: Responsabile del servizio di conservazione (Service Operation Manager)	
Nominativo	Maria Elena Medina
Attività di competenza	<ul style="list-style-type: none"> 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. Gestione dell'esercizio delle componenti software del sistema di conservazione
Periodo nel ruolo	Dal 2005 ad oggi
Eventuali deleghe	Nessuna
Rapporto con DocFlow	Contratto a tempo indeterminato

Ruolo: Responsabile sicurezza dei sistemi per la conservazione	
Nominativo	Roberto Dragone
Attività di competenza	<ul style="list-style-type: none"> 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. Rapporti con i fornitori di servizi al fine di garantire la sicurezza dei sistemi.

Periodo nel ruolo	Dal 2015 ad oggi
Eventuali deleghe	Nessuna
Rapporto con DocFlow	Contratto a tempo indeterminato

Ruolo: Responsabile funzione archivistica di conservazione	
Nominativo	Giuseppe Di Dio
Attività di competenza	<ul style="list-style-type: none"> 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.
Periodo nel ruolo	Dal 2015
Eventuali deleghe	Da gennaio 2018 – Alessandro De Pasquale – Tutte le attività di competenza.
Rapporto con DocFlow	Contratto a tempo determinato, durata 5 anni

Ruolo: Responsabile trattamento dati personali	
Nominativo	Francesca Di Bella
Attività di competenza	<ul style="list-style-type: none"> Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali. Garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di

	sicurezza e di riservatezza
Periodo nel ruolo	Dal 2005 ad oggi
Eventuali deleghe	Nessuna
Rapporto con DocFlow	Componente CdA

Ruolo: Responsabile sistemi informativi per la conservazione	
Nominativo	Roberto Dragone
Attività di competenza	<ul style="list-style-type: none"> • Gestione dell'esercizio delle componenti hardware 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.
Periodo nel ruolo	Dal 2015 ad oggi
Eventuali deleghe	Nessuna
Rapporto con DocFlow	Contratto a tempo indeterminato

Ruolo: Responsabile sviluppo e manutenzione del sistema di conservazione	
Nominativo	Marco Faini

Attività di competenza	<ul style="list-style-type: none"> • 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.
Periodo nel ruolo	Dal 2005 ad oggi
Eventuali deleghe	Nessuna
Rapporto con DocFlow	Contratto a tempo indeterminato

[Torna al sommario](#)

4.1 Responsabile della conservazione

Il Responsabile della Conservazione è il Cliente, nella persona fisica formalmente nominata all'interno del soggetto titolare dei documenti oggetto di conservazione, quale responsabile dell'insieme delle attività finalizzate alla conservazione dei documenti informatici nell'ambito della contratto di outsourcing verso DocFlow conformemente a quanto previsto dal DPCM 3 dicembre 2013.

In qualità di Titolare dei documenti informatici oggetto di conservazione, il Cliente, attraverso il proprio Responsabile della Conservazione, definisce e attua le politiche complessive del sistema di conservazione governandone quindi la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo esplicitato nel Manuale della Conservazione. Tale Manuale verrà condiviso con il conservatore DocFlow che si impegnerà a rispettarlo.

Pertanto, ai fini del presente Manuale i ruoli di Produttore, Titolare del trattamento e di Responsabile della conservazione sono ricoperti dal Cliente, mentre i ruoli di Responsabile del servizio di Conservazione e Responsabile esterno del trattamento dei dati sono ricoperti da DocFlow.

Il nominativo ed i riferimenti del Responsabile della conservazione sono indicati nell'allegato "Specificità del contratto" nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

[Torna al sommario](#)

4.2 Modello organizzativo

Il sistema di conservazione che DocFlow ha adottato applica il modello organizzativo conforme a quanto stabilito dalle vigenti regole tecniche, DPCM 3 dicembre 2013 alla lettera b) comma 2 dell'articolo 5, pertanto DocFlow opererà come soggetto affidatario del servizio di conservazione. L'affidamento del servizio è totale o parziale, a seconda di quanto specificato nel documento: Specificità del contratto.

Il modello organizzativo DocFlow è stato realizzato tenendo conto del modello OAIS (Open Archival Information System), ovvero una struttura organizzata di persone e sistemi, che abbia come compito la conservazione degli oggetti previsti dall'art. 4 del DPCM 3 dicembre 2013.

Dalle regole tecniche vigenti e, sulla base dello stesso modello OAIS, si possono identificare i seguenti ruoli fondamentali: Produttore, Utente, Responsabile della conservazione.

[Torna al sommario](#)

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Il sistema di conservazione che DocFlow ha adottato applica il modello organizzativo conforme a quanto stabilito dalle vigenti regole tecniche, DPCM 3 dicembre 2013 alla lettera b) comma 2 dell'articolo 5, pertanto DocFlow opererà come soggetto affidatario del servizio di conservazione. L'affidamento del servizio è totale o parziale, a seconda di quanto specificato nel documento: Specificità del contratto.

Il modello organizzativo DocFlow è stato realizzato tenendo conto del modello OAIS (Open Archival Information System), ovvero una struttura organizzata di persone e sistemi, che abbia come compito la conservazione degli oggetti previsti dall'art. 4 del DPCM 3 dicembre 2013.

Il Cliente affida in outsourcing il servizio di Conservazione a DocFlow che assume il ruolo di Conservatore. Sarà onere di DocFlow svolgere tutte le attività necessarie alla corretta conservazione dei documenti informatici ad esso affidati così come previste dalle regole tecniche di cui al DPCM del 3 dicembre 2013 e dagli standard tecnici da questi richiamati. In particolare DocFlow curerà la corretta esecuzione delle attività ad esso commissionate dal Cliente che gli affida la conservazione dei propri documenti informatici. Tutti i soggetti coinvolti nel servizio di Conservazione sono stati incaricati al trattamento dei dati per l'attività di conservazione.

Di seguito riporta l'organigramma della struttura organizzativa coinvolta nel servizio di Conservazione:



Figura 1 - Organigramma

[Torna al sommario](#)

5.2 Strutture organizzative

Di seguito si descrive lo schema del processo di conservazione, le relative attività di gestione dei sistemi informativi con l'indicazione del paragrafo in cui sono dettagliate e il riferimento delle funzioni aziendali responsabili.

Attività proprie di ciascun soggetto coinvolto nel servizio di conservazione		
Attività	Descrizione	Riferimento dettagli
Attivazione del servizio di Conservazione (a seguito della sottoscrizione del contratto).	Il cliente sottoscrive con DocFlow un contratto per l'attivazione del servizio di conservazione in outsourcing.	par. 8.4.1
Acquisizione, verifica e gestione dei Pacchetti di versamento e generazione del Rapporto di versamento.	I pacchetti di versamento vengono verificati per controllare l'identificazione certa del soggetto, i formati e i metadati concordati, vengono inoltre effettuate eventuali altre verifiche concordate con il Cliente. Viene generato il rapporto di versamento con l'esito positivo o la notifica delle anomalie e dello scarto del pacchetto.	par. 7.1 par. 7.2 par. 7.3 par. 7.4
Preparazione e gestione dei Pacchetti di archiviazione.	Uno o più pacchetti di versamento accettati vengono trasformati in Pacchetti di Archiviazione, i quali conterranno, oltre agli oggetti da conservare, l'indice del Pacchetto di Archiviazione formato secondo le regole dello standard SInCRO. L'IdPA viene sottoscritto con firma digitale dal Responsabile del servizio di Conservazione e viene marcato temporalmente	par. 7.5
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta.	I pacchetti di Distribuzione sono creati a partire da richieste effettuate tramite il portale Web dedicato dal Cliente. Possono essere trasferiti localmente al Cliente.	par. 7.6 par. 7.7
Scarto dei pacchetti di archiviazione	I Pacchetti di archiviazione possono essere scartati solo dal responsabile del servizio di conservazione su richiesta del responsabile della conservazione o in fase di chiusura contratto	par. 7.8
Chiusura del servizio di conservazione al termine del contratto	Vengono generati e messi a disposizione del Cliente uno o più pacchetti di distribuzione coincidenti con i pacchetti di	par. 7.8.1

	<p>archiviazione e comprendenti tutti i documenti afferenti al Cliente stesso.</p> <p>A consegna avvenuta si procederà con l'eliminazione di tutti i dati del Cliente.</p>	
--	--	--

Attività proprie di gestione dei sistemi informativi		
Attività	Descrizione	Riferimento dettagli
Conduzione e manutenzione del sistema di conservazione	Le attività di manutenzione vengono svolte sia sui processi che sulle strutture hardware e software. Quotidianamente vengono verificate le attività sulle infrastrutture, oltre a una pianificazione delle eventuali procedure straordinarie per il caso di anomalie.	par. 7.10.1
Monitoraggio del sistema di conservazione.	Monitoraggio del sistema di Log per la registrazione degli accessi e degli eventi. Vengono anche monitorate le attività di verifica dell'integrità degli archivi e la gestione delle anomalie.	par. 7.10.2
Change management.	Sono definite le politiche, le priorità e le tempistiche di adeguamento all'evoluzione tecnologica per far sì che il sistema di conservazione garantisca nel tempo l'integrità, la disponibilità e la sicurezza del sistema medesimo.	par. 7.10.3
Verifica periodica di conformità normativa e standard di riferimento.	La conformità all'evoluzione normativa e agli standard in materia di conservazione di lungo periodo, è costantemente monitorata ed eventualmente aggiornata grazie al lavoro di supervisione svolto dal Responsabile del servizio di conservazione.	par. 7.10.4

[Torna al sommario](#)

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

DocFlow opera soprattutto nel settore delle aziende private pertanto le tipologie di documenti conservati sono prevalentemente orientate ai documenti aziendali.

Di seguito sono descritti le tipologie dei pacchetti e degli oggetti in esso contenuti sottoposti a conservazione.

[Torna al sommario](#)

6.1 Documenti conservati

I documenti sottoposti al processo di conservazione sono elencati di seguito.

Negli accordi di servizio (specificità di contratto) sono elencati i documenti trattati per ogni singolo cliente.

Prog.	Descrizione Tipo documento/Classe documentale	Formati conservati	Firma digitale	Visualizzatore
1	Fatture Emesse e relativi documenti di rettifica	PDF /XML	O	Acrobat/browser
2	Fatture Ricevute e relativi documenti di rettifica	PDF /XML	O	Acrobat/browser
3	Fatture elettroniche emesse verso la PA e relative ricevute da SDI	XML	S	browser
4	Docum. Trasporto Attivi	PDF	N	Acrobat
5	Docum. Trasporto Passivi	PDF	N	Acrobat
6	Libri contabili	PDF	S	Acrobat
7	Libri IVA	PDF	S	Acrobat
8	Registri assicurativi	PDF	S	Acrobat
9	Posta elettronica certificata e relative ricevute	EML	S	Outlook exp.
10	Contratti	PDF	S	Acrobat
11	Documenti del protocollo/Corrispondenza e registri	PDF	O	Acrobat
12	Altri documenti	PDF	O	Acrobat

Legenda Firma digitale S=Si N=No O=Opzionale

Tutti i documenti trattati dal sistema di conservazione DocFlow devono essere compresi tra i seguenti:

- Formato PDF e PDF/A (estensione .pdf) MIME type: application/pdf
Visualizzatore: Adobe Reader
Proprietario/Produttore: Adobe Systems
Standard: ISO32000-1, ISO 19005-1:2005 (vers. PDF 1.4), ISO 19005-2:2011 (vers. PDF 1.7)
- Formato XML (estensione .xml) MIME type: application/xml o text/xml
Proprietario/Produttore: W3C
Visualizzatore: Editor testuali
- Formato TXT (estensioni varie) MIME type: application/text
Visualizzatore: Editor testuali
- Formato EML (estensione .eml) MIME type: message/rfc822 Standard: RFC2822
Visualizzatore: Software per la gestione posta elettronica (es. Mozilla Thunderbird, Outlook express)

- Formato TIFF (estensione .tif) MIME type: image/tiff Standard ISO 12639 e ISO 12234
Proprietario/Produttore: Adobe
Visualizzatore: Visualizzatore foto di Windows
- Formato firma digitale CAAdES (estensione .p7m) MIME type: application/pkcs7-mime
Visualizzatore: Software di firma digitale Standard:
ETSI TS 101 733 Electronic Signature and Infrastructure (ESI) – CMS Advanced Electronic Signature (CAAdES)

I documenti firmati con firma elettronica CAAdES devono essere in uno dei formati indicati.

Tutti i formati indicati dispongono di visualizzatori standard o di pubblico dominio per cui non sono richieste licenze.

In particolari casi, indicati per le specifiche tipologie documentali, i documenti possono essere contenuti in archivi compressi di tipo ZIP.

Lo ZIP è un formato di compressione dei dati molto diffuso. L'algoritmo di compressione, usato è basato su una variante dell'algoritmo LZW.

- Formato ZIP (estensione .zip) Tipo MIME application/zip
Proprietario/Produttore Pkware
Licenza: Specifiche pubbliche, esistono implementazioni con licenza GPL

Eventuali altri formati potranno essere gestiti, su richiesta del Responsabile della conservazione, in tal caso questi verranno indicati nel documento Specificità del contratto, similmente a quanto indicato in questo documento per i formati sopraelencati.

[Torna al sommario](#)

6.2 Pacchetto di versamento

Si tratta del pacchetto informativo inviato dal produttore al sistema di conservazione e descritto negli accordi di servizio (Specificità del contratto). Il Contratto di servizio (v. modello OASIS; submission agreement) definisce tutte le componenti informative che il sistema di conservazione necessita per creare i Pacchetti di versamento..

Nel sistema di conservazione, sono accettati pacchetti di versamento che rispondono alle caratteristiche tecnologiche e informative previste nei rispettivi Contratti di servizio.

Possono essere concordate, in fase di accordi contrattuali, modalità di versamento:

- automatiche
- semiautomatiche
- manuali

Possono essere adottate modalità differenti per ciascuna tipologia di documenti.

Nel caso di versamento manuale, il soggetto produttore può accedere all'interfaccia web del sistema la quale permette di inserire i metadati obbligatori, quelli opzionali, la classificazione che si riferisce allo strumento archivistico versato in fase di start-up del sistema.

Si possono anche prevedere, all'interno del Contratto di servizio, versamenti semiautomatizzati o totalmente automatizzati per alcune tipologie documentarie: ad esempio, nel caso di fatture attive estratte da un sistema ERP, si può prevedere un'estrazione settimanale dal sistema con l'attribuzione automatizzata ad un modello di metadati prestabilito.

Il pacchetto di versamento è composto dai documenti stessi e da un indice avente il seguente schema:

```
<?xml version="1.0" encoding="iso-8859-1"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="XMLDOCS">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="FIELDS">
          <xs:complexType>
            <xs:sequence>
              <xs:element maxOccurs="unbounded" name="FIELD">
                <xs:complexType>
                  <xs:attribute name="dbfield" type="xs:string" use="required" />
                  <xs:attribute name="caption" type="xs:string" use="required" />
                  <xs:attribute name="search" type="xs:unsignedByte" use="required" />
                  <xs:attribute name="profile" type="xs:unsignedByte" use="required" />
                  <xs:attribute name="result" type="xs:unsignedByte" use="required" />
                  <xs:attribute name="order" type="xs:unsignedByte" use="required" />
                  <xs:attribute name="type" type="xs:string" use="required" />
                  <xs:attribute name="idAipa" type="xs:string" use="required" />
                  <xs:attribute name="check" type="xs:string" use="optional" />
                  <xs:attribute name="startWithPrefix" type="xs:boolean" use="optional" />
                />
              <xs:attribute name="preflen" type="xs:unsignedByte" use="optional" />
              <xs:attribute name="separatore" type="xs:string" use="optional" />
              <xs:attribute name="numlen" type="xs:string" use="optional" />
            />
          />
        />
      />
    />
  />
  <xs:element name="DOCUMENTS">
    <xs:complexType>
      <xs:sequence>
        <xs:element maxOccurs="unbounded" name="DOCUMENT">
          <xs:complexType>
            <xs:attribute name="DOCNUMBER" type="xs:string" use="required" />
            <xs:attribute name="system_id" type="xs:unsignedInt" use="required" />
            <xs:attribute name="version_id" type="xs:unsignedInt" use="required" />
            <xs:attribute name="extension" type="xs:string" use="required" />
            <xs:attribute name="NUM_DOC" type="xs:unsignedInt" use="required" />
            <xs:attribute name="DATA_DOC" type="xs:unsignedInt" use="required" />
            <xs:attribute name="CODFISC" type="xs:string" use="required" />
          />
        />
      />
    />
  />
</xs:schema>
```

```

        <xs:attribute name="PARIVA" type="xs:string" use="required" />
        <xs:attribute name="RAGSOC" type="xs:string" use="required" />
        <xs:attribute name="NOME" type="xs:string" use="required" />
        <xs:attribute name="COGNOME" type="xs:string" use="required" />
        <xs:attribute name="Hash" type="xs:string" use="required" />
        <xs:attribute name="RIFTEMP" type="xs:string" use="required" />
    </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

Nel caso che il pacchetto di versamento concordato con il produttore differisca dall'esempio indicato, questo verrà documentato nelle specificità di contratto.

Nel caso che i controlli non evidenzino anomalie rispetto ai controlli concordati, il sistema di conservazione produce il rapporto di versamento che viene sottoscritto, con firma elettronica qualificata dal responsabile del servizio di conservazione DocFlow (service manager) e viene apposta un riferimento temporale opponibile a terzi tramite una marca temporale rilasciata da una Time Stamping Authority accreditata AgID.

Il rapporto di versamento contiene i dati descrittivi dei documenti e l'impronta elettronica di ciascun documento stesso (Hash) calcolata secondo lo standard SHA-256.

In caso i controlli evidenzino una o più anomalie nei documenti del pacchetto, l'intero pacchetto viene respinto e dovrà essere nuovamente inviato dal produttore.

Il rapporto di versamento è in formato XML con il seguente schema:

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="RDV">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Summary">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ErrorCounters">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element maxOccurs="unbounded" name="Counter">
                      <xs:complexType>
                        <xs:attribute name="Type" type="xs:string" use="required" />
                        <xs:attribute name="Description" type="xs:string" use="required"
/>
                        <xs:attribute name="Value" type="xs:unsignedByte" use="required"
/>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

```

        <xs:attribute name="RifTemp" type="xs:string" use="required" />
        <xs:attribute name="TotalDocuments" type="xs:unsignedByte" use="required" />
        <xs:attribute name="CorrectDocuments" type="xs:unsignedByte" use="required"
/>

        <xs:attribute name="WrongDocuments" type="xs:unsignedByte" use="required" />
    </xs:complexType>
</xs:element>
<xs:element name="Documents">
    <xs:complexType>
        <xs:sequence>
            <xs:element maxOccurs="unbounded" name="Document">
                <xs:complexType>
                    <xs:attribute name="Docnumber" type="xs:unsignedShort" use="required"
/>

                    <xs:attribute name="Docname" type="xs:unsignedShort" use="required" />
                    <xs:attribute name="RagSoc" type="xs:string" use="required" />
                    <xs:attribute name="Cognome" type="xs:string" use="required" />
                    <xs:attribute name="Nome" type="xs:string" use="required" />
                    <xs:attribute name="CodFisc" type="xs:string" use="required" />
                    <xs:attribute name="ParIva" type="xs:string" use="required" />
                    <xs:attribute name="NumeroDoc" type="xs:string" use="required" />
                    <xs:attribute name="DataDoc" type="xs:string" use="required" />
                    <xs:attribute name="MeseDoc" type="xs:unsignedByte" use="required" />
                    <xs:attribute name="AnnoDoc" type="xs:unsignedShort" use="required" />
                    <xs:attribute name="Hash" type="xs:string" use="required" />
                    <xs:attribute name="TipoDoc" type="xs:string" use="required" />
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:attribute name="Company" type="xs:string" use="required" />
<xs:attribute name="DocType" type="xs:string" use="required" />
<xs:attribute name="VersId" type="xs:unsignedShort" use="required" />
</xs:complexType>
</xs:element>
</xs:schema>

```

Qualora il rapporto di versamento concordato con il cliente sia differente da quello generale, questo è indicato nelle specificità di contratto.

Viene generato un solo rapporto di versamento per ogni pacchetto di versamento.

Il rapporto di versamento viene memorizzato nel sistema e conservato nel pacchetto di archiviazione qualora il pacchetto di versamento sia accettato.

[Torna al sommario](#)

6.3 Pacchetto di archiviazione

Con la modalità prevista dagli accordi di servizio (specificità di contratto) Il responsabile del servizio di conservazione forma il pacchetto di archiviazione. La struttura del pacchetto di archiviazione è conforme allo standard SInCRO illustrato, a livello indicativo, dall'allegato 4 al DPCM 3 dicembre 2013, secondo lo schema seguente:

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:sincro="http://www.uni.com/U3011/sincro/"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.uni.com/U3011/sincro/" elementFormDefault="qualified"
attributeFormDefault="qualified">

```

```

    <xs:annotation>
      <xs:documentation xml:lang="en"> Definition of simple types
</xs:documentation>
    </xs:annotation>
    <xs:simpleType name="Label">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="Path">
      <xs:restriction base="xs:anyURI" />
    </xs:simpleType>
    <xs:simpleType name="Name">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="Version">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="Producer">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="TimeInfo">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="FirstName">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="LastName">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="FormalName">
      <xs:restriction base="xs:string" />
    </xs:simpleType>
    <xs:simpleType name="EmptyString">
      <xs:restriction base="xs:string">
        <xs:maxLength value="0" />
      </xs:restriction>
    </xs:simpleType>
    <xs:annotation>
      <xs:documentation xml:lang="en"> Definition of attributes
</xs:documentation>
    </xs:annotation>
    <xs:attribute name="version" type="xs:NMTOKEN" fixed="1.0" />
    <xs:attribute name="url" type="xs:anyURI" fixed="http://www.uni.com/U3011/sincro/"
/>
    <xs:attribute name="XMLScheme" type="xs:anyURI" />
    <xs:attribute name="scheme" type="xs:string" default="local" />
    <xs:attribute name="canonicalXML" type="xs:boolean" />
    <xs:attribute name="function" type="xs:NMTOKEN" default="SHA-1" />
    <xs:attribute name="extension" type="xs:NMTOKEN" />
    <xs:attribute name="language" type="xs:language" default="it" />
    <xs:attribute name="format" type="xs:string" />
    <xs:attribute name="encoding">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="7bit" />
          <xs:enumeration value="8bit" />
          <xs:enumeration value="base64" />
          <xs:enumeration value="binary" />
          <xs:enumeration value="quotedprintable" />
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>

```

```

        <xs:enumeration value="xtoken" />
    </xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="normal" type="xs:dateTime" />
<xs:attribute name="type">
    <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="person" />
            <xs:enumeration value="organization" />
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
<xs:attribute name="otherRole" type="xs:string" />
<xs:attribute name="role">
    <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
            <xs:enumeration value="PreservationManager" />
            <xs:enumeration value="Operator" />
            <xs:enumeration value="PublicOfficer" />
            <xs:enumeration value="Delegate" />
            <xs:enumeration value="OtherRole" />
        </xs:restriction>
    </xs:simpleType>
</xs:attribute>
<xs:annotation>
    <xs:documentation xml:lang="en"> Definition of complex types
</xs:documentation>
</xs:annotation>
<xs:complexType name="EmbeddedMetadata">
    <xs:complexContent>
        <xs:extension base="xs:anyType">
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:complexType name="Identifier">
    <xs:simpleContent>
        <xs:extension base="xs:NMTOKEN">
            <xs:attribute ref="sincro:scheme" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Agent_ID">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="scheme" use="required">
                <xs:simpleType>
                    <xs:restriction base="xs:NMTOKEN">
                        <xs:enumeration value="TaxCode" />
                        <xs:enumeration
value="VATRegistrationNumber" />
                        <xs:enumeration
value="NationalHealthCareAuthority" />
                        <xs:enumeration value="OtherScheme" />
                    </xs:restriction>
                </xs:simpleType>
            </xs:attribute>
            <xs:attribute name="otherScheme" type="xs:string" />

```



```

        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="Description">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute ref="sincro:language" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="MoreInfo">
    <xs:choice>
        <xs:element name="EmbeddedMetadata" type="sincro:EmbeddedMetadata" />
        <xs:element name="ExternalMetadata" type="sincro:File" />
    </xs:choice>
    <xs:attribute ref="sincro:XMLScheme" use="required" />
</xs:complexType>
<xs:complexType name="Hash">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute ref="sincro:canonicalXML" />
            <xs:attribute ref="sincro:function" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="PreviousHash">
    <xs:simpleContent>
        <xs:extension base="sincro:Hash">
            <xs:attribute name="relatedIdC" type="xs:NMTOKEN"
use="required" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="CreatingApplication">
    <xs:sequence>
        <xs:element name="Name" type="sincro:Name" />
        <xs:element name="Version" type="sincro:Version" />
        <xs:element name="Producer" type="sincro:Producer" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LawAndRegulations">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute ref="sincro:language" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="SourceIdC">
    <xs:sequence>
        <xs:element name="ID" type="sincro:Identifier" />
        <xs:element name="Path" type="sincro:Path" minOccurs="0" />
        <xs:element name="Hash" type="sincro:Hash" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="SourcePdA">
    <xs:sequence>
        <xs:element name="ID" type="sincro:Identifier" />
        <xs:element name="IdC_ID" type="sincro:Identifier" minOccurs="0" />

```

```

        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="VdCGroup">
        <xs:sequence>
            <xs:element name="Label" type="sincro:Label" />
            <xs:element name="ID" type="sincro:Identifier" minOccurs="0" />
            <xs:element name="Description" type="sincro:Description"
minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="PdA">
        <xs:sequence>
            <xs:element name="ID" type="sincro:Identifier" />
            <xs:element name="SourcePdA" type="sincro:SourcePdA" minOccurs="0"
maxOccurs="unbounded" />
            <xs:element name="VdCGroup" type="sincro:VdCGroup" minOccurs="0" />
            <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="FileGroup">
        <xs:sequence>
            <xs:element name="Label" type="sincro:Label" minOccurs="0" />
            <xs:element name="File" type="sincro:File" maxOccurs="unbounded" />
            <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="File">
        <xs:sequence>
            <xs:element name="ID" type="sincro:Identifier" />
            <xs:element name="Path" type="sincro:Path" minOccurs="0" />
            <xs:element name="Hash" type="sincro:Hash" />
            <xs:element name="PreviousHash" type="sincro:PreviousHash"
minOccurs="0" />
            <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
        </xs:sequence>
        <xs:attribute ref="sincro:encoding" default="binary" />
        <xs:attribute ref="sincro:extension" />
        <xs:attribute ref="sincro:format" use="required" />
    </xs:complexType>
    <xs:complexType name="SelfDescription">
        <xs:sequence>
            <xs:element name="ID" type="sincro:Identifier" />
            <xs:element name="CreatingApplication"
type="sincro:CreatingApplication" />
            <xs:element name="SourceIdC" type="sincro:SourceIdC" minOccurs="0"
maxOccurs="unbounded" />
            <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="NameAndSurname">
        <xs:sequence>
            <xs:element name="FirstName" type="sincro:FirstName" />
            <xs:element name="LastName" type="sincro:LastName" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AgentName">
        <xs:choice>
            <xs:element name="NameAndSurname" type="sincro:NameAndSurname" />

```

```

        <xs:element name="FormalName" type="sincro:FormalName" />
    </xs:choice>
</xs:complexType>
<xs:complexType name="Agent">
    <xs:sequence>
        <xs:element name="AgentName" type="sincro:AgentName" minOccurs="0" />
        <xs:element name="Agent_ID" type="sincro:Agent_ID" minOccurs="0"
maxOccurs="unbounded" />
        <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
    </xs:sequence>
    <xs:attribute ref="sincro:type" use="required" />
    <xs:attribute ref="sincro:role" use="required" />
    <xs:attribute ref="sincro:otherRole" />
</xs:complexType>
<xs:complexType name="Process">
    <xs:sequence>
        <xs:element name="Agent" type="sincro:Agent" maxOccurs="unbounded" />
        <xs:element name="TimeReference" type="sincro:TimeReference" />
        <xs:element name="LawAndRegulations" type="sincro:LawAndRegulations"
minOccurs="0" />
        <xs:element name="MoreInfo" type="sincro:MoreInfo" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
<xs:complexType name="TimeReference">
    <xs:choice>
        <xs:element name="DetachedTimeStamp" type="sincro:DetachedTimeStamp"
/>
        <xs:element name="AttachedTimeStamp" type="sincro:AttachedTimeStamp"
/>
        <xs:element name="TimeInfo" type="sincro:TimeInfo" />
    </xs:choice>
</xs:complexType>
<xs:complexType name="AttachedTimeStamp">
    <xs:simpleContent>
        <xs:extension base="sincro:EmptyString">
            <xs:attribute ref="sincro:normal" use="required" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="DetachedTimeStamp">
    <xs:simpleContent>
        <xs:extension base="xs:anyURI">
            <xs:attribute ref="sincro:normal" use="required" />
            <xs:attribute ref="sincro:encoding" default="binary" />
            <xs:attribute ref="sincro:format" use="required" />
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
<xs:complexType name="IPdA">
    <xs:sequence>
        <xs:element name="SelfDescription" type="sincro:SelfDescription" />
        <xs:element name="PdA" type="sincro:PdA" />
        <xs:element name="FileGroup" type="sincro:FileGroup"
maxOccurs="unbounded" />
        <xs:element name="Process" type="sincro:Process" />
    </xs:sequence>
    <xs:attribute ref="sincro:version" />
    <xs:attribute ref="sincro:url" />

```

```

        </xs:complexType>
        <xs:annotation>
            <xs:documentation xml:lang="en"> Definition of root element
        </xs:documentation>
        </xs:annotation>
        <xs:element name="IPdA" type="sincro:IPdA" />
    </xs:schema>

```

A seconda del tipo di documento e degli accordi di servizio (specificità di contratto) vengono formate le sezioni "MoreINFO" con i dati concordati per i ciascun tipo di documento.

La struttura della sezione MoreINFO per le seguenti tipologie documentali:

- Fatture e relativi documenti di rettifica passivi
- Fatture e relativi documenti di rettifica attivi
- Fatture elettroniche verso la PA e relative comunicazioni da Sdl
- Libri e registri contabili
- Libri e registri assicurativi
- Contratti elettronici

è la seguente:

```

<?xml version="1.0" encoding="utf-8"?>
<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" >
  <xs:element name="CustomMetadata">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="Company" type="xs:string" />
        <xs:element name="RagSoc" type="xs:string" />
        <xs:element name="Cognome" type="xs:string" />
        <xs:element name="Nome" type="xs:string" />
        <xs:element name="CodFisc" type="xs:string" />
        <xs:element name="ParIva" type="xs:string" />
        <xs:element name="NumeroDoc" type="xs:string" />
        <xs:element name="DataDoc" type="xs:string" />
        <xs:element name="MeseDoc" type="xs:string" />
        <xs:element name="AnnoDoc" type="xs:string" />
        <xs:element name="TipoDoc" type="xs:string" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>

```

La struttura della sezione MoreINFO per le seguenti tipologie documentali:

- Posta elettronica certificata e relative ricevute
- Corrispondenza

è la seguente:

```

<?xml version="1.0" encoding="UTF-8"?>
-<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
-<xs:element name="CustomMetadata">
-<xs:complexType>
-<xs:sequence>
<xs:element name="Company" type="xs:string"/>
<xs:element name="registro" type="xs:string"/>
<xs:element name="numeroprotocollo" type="xs:string"/>
<xs:element name="dataprotocollo" type="xs:string"/>
<xs:element name="datachiusura" type="xs:string"/>
<xs:element name="fascicolo" type="xs:string"/>
<xs:element name="oggettodocumento" type="xs:string"/>
<xs:element name="tipoprotocollo" type="xs:string"/>
-<xs:element name="soggettoprodotto">
-<xs:complexType>
-<xs:sequence>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="codicefiscale" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
-<xs:element name="destinatario">
-<xs:complexType>
-<xs:sequence>
<xs:element name="nome" type="xs:string"/>
<xs:element name="cognome" type="xs:string"/>
<xs:element name="codicefiscale" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="allegato" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

Qualora fosse concordata con i clienti una diversa composizione delle sezioni “MoreINFO” per ogni cliente e/o per un particolare tipo di documento è riportata negli accordi di servizio (specificità di contratto).

Il pacchetto di archiviazione contiene anche i rapporti di versamento relativi a tutti i pacchetti di versamento contenuti nel pacchetto di archiviazione.

Il responsabile del servizio di conservazione DocFlow appone la propria firma elettronica qualificata e la marca temporale al pacchetto di archiviazione.

[Torna al sommario](#)

6.4 Pacchetto di distribuzione

Sono previste due tipologie di pacchetto di esibizione, uno, ai fini dell'interoperabilità, coincidente al pacchetto di archiviazione e uno specifico risultante dalla selezione fatta dagli utenti abilitati che contiene solo i documenti scelti.

In entrambi i casi il pacchetto viene firmato dal responsabile della conservazione, dal responsabile del servizio di conservazione o da un loro delegato.

Il formato delle due tipologie di pacchetto è lo stesso, cambia solo il contenuto, coincidente con il pacchetto di archiviazione o a scelta dell'utente.

Le eventuali personalizzazioni della seconda tipologia di pacchetto, specifiche di un contratto, sono descritte nell'allegato "Specificità del contratto".

Schema del pacchetto di distribuzione:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:sincro="http://www.uni.com/U3011/sincro/" attributeFormDefault="unqualified"
elementFormDefault="qualified" targetNamespace="http://www.uni.com/U3011/sincro/"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:import />
  <xs:element name="IPdE">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="SelfDescription">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ID">
                <xs:complexType>
                  <xs:simpleContent>
                    <xs:extension base="xs:string">
                      <xs:attribute ref="sincro:scheme" use="required" />
                    </xs:extension>
                  </xs:simpleContent>
                </xs:complexType>
              </xs:element>
              <xs:element name="CreatingApplication">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element name="Name" type="xs:string" />
                    <xs:element name="Version" type="xs:decimal" />
                    <xs:element name="Producer" type="xs:string" />
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="PdE">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ID">
                <xs:complexType>
```

```

        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute ref="sincro:scheme" use="required" />
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
    <xs:element name="SourcePdA">
      <xs:complexType>
        <xs:sequence>
          <xs:element name="ID" type="xs:string" />
        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="FileGroup">
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" name="File">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="ID" type="xs:unsignedShort" />
            <xs:element name="Hash">
              <xs:complexType>
                <xs:simpleContent>
                  <xs:extension base="xs:string">
                    <xs:attribute ref="sincro:function" use="required" />
                  </xs:extension>
                </xs:simpleContent>
              </xs:complexType>
            </xs:element>
            <xs:element name="MoreInfo">
              <xs:complexType>
                <xs:sequence>
                  <xs:element name="EmbeddedMetadata">
                    <xs:complexType>
                      <xs:sequence>
                        <xs:element ref="CustomMetadata" />
                      </xs:sequence>
                    </xs:complexType>
                  </xs:element>
                </xs:sequence>
                <xs:attribute ref="sincro:XMLScheme" use="required" />
              </xs:complexType>
            </xs:element>
          </xs:sequence>
          <xs:attribute ref="sincro:format" use="required" />
        </xs:complexType>
      </xs:element>
    </xs:sequence>
    <xs:attribute ref="sincro:format" use="required" />
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Process">
  <xs:complexType>
    <xs:sequence>
      <xs:element maxOccurs="unbounded" name="Agent">

```

```
<xs:complexType>
  <xs:sequence>
    <xs:element name="Agent_ID">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute ref="sincro:scheme" use="required" />
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
  <xs:attribute ref="sincro:role" use="required" />
  <xs:attribute ref="sincro:type" use="required" />
</xs:complexType>
</xs:element>
<xs:element name="TimeReference">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="TimeInfo" type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute ref="sincro:url" use="required" />
<xs:attribute ref="sincro:version" use="required" />
</xs:complexType>
</xs:element>
<xs:attribute name="url" type="xs:string" />
<xs:attribute name="version" type="xs:decimal" />
<xs:attribute name="scheme" type="xs:string" />
<xs:attribute name="format" type="xs:string" />
<xs:attribute name="function" type="xs:string" />
<xs:attribute name="XMLScheme" type="xs:string" />
<xs:attribute name="role" type="xs:string" />
<xs:attribute name="type" type="xs:string" />
</xs:schema>
```

[Torna al sommario](#)

7 II PROCESSO DI CONSERVAZIONE

Il sistema di conservazione di DocFlow è stato realizzato in conformità alle disposizioni vigenti in materia e assicura la conservazione elettronica di lungo periodo a norma di legge. Adotta regole, procedure e tecnologie certificate e che garantiscono il mantenimento delle caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità di tutti i documenti sottoposti al processo di conservazione, per tutto il periodo di conservazione richiesto e fino al suo scarto.

Sono trattati:

- **Pacchetti di versamento:** pacchetti informativi inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel presente manuale di conservazione.
- **Pacchetti di archiviazione:** pacchetti informativi composti dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del DPCM 3/12/2013 e secondo le modalità riportate nel presente manuale di conservazione.
- **Pacchetti di distribuzione:** pacchetti informativi inviati dal sistema di conservazione all'utente in risposta ad una sua richiesta.

In conformità con quanto stabilito dall'art. 9 del DPCM 3 Dicembre 2013, il processo di conservazione a previsto da DocFlow prevede:

- 1) l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- 2) la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste nel presente Manuale e con gli accordi con il Cliente;
- 3) il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui al punto 2) abbiano evidenziato delle anomalie;
- 4) la generazione, in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, opponibile a terzi, e tutte le impronte calcolate su ciascun documento contenuto;
- 5) la preparazione, l'apposizione della firma digitale del Responsabile del servizio di Conservazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nell'allegato 4 del DPCM 3 Dicembre 2013 e secondo le modalità riportate nel presente Manuale;
- 6) la preparazione del pacchetto di distribuzione ai fini dell'esibizione richiesta dal Cliente;
- 7) ai fini della interoperabilità tra sistemi di conservazione, la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione.

Di seguito sono descritte le attività riguardanti la gestione delle attività relative agli specifici contratti stipulati con i singoli Clienti.

A seguito della sottoscrizione di un contratto per la conservazione sono previste una serie di attività che prevedono la definizione delle specificità del contratto, la sottoscrizione degli accordi, delle deleghe e le eventuali nomine.

Sulla base delle specificità di contratto può essere coinvolto il Servizio Sviluppo e manutenzione del sistema di conservazione per la realizzazione di interfacce specifiche o preelaborazioni. Il servizio di Conservazione provvede alla configurazione del sistema e l'abilitazione degli utenti e a richiedere al responsabile del servizio di conservazione il collaudo del sistema.

[Torna al sommario](#)

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

I pacchetti di versamento sono inviati o messi a disposizione dal produttore. Il Servizio di Conservazione provvede ad effettuare i controlli concordati con le specificità di contratto.

In caso che i controlli non evidenzino anomalie rispetto ai controlli concordati, il sistema di conservazione produce il rapporto di versamento che viene sottoscritto, con firma elettronica qualificata dal responsabile del servizio di conservazione DocFlow (service manager) e viene apposta un riferimento temporale opponibile a terzi tramite una marca temporale rilasciata da una Time Stamping Authority accreditata AgID.

Il rapporto di versamento contiene i dati descrittivi dei documenti e l'impronta elettronica di ciascun documento stesso (Hash) calcolata secondo lo standard SHA-256.

In caso i controlli evidenzino una o più anomalie nei documenti del pacchetto, l'intero pacchetto viene respinto e dovrà essere nuovamente inviato dal produttore.

Il rapporto di versamento è in formato XML con lo schema riportato al paragrafo 6.2.

Qualora il rapporto di versamento concordato con il cliente sia differente da quello generale, questo è indicato nelle specificità di contratto.

Viene generato un solo rapporto di versamento per ogni pacchetto di versamento.

Il rapporto di versamento viene conservato nel pacchetto di conservazione.

Esempio di log della generazione del pacchetto di versamento:

```
2016-03-17 12:37:52.4800 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]##### NEW VERSAMENTO #####
2016-03-17 12:37:52.4940 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]EXTRAINFO:
<INFO><COMPANIES><COMPANY><ID>IT10</ID><PATH>\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10</PATH><TYPES><TY
PE><CHECKCOUNTER>false</CHECKCOUNTER><PATH
/><NAME>*</NAME><FILE_SEM>Dati.xml.p7m</FILE_SEM></TYPE></TYPES></COMPANY></COMPANIES></INFO>
2016-03-17 12:37:52.5310 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]type.FileSem Dati.xml.p7m
2016-03-17 12:37:52.5420 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]--> NewVersamento versamentoPath
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\XXXXXX\Bollati [AA] 000076 2016-02-28 type.Path type.Name*
type.CheckCounterFalse c.Id IT10
2016-03-17 12:37:52.5690 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Creating work file
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\XXXXXX\Bollati [AA] 000076 2016-02-28\WORK_170320161237525690
2016-03-17 12:38:02.4449 [INFO ]: [Engine][Aipadocs.Controller.PollingServices.QueueServiceComponent.Process]Wake up
2016-03-17 12:38:04.2711 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]fieldsFilePath
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\XXXXXX\Fields.xml
2016-03-17 12:38:04.2851 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.CompanyId versCfg.TipoDoc
2016-03-17 12:38:04.2991 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.CompanyId-IT10-
2016-03-17 12:38:04.2991 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.TipoDoc-Registri-
2016-03-17 12:38:04.3431 [INFO ]: [AIPADOCs][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.mainContent
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\XXXXXX\Bollati [AA] 000076 2016-02-28\Dati.xml.p7m
```

```

2016-03-17 12:38:04.3511 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Restart False
2016-03-17 12:38:06.8834 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted docPDV: 4458
2016-03-17 12:38:06.9714 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted TsrDoc:
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\XXXXX\Bollati [AA] 000076 2016-02-28\Dati.xml.p7m.tsr
2016-03-17 12:38:06.9714 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]idPDV 4458
2016-03-17 12:38:07.0484 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]## METADATI: @@
2016-03-17 12:38:07.0484 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey DOCUMENTTYPE.DESCRPTION item.idAipa
TipoDoc
2016-03-17 12:38:07.0484 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey PD_DOC_BARCODE item.idAipa Nome
2016-03-17 12:38:07.0484 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey PD_DOC_BARCODE item.idAipa Nome
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey FK_SOCIETA.COD_SOCIETA item.idAipa
#Extrainfo#
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey FK_SOCIETA.DESC_SOCIETA item.idAipa
RagSoc
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey FK_SOCIETA.PIVA_SOCIETA item.idAipa
Parlva
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey PD_DOC_BARCODE item.idAipa Nome
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey PD_FILE_DATE item.idAipa DataDoc
2016-03-17 12:38:07.0494 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey ANNO item.idAipa #Extrainfo#
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey MESE item.idAipa #Extrainfo#
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey DOCNAME item.idAipa #Extrainfo#
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey PD_DOC_BARCODE item.idAipa Nome
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey RIFTEMP item.idAipa RIF_TEMPORALE
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey FILE_SIZE item.idAipa #Extrainfo#
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey EXTENSION item.idAipa EXTENSION
2016-03-17 12:38:07.0504 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey HASH item.idAipa HASH
2016-03-17 12:38:07.0514 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]item.XmlKey DOCNUMBER item.idAipa
2016-03-17 12:38:12.4490 [INFO ]: [Engine][Aipadocs.Controller.PollingServices.QueueServiceComponent.Process]Wake up
2016-03-17 12:40:17.2704 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.AllDocs.Count: 13
2016-03-17 12:40:17.2714 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.CheckCount: False
2016-03-17 12:40:17.8235 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4459
2016-03-17 12:40:18.4766 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4460
2016-03-17 12:40:18.9536 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4461
2016-03-17 12:40:21.4959 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4469
2016-03-17 12:40:21.6399 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4470
2016-03-17 12:40:21.7879 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted doc id 4471
2016-03-17 12:40:22.6260 [INFO ]: [Engine][Aipadocs.Controller.PollingServices.QueueServiceComponent.Process]Wake up
2016-03-17 12:40:28.9116 [ERROR ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Error during sign RDV operation. Causa errore:
System.Exception: [4096]Il certificato e' scaduto
  at Aipadocs.Engine.Sign.SignHelper.SignContent(Byte[] contentToSign, String username, String password, String pin)
  at AipadocsExtension.Versamento.Versamento.InsertRDV(VersamentoCfg versCfg, String docRDVFPPath, Boolean onError)
2016-03-17 12:40:29.0786 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Inserted RDV: 4472
2016-03-17 12:40:29.1216 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Adding Relation 4458 - 4472
2016-03-17 12:40:29.2336 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.BlockingErrors False
2016-03-17 12:40:29.2336 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.OnWarning OK
2016-03-17 12:40:29.2336 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]pdvKODocs.Count 3
2016-03-17 12:40:29.2336 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]versCfg.CounterErrors False
2016-03-17 12:40:29.2536 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]pdvStatus Acquisito
2016-03-17 12:40:29.2786 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]Deleting Folder:
\\sp2013yubik.dftest.local\es\DocFlow\Aipadocs2\Riversamenti\IT10\ArcaAss\Bollati [AA] 000076 2016-02-28
2016-03-17 12:40:29.3566 [ERROR ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]System.IO.IOException: The directory is not empty.
  at System.IO.__Error.WinIOError(Int32 errorCode, String maybeFullPath)
  at System.IO.Directory.DeleteHelper(String fullPath, String userPath, Boolean recursive, Boolean throwOnTopLevelDirectoryNotFound)
  at System.IO.Directory.Delete(String fullPath, String userPath, Boolean recursive, Boolean checkHost)
  at AipadocsExtension.Versamento.Versamento.DeleteFolderVersamento(String fullFolderPath)
2016-03-17 12:40:29.3576 [INFO ]: [AIPADOCS][2cf9045c-1915-49bd-8aa4-2ab9d9b48bd6]@@@@@@@@@ END VERSAMENTO
@@@@@@@@@

```

[Torna al sommario](#)

7.1.1 Ricezione documenti via WEB

Il produttore dei documenti si collega al sito web dedicato mediante le sue credenziali consegnate in fase di start up del servizio secondo le modalità descritte dall'apposita istruzione operativa e carica i documenti da conservare.

Il firewall permette l'accesso esclusivamente agli IP comunicati e configurati. Il cliente può caricare uno zip o un singolo file di tipo Tiff, PDF o XML. La connessione è prevista solo con protocollo sicuro HTTPS. Il sistema registra il caricamento dei documenti su appositi file di log e pubblica su web immediatamente la lista dei documenti caricati. La lista è visibile sia dal cliente che dagli operatori DocFlow.

Ad ogni accesso il servizio registra in un file di LOG con l'indicazione dell'autore del trasferimento, della data e dell'ora e dei documenti trasferiti. I Log sono giornalieri e sono configurati con una retention di 180 giorni.

[Torna al sommario](#)

7.1.2 Ricezione documenti via FTP/SFTP

Il produttore trasferisce tramite protocollo FTP/SFTP i documenti da conservare, utilizzando le credenziali consegnate da DocFlow come da apposita istruzione operativa.

L'accesso avviene mediante l'indirizzo pubblico dichiarato e riconosciuto dal Firewall come descritto nel precedente paragrafo.

Ad ogni accesso il servizio di FTP crea un LOG con l'indicazione dei tempi e dei documenti trasferiti. I Log sono giornalieri e sono configurati con una retention di 180 giorni.

[Torna al sommario](#)

7.1.3 Ricezione documenti ERP

Il sistema documentale di DocFlow si collega al sistema ERP del cliente con le credenziali raccolte come descritto nel paragrafo 7.1.2 e registrate nell'apposito modulo "configurazione ambiente SaaS". Il sistema procede con l'estrazione dei documenti da conservare e archiviazione temporanea sull'apposita cartella di sistema. I Log sono giornalieri e sono configurati con una retention di 180 gg.

[Torna al sommario](#)

7.1.4 Ricezione documenti E-mail/PEC

Il produttore invia i documenti ad un indirizzo di posta accessibile a DocFlow. Le caselle possono essere intestate al cliente o a DocFlow. Il sistema documentale accede alle caselle con le credenziali raccolte come descritto nel paragrafo 7.1.2 e registrate nell'apposito modulo "configurazione ambiente SaaS" e scarica il contenuto in una cartelle di sistema dedicata al cliente. I Log sono giornalieri e sono configurati con una retention di 180 gg.

[Torna al sommario](#)

7.2 Verifiche effettuate sui pacchetti di versamento e generazione del rapporto di versamento e presa in carico

In base alle modalità di configurazione del servizio concordato per il singolo cliente, il sistema archivia il pacchetto in una struttura dati all'interno della quale sono inseriti i metadati. Tali operazioni eseguite dai servizi sono descritte nella documentazione tecnica di ciascun cliente. Tramite un servizio di monitoraggio il sistema controlla la struttura dei metadati e indicizza i documenti creando il file indice (dati.xml) e predisponendo i documenti per la validazione ponendoli in una apposita cartella.

Il sistema in fase di creazione dell'indice esegue i seguenti controlli:

- Controllo dell'identificazione certa del soggetto che ha formato il documento e del relativo ente produttore.
- Controllo consistenza documenti. Il sistema controlla che i documenti referenziati nel file xml del pacchetto di versamento esistano e che siano consistenti (dimensione > 0).
- Controllo formale metadati. Il sistema controlla il file indice e verifica che i metadati definiti come obbligatori siano compilati.
- Controllo numerazione documenti e sequenzialità. Nel caso in cui sia previsto dal contratto, il sistema controlla la sequenzialità e la cronologia dei documenti ricevuti secondo quanto definito nel file indice del pacchetto di versamento. Il sistema inoltre verifica la sequenzialità anche rispetto al pacchetto precedente con la stessa tipologia di documenti.

Eventuali errori nella generazione del file indice o nei metadati vengono segnalati dal sistema agli operatori del Service e gestiti con il supporto del cliente come descritto nel paragrafo 6.2.6.

[Torna al sommario](#)

7.2.1 Verifica segnalazione di errore

Nel caso di errori durante la generazione del file indice, il sistema crea una anomalia a sistema con il codice di errore. Il responsabile del servizio di Sviluppo e Manutenzione verifica l'eventuale anomalia, la qualifica inserendo un commento e la priorità e l'assegna ad un Application Developer. Il sistema notifica la richiesta di risoluzione e pone l'item nello stato di "assegnato".

[Torna al sommario](#)

7.2.2 Risoluzione anomalia

L'Application Developer riceve la richiesta di risoluzione dell'anomalia e procede con la sua risoluzione. Le eventuali mail con il cliente o altri attori coinvolti sono tracciate dal sistema e visibili al Project Manager di riferimento e dal Responsabile del servizio di Conservazione. Nel caso in cui l'anomalia non sia risolta nei tempi previsti dal contratto (SLA), il sistema invia una mail di sollecito al Responsabile del Servizio di Conservazione. Una volta risolta, la segnalazione viene chiusa con la descrizione delle attività eseguite.

[Torna al sommario](#)

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

Dopo aver acquisito il pacchetto di versamento come descritto precedentemente, una routine del software esegue una verifica formale e sostanziale dei documenti e del file indice generato dal sistema:

- Il sistema controlla che i documenti referenziati nel file dati.xml del pacchetto di versamento esistano e che siano consistenti (dimensione > 0).
- Se il pacchetto contiene documenti firmati digitalmente, il sistema verifica la validità della firma e dell'eventuale marca temporale.
- nel caso in cui sia previsto dal contratto, il sistema controlla la firma digitale e la marca temporale dei documenti. In particolare il sistema verifica la validità dei certificati e la loro corrispondenza con quella indicata nel contratto.
- Il sistema controlla il file indice e verifica che i metadati definiti come obbligatori siano compilati.
- Nel caso in cui sia previsto dal contratto, il sistema controlla la sequenzialità e la cronologia dei documenti ricevuti secondo quanto definito nel file indice del pacchetto di versamento. Il sistema inoltre verifica la sequenzialità anche rispetto al pacchetto precedente con la stessa tipologia di documenti.

Nel caso in cui i controlli vengano superati, il sistema etichetta il pacchetto come "archiviabile", mentre nel caso in cui i controlli non vengono superati il sistema etichetta il pacchetto come "non archiviabile". Il sistema genera il rapporto di versamento (file rapporto.xml) descritto nel paragrafo 6.2 con il resoconto dell'acquisizione, che viene firmato dal responsabile del servizio di conservazione (file rapporto.xml.p7m) e a cui viene apposta la marca temporale (file rapporto.xml.p7m.tsr) in alternativa al formato CaDes-BES illustrato, potrà essere utilizzato il formato CaDes-T che contiene firma e marca in un unico file (file rapporto.xml.p7m).

Il rapporto di versamento sottoscritto sostituisce, nei casi indicati nel documento di specificità di contratto, la firma richiesta dal comma 1 dell'art. 4 del DM 17 giugno 2014.

Il rapporto di versamento contiene le informazioni di sommario ed eventualmente i seguenti messaggi di errore:

- Errore hash errato
- Errore file inesistente
- Errore metadato mancante
- Errore sequenza
- Errore formato data
- Altri eventuali errori concordati con il cliente definiti nelle specifiche contrattuali.

Il sistema procede all'archiviazione del rapporto di versamento, del file indice del pacchetto di versamento e nel caso in cui non risultino errori, dei documenti allegati. Tali informazioni vengono rese disponibili sull'interfaccia web sia al Cliente che al responsabile del servizio di conservazione. Al termine delle operazioni il servizio procede all'acquisizione del pacchetto se "archiviabile" e dei relativi metadati prodotti dall'elaborazione nell'applicativo di conservazione ed elimina i pacchetti già elaborati dalla cartella. I pacchetti non archiviabili vengono trasferiti in un'apposita struttura di scarto accessibile al cliente per le verifiche.

[Torna al sommario](#)

7.4 Rifiuto/Acettazione del pacchetto di versamento

Il sistema invia una email di notifica con l'accettazione o il rifiuto formale del pacchetto di versamento. Il messaggio riporta l'indice dei documenti e, in caso di rifiuto, l'elenco degli errori.

Il responsabile della conservazione, presso il cliente, o suo delegato, può collegarsi all'interfaccia web mediante le proprie credenziali di accesso, e visualizza la lista dei pacchetti di versamento di propria competenza, ed in particolare quelli che hanno generato errore durante il controllo formale. Nel caso di errori sarà necessario inviare nuovamente l'intero pacchetto di versamento.

[Torna al sommario](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

Con la modalità prevista dagli accordi di servizio (specificità di contratto) il Servizio di Conservazione forma il pacchetto di archiviazione. La struttura del pacchetto di conservazione è riportata nel paragrafo 6.2.

A seconda del tipo di documento e degli accordi di servizio (specificità di contratto) vengono formate le sezioni "MoreINFO" con i dati concordati per i ciascun tipo di documento.

Le strutture delle sezioni MoreINFO per le varie tipologie di documenti sono anch'esse riportate nel paragrafo 6.2.

Qualora fosse concordata con i clienti una diversa composizione delle sezioni "MoreINFO" per un cliente e/o per un particolare tipo di documento è riportata negli accordi di servizio (specificità di contratto).

Il pacchetto di archiviazione contiene anche i rapporti di versamento relativi a tutti i pacchetti di versamento contenuti nel pacchetto di archiviazione.

Il responsabile del servizio di conservazione DocFlow appone la propria firma elettronica qualificata e la marca temporale al pacchetto di archiviazione.

[Torna al sommario](#)

7.5.1 Generazione del pacchetto di archiviazione

In seguito alla notifica positiva del rapporto di versamento, Il sistema genera il pacchetto di archiviazione ovvero un indice di archiviazione per tutti i pacchetti di versamento da conservare secondo le regole di schedulazione della società cliente come definito nel presente manuale di conservazione.

La policy di apposizione della firma è legata alla company. Sono gestite due possibilità:

- Automatica.

La firma del responsabile del servizio di conservazione (o suo delegato) viene apposta in modalità automatica dal sistema utilizzando un dispositivo HSM (Hardware Security Module) conforme alle norme per la firma elettronica qualificata, installato presso l'Internet Data Center, per l'apposizione delle firme digitali: il sistema può apporre velocemente un numero elevato di firme digitali in tutta sicurezza attraverso una procedura automatizzata, poiché le chiavi e i certificati dell'utente sono custoditi in maniera sicura all'interno del dispositivo. Il sistema invia una notifica al titolare delle del certificato di firma qualificato e tutti gli utenti coinvolti (configurati a livello di azienda).

- Firma non automatica.

La firma viene apposta dall'utente ovvero dal Delegato del Responsabile della Conservazione digitale tramite un dispositivo per la firma sicura gestita dal cliente (SmartCard, Token, HSM, firma remota).

Quindi, una volta preparato l'indice, il relativo pacchetto di archiviazione rimane nello stato "Attesa Firma". A questo punto viene notificato via mail l'utente preposto (configurato con la company) che, tramite UI, potrà eseguire la firma tramite il relativo dispositivo di firma. La sicurezza è garantita solo dal dispositivo di firma. Una volta eseguita la firma, il sistema invia una notifica a tutti gli utenti coinvolti.

[Torna al sommario](#)

7.5.1.1 Notifica pacchetto in attesa di firma digitale non automatica

Nel caso di pacchetto di archiviazione in attesa di firma non automatica, il sistema notifica via mail al responsabile della conservazione o a suo delegato che i documenti sono in attesa di firma digitale.

[Torna al sommario](#)

7.5.2 Firma digitale

Il responsabile del servizio di conservazione, nel caso sia attiva la modalità di firma automatica, firma, automaticamente e per ogni firma appone anche la marca temporale.

In caso di firma non automatica, il responsabile della conservazione si collega all'interfaccia web tramite le proprie credenziali e firma il pacchetto utilizzando il proprio dispositivo di firma/certificato e per ogni firma appone anche la marca temporale.

[Torna al sommario](#)

7.5.2.1 Gestione del pacchetto di archiviazione

Il sistema verifica la validità della firma e dell'eventuale marca temporale, genera ed archivia il file indice firmato e marcato in modo tale da poterlo consultare e visualizzare agevolmente i documenti correlati (documenti del pacchetto di versamento, il file indice generato dal sistema di conservazione e il rapporto di versamento precedentemente generato).

[Torna al sommario](#)

7.5.3 Notifica conservazione

Il sistema notifica a tutti gli utenti coinvolti a livello società (configurati coerentemente con il contratto) sia la generazione del nuovo pacchetto di archiviazione sia l'avvenuta archiviazione di ciascun pacchetto di versamento.

[Torna al sommario](#)

7.6 Preparazione e gestione dei pacchetti di distribuzione

Gli utenti abilitati possono richiedere al sistema la creazione di un pacchetto di esibizione.

La richiesta di creazione di un pacchetto di esibizione avviene selezionando i documenti da includervi, il sistema prepara un file indice in formato XML e prepara un pacchetto software contenente l'indice con la descrizione dei documenti, i documenti e il software per la ricerca, selezione e visualizzazione dei documenti.

I pacchetti di esibizione possono essere firmati con firma elettronica qualificata dal responsabile del servizio di conservazione, dal responsabile della conservazione o da un loro delegato, se la firma è richiesta. In caso di apposizione della firma viene apposta anche la marca temporale.

Particolari tipi di pacchetto di esibizione possono essere richiesti, in particolare quello che coincide con un pacchetto di archiviazione e che potrà essere utilizzato per la migrazione e l'interoperabilità dei sistemi.

I pacchetti di esibizione quando sono creati sono posti nello stato di "attivo" e fintanto che il pacchetto non viene disattivato, i pacchetti di archiviazione che contengono documenti compresi in un pacchetto di esibizione "attivo", non potranno essere cancellati. Per cancellarli occorrerà porre nello stato "non attivo" il pacchetto di esibizione.

L'utente può identificare i pacchetti di archiviazione o i singoli documenti che dovranno essere parte di una esibizione.

[Torna al sommario](#)

7.6.1 Definizione del pacchetto di distribuzione

L'utente si collega all'interfaccia e inizializza la richiesta di un nuovo pacchetto di distribuzione selezionando i contenuti da esibire. Terminata la fase di selezione viene richiesta la generazione del pacchetto di distribuzione.

[Torna al sommario](#)

7.6.2 Creazione del pacchetto di distribuzione

A fronte della richiesta dell'utente il sistema produce il pacchetto di esibizione contenente i documenti richiesti e i riferimenti ai pacchetti di archiviazione selezionati. In caso di richiesta di masterizzazione il pacchetto di distribuzione viene diviso per permetterne la masterizzazione.

I documenti esibiti sono marcati in modo che non vengano eliminati dal sistema prima della scadenza del periodo di retention previsto dalla legge (solitamente 10 + 1 anni).

L'indice del pacchetto è un file xml, che contiene l'impronta hash dei documenti e che viene firmato e marcato temporalmente. I documenti del pacchetto sono arricchiti con i metadati, i quali possono essere personalizzati per ogni singolo cliente.

Il formato è indicato al paragrafo 6.4.

[Torna al sommario](#)

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

Il Produttore segnala a DocFlow, su apposita documentazione correlata dagli allegati autorizzativi e di identificazione, i propri delegati alla visualizzazione e al download dei documenti informatici originali.

Verranno così inviate le credenziali per accedere al *portale della conservazione* con la modalità del canale separato (username via mail e password via cellulare).

La piattaforma, consente al Soggetto Produttore di effettuare sia la produzione di duplicati e copie informatiche sia l'esibizione a norma dei documenti conservati.

Il collegamento al portale avviene tramite connessione sicura SSL.

Una volta accreditato dal portale, l'utente ha accesso ai servizi concessi alla sua utenza.

A quel punto detti utenti sono in grado di:

- Visualizzare direttamente i documenti informatici originali conservati
- Scaricare i documenti informatici conservati (duplicati) e, eventualmente, i file di evidenza della conservazione (indice di conservazione Unisincro)
- Richiedere e scaricare i pacchetti di esibizione da consegnare alle autorità competenti, in caso di necessità.
- Produrre eventualmente una copia conforme richiedendo la presenza di un pubblico ufficiale.

La procedura per visualizzare i documenti conservati è semplice e intuitiva.

Il Produttore o un suo delegato all'attività di consultazione e produzione di duplicati informatici, ricerca i documenti attraverso i campi che l'interfaccia grafica mette a disposizione. Si tratta degli stessi metadati definiti per la tipologia dei documenti richiesta indicati negli accordi di servizio e eventualmente, nelle Specificità di contratto.

Una volta visualizzati i file conservati, l'utente può richiedere al Responsabile del servizio di conservazione una copia, attraverso una funzione disponibile sul portale.

Sarà così possibile per il Soggetto Produttore avere una copia del Pacchetto di Distribuzione contenente i documenti conservati, l'indice del pacchetto firmato e dotato di marca temporale e un'estrazione dei metadati associati ai documenti.

Infine, ai fini del DPCM 3 dicembre 2013, allo scopo di garantire la leggibilità nel tempo dei documenti conservati nonostante l'obsolescenza dei sistemi e dei software che li hanno prodotti, DocFlow produrrà copie conformi all'originale.

Qualora sia richiesta l'attestazione di conformità all'originale di copie di documenti informatici originali, conservati dal sistema di conservazione, nello specifico caso di documenti che rischiano di divenire illeggibili per obsolescenza tecnologica, DocFlow provvederà a richiedere la presenza di un Pubblico Ufficiale, qualora il suo intervento sia richiesto, per assolvere a tale obbligo.

[Torna al sommario](#)

7.7.1 Intervento del Pubblico Ufficiale

Qualora fosse richiesta la presenza di un pubblico ufficiale per l'attestazione di conformità all'originale di copie di documenti informatici originali, conservati dal sistema di conservazione, il produttore avrà cura di gestire tale scelta. DocFlow rimanda la gestione di tale attività al soggetto produttore le cui modalità di intervento sono esplicitate nel contratto di affidamento. Il conservatore garantisce la messa a disposizione dell'originale informatico attraverso un Pacchetto di esibizione eventualmente firmato dal responsabile del servizio di conservazione.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di conservazione

L'eliminazione dei dati conservati può avvenire sia per esplicita richiesta del cliente sia per scadenza dei termini di conservazione sia per scadenza contratto.

Richiesta esplicita del Titolare dei documenti. Il Responsabile della Conservazione, per conto del Titolare può richiedere l'eliminazione dei pacchetti mediante una formale richiesta via PEC o cartacea. La richiesta viene ricevuta e verificata dal responsabile del servizio di conservazione e in seguito archiviata nel documentale aziendale e legata alla commessa.

Scadenza dei termini di conservazione. Il sistema verifica la presenza di pacchetti in scadenza sulla base del contratto di servizio (specificità di contratto) e li pone all'attenzione del personale che gestisce il servizio di conservazione che, prima di procedere, esegue le opportune verifiche legali.

Eseguite le opportune verifiche e comunicata formalmente al produttore la lista dei documenti di cui è stata richiesta la cancellazione. Avendo avuto conferma dal cliente Il Responsabile del servizio di conservazione si collega al sistema di conservazione e avvia la procedura di cancellazione. Questa innanzitutto verifica se esistono pacchetti di archiviazione o documenti referenziati da Esibizioni attive, nel qual caso la cancellazione è impedita. Per tutti i pacchetti cancellabili il sistema procede con la cancellazione degli stessi e dei documenti referenziati.

Nel caso di **chiusura di contratto** il Responsabile del servizio di conservazione deve preventivamente provvedere ad estrarre tutti i documenti del cliente per mezzo di Pacchetti di Esibizione coincidenti con i pacchetti di archiviazione.

Il sistema notifica a tutti gli utenti coinvolti, in DocFlow oppure presso il produttore (configurati coerentemente con il contratto di servizio), l'eliminazione dei pacchetti di archiviazione.

In caso di archivi pubblici e privati di particolare interesse storico e culturale, le procedure di scarto avvengono previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.

[Torna al sommario](#)

7.8.1 Chiusura del servizio di conservazione

A seguito della cessazione del contratto per la conservazione dei documenti la B.U Sales o la B.U. Backoffice segnalano al Servizio di Conservazione la fine del contratto.

Il Servizio di conservazione provvede a creare un pacchetto di esibizione per ogni pacchetto di archiviazione e provvede poi ad eliminare i pacchetti di archiviazione

I pacchetti di esibizione così realizzati vengono inviati al produttore se previsto dagli accordi di servizio (specificità di contratto).

A consegna avvenuta vengono eliminati tutti i dati relativi al produttore ed ai suoi utenti.

[Torna al sommario](#)

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

Per una corretta erogazione di un servizio di conservazione a norma che risponda alle caratteristiche richieste dallo standard OAIS, una qualsiasi applicazione di conservazione deve essere in grado di esportare i documenti conservati in un formato che garantisca l'integrità della conservazione stessa.

L'applicazione del sistema di conservazione, essendo progettata secondo lo standard OAIS è in grado di esportare i singoli pacchetti di archiviazione generati durante gli anni, seguendo le regole che permettono successivamente di importare i pacchetti in un altro sistema OAIS *compliant*.

Il sistema conservazione è predisposto per gestire i formati che possono maggiormente garantire i principi di interoperabilità tra i sistemi di conservazione, in base alla normativa vigente riguardante le specifiche tipologie documentali.

A tal fine il sistema di conservazione, in conformità a quanto previsto dall'allegato 2 del DPCM 3 Dicembre 2013, adotta i principali standard di formati e di gestione di tracciati di dati così come di seguito riportato:

- Per l'accettazione degli oggetti da conservare, l'aderenza ai formati previsti dal presente Manuale e dall'allegato 2 delle regole tecniche richiamate;
- Per la generazione dell'Indice del pacchetto di archiviazione, l'aderenza allo standard UNI 11386 SInCRO secondo lo schema allegato al DPCM 3 dicembre 2013;
- ai fini della generazione dei pacchetto di distribuzione, come specificato dall'articolo 9, comma 1, lett. h) delle regole tecniche coincidenti con i pacchetti di archiviazione..

In particolare, per il caso specifico di trasferimento/versamento da altro conservatore – e sempre in accordo con il soggetto Produttore – il sistema di conservazione prenderà in carico solamente i pacchetti di distribuzione generati in conformità al “Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali”, (c.d. SInCRO), ossia dalla norma UNI 11386 dell'ottobre 2010.

[Torna al sommario](#)

7.10 Attività proprie di gestione dei sistemi informativi

Di seguito sono descritte le attività riguardanti la gestione del sistema di conservazione:

7.10.1 conduzione e manutenzione del sistema di conservazione

Il sistema di conservazione è gestito dal Servizio di Conservazione che provvede alle attività ordinarie e straordinarie per la operatività.

Qualora le attività dovessero richiedere particolari competenze o risorse, il responsabile dell'unità potrà richiedere l'intervento del Servizio di sviluppo e manutenzione per far fronte alle esigenze del caso.

[Torna al sommario](#)

7.10.2 monitoraggio del sistema di conservazione

Il responsabile del servizio di conservazione provvede a monitorare il sistema di conservazione in merito a prestazioni, sicurezza, presenza di errori e anomalie.

Il controllo avviene tramite procedure automatiche e manuali descritte nel capitolo relativo alla sicurezza.

[Torna al sommario](#)

7.10.3 change management

I criteri di accettazione per i nuovi sistemi, aggiornamenti e nuove versioni sono preventivamente stabilite e vengono effettuate prove appropriate durante lo sviluppo e prima dell'approvazione. Tutti gli sviluppi interni sono testati anche su sistemi di test. L'accettazione del nuovo software è considerata dopo aver verificato se il suddetto software adempie ai criteri di accettazione. Il Responsabile di Sviluppo e Manutenzione del sistema di conservazione unitamente al proprio staff è responsabile di tali controlli.

[Torna al sommario](#)

7.10.4 verifica periodica di conformità a normativa e standard di riferimento.

La verifica periodica di conformità a normativa e standard di riferimento avviene a cura del Responsabile della funzione archivistica e del Responsabile dello sviluppo e manutenzione del sistema di conservazione.

La verifica avviene sia con incontri formali e programmati, sia occasionalmente a seguito di variazioni e/o novità nella normativa e negli standard di riferimento

[Torna al sommario](#)

8 IL SISTEMA DI CONSERVAZIONE

8.1 Componenti Logiche

Di seguito lo schema e la descrizione delle entità funzionali relative al sistema di conservazione e al suo funzionamento.

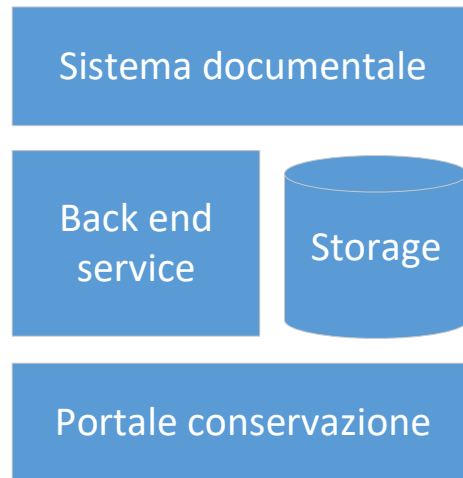


Figura 2 - Componenti logiche

Sistema documentale: riceve i pacchetti di versamento o i documenti da parte del Cliente. I documenti sono ricevuti da con le modalità concordate con i singoli Clienti e dettagliato nelle specificità di contratto. Prepara, se richiesto, il pacchetto di versamento acquisendo i metadati concordati con le specificità di contratto concordate.

Back end service: effettua il controllo dei PdV, genera il rapporto di versamento, firmandolo in maniera automatica e scartando i pacchetti che non superano i controlli. Genera i pacchetti di archiviazione, appone la firma digitale del Responsabile del Servizio di Conservazione e appone la marca temporale. Effettua i controlli di coerenza tra PdV e PdA e provvede all'archiviazione sui sistemi di storage.

Portale conservazione: consente agli utenti del Cliente e del Conservatore l'accesso ai documenti ed alle relative procedure consentite. In particolare è consentita la ricerca e consultazione dei documenti conservati e la richiesta di preparazione e, eventualmente, sottoscrizione dei pacchetti di distribuzione.

[Torna al sommario](#)

8.2 Componenti Tecnologiche

Le componenti tecnologiche di cui al precedente paragrafo 8.1 sono implementate usando le seguenti tecnologie:

Sistema documentale: il programma che gestisce i pacchetti di versamento è basato su tecnologia Microsoft framework .Net, Microsoft ASP e FTP. Usa il database Microsoft SQL Server.

Back end service: che gestisce i controlli dei PdV e la generazione dei pacchetti di archiviazione è basato su Microsoft framework .Net e database Microsoft SQL Server.

Portale di conservazione: che gestisce l'iterazione con il sistema di conservazione è sviluppato su tecnologia Microsoft ASP.NET e usa il database Microsoft SQL Server

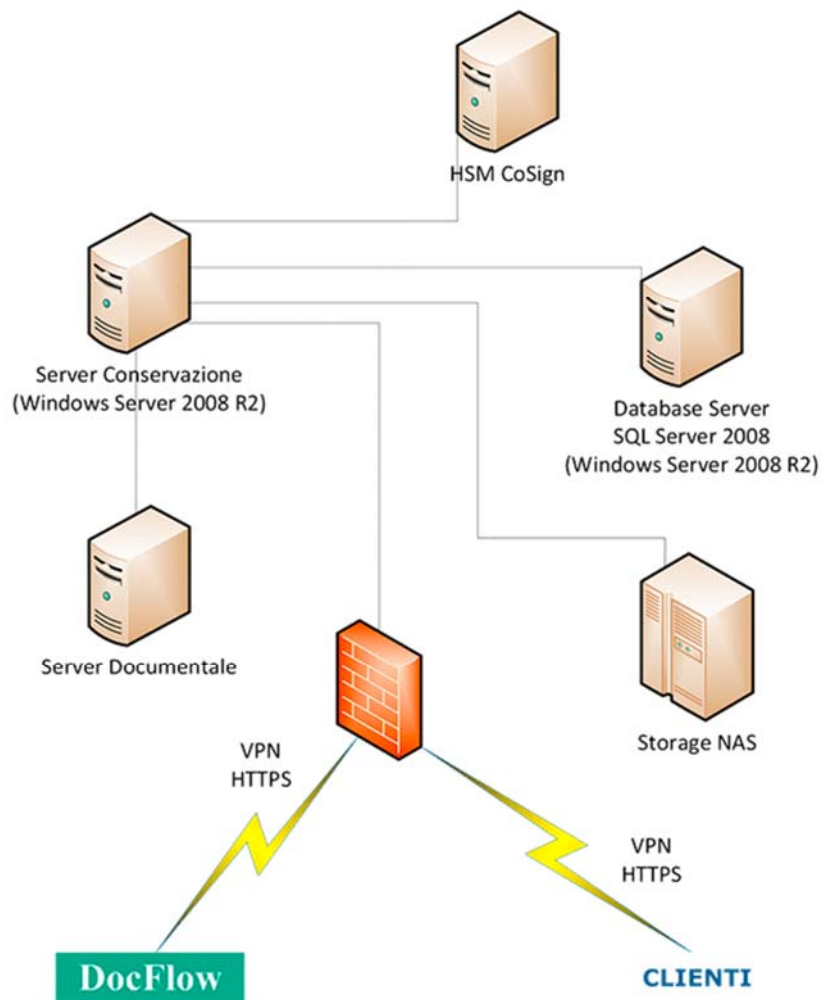


Figura 3 - Componenti tecnologiche

8.3 Componenti Fisiche

Le macchine che costituiscono l'infrastruttura sono per la maggior parte costituiti da apparati virtuali. Questi ultimi vengono ospitati all'interno di un Datacenter che garantisce continuità di servizio tramite formula SaaS.

Tramite la suddetta formula vengono erogati anche tutti i servizi riguardanti networking, firewalling e security, ed include la manutenzione di tutti gli apparati.

A completare il sistema di conservazione sono utilizzati due apparati HSM ridondati tramite configurazione High Availability che forniscono i servizi di Firma Elettronica.

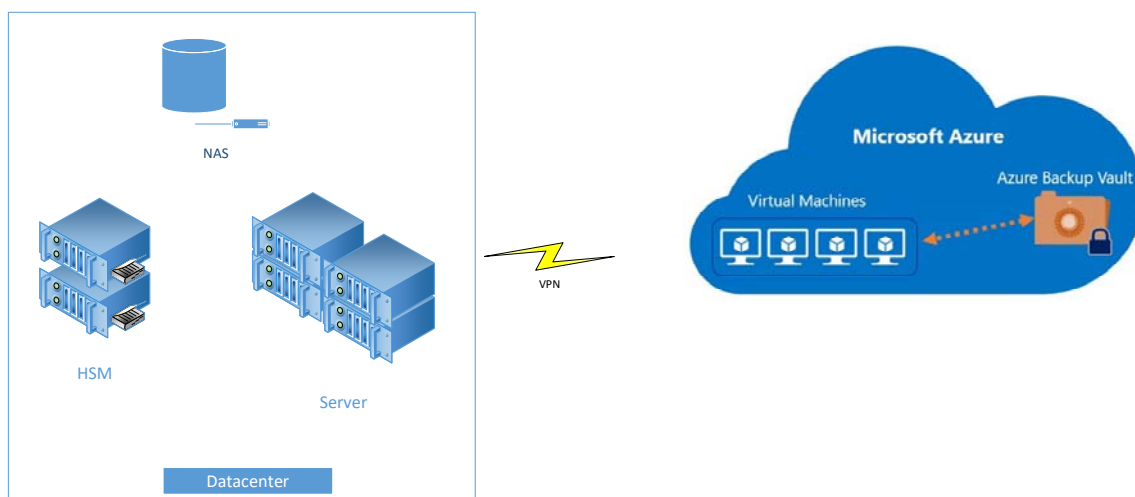


Figura 4 - Componenti fisiche

I documenti da conservare vengono importati in maniera automatica dai servizi di conservazione che utilizzano il Server Documentale per elaborare dati.

Da questo si procede quindi all'archiviazione dei documenti sul NAS, utilizzando il Database Server per estrarre i dati necessari alla compilazione della banca dati che identificherà i documenti da conservare.

A questo punto del processo, i servizi sul server di Conservazione interrogano il Database per recuperare l'elenco dei documenti da conservare, e questi ultimi vengono processati applicando Firma Elettronica e Marca Temporale, rilasciati dal dispositivo di firma HSM.

[Torna al sommario](#)

8.4 Procedure di Gestione e di evoluzione

8.4.1 Start up del servizio

Il processo di start up garantisce la presa in carico del servizio di conservazione in base alle caratteristiche dei documenti da conservare indicati nelle specificità di contratto nel rispetto del presente manuale di conservazione.

[Torna al sommario](#)

8.4.1.1 Gestione apertura commessa in SaaS

All'arrivo di un ordine di attività progettuali che preveda l'attivazione del servizio di conservazione, dopo l'apertura della commessa di progetto viene organizzato il kick off coinvolgendo il Project Manager, il Direttore Tecnico, il Commerciale e l'Experience Manager individuato dalla Direzione Operativa.

Alla conclusione del kick Off viene notificata all'area SAAS la partenza dei lavori e la data prevista di attivazione del servizio mediante il sistema informatico con la creazione di una commessa saas in set up.

Le informazioni ricavabili dai dati di commessa sono

- ragione Sociale Cliente;
- descrizione servizi da attivare;
- riferimento della commessa progettuale;
- contratto cliente
- offerta commerciale

L'Experience Manager provvede a coinvolgere gli incaricati per la gestione delle deleghe necessarie ad operare e la redazione delle specificità di contratto.

L'incaricato delle deleghe si occuperà dei rapporti con il cliente, e di adattare e di far approvare in azienda quanto concordato.

L'incaricato delle specificità di contratto si occuperà di redigere il documento di specificità di contratto relativo al servizio di conservazione per i clienti.

[Torna al sommario](#)

8.4.1.2 Apertura commessa Servizi

All'attivazione del servizio l'Experience Manager informa l'Amministrazione Vendite la quale provvederà ad attivare la commessa di servizio precedentemente in set up.

[Torna al sommario](#)

8.4.1.3 Organizzazione del servizio

Il Project Manager designato, una volta ricevuta la notifica automatica di assegnazione commessa, visualizza il contratto e organizza il servizio. Pianifica le attività in relazione alle quantità dei documenti da conservare e al flusso dei dati necessari per la creazione degli indici di archiviazione.

[Torna al sommario](#)

8.4.1.4 Richiesta attivazione del canale di comunicazione

Il Project Manager designato richiede mediante l'apposito sistema informatico l'intervento del System Administrator, per la configurazione del Firewall, indicando i parametri di sistema necessari alla acquisizione del pacchetto di versamento. La richiesta è completata con i dati necessari alla configurazione (IP e i protocolli di comunicazione) contenuti nell'apposito modulo. Il Project Manager verifica prima dell'invio della richiesta che la sia congruente con il contratto.

[Torna al sommario](#)

8.4.1.5 Approvazione dell'attività di attivazione del canale di comunicazione

L'attività viene preventivamente approvata dall'ICT Governance Manager il quale verifica che la richiesta sia congruente con l'infrastruttura ed eventualmente aggiunge ulteriori indicazioni.

[Torna al sommario](#)

8.4.1.6 Attivazione del canale di comunicazione

Il System Administrator richiede al datacenter l'attività di configurazione tramite il sistema di ticketing messo a disposizione dai gestori del datacenter. A chiusura dell'attività, il sistema invia una notifica ai Sistemi informativi DocFlow. Il System Administrator provvede a verificare l'efficacia dell'intervento e nel caso in cui il test sia positivo chiude la Richiesta di Attività. Il sistema invia una notifica al richiedente e all'area ICT & Infrastructure.

[Torna al sommario](#)

8.4.1.7 Configurare servizi di conservazione

Il Project Manager configura il servizio di conservazione in base alle indicazioni contenute nel manuale di gestione operativa del software che trasferisce il pacchetto di versamento fornito dal Cliente o dal Project Manager DocFlow nel caso di progetto interno di sviluppo.

In particolare:

- crea l'utente esterno per accesso ai sistemi DocFlow o l'utenza DocFlow per l'accesso ai sistemi del Cliente;
- configura la cartella di sistema;
- configura i controlli previsti sul contratto;
- consegna/richiede al cliente le credenziali di accesso per l'acquisizione del pacchetto di versamento;
- configura i servizi necessari al ricevimento del pacchetto di versamento;
- configura gli stylesheet, se necessari, alla visualizzazione dei pacchetti di versamento e archiviazione.

Il codice sorgente del Software applicativo finito è gestito con un apposito programma software. Le personalizzazioni realizzate per i clienti sono archiviate nell'apposita directory sul server aziendale.

La rintracciabilità è assicurata dalla possibilità di poter sempre identificare il prodotto/servizio finito, attraverso il numero di commessa interna e il nome del destinatario finale e di poterlo correlare con i documenti di progettazione, sviluppo e installazione.

[Torna al sommario](#)

8.4.1.8 Collaudo e validazione

Il Project Manager esegue le prove previste per accertare il raggiungimento degli standard richiesti, anche con il supporto del cliente ed esegue il controllo finale per verificare la conformità alle richieste contrattuali.

I controlli sono registrati su apposita modulistica, la quale è conservata secondo quanto previsto dalla procedura per la gestione delle registrazioni.

[Torna al sommario](#)

8.4.2 Modifiche al sistema

In caso di variazioni normative, contrattuali, tecnologiche o relative a valutazioni di opportunità in ambito della sicurezza, saranno valutati dal Responsabile del servizio di conservazione, dall'Archivista, dal Responsabile dello Sviluppo dei sistemi e dal Responsabile della sicurezza, eventuali modifiche al sistema di conservazione.

Le modifiche saranno affidate a risorse che abbiano la necessaria competenza professionale e saranno pianificate in modo da minimizzare gli impatti sulle funzionalità del sistema. Eventualmente le risorse disponibili non fossero sufficienti si provvederà alla formazione di altre persone.

Le nuove implementazioni dovranno essere valutate conformemente a quanto previsto dal punto 8.4.1.8 e al punto 7.10.3.

[Torna al sommario](#)

8.5 Gestione e conservazione dei log

In accordo con quanto previsto all'interno del SGSI aziendale, tutti gli accessi al sistema di conservazione sono regolarmente monitorati; in tal modo i tentativi di accesso non autorizzati sono prevenuti e, inoltre, in caso di incidente, è possibile certificare in maniera inequivocabile l'avvenuto accesso non autorizzato.

In particolare, la procedura in oggetto regola il processo di gestione delle seguenti tipologie di file di log:

- Log di security software;
- Log di sistema;
- Log applicativi;
- Log di base dati;
- Log regolamentati dalla normativa vigente (attività degli Amministratori di Sistema).

Tali tipologie di log sono conservati per un periodo non superiore a quello strettamente necessario per l'espletamento degli adempimenti di legge. In particolare, DocFlow ha definito un periodo di conservazione almeno di 180 giorni.

La necessità di proroga dei tempi di conservazione deve essere formalmente autorizzata dal responsabile designato e resa nota agli uffici interessati.

I sistemi su cui risiedono i file di log precedentemente indicati devono garantire la riservatezza, integrità e disponibilità delle registrazioni. Superato il limite massimo del periodo di conservazione, i log devono essere cancellati dal sistema che li ha generati e dai sistemi di backup con tecniche atte a garantire l'irrecuperabilità degli stessi. Qualora le informazioni di log facciano riferimento a dati personali di cui il trattamento sia ritenuto concluso (es. un utente che non sia più in azienda si procede alla cancellazione degli stessi da tutti i sistemi, dispositivi e supporti utilizzati per la memorizzazione).

Le modalità di gestione delle diverse tipologie di log sono descritti all'interno della specifica Istruzione operativa.

[Torna al sommario](#)

9 MONITORAGGIO E CONTROLLI

Il sistema di conservazione richiede, data la natura del servizio cui è preposto, una particolare cura per il monitoraggio ed il controllo sistema stesso. Di seguito la descrizione generale della strategia della conservazione e dei conseguenti obiettivi di monitoraggio e controllo (Regole Tecniche: art. 8, comma 2, lettera h).

[Torna al sommario](#)

9.1 Procedure di monitoraggio

Il processo di monitoraggio, mira a misurare ed analizzare periodicamente le performance del sistema di conservazione e, in generale, dell'intero sistema di Information Security ed il livello di compliance dei processi di sicurezza al modello di governance predefinito.

Il processo monitoraggio prevede tre livelli:

- Attività di monitoraggio di I livello (KPI di sicurezza): il responsabile della sicurezza effettua un monitoraggio degli eventi di sicurezza logica ed una raccolta dei relativi indicatori, inviati mensilmente ai responsabili del servizio
- Attività di Monitoraggio di II livello (KPI Infosec): verifica della corretta attuazione a livello operativo di processi e procedure definiti per gli Information Security Domain e Management Process. L'attività di monitoraggio di II livello prevede la valorizzazione dei KPI minimi definiti per tutti gli Information Security Domain e Management Process, che vengono inviati semestralmente alla direzione.
- Attività di Monitoraggio di III livello (audit interni): verifica della corretta attuazione del modello di Information Security Governance attraverso audit condotti internamente da parte della funzione responsabile della sicurezza, con successivo coinvolgimento e condivisione dei risultati con la direzione.

Le attività di monitoraggio prevedono l'identificazione di eventuali aree di debolezza, con la definizione, laddove necessario, di piani/ proposte di miglioramento che andranno in input al relativo processo.

Al monitoraggio dei KPI si affianca il monitoraggio applicativo.

Ulteriori procedure aggiuntive richieste dal soggetto Produttore sono descritte nell'allegato "Specificità del contratto".

[Torna al sommario](#)

9.2 Controlli

Il sistema di conservazione implementa numerosi funzionalità per il controllo del corretto svolgimento dei processi, segnalando eventuali errori o anomalie al personale incaricato dell'amministratore del sistema.

I controlli effettuati si distinguono nelle due tipologie: controlli di processo e controlli periodici.

[Torna al sommario](#)

9.2.1 Mantenimento della leggibilità nel tempo

Al fine di assicurare la leggibilità nel tempo, il Responsabile della conservazione predispone, controlli periodici, con cadenza non superiore ai cinque anni al fine di verificare che i dati non siano corrotti, i sistemi hardware e software non siano obsoleti e i formati dei documenti conservati siano tuttora supportati.

I predetti controlli saranno effettuati dal Responsabile del servizio di conservazione, dal Responsabile dei sistemi per la conservazione, dal Responsabile dello sviluppo dei sistemi, dall'Archivista.

Al fine di evitare che l'evidenza delle summenzionate illeggibilità appaia quando il processo sia ormai irreversibile, ad ogni controllo sullo stato dei fatti, seguirà una valutazione preventiva dell'evoluzione di mercato e tecnologica in modo da poter decidere ed attuare azioni preventive.

[Torna al sommario](#)

9.2.2 Controlli di processo

I controlli di processo si svolgono in maniera sincrona all'elaborazione dei pacchetti soggetti al processo di conservazione.

Il sistema implementa numerosi controlli automatici a garanzia dell'integrità e della coerenza dei dati movimentati dal sistema; i controlli automatici richiedono l'intervento del Responsabile della funzione di Conservazione solo al verificarsi di eventi anomali non gestibili in modo automatico.

Tra i controlli, quelli automatici riguardano la coerenza e conformità dei metadati trasferiti dal Produttore all'interno di ciascun PdV. Nello specifico, la piattaforma di conservazione è in grado di assegnare, in fase di configurazione del servizio, a ciascun metadato un controllo specifico secondo il seguente schema:

- Incrementale: verifica che il valore associato al documento in verifica sia maggiore o uguale al valore dell'ultimo documento caricato;
- Ordinato: permette di ordinare i documenti per i valori associati all'indice configurato;
- Elapsed: verifica che la data relativa all'indice selezionato più il numero di giorni stabilito in fase di configurazione come valore di riferimento, sia maggiore della data attuale.
- Obbligatorio: verifica che l'indice selezionato sia sempre valorizzato.
- Sequenziale: verifica che il valore associato al documento in verifica sia immediatamente successivo al valore dell'ultimo documento caricato.

[Torna al sommario](#)

9.2.3 Controlli di sistema

Il responsabile del servizio di conservazione supervisiona e controlla la gestione dei problemi e del rispetto dei livelli di servizio per tutte le applicazioni e tramite delle Dashboard di monitoraggio controlla lo stato di salute dell'infrastruttura e dei servizi e, in caso di criticità, contatta proattivamente, gli specialisti dell'unità assistenza e del servizio sviluppo e manutenzione.

Il sistema di monitoraggio utilizzato ha lo scopo di controllare lo stato di funzionamento e le performance delle applicazioni dei sistemi e dei servizi erogati, compresa la piattaforma di conservazione ed è in grado di inviare, anche in automatico, segnalazioni mail ai responsabili del service per le azioni di ripristino in caso di anomalie.

I controlli attivi sulla piattaforma di monitoraggio sono suddivisi nelle seguenti aree:

- System Management, Application Management e flussi di lavorazione.
- User Experience
- Transaction management

Gli allarmi generati dal sistema di monitoraggio sono classificati in base al loro impatto sul servizio in:

- **Critical:** eventi bloccanti con impatto diretto sul corretto funzionamento del sistema, dell'applicazione e/o del servizio;
- **Warning:** eventi non bloccanti che segnalano un degrado prestazionale del sistema, dell'applicazione e/o del servizio;
- **Normal:** eventi di rientro che segnalano il ripristino delle corrette funzionalità di un sistema, di un'applicazione e/o di un servizio in seguito ad un evento Critical o a un Warning.

Le persone addette al servizio di conservazione, supervisionano quotidianamente la piattaforma con lo scopo di individuare le cause dei malfunzionamenti registrati nel periodo, analizzare le soluzioni contingenti adottate per il superamento del problema e sviluppare eventuali proposte per rimedi strutturali.

[Torna al sommario](#)

9.2.3.1 Riesame del servizio

Qualora necessario, il Responsabile del Servizio di Conservazione effettua un riesame generale del servizio insieme ai soggetti incaricati, al fine di accertare la conformità del sistema al livello di servizio atteso, analizzare le cause di eventuali incidenti o disservizi e promuovere attività di prevenzione o miglioramento.

Qualora necessario, una riunione di riesame può essere indetta a fronte di particolari eventi (ad esempio, a titolo non esaustivo, cambi tecnologici, normativi o di requisiti funzionali, stagionalità di carico elaborativo, arrivo consistente e non pianificato di nuova clientela, ecc.).

Per ogni riunione è redatto un apposito verbale contenente i punti trattati e la sintesi della discussione.

[Torna al sommario](#)

9.2.3.2 *Auditing generale del servizio*

Il Responsabile della Funzione Archivistica di Conservazione pianifica e implementa processi di audit che coinvolgono aspetti di processo, organizzazione, tecnologici e logistici. L'obiettivo è accertare la conformità del sistema alle leggi, ai regolamenti, al contratto, alla documentazione generale del servizio, ai principi che ispirano il sistema qualità e al presente Manuale della Conservazione.

L'audit è un processo almeno annuale fondamentale per lo screening del sistema, in quanto consente l'individuazione delle aree critiche di intervento e la pianificazione dei necessari interventi sul sistema o sul servizio, ragion per cui viene svolto periodicamente.

Prima dell'avvio delle attività di verifica il piano di dettaglio viene discusso con il Responsabile del Servizio di Conservazione ed in esso vengono riportati:

- i nominativi degli auditor e del loro Responsabile (nel caso di visite di verifica dei risultati di azioni correttive o interessanti un aspetto molto limitato, l'attività di audit può essere svolta da una sola persona);
- le aree sottoposte a verifica e i rispettivi responsabili coinvolti;
- la data prevista per l'inizio ed il termine dell'audit;
- gli obiettivi dell'attività e il campo di applicazione.

Prima dello svolgimento della sessione di verifica, il Responsabile dell'attività di audit può decidere di esaminare documenti concernenti l'ambito di analisi allo scopo di valutarne l'adeguatezza, così come precedenti Verbali di Audit per annotare la presenza di eventuali azioni correttive in corso d'opera e registrare eventuali osservazioni da chiarire o approfondire in sede di audit.

L'esecuzione dell'audit si articola in colloqui, esami di documenti, indagini sul modo di operare e può essere supportata dall'utilizzo di liste di riscontro per la raccolta delle evidenze.

Durante la verifica vengono valutate la realizzazione e l'efficacia delle eventuali azioni correttive intraprese per risolvere "Non Conformità" precedentemente evidenziate sulla base dell'analisi effettuata.

Le evidenze raccolte in fase di audit vengono classificate in funzione delle non conformità rilevate.

Quando si identifica un mancato soddisfacimento sistematico di un requisito, sia esso di natura normativa, il mancato rispetto di uno standard o di una security policy, tale da compromettere il raggiungimento degli obiettivi del processo e/o precluderne il controllo viene emessa una non conformità.

Sono tre le parti in cui si articola la documentazione di una "Non Conformità":

- l'evidenza emersa dall'audit
- l'indicazione del requisito a fronte del quale è stata rilevata la non conformità
- la formulazione della non conformità.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalia

9.3.1 Incident management

DocFlow è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione, in modo da individuare previamente ogni potenziale causa di incidente e provvedere alla sua rimozione, scongiurando il blocco del sistema o il danneggiamento dei files in esso contenuti.

Qualora si verificasse un incidente di sistema o di processo, le operazioni di ripristino della funzionalità seguono una procedura definita e documentata all'interno del proprio Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla ISO27001:2013. Per ogni incidente con impatti sul rispetto della normativa, viene redatto un apposito verbale.

Il responsabile del servizio di conservazione mantiene i verbali degli incidenti e delle contromisure attuate, e tali documenti diventano oggetto della successiva riunione di riesame e vengono inviati al sistema di conservazione.

[Torna al sommario](#)