

# MANUALE DI CONSERVAZIONE DI INDICOM eDOCUMENT CARE SRL

## EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
<i>Redazione</i>		Giancarla Porro	dRSDC
		Massimiliano Barbisotti	dRSIC
<i>Verifica</i>		Roberto Chieselli	RSCI
			RSMC
<i>Approvazione</i>		Gianluigi Porro	RSDC Legale Rappresentante

## REGISTRO DELLE VERSIONI

Versione	Data emissione	Modifiche apportate	Osservazioni
1.0	18.12.2015	Prima emissione	
2.0	06.06.2016	Recepimento richieste AgID verbale del 09.03.2016	
2.1	08.01.2018	Modifica 5.1 Premessa Modifica 4 Ruoli e responsabilità e 5.2 organigramma Modifica 6.4 Piano di cessazione	
3.0	18.01.2018	Modifica carta intestata Modifica per aggiornamento schemi grafici Modifica 8.2 componenti tecnologiche e fisiche Modifica cap. 9	
3.1	11.07.2018	Aggiornamento Indice Aggiornamento 3.4 Certificazioni Modifica 4 Ruoli e responsabilità e 5.2 organigramma	
4.0	28.01.2021	Aggiornamento per attivazione seconda piattaforma di conservazione (ArchiCons)	





## SOMMARIO

<b>1</b>	<b>SCOPO E AMBITO DEL DOCUMENTO .....</b>	<b>5</b>
<b>1.1</b>	<b>Contesto di riferimento.....</b>	<b>5</b>
<b>1.2</b>	<b>Software per la Conservazione.....</b>	<b>6</b>
<b>2</b>	<b>TERMINOLOGIA (GLOSSARIO E ACRONIMI) .....</b>	<b>6</b>
<b>2.2</b>	<b>Glossario .....</b>	<b>6</b>
<b>2.3</b>	<b>Acronimi .....</b>	<b>9</b>
<b>3</b>	<b>NORMATIVA E STANDARD DI RIFERIMENTO .....</b>	<b>11</b>
3.1	Riferimenti normativi.....	11
3.2	Riferimenti tecnici.....	11
3.3	Standard di riferimento.....	12
3.4	Certificazioni .....	12
<b>4</b>	<b>RUOLI E RESPONSABILITA' .....</b>	<b>13</b>
4.1	Cronologia Incarichi .....	13
4.2	Incarichi in essere.....	14
4.3	Altri ruoli .....	16
<b>5</b>	<b>STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE .....</b>	<b>17</b>
5.1	Organigramma .....	17
5.2	Struttura organizzativa.....	18
<b>6</b>	<b>OGGETTI SOTTOPOSTI A CONSERVAZIONE.....</b>	<b>22</b>
6.1	Oggetti conservati.....	23
6.2	Pacchetto di versamento .....	25
6.3	Pacchetto di archiviazione .....	27
6.4	Pacchetto di distribuzione.....	28
<b>7</b>	<b>IL PROCESSO DI CONSERVAZIONE .....</b>	<b>30</b>
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico.....	32
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti .....	34
7.2.1	Controllo Formale .....	34

7.2.2	Controllo sui METADATI.....	34
7.2.3	Log e Registri dei Pacchetti di Versamento.....	35
7.2.4	Controllo sulle firme .....	36
7.2.5	Controlli sui Formati.....	36
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico. ....	37
7.3.1	Attributi calcolati dal sistema (fase di versamento) .....	37
7.3.2	Struttura del rapporto di versamento .....	38
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	39
7.5	Preparazione e gestione del pacchetto di archiviazione .....	40
7.5.1	Creazione del Pacchetto di Archiviazione.....	41
7.5.2	Risoluzione delle anomalie o forzatura del processo di conservazione .....	41
7.5.3	Generazione dell'IPdA.....	41
7.5.4	Sottoscrizione dell'IPdA .....	42
7.5.5	Apposizione della marca temporale .....	43
7.5.6	Memorizzazione del PdA nel Supporto di Conservazione .....	44
7.6	Predisposizione delle copie di backup .....	44
7.7	I log delle operazioni di conservazione .....	44
7.8	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione .....	44
7.9	Produzioni di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti .....	46
7.10	Scarto dei pacchetti di archiviazione .....	46
7.11	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori .....	47
<b>8</b>	<b>IL SISTEMA DI CONSERVAZIONE.....</b>	<b>48</b>
8.1	Componenti Logiche del Sistema ConSEDFx.....	49
8.1.1	Front/end applicativo.....	49
8.1.2	Schedule & Business Logic .....	49
8.1.3	Database .....	50
8.1.4	Workarea.....	50
8.1.5	Engine documentale .....	50

8.2	Componenti Logiche del Sistema ArchiCons.....	50
8.3	Componenti Fisiche della piattaforma ConSEDFx.....	52
8.3.1	Procedure di gestione e di evoluzione.....	53
8.3.2	Gestione e conservazione dei log .....	54
8.3.3	Monitoraggio del sistema .....	54
8.3.4	Change management .....	54
8.3.5	Verifica periodica di conformità a normativa e standard di riferimento.....	54
8.4	Componenti Fisiche della piattaforma ArchiCons.....	55
<b>9</b>	<b>MONITORAGGIO E CONTROLLI .....</b>	<b>57</b>
9.1	Procedure di monitoraggio .....	57
9.2	Verifica dell'integrità degli archivi .....	58
9.3	Soluzioni adottate in caso di anomalie .....	59

## 1 SCOPO E AMBITO DEL DOCUMENTO

Il presente documento è il Manuale della Conservazione di Indicom eDocument Care Srl, di seguito IDC, redatto ai sensi dell'art. 8 DPCM del 3 dicembre 2013.

Il manuale ha lo scopo di specificare le regole e le procedure per la conservazione a norma dei documenti informatici e riporta dettagliatamente le informazioni sull'organizzazione e i soggetti coinvolti nel processo di conservazione. Descrive inoltre il processo di conservazione nelle sue fasi operative e tutte le attività svolte per rispettare gli standard di riferimento, nonché le misure di sicurezza adottate (si veda il documento "Piano per la Sicurezza" e la "Politica di classificazione delle informazioni – ISPD").

Eventuali particolarità legate alle singole forniture del Servizio di Conservazione, condivise con il singolo Cliente, sono descritte nel documento "Specificità del contratto".

Si evidenzia che Il servizio viene erogato nel rispetto dei requisiti di continuità, sicurezza fisica e logica, e monitoraggio, che i Data Center ove risiedono le piattaforme di conservazione garantiscono e descrivono negli specifici documenti di certificazione.

IDC ha implementato nel suo Sistema di Gestione della Sicurezza delle Informazioni (SGSI), un impianto di policy che rappresenta il contesto di riferimento costante nella gestione del servizio di conservazione.

### 1.1 Contesto di riferimento

Indicom Group è partner tecnologico di riferimento per Imprese, Associazioni di Categoria e Studi di Professionisti per i servizi di Information Management e Back Office Amministrativo in outsourcing.

Il Gruppo nasce nel 2001 come Indicom Document Care, dall'esperienza ventennale dei suoi soci fondatori e del loro team di professionisti, concentrandosi fin dall'inizio sull'offrire servizi di Gestione Documentale e Business Process Outsourcing.

Allo scopo di garantire una maggiore capillarità sul territorio nazionale, nel 2005 Indicom si espande. Nasce così Indicom Centro Nord, società con sede a Riccione (RN) specializzata nell'offrire soluzioni di dematerializzazione e Gestione degli Archivi cartacei per imprese e Curatori fallimentari.

Nel 2014, in linea con l'evoluzione del panorama normativo in ambito fiscale ed amministrativo, nasce Indicom eDocument Care (di seguito IDC), specializzata nel fornire soluzioni di Fatturazione Elettronica, Conservazione Digitale a Norma, Consulenza Normativa e Firma Digitale. A luglio 2015 IDC ha ottenuto la Certificazione ISO/IEC 27001 e, un anno dopo, è ufficialmente diventata Conservatore Accreditato AgID – Agenzia per l'Italia Digitale.

Alle altre due società del Gruppo rimangono in carico i servizi di gestione documentale, BPO, Information Management, ecc. ecc.

Con decorrenza 1° agosto 2020 ha avuto effetto la fusione per l'incorporazione di Indicom S.r.l. e Indicom Centro Nord S.r.l. in Indicom eDocument Care S.r.l..

L'operazione rappresenta un rafforzamento dell'attuale struttura che, attraverso una gestione unitaria e coordinata dell'azienda e un maggiore controllo, persegue gli obiettivi di miglioramento dei propri processi interni.

Grazie alla fusione, infatti, viene garantita ai Clienti una proposta sempre più ottimizzata ed efficiente dei servizi offerti da IDC.

Vengono così infatti riunite, sotto un'unica realtà, tutte le attività affidate precedente alle società del gruppo, che nel loro complesso costituiscono l'intero processo di gestione documentale, dalla produzione dei documenti informatici alla conservazione digitale:

- attività di dematerializzazione dei documenti analogici (normalizzazione, scansione, indicizzazione, ecc.)
- indicizzazione
- attività di preparazione e aggregazione dei documenti informatici propedeutiche al versamento nel Sistema di Conservazione
- accesso alla piattaforma di gestione documentale per la consultazione operativa dei documenti non ancora sottoposti al processo di conservazione.
- processo di conservazione digitale a norma, come dettagliato nel presente Manuale, erogato in modalità fulloutsourcing

## 1.2 Software per la Conservazione

Per i processi di conservazione IDC utilizza il software ConSEDFx, piattaforma sviluppata da Wicome Srl, e il software ArchiCons, di proprietà di Archivium Srl, Conservatore accreditato AgID.

IDC utilizza i sistemi in piena autonomia, operando direttamente quale conservatore per conto dei propri clienti. Entrambe le piattaforme rispettano l'impianto normativo vigente e sono in linea con le Regole Tecniche emanate da AgID.

[Torna al sommario](#)

## 2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

### 2.2 Glossario

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

Termine	Definizione
Aggregatore	soggetto terzo al Cliente che si occupa di aggregare e confezionare i Lotti di Archiviazione in Pacchetti di Versamento, secondo quanto previsto dal manuale della conservazione e dagli accordi di servizio
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
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
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 analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
documento informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti
uplicazione dei documenti informatici	Produzione di duplicati informatici
ente produttore	persona fisica o giuridica 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.
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

Termine	Definizione
firma elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
firma elettronica avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, create con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati
firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un Sistema di chiavi crittografiche, una pubblica e una private, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
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
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
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
marca temporale	È il risultato di una procedura informatica – detta servizio di marcatura temporale – grazie alla quale si attribuisce a un documento informatico un riferimento temporale opponibile a terzi
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	detto anche PdD, pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	Detto anche PdV, pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato e descritto nel manuale di conservazione

Termine	Definizione
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
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	soggetto che determina quali documenti debbano essere inviati in conservazione. Il Produttore garantisce la corretta produzione dei documenti informatici, nel rispetto della normativa vigente.
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'art. 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	detto anche SdC, sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
Titolare	Il Titolare è soggetto produttore dei documenti informatici da conservare individuato come definito dall'art. 5, co.2, lett. a) del DPCM 3 dicembre in materia di sistemi di conservazione.
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](#)

## 2.3 Acronimi

Abbreviazione	Significato
ACQ	Responsabile Acquisti
AgID	Agenzia per l'Italia Digitale
AMM	Responsabile Amministrazione, Servizi Generali, Personale
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
COMM	Responsabile Commerciale

Abbreviazione	Significato
CRL	certificate revocation list, liste di certificati digitali revocati
CS	Responsabile operativo Conservazione Digitale a norma
DIR	Direzione
DLgs	Decreto Legislativo
DM	Decreto Ministeriale
DMEF	Decreto Ministero dell'Economia e delle Finanze
DPC	Responsabile Digital Processing Compliance
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
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
IDV	Indice di Versamento
IMPRONTA	a sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
ISPD	Information. Security Policy Document
OP	Responsabile Operazioni
P7M	Estensione dei file firmati con standard PKCS#7
PAeS	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
PdD	Pacchetto di Distribuzione
PdV	Pacchetto di Versamento
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
PROG	Responsabile Area Progetti
R&S	Responsabile Ricerca e Sviluppo
RDC	Responsabile della conservazione
RSDC	Responsabile del servizio di conservazione
RFAC	Responsabile della funziona archivistica
RP	Responsabile del trattamento dei dati personali
RSIC	Responsabile dei sistemi Informatici per la conservazione
RSSC	Responsabile Sicurezza dei sistemi per la conservazione
SdC	Sistema di Conservazione
SI	Responsabile Sistemi
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
SMC	Responsabile dello sviluppo e della manutenzione del SdC
UD	Unità Documentaria
UTC	UniversalTime Coordinated (Misura del tempo come stabilito dall'International Radio Consultative Committee –CCIR)
WORM	Write Once Read More

[Torna al sommario](#)

### 3 NORMATIVA E STANDARD DI RIFERIMENTO

Di seguito sono elencati, in ordine cronologico, i principali riferimenti normativi a livello nazionale per l'attività di conservazione.

#### 3.1 Riferimenti normativi

-**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*;

-**Decreto del Presidente della Repubblica del 26/10/1972 n. 633 e s.m.i.** *Istituzione e disciplina dell'imposta sul valore aggiunto*;

-**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 del 28/12/2000 n. 445** *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (G.U. n. 42 del 20 febbraio 2001)*

-**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 – modificato al 22 luglio 2014.*

-**Decreto Legislativo 7 marzo 2005 n.82** *Codice dell'amministrazione digitale (G.U. n.112 del 16 maggio 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 ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.*

[Torna al sommario](#)

#### 3.2 Riferimenti tecnici

-**Decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004** *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (G.U. n. 98 del 27 aprile 2004)*

- **DPCM 22 febbraio 2013** *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71. (13A04284) (GU n.117 del 21-5-2013)*

- **DMEF 3 aprile 2013, n. 55** *Regolamento in materia di emissione, trasmissione e ricevimento della fattura elettronica da applicarsi alle amministrazioni pubbliche ai sensi dell'articolo 1, commi da 209 a 213, della legge 24 dicembre*

- **DPCM 3 dicembre 2013** *Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20. commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1 del Codice dell' amministrazione digitale di cui al decreto legislativo n. 82 del 2005*

Eventuali norme specifiche relative alle diverse tipologie di documenti riguardanti il contratto di erogazione del servizio di conservazione sono riportate nell'allegato "Specificità del contratto".

[Torna al sommario](#)

### 3.3 Standard di riferimento

Gli standard di riferimento per l'attività di conservazione di IDC corrispondono a quelli elencati nell'allegato 3 del DPCM 03 Dicembre 2013 – Regole Tecniche in materia di Sistema di Conservazione:

- **ISO 14721:2012 OAIS** (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- **ISO/IEC 27001:2017**, Information technology - Security techniques - Information security management systems Requirements, Requisiti di un ISMS (Information Security Management System);
- **ETSI TS 101 533-1 V 1.3.1** (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 V 1.3.1 (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](#)

### 3.4 Certificazioni

-Certificazione **UNI EN ISO 9001:2015** - progettazione ed erogazione di servizi di conservazione digitale a norma e fatturazione elettronica

- Ente Certificatore: CISQ/Certiquality Srl
- N° Certificato: 22176
- N° IQNet: IT-99880
- *Prima emissione:* 15/07/2015
- Data Scadenza: 13/07/2021

-Certificazione **UNI CEI ISO/IEC 27001:2017** - gestione della sicurezza logica, fisica e organizzativa delle informazioni e dei documenti legati al processo di conservazione digitale

- Ente Certificatore: CISQ/Certiquality Srl
- N° Certificato: 22177
- Prima emissione: 15/07/2015
- Data Scadenza: 13/07/2021

-Certificazione di conformità ai requisiti individuati all'art. 24 del Regolamento UE 9101/2014 eIDAS

- Ente Certificatore: CISQ/Certiquality Srl
- N° Certificato: 25372
- Data Rilascio: 12/04/2018
- Data Scadenza: 10/04/2022

[Torna al sommario](#)

## 4 RUOLI E RESPONSABILITA'

### 4.1 Cronologia Incarichi

RUOLO	NOMINATIVO	ASSUNZIONE INCARICO	DATA CESSAZIONE
RSDC	<b>Gianluigi Porro</b>	dicembre-15	
dRSDC	<b>Giancarla Porro</b>	dicembre-15	
RFAC	Nicola Savino	dicembre-15	gennaio-18
	<b>Pietro Rocca</b>	gennaio-18	
dRFAC	Pietro Rocca	dicembre-15	gennaio-18
RP	Nicola Savino	dicembre-15	gennaio-18
	<b>Roberto Chieselli</b>	gennaio-18	

RUOLO	NOMINATIVO	ASSUNZIONE INCARICO	DATA CESSAZIONE
RSSC	Roberto Chieselli	dicembre-15	gennaio-18
	Marco Mariani	gennaio-18	giugno-18
	<b>Roberto Chieselli</b>	giugno-18	
dRSSC			
RSIC	<b>Roberto Chieselli</b>	dicembre-15	
dRSIC	<b>Massimiliano Barbisotti</b>	luglio-18	
RSMC	Marco Mariani	dicembre-15	gennaio-18
	Luigi Conti	gennaio-18	giugno-18
	<b>Roberto Chieselli</b>	giugno-18	
dRSMC	Luigi Conti	dicembre-15	gennaio-18
	Claudio Orlandi	gennaio-18	Ottobre-18
	<b>Filippo Amadini</b>	luglio-18	

Le attività sono assegnate in base ai ruoli aziendali definiti, conformemente a quanto previsto nel documento "profili professionali" pubblicato da AgID. I ruoli coinvolti nel processo di conservazione sono descritti nel seguente prospetto:

#### 4.2 Incarichi in essere

Ruoli	Nominativo	Attività di competenza	Delegati
<b>Responsabile del servizio di conservazione</b> <b>[RSDC]</b>	Gianluigi Porro	<ul style="list-style-type: none"> <li>-Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione;</li> <li>-Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;</li> <li>-Corretta erogazione del servizio di conservazione all'ente produttore;</li> <li>-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</li> </ul>	<b>Giancarla Porro [dRSDC]</b> <ul style="list-style-type: none"> <li>-Definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente;</li> <li>-Corretta erogazione del servizio di conservazione all'ente produttore;</li> <li>-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</li> </ul>

		<p><i>-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;</i></p>	<p><i>trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</i></p>
<p><b>Responsabile Sicurezza dei sistemi per la conservazione [RSSC]</b></p>	<p>Roberto Chieselli</p>	<p><i>-Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle policy e procedure interne di sicurezza;</i></p> <p><i>-Segnalazione delle eventuali difformità al Responsabile del servizio di Conservazione e mette in atto le necessarie azioni correttive.</i></p>	
<p><b>Responsabile funzione archivistica di conservazione RFAC</b></p>	<p>Pietro Rocca</p>	<p><i>-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;</i></p> <p><i>-Definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</i></p> <p><i>-Monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</i></p> <p><i>-Collabora 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.</i></p>	
<p><b>Responsabile trattamento dati personali RP</b></p>	<p>Roberto Chieselli</p>	<p><i>-Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</i></p> <p><i>-Garanzia che il trattamento dei dati affidati dai clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati</i></p>	

		<i>personali, con garanzia di sicurezza e di riservatezza.</i>	
<b>Responsabile sistemi informativi per la conservazione</b>  <b>RSIC</b>	Roberto Chieselli	<ul style="list-style-type: none"> <li>-Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</li> <li>-Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</li> <li>-Segnalazione di eventuali difformità degli SLA al Responsabile del servizio di conservazione e messa in atto delle necessarie azioni correttive;</li> <li>-Pianificazione dello sviluppo delle infrastrutture tecnologiche del SdC;</li> <li>-Controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del Servizio di Conservazione</li> </ul>	<p><b>Massimiliano Barbisotti (dRSIC)</b></p> <ul style="list-style-type: none"> <li>-Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</li> <li>-Monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</li> <li>-Segnalazione di eventuali difformità degli SLA al Responsabile del servizio di conservazione e messa in atto delle necessarie azioni correttive;</li> </ul>
<b>Responsabile sviluppo e manutenzione del sistema di conservazione</b>  <b>RSMC</b>	Roberto Chieselli	<ul style="list-style-type: none"> <li>-Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione;</li> <li>-Pianificazione e monitoraggio dei processi di sviluppo del sistema di conservazione;</li> <li>-Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;</li> <li>-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;</li> <li>-Gestione dello sviluppo dei siti web e portali connessi al servizio di conservazione.</li> </ul>	<p><b>Filippo Amadini (dRSMC)</b></p> <ul style="list-style-type: none"> <li>-Monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione;</li> <li>-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;</li> </ul>

#### 4.3 Altri ruoli

La conservazione digitale degli archivi aziendali è un processo che prevede necessariamente il coinvolgimento e la stretta collaborazione tra Titolare degli archivi e Conservatore.

In questa ottica, vengono individuate altre figure necessarie al completamento delle operazioni:

- Titolare:** Titolare dell'archivio oggetto di conservazione (Cliente). Mantiene la responsabilità sul contenuto dei documenti
- Produttore:** soggetto che determina quali documenti debbano essere inviati in conservazione. Il Produttore garantisce la corretta produzione dei documenti informatici, nel rispetto della normativa vigente. Ha inoltre la responsabilità della verifica del buon esito del versamento. Nella Pubblica Amministrazione il Produttore è soggetto interno all'organizzazione.
- Utente:** soggetto interno o esterno al Cliente, autorizzato dal Responsabile della Conservazione ad accedere al Sistema per la consultazione dei documenti
- Responsabile della conservazione:** persona fisica individuata all'interno del Cliente o, solo per i soggetti privati, all'esterno dell'organizzazione del Cliente e del Conservatore, dotata di idonee competenze volte a garantire il controllo del processo di Conservazione. Il RDC collabora con il Conservatore. Il RDC determina quali Utenti possono accedere al SdC e quali classi documentali debbano essere inviate al processo. Il RDC redige il Manuale della Conservazione del Cliente
- Aggregatore:** soggetto terzo al Cliente che si occupa di aggregare e confezionare i Lotti di Archiviazione in Pacchetti di Versamento, secondo quanto previsto dal manuale della conservazione e dagli accordi di servizio. L'aggregatore, o versante, assume la responsabilità per gli aspetti tecnologici del processo e non può in alcun modo essere responsabile del contenuto dei documenti oggetto di versamento e conservazione. IDC può assumere questo ruolo se debitamente indicato nell'accordo di servizio

Tutti i nominativi dei soggetti coinvolti sono indicati nella documentazione tecnica di contratto.

[Torna al sommario](#)

## **5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE**

### **5.1 Organigramma**

Qui di seguito l'organigramma del servizio di Conservazione a norma:

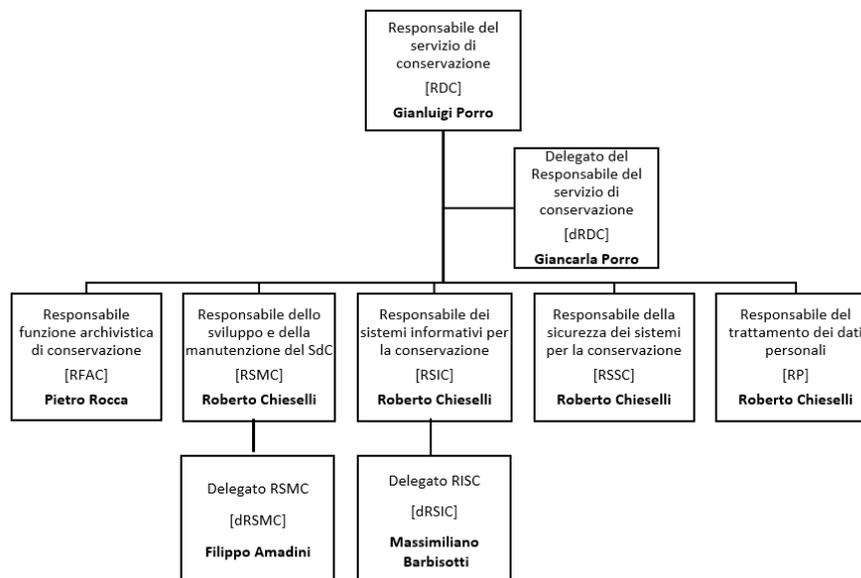


Figura 1 - Organigramma

[Torna al sommario](#)

## 5.2 Struttura organizzativa

Il sistema di conservazione digitale di IDC è logicamente separato dal sistema documentale, la cui gestione ricade sotto la responsabilità dell'Ente produttore, sia esso il Cliente o un terzo delegato dal Cliente stesso.

Il processo di conservazione, qui presentato in dettaglio e secondo le indicazioni fornite dalla norma, mostra una struttura e un'organizzazione, nonché una politica gestionale, atte a garantirne l'aderenza alla normativa vigente in materia di conservazione digitale. Il Responsabile del servizio di conservazione, insieme alle altre figure professionali individuate ed elencate in questo manuale, ha definito l'operatività e le attività di conservazione coerentemente con le politiche di efficienza gestionale e di risorse dell'azienda Indicom eDocument Care Srl, per far in modo che tutte le attività siano organizzate per produrre massima efficienza nell'ambito del processo globale di conservazione digitale.

Per il personale coinvolto nel servizio sono previste, ad esempio, le seguenti attività di formazione:

- il corretto utilizzo dei sistemi impiegati a supporto dell'attività quotidiana (e-mail, software ecc.);
- la responsabilità ed il ruolo;
- sessioni di formazione ove si tratti di personale in nuovo ingresso
- aggiornamento professionale dimostrabile con attestato di partecipazione rilasciato internamente o da ente esterno, a seguito di modifiche a norme e/o funzionalità e/o processi gestionali, e/o requisiti di sicurezza

L'analisi di eventuali problematiche viene assegnata dal RSDC alla funzione o alle funzioni competenti. Il risultato delle analisi viene condiviso con le funzioni coinvolte nella risoluzione, e le azioni correttive vengono coordinate e supervisionate dal RSDC.

Ove necessario è cura del RSDC coinvolgere nel processo di analisi e risoluzione il RDC dell'archivio di riferimento.

Il RSDC, inoltre, pianifica nel dettaglio, insieme alle funzioni da lui delegate a tali compiti, gli interventi di manutenzione necessari per garantire il mantenimento delle condizioni di sicurezza ed il minore impatto sulla produzione.

Di seguito lo schema che descrive sinteticamente il processo di conservazione e il coinvolgimento delle singole funzioni all'interno delle diverse fasi:

<b>Attività</b>	<b>Descrizione</b>	<b>Referente</b>
definizione e attuazione delle politiche complessive e di gestione del Sistema	predisposizione e aggiornamento del <i>Manuale di conservazione</i> in funzione delle tipologie documentali da conservare; pianificazione dei progetti di sviluppo del sistema di conservazione	RSDC – RSSC – DPC
attivazione del servizio di conservazione	gestione della parte contrattuale, compresi documenti di delega a RSDC, Privacy, credenziali di firma, deleghe, ecc. ecc.	COMM – OP – PROG – CS – RP
attivazione del servizio di conservazione	redazione del documento <i>Specificità del contratto</i> che contiene le tipologie documentali oggetto di conservazione, le modalità di trasferimento da parte dell'ente produttore, la descrizione archivistica dei documenti e delle aggregazioni documentali; definizione del set di metadati di conservazione	RDC – PROG – RFAC – CS – OP
acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	presa in carico dei PdV così come trasmessi dal Produttore; verifica della conformità del PdV agli standard condivisi nel documento <i>Specificità del contratto</i> ; applicazione dei seguenti controlli: verifica di leggibilità dei file, presenza dati minimi obbligatori, verifica presenza e validità della firma digitale (ove prevista); trasmissione e memorizzazione del rapporto di versamento, comprensivo di eventuali anomalie	RSDC – RSMC – CS – OP
preparazione e gestione del pacchetto di archiviazione	eventuale aggregazione dei documenti secondo quanto previsto nel documento <i>Specificità del contratto</i> , nel rispetto della normativa vigente in materia di conservazione digitale di documenti informatici e documenti fiscalmente rilevanti; applicazione di specifici controlli di conformità definiti in base alla classe di appartenenza del documento trattato, del formato di conservazione, della sua rilevanza fiscale, ecc. ecc.; creazione degli indici di conservazione nel formato UNI SinCRO e chiusura del PdA tramite apposizione della firma digitale del RDC e della Marca Temporale	RSDC – OP – RSMC – CS
preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	assicurare assistenza al Cliente in occasione di verifiche da parte delle Amministrazioni competenti o da parte di organismi di controllo interni	RSDC – CS – RFAC – DPC

<b>Attività</b>	<b>Descrizione</b>	<b>Referente</b>
predisposizione della presenza di un Pubblico Ufficiale qualora si renda necessario	valutare e pianificare la necessità della presenza di un Pubblico Ufficiale in tutti i casi in cui sia richiesta la sua presenza, garantendo l'assistenza e le risorse necessarie utili alle attività di controllo e certificazione	RSDC – CS – RFAC - DPC
scarto dei pacchetti di archiviazione	individuazione e segnalazione al Titolare dell'archivio dei PdA che hanno raggiunto i limiti di conservazione previsti dalla normativa vigente; eliminazione degli stessi previa autorizzazione da parte del Titolare degli archivi e/o autorizzazione delle Soprintendenze Archivistiche provinciali di competenza, qualora necessario.	RSDC – RFAC – RSIC - PROG
chiusura del servizio di conservazione (al termine di un contratto)	messa a disposizione delle copie dei documenti conservati; predisposizione di un elenco di consistenza contenete i documenti conservati, versati in attesa di conservazione, da versare. Il verbale deve essere controfirmato dal Cliente, o da terzo soggetto delegato. Viene definito un tempo limite di 90 gg all'interno del quale il Cliente può, in completa autonomia, procedere al download dei PdD e segnalare eventuali anomalie o irregolarità	RSDC – RP - COMM – RSIC – CS - PROG
conduzione e manutenzione del sistema di conservazione	verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; creazione delle copie di sicurezza; migrazione dei documenti conservati su supporti tecnologici più evoluti, qualora si renda necessario;	RSSC – RSIC – RSMC - CS
monitoraggio del sistema di conservazione	coordinare lo sviluppo e la manutenzione delle componenti software del SdC; verificare la funzionalità del SI e dei SW aziendali direttamente o indirettamente coinvolti nel processo di conservazione; garantire la sicurezza fisica e logica dei sistemi informatici che operano nel SdC e delle copie di sicurezza prodotte	RSSC – RSIC - RSMC
change management	i processi sono gestiti in conformità al Piano della Sicurezza e alle procedure ISO 27001:2017 e ISO 9001:2015 Le esigenze possono essere determinate da richieste dirette del Cliente ,da modifiche al quadro giuridico e normativo di riferimento, da evoluzioni tecnologiche. Vengono sempre identificati i ruoli e i processi coinvolti e assegnate le responsabilità, così come vengono valutate e messe a disposizione le risorse necessarie: personale, piani di formazione, HW, ecc. ecc.	DIR – RSDC – AMM – RSIC - RSMC - DPC

Attività	Descrizione	Referente
verifica periodica di conformità a normativa e standard di riferimento	aggiornamento e formazione continua delle funzioni interessate relativamente alle novità normative in materia di conservazione e dematerializzazione;	RSDC - DPC
Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali	Assicurare che i processi di conservazione rispettino quanto previsto dalla normativa	RP

Di seguito la matrice delle responsabilità con i principali attori coinvolti nel processo di conservazione a norma:

Area del processo	Attività	RDC o suo delegato	RSDC o suo delegato	Produttore o suo delegato
Produzione del documento informatico	Imputazione dei dati contabili sul gestionale			<b>O - V - R</b>
	Estrazione e produzione dei metadati del documento	<b>V</b>		<b>O - V - R</b>
	Eventuale invio a Indicom del flusso dati tramite canale sicuro	<b>V</b>		<b>O - V - R</b>
	Produzione del documento in formato PDF e invio a Indicom tramite canale sicuro	<b>V</b>		<b>O - V - R</b>
	Eventuale elaborazione flusso dati e produzione documento informatico	<b>V</b>		<b>O - V - R</b>
	apposizione della firma digitale tramite HSM sicuro e certificato	<b>V</b>		<b>O - R</b>
	Eventuale apposizione della Marca Temporale (dove richiesto/previsto)	<b>V</b>	<b>V</b>	<b>O - R</b>
	Produzione e invio del PdV (Pacchetto di Versamento)	<b>V</b>	<b>V</b>	<b>O - R</b>
Processo di conservazione	Download dei dati e dei documenti su DB	<b>V</b>	<b>O-R</b>	
	Controlli di conformità alla normativa vigente	<b>V</b>	<b>O-R</b>	
	Produzione e invio del RdV		<b>O-R</b>	<b>V</b>
	Produzione del PdA (Pacchetto di Archiviazione)	<b>V</b>	<b>O-R</b>	
	Apposizione di firma digitale e marca temporale sull' Pacchetto di Archiviazione conforme all'UNISINCRO 11386:2010	<b>V</b>	<b>O-R</b>	
Altre attività	Ricerca, consultazione e download dei PdD	<b>O-R-V</b>	<b>V</b>	
	Pagamento imposta di bollo (ove richiesto)			<b>O - V - R</b>

	Verifica periodica leggibilità documenti conservati	<b>V</b>	<b>O-R</b>	
	Aggiornamento Manuale CS	<b>V</b>	<b>O-R</b>	

**O** = **Opera**  
**R** = **Responsabile**  
**V** = **Verifica**

[Torna al sommario](#)

## 6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

I SdC adottati da IDC sono conformi a quanto previsto dalle regole tecniche di cui al DPCM 3 dicembre 2013 ed allo standard ISO 14721:2012 OAIS (Open Archival Information System) e successive modifiche.

Il processo prevede quindi l'utilizzo di Pacchetti Informativi, che rappresentano lo stato della documentazione nelle fasi di vita all'interno del SdC:

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

Come previsto dalle "Regole tecniche in materia di sistema di conservazione" dell'art. 3, c. 1 del Decreto della Presidenza del Consiglio dei Ministri 3 dicembre 2013, i SdC di IDC assicurano dalla presa in carico fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie degli oggetti in essi conservati, garantendone oltre all'autenticità, all'integrità, all'affidabilità e alla leggibilità anche la reperibilità. IDC ha definito una policy per assicurare la conservazione nel tempo delle informazioni, la tipologia degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti. Sono descritte e verificate le caratteristiche e le proprietà degli oggetti preservati, al fine di confermare l'autenticità od individuare errori rispetto a tali oggetti. E' mantenuta la documentazione delle tipologie degli oggetti sottoposti a conservazione, per rendere chiari ai fruitori le caratteristiche e le proprietà degli oggetti preservati. Il servizio di conservazione permette di associare a ciascun documento che compone l'unità documentaria un set di metadati. Quest'ultimi rendono agevole la ricerca di un documento, permettono di identificarli, collocarli e fornire un riferimento alla struttura di ogni documento e al suo formato. I metadati permettono inoltre di individuare gli elementi che possono attestare l'integrità e l'autenticità dei documenti versati.

Avremo pertanto:

- metadati identificativi dell'unità documentaria da versare
- metadati che descrivono il documento principale versato
- metadati che descrivono ogni singolo allegato/annesso/annotazione versata (se presenti)

Oltre a questi metadati il sistema memorizzerà anche gli indici associati al processo di conservazione.

In fase di versamento ogni unità documentaria viene descritta da un serie di metadati, raggruppati in macro-classi.

[Torna al sommario](#)

## 6.1 Oggetti conservati

Il processo di conservazione digitale si effettua sugli aggregati logici definiti unità documentarie (UD). Queste sono composte da uno o più documenti, di cui almeno un *documento principale*. In aggiunta a questo è possibile associare n documenti *allegati*, n documenti *annessi* (documenti prodotti generalmente in un momento successivo rispetto al documento principale) e n documenti *annotazioni*.

L'Unità Documentaria è identificata univocamente dai seguenti valori:

- AZIENDA
- TIPO DOCUMENTO
- ANNO
- IDENTIFICATIVO

L'identificativo per alcune classi documentali consiste in una combinazione di metadati che identificano univocamente il documento (es: per i LUL l'identificativo univoco è composto dai metadati 'anno', 'pagina da' e 'pagina a')

Le UD sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'Ente produttore.

Tutti gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- a) pacchetti di versamento;
- b) pacchetti di archiviazione;
- c) pacchetti di distribuzione.

Nella documentazione tecnica condivisa con il Cliente vengono definiti:

- l'elenco dei documenti conservati, i formati e la loro natura
- il formato del PdV e le modalità di versamento nel SdC da parte del Produttore
- l'elenco e la descrizione di eventuali metadati specifici associati ai documenti, in aggiunta a quelli minimi obbligatori previsti dalla normativa vigente
- il periodo di conservazione e le modalità di scarto dei PdA
- qualsiasi altra informazione ritenuta utile a definire e regolamentare lo specifico processo di conservazione

Tutti i formati gestiti sono coerenti con il punto 5 dell'Allegato 2 alle Regole Tecniche e sono elencati e descritti in un registro interno al sistema di conservazione.

I formati gestiti dal sistema per la conservazione di specifiche tipologie documentarie sono concordati con il Produttore ed esplicitati all'interno del documento *Specificità del contratto*

I principali formati previsti per i documenti sono:

- XML: tutte le versioni gestite dal Sdl e dal NSO
- PDF (in diverse versioni, principalmente 1.3 e 1.4)

- PDF/A
- Messaggi PEC (.msg, .eml)
- Archivi compressi in formato .zip

I principali formati previsti per gli Indici di Versamento - IdV contenuti nel PdV sono:

- XML
- TXT

I formati di firma ammessi sono:

- PAdES: ETSI TS 102 778
- CAdES: ETSI TS 101 733
- XAdES: ETSI TS 101 903

Queste le principali tipologie documentali conservate attraverso la piattaforma IDC:

Documenti sottoposti a conservazione digitale	Processo di conservazione adottato	Formato del documento conservato	Periodicità di conservazione	Campi di ricerca utilizzati
<b>Fatture Attive</b>	Conservazione digitale di documento elettronico o analogico	XML, eventualmente con firma CAdES o XAdES  PDF con firma PAdES o CAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
<b>Fatture Passive</b>	Conservazione digitale di documento elettronico o analogico	XML, eventualmente con firma CAdES o XAdES  PDF con firma PAdES o CAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
<b>DDT Attivi</b>	Conservazione digitale di documento informatico	PDF con firma PAdES o CAdES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi

Documenti sottoposti a conservazione digitale	Processo di conservazione adottato	Formato del documento conservato	Periodicità di conservazione	Campi di ricerca utilizzati
<b>DDT Passivi</b>	Conservazione digitale di documento informatico	PDF con firma PAdES o CADES	almeno annuale	-Cognome -Nome -Denominazione -Codice fiscale -Partita Iva -Data -Associazioni logiche dei campi
<b>Libri e Registri Contabili, Dichiarativi</b>	Conservazione digitale di documento informatico	PDF con firma PAdES o CADES	almeno annuale	-Tipo documento -Anno -mese -funzione "ricerca" del formato PDF
<b>LUL</b>	Conservazione digitale di documento informatico	PDF con firma PAdES o CADES	Mensile	-Cognome -Nome -CF -Anno -Mese
<b>Corrispondenza</b>	Conservazione digitale di documento informatico	.msg, .eml	almeno annuale	-Destinatario/Mittente -Oggetto -Data

Le tipologie sopra rappresentate sono quelle maggiormente trattate dalle piattaforme di IDC; le procedure qui descritte valgono anche per altre tipologie documentali, indipendentemente dalla loro natura fiscale, amministrativa, giuridica o sanitaria.

Il documento *Specificità del contratto* contiene i dettagli di processo legati alle diverse tipologie documentali trattate.

[Torna al sommario](#)

## 6.2 Pacchetto di versamento

Il versamento dei documenti viene effettuato in modalità asincrona e prevede che il sistema versante possa inviare una singola Unità Documentaria (UD) o Unità archivistiche.

Il pacchetto che compone un'operazione di versamento, denominato Pacchetto di Versamento (PdV), è composto da:

- Un Indice di Versamento (IdV) contenente le informazioni generali del PdV, i metadati associati a ciascuna unità documentaria versata
- le unità documentarie oggetto dell'operazione di versamento dichiarate nell'IDV

Il trasferimento del pacchetto all'interno del sistema può avvenire in modalità automatica o manule tramite canale di trasferimento file non esposto all'esterno ma raggiungibile solo dal perimetro sicuro di IDC.

La risposta di presa in carico del PdV viene inviata al sistema versante, dopo aver effettuato i controlli di congruenza relativi al pacchetto versato, così come descritto al Capitolo 7.

A caricamento avvenuto il sistema effettua i seguenti controlli :

- conformità del PdV alle caratteristiche concordate nel documento *Specificità del Contratto* (formato PdV, formato oggetti contenuti, ecc )
- presenza, ove previsto nel documento *Specificità del contratto*, o secondo quanto imposto dalla normativa vigente, della firma digitale
- che il file sia integro e non corrotto
- verifica presenza indici obbligatori all'interno dei metadati. Per quanto riguarda i documenti rilevanti ai fini fiscali i campi obbligatori sono, ad esempio, i seguenti:
  - *Ragione sociale o Nome e Cognome*
  - *PIVA e/ o Codice Fiscale*
  - *Numero documento*
  - *Data documento*

Tale risposta, denominata Rapporto di Versamento, riporta l'esito dell'operazione di versamento per ciascuna UD versata. Per i dettagli e la struttura si veda il capitolo 7.3.1

L'IdV è sempre in formato XML; i metadati i metadati gestiti per ciascuna tipologia documentale sono descritti nella documentazione tecnica condivisa con il Cliente.

Il sistema gestisce un'anagrafica centralizzata degli Enti censiti e dei relativi Utenti.

La configurazione degli Utenti all'interno del Sistema di Conservazione prevede la valorizzazione delle seguenti informazioni, alcune delle quali gestite attraverso il documento *Specificità del Contratto*:

Produttore:

- Nome e Cognome
- Tipo documento (Carta Identità, Codice fiscale)
- Numero documento
- Codice Fiscale
- Ente
- Indirizzo e-mail

L'utente produttore viene in questo modo collegato ad un Ente.

Ente:

- Ragione Sociale
- P Iva
- Indirizzo
- Città

- Telefono

[Torna al sommario](#)

### 6.3 Pacchetto di archiviazione

Il Pacchetto di Archiviazione – PdA - è il pacchetto informativo con cui il SdC conserva i documenti informatici e il loro indice di conservazione con garanzia di integrità e reperibilità nel tempo. Esso viene formato in seguito all'elaborazione di uno o più Pacchetti di Versamento.

L'indice di conservazione, IdC, è un file in formato XML UNI SInCRO, secondo la norma UNI 11386 : 2010, che riporta per ogni documento archiviato alcune informazioni del file stesso tra cui una stringa URN e un'impronta HASH.

L'URN è una stringa che rappresenta in maniera univoca il file stesso senza determinarne l'ubicazione mentre la stringa di HASH rappresenta un'impronta del documento ricavata dalla sequenza di bit del file stesso che garantisce nel tempo il controllo della corrispondenza esatta del contenuto originale

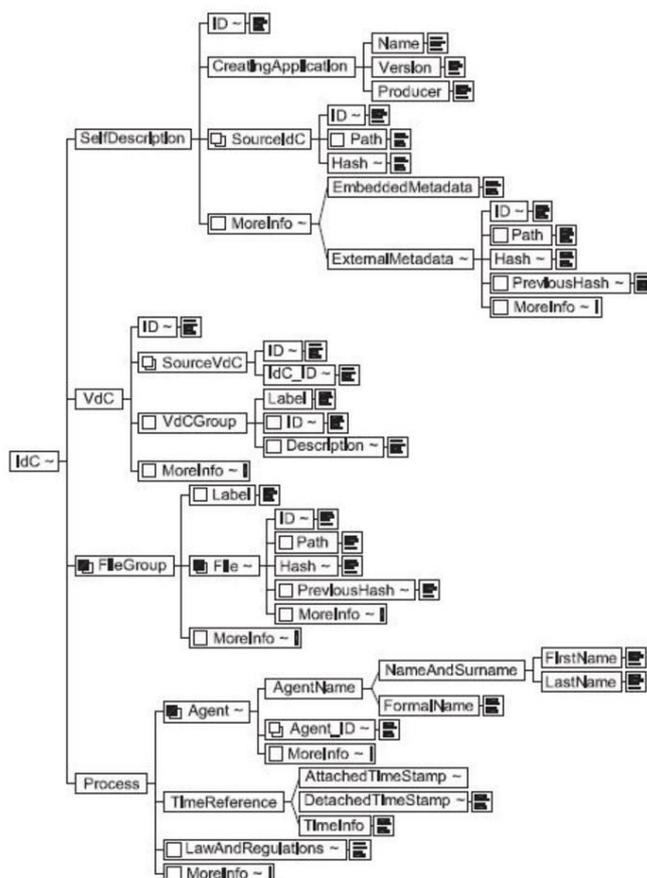
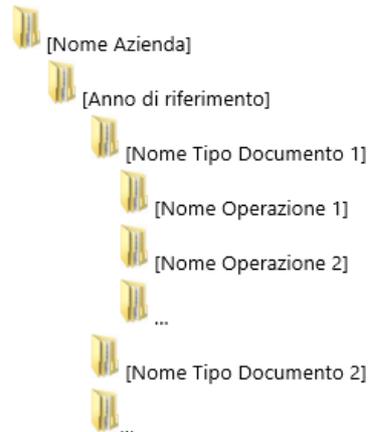


Figura 2 – Struttura Indice PdA

Le operazioni di conservazione riferite a una tipologia di conservazione, sono ordinate in modo cronologico per periodo di riferimento.

Dentro ciascun folder associato ad un'operazione di conservazione risulta memorizzato il PdA (Pacchetto di Archiviazione), ovvero l'indice di conservazione e le unità documentarie (documenti, allegati, annessi) conservate.



*Figura 3 - Struttura cartelle operazioni*

La relazione che lega i PdA con i PdV è di tipo "molti a molti" ovvero: più PdA possono far riferimento a uno stesso PdV e viceversa più PdV possono far riferimento ad uno stesso PdA.

Univoca è invece la relazione esistente tra una UD e il PdV mediante cui è stata versata nel sistema di conservazione e il PdA mediante cui è stata conservata.

Detta relazione è gestita dal software di conservazione ed è presente nella base dati ad esso associata.

L'IdC del pacchetto di archiviazione verrà quindi firmato e marcato temporalmente dal responsabile del servizio di conservazione, entro i limiti di tempo di conservazione imposti dalle normative in vigore, garantendo quindi integrità, autenticità, robustezza, certezza e immodificabilità. Si precisa inoltre che il sistema di conservazione qui presentato, effettua un controllo sulla validità del certificato di firma del responsabile del servizio di conservazione e sulla validità e disponibilità delle marche temporali.

[Torna al sommario](#)

## **6.4 Pacchetto di distribuzione**

Il sistema permette la ricerca nel tempo di tutti i pacchetti di archiviazione precedentemente creati, tramite interfaccia web accessibile tramite sistema di autenticazione e autorizzazione. A fronte di una ricerca da parte dell'utente il sistema mette a disposizione un oggetto detto Pacchetto di Distribuzione.

Il Pacchetto di Distribuzione (di seguito PdD) è composto da un archivio compresso in formato .zip contenente:

- L'IPdA associato all'operazione di conservazione, sottoscritto digitalmente dal Responsabile del Servizio di Conservazione (firma CaDES)

- la marca temporale apposta sull'IPdA sottoscritto che attesta data e ora in cui è avvenuta la conservazione
- le unità documentarie associate all'operazione di conservazione oggetto di richiesta
- un'applicazione web che consente la navigazione e la consultazione dei documenti conservati

L'applicazione web, fruibile tramite l'utilizzo di un qualsiasi browser web, riporta le seguenti informazioni:

- descrizione dell'operazione di conservazione
- dati identificativi dell'ente versante
- dati identificativi del responsabile della conservazione
- dati identificativi della firma apposta sull'operazione di conservazione
- informazioni sulla marca temporale apposta sull'IPdA
- elenco delle UD inserite nell'operazione di conservazione
- elenco dei PdV da cui hanno origine i documenti contenuti nel PdD

Per ciascuna UD l'applicazione web espone i metadati ad essa associati e l'elenco degli oggetti digitali che la compongono.

Tutti gli oggetti digitali che compongono un'operazione di conservazione sono fruibili dall'applicazione web.

Le modalità di accesso, ricerca, esibizione e distribuzione dei documenti conservati sono descritti nel Manuale Utente del sistema IDC

Le funzioni di cui sopra sono disponibili al Cliente per un periodo di 3 mesi dalla data di cessazione del contratto, così come descritto nel documento Piano di cessazione dell'attività. Eventuali accordi diversi sono espressi all'interno del Contratto di servizio.

[Torna al sommario](#)

## 7 IL PROCESSO DI CONSERVAZIONE

Il processo di conservazione digitale si effettua sugli aggregati logici definiti unità documentarie (UD): queste ultime sono formate da uno o più documenti considerati come un tutto unico e costituiscono le unità elementari di cui si compone l'archivio dell'Ente produttore.

Il processo di conservazione digitale avviene secondo le modalità sintetizzate nei seguenti punti:

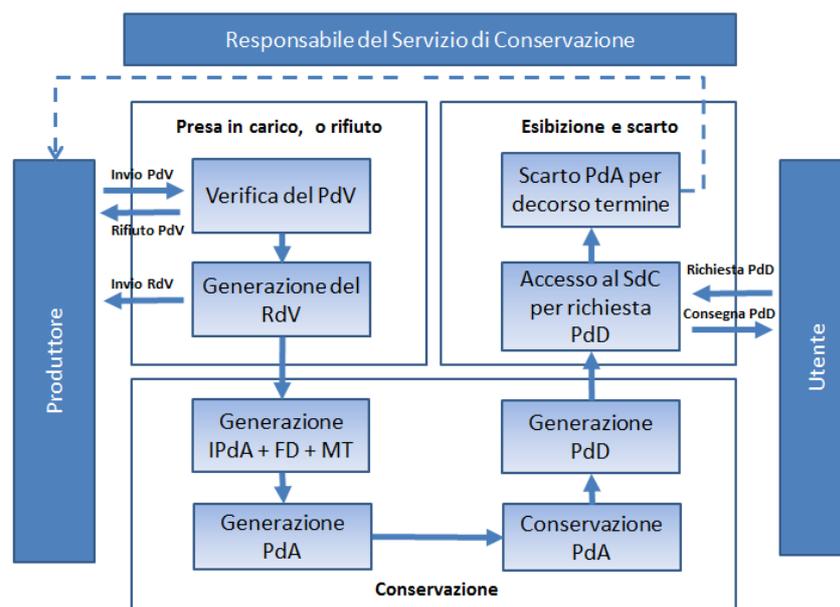


Figura 4- Schema processo di conservazione

- Presa in carico, acquisizione o rifiuto
  - L'Ente produttore invia in conservazione le unità documentarie aggregate in Pacchetti di Versamento (PdV). Il sistema esegue i controlli automatici di congruenza sui PdV versati, che ne determinano la presa in carico.
  - Il sistema genera il Rapporto di Versamento (RdV) che viene messo a disposizione dell'Utente per eventuali esigenze applicative
- Conservazione
  - Il sistema, con cadenza opportuna, definisce il Pacchetto di Archiviazione (PdA) che consiste in una o più UD, costituito secondo criteri totalmente configurabili che ne determinano i rispettivi contenuti e le dimensioni, ai quali si applica unitariamente il processo di conservazione digitale. Il sistema di conservazione gestisce esclusivamente PdA omogenei, ovvero composti da UD della stessa tipologia.
  - Il sistema è configurato per effettuare controlli automatici di congruenza del PdA; in aggiunta è possibile prevedere una ulteriore fase di verifica manuale a cura degli operatori incaricati.
  - La procedura di chiusura prevede:

- la generazione dell'Indice Pacchetto di Archiviazione (IPdA – UNI-SinCRO)
- la firma digitale del Responsabile del Servizio di conservazione che attesta il regolare svolgimento del processo di conservazione
- l'apposizione della marca temporale.
- Il PdA è archiviato nell'archivio di conservazione
- Per ogni operazione di conservazione il sistema genera il relativo Pacchetto di Distribuzione (PdD), per consentire l'esibizione e la fruizione dei archiviati documenti conservati
- Esibizione
  - gli utenti autorizzati possono acceder alla piattaforma e ricercare, visualizzare e scaricare i PdA

Alla decorrenza dei termini di conservazione viene effettuato lo scarto dei PdA

IDC, se necessario, mette a disposizione del Cliente/produttore un Sistema di Gestione Documentale al quale vengono conferiti i documenti tramite processo di Presa in Carico – PIC, deputato ad effettuare eventuali controlli di integrità degli archivi (sequenza numerica, doppi, ecc. ecc.).

Il SdG di IDC provvede quindi ad aggregare i documenti forniti dal cliente in calssi omogenee e, utilizzando gli indici che li accompagnano, a formare il PdV in formato compatibile con quanto attesa di SdC di IDC.:

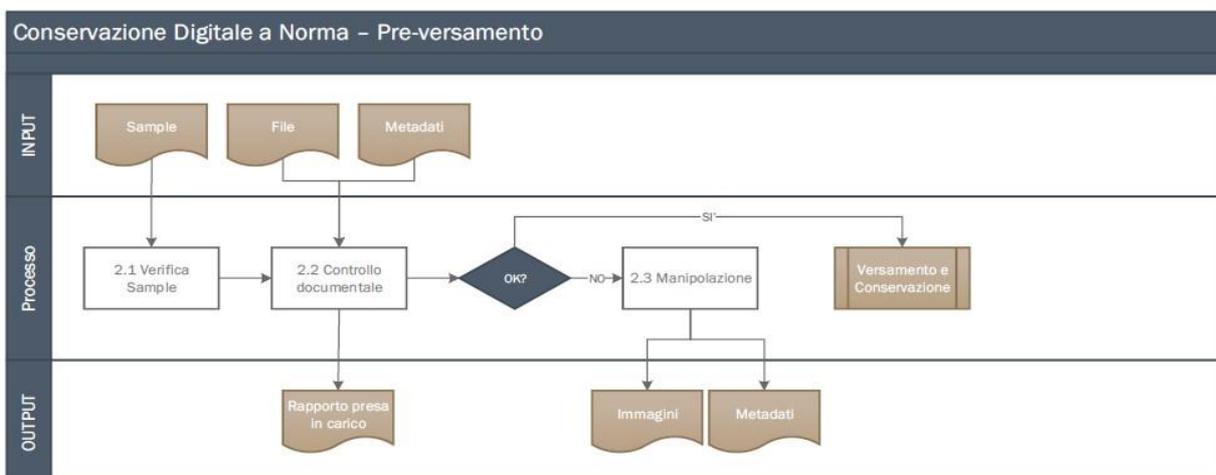


Figura 5- Pre-versamento



Figura 6 - Versamento e Conservazione

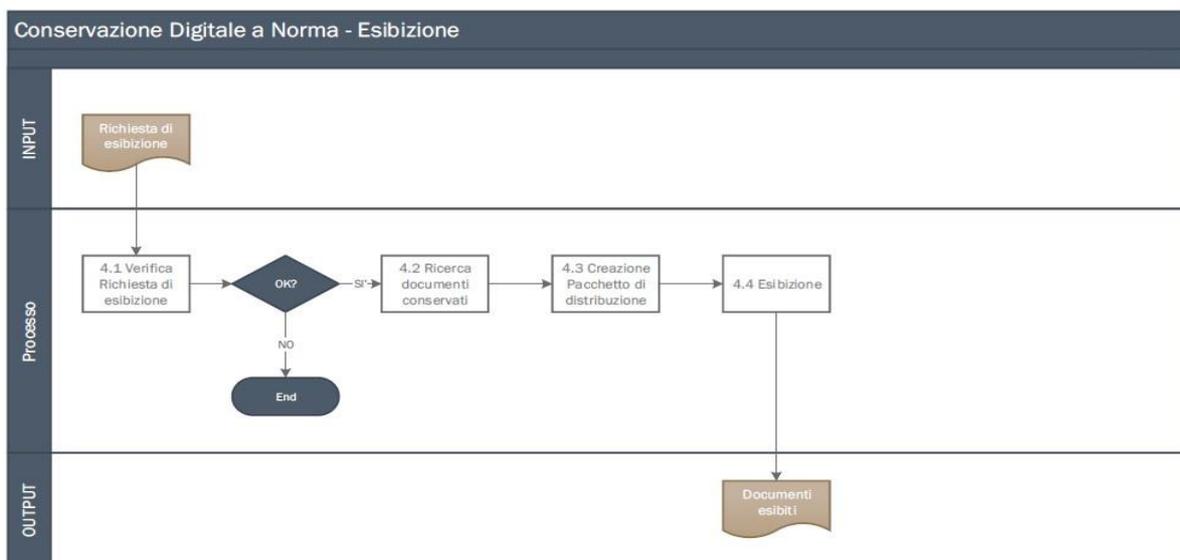


Figura 7 - Esibizione

[Torna al sommario](#)

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

IDC prevede che il Cliente possa fornire i documenti da conservare a norma attraverso altri Servizi messi a disposizione del Cliente stesso:

Servizio di scansione e archiviazione ottica:

il Cliente fornisce ad IDC la documentazione in formato cartaceo. IDC, attraverso i propri operatori specializzati, si occupa della scansione dei documenti, della generazione degli indici e dei metadati finalizzati alla futura consultazione ed esibizione. I Clienti hanno a disposizione piattaforme e Servizi Web che consentono loro di

generare e/o caricare i documenti oggetto di Conservazione Digitale a Norma. Il servizio "Versamento e Conservazione" emette un Report per confermare l'avvenuta presa in carico dei documenti.

Servizio di Upload sFTP: il Cliente ha facoltà di caricare in autonomia, su un'area riservata e soggetta alle regole di sicurezza informatica adottate da IDC, i pacchetti di versamento (IdV + documenti) oppure, in alternativa, le immagini dei documenti da sottoporre a conservazione digitale a norma ed eventualmente dei relativi metadati.

In questo caso sarà cura di IDC normalizzare i documenti ai fini della conservazione sulla base delle modalità previste in offerta economica. Nel progetto tecnico economico vengono individuate eventuali procedure di manipolazione e gestione documentale preparatoria al servizio di conservazione digitale a norma.

A valle dei Servizi a supporto della Conservazione Digitale a Norma, il processo continua come descritto nel Manuale di conservazione.

È possibile che il Cliente invii a IDC i documenti da conservare corredati dalle strutture di indici da abbinare. L'indicizzazione dei documenti può eventualmente anche essere effettuata in service direttamente da operatori qualificati di IDC in base a quanto specificatamente concordato con il Cliente all'interno del sistema di gestione documentale.

In questi casi IDC assume il ruolo di Aggregatore incaricato alla produzione del PdV.

Il versamento dei documenti viene effettuato in modalità asincrona e prevede che il sistema versante possa inviare una singola Unità Documentaria (UD).

L'unità minima di versamento è l'Unità Documentaria. Ogni unità documentaria è composta da uno o più documenti, di cui almeno un *documento principale*. In aggiunta a questo, è possibile gestire documenti *allegati*, documenti *annessi* (documenti prodotti generalmente in un momento successivo rispetto al documento principale) e *annotazioni*.

Più in dettaglio il processo si compone dei seguenti passi operativi:

Il Produttore produce il PdV così come definito nella documentazione tecnica condivisa e lo trasferisce al SdC secondo le modalità descritte nel paragrafo 6.2. (Pacchetto di versamento)

Un processo gestito dal sistema effettua il versamento delle UD attivando, in modalità sincrona e in un contesto transazionale, i sotto-processi:

- Acquisizione dei metadati che caratterizzano la UD
- esecuzione dei controlli operati dal sistema di conservazione in fase di versamento

[Torna al sommario](#)

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

### 7.2.1 Controllo Formale

La comunicazione con il servizio di versamento utilizza prevalentemente lo scambio di messaggi XML strutturati, il cui contenuto viene sottoposto alla validazione attraverso appositi XSD. L'utilizzo degli XSD permette:

- la validazione del contenuto di un elemento o di un attributo rispetto a un determinato tipo di dato;
- la verifica della presenza dei metadati definiti come obbligatori (se questi sono assenti, l'XML non sarà validato nell'applicativo);
- la validazione di espressioni regolari (es. la verifica che un determinato attributo preveda l'immissione di una stringa composta da un numero predefinito di valori).

Ogni XML sarà composto da alcune parti fisse (comuni a tutte le tipologie versate, quindi si definisce uno schema XSD generale) e di altre specifiche per la tipologia documentaria di riferimento.

Nel caso l'indice del pacchetto di versamento consista in un file di testo, il controllo formale consisterà nella verifica della struttura del file sulla base delle specifiche contenute nel documento *Specificità del Contratto*.

[Torna al sommario](#)

### 7.2.2 Controllo sui METADATI

A seconda di quanto previsto dagli accordi contrattuali, alcuni controlli potranno essere gestiti dal Portale di Gestione, nella fase di pre-versamento, o dal SdC durante la fase di versamento:

1. Questi i controlli formali applicati a tutte le classi documentali: la verifica della presenza dei metadati definiti come obbligatori per ciascuna tipologia di documento;
2. la validazione dei tipi di dato.
3. controllo dell'univocità della chiave (il sistema controlla che l'unità documentaria non sia stata già versata)

Di seguito i controlli applicati ai principali documenti aventi rilevanza fiscale:

Metadato	Descrizione del controllo	Applicazione
Codice Azienda	Non può essere vuoto	Tutte le tipologie di documento
Produttore	Non può essere vuoto Deve essere coerente con quanto definito nel documento Specificità del contratto	Tutte le tipologie di documento
Tipo Documento	Non può essere vuoto	Tutte le tipologie di documento
Anno	non può essere vuoto	Tutte le tipologie di documento
Numero Documento (Numero Fattura / Protocollo Iva ...)	non può essere vuoto	Tutte le tipologie di documento

Numero Documento (Numero Fattura / Protocollo Iva ...)	E' possibile configurare la formattazione del numero fattura e il sistema verifica che il progressivo sia un campo numerico	Tutte le tipologie di documento
Partita IVA	controlli di congruenza sul formato	Fattura Cliente e Fattura Fornitore
Data Documento / Data Registrazione	non può essere vuoto	Tutte le tipologie di documento
Congruenza metadati-documenti	Ad ogni set di metadati associati ad una UD deve corrispondere un oggetto digitale (pdf o tif) e viceversa (eventuali eccezioni vengono segnalate nella base dati di staging presente in Oracle)	Fattura Cliente e Fattura Fornitore

I controlli possono dare un esito positivo o negativo – in questo secondo caso vengono presi in considerazione due tipologie di errori: bloccanti e non.

Se si è in presenza di un errore bloccante, il sistema produce una segnalazione (rapporto di scarto) messa a disposizione del cliente cosicchè possa definire la gestione dell'anomalia e giungere al completamento del processo. Se l'errore non è bloccante, sarà l'operatore interno a verificare eventuali regole predefinite con il cliente, agendo dunque di conseguenza secondo istruzioni, oppure, in mancanza di esse provvederà a contattare il referente del cliente.

Ogni volta che il sistema di versamento effettua le operazioni di controllo sui pacchetti di versamento, l'evento viene appositamente tracciato all'interno del log system.

[Torna al sommario](#)

### 7.2.3 Log e Registri dei Pacchetti di Versamento

Tutte le operazioni di versamento effettuate dal Produttore, identificato in modo certo, vengono tracciate in specifici log applicativi direttamente sul database di conservazione, in una tabella dedicata ai log di versamento, e indicando le tipologie delle informazioni contenute nel pacchetto di versamento.

Le informazioni sui PdV sono rese disponibili agli operatori attraverso interfaccia Web:

Dati Operazione:	Codice Versamento, Azienda, Descrizione, Data Versamento, numero anomalie, dettaglio documenti scartati, totale documenti
Documenti:	elenco dei documenti contenuti nel PdV
Annessi:	Indice del PdV, RdV
Visibilità:	profilo dell'utente collegato
Anomalie:	registro delle anomalie rilevate dalla piattaforma
Storico:	registro delle attività legate al PdV

I log dei processi di conservazione su piattaforma ConSED vengono mantenuti online per tutta la durata del periodo di conservazione ed esportati ogni notte tramite una procedura automatica sul Syslog centrale, da cui giornalmente viene prodotto un file firmato digitalmente dal RSDC.

Tutti i log relativi alle operazioni sulla suite ArchiCons vengono sottoposti a processo di conservazione e mantenuti per l'intera durata del contratto.

L'accesso al database dei log è consentito solo agli amministratori del sistema e al responsabile del servizio di conservazione, che hanno la possibilità di effettuare un export del log ricercato, firmato e marcato dal responsabile.

[Torna al sommario](#)

#### **7.2.4 Controllo sulle firme**

Durante la presa in carico del PdV viene eseguita la verifica di conformità delle firme presenti.

Eventuali accordi specifici sono riportati nel documento *Specificità del contratto*.

Segue l'elenco dei possibili controlli operati dal sistema:

1. Controllo di obbligatorietà: il controllo ha lo scopo di appurare la presenza di una firma digitale che attesti la provenienza e l'autenticità del documento. Il controllo viene svolto su tutti i documenti aventi rilevanza fiscale. .
2. Controllo di conformità della firma (embedded o detached): verifica se la sua struttura è conforme rispetto a uno dei formati riconosciuti (CADES, PAdES o XAdES).
3. Controllo di tipo crittografico: verifica l'autenticità del documento.
4. controllo di tipo catena-trusted: verifica che il certificato utilizzato per la sottoscrizione del documento sia stato emesso da una Certification Authority accreditata per la PA. controllo sul tipo certificato: verifica gli attributi del certificato che deve essere abilitato per la sottoscrizione.
5. controllo di tipo certificato: verifica la scadenza del certificato. controllo di tipo CRL: l'ultimo controllo viene effettuato solo sul primo documento di ciascun PdV ed ha lo scopo di verificare che il certificato non sia stato revocato.

Se in un PdV è presente almeno una UD che viene scartata, il sistema effettua lo scarto della singola UD o dell'intero PdV, sulla base di specifici accordi con il Cliente

[Torna al sommario](#)

#### **7.2.5 Controlli sui Formati**

Il sistema controlla che il formato del file versato corrisponda ad uno dei formati ammessi per la struttura e che sia conforme a quanto stabilito nel documento *Specificità del contratto*.

[Torna al sommario](#)

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

La chiamata al servizio di versamento, da parte di un applicativo autorizzato, determina la registrazione dei documenti versati nel SdC e una risposta, denominata Rapporto di Versamento (RdV).

Il RdV costituisce il documento di controllo e di presa di responsabilità del Responsabile del Servizio di Conservazione verso il Produttore e viene messo a disposizione sul SdC.

La responsabilità di assicurarsi della corretta presa in carico di tutti i documenti da parte del SdC è in carico al Produttore. A questo scopo, il RdV può essere reso disponibile al Produttore in una cartella dedicata anche attraverso un canale sFTP accessibile previa autenticazione, e utilizzato per un'integrazione applicativa con un sistema documentale. In questo modo il Produttore può provvedere ad aggiornare i propri archivi per verificare il buon esito del caricamento in conservazione e individuare eventuali incompletezze o anomalie nel processo.

Nelle piattaforme di conservazione di IDC sono presenti le funzionalità che consentono la fruizione e il monitoraggio delle operazioni di versamento e delle anomalie.

Per la gestione dei log e dei registri si veda quanto previsto al paragrafo 7.2.3

[Torna al sommario](#)

#### **7.3.1 Attributi calcolati dal sistema (fase di versamento)**

In fase di versamento il sistema di conservazione calcola in automatico i seguenti attributi, che si aggiungono a quelli dichiarati dall'applicativo versante per descrivere ogni singolo file:

- chiave dei documenti versati  
Il sistema genera la chiave di ogni documento presente all'interno dell'Unità Documentaria. Tale chiave è generata sulla base della chiave dell'Unità Documentaria, in base alla tipologia di appartenenza del documento viene quindi assegnato un progressivo all'interno di tale tipologia.
- hash calcolato  
il sistema procede a calcolare l'hash del file versato e a salvare sul database, oltre a l'hash calcolato, l'algoritmo utilizzato per generarlo e il tipo di encoding
- dimensione del file versato  
calcolato sul file
- formato del file calcolato  
il file viene sottoposto ad apposito controllo per stabilirne il reale formato

[Torna al sommario](#)

### 7.3.2 Struttura del rapporto di versamento

La chiamata al servizio di versamento da parte dell'applicativo dell'ente produttore determina una risposta, denominata Rapporto di Versamento (RdV), che si compone dei seguenti oggetti:

- i dati identificativi del Produttore
- l'indicazione della tipologia dei documenti versati
- il riferimento che identifica l'operazione di versamento
- il riferimento temporale associato all'operazione di versamento
- il numero e l'elenco dei documenti versati con successo
- il numero e l'elenco delle anomalie riscontrate in fase di versamento
- data e ora di creazione del RdV (RT)

Per la determinazione di tutti i riferimenti temporali viene utilizzato l'orario del server che ospita il SdC, il quale a sua volta è sincronizzato con un servizio NTP affidabile.

Per ciascun documento il sistema riporta il riferimento univoco al documento del sistema versante e il l'ID interno del documento prodotto dal sistema di conservazione

Di seguito la struttura del RdV di Archicons:

```
[AAAA-MM-GGT17:18:09+02:00] Rapporto di Versamento dell'Azienda NNNN
[AAAA-MM-GGT17:18:09+02:00] Utente XYZ
[AAAA-MM-GGT17:18:09+02:00] Firmatario Autorizzato XXX
[AAAA-MM-GGT17:18:09+02:00] Nome Modello modFatturaElettronica
[AAAA-MM-GGT17:18:09+02:00] Analisi cartella di versamento numero 9
[AAAA-MM-GGT17:18:09+02:00]
[AAAA-MM-GGT17:18:09+02:00]
[AAAA-MM-GGT17:18:09+02:00] Trovato File:
[AAAA-MM-GGT17:18:09+02:00] Nome File: IT09468600011_14020.xml.p7m
[AAAA-MM-GGT17:18:09+02:00] Dimensione File: 5502 Byte [AAAA-MM-
GGT17:18:09+02:00] Hash File (SHA256):
5b27632e28d6f47ce590461b8c0420d802d4a3a581cda43b724f6961ef149b40
[AAAA-MM-GGT17:18:09+02:00] Tipo File: application/pkcs7-mime
[AAAA-MM-GGT17:18:09+02:00] Estensione File: p7m
[AAAA-MM-GGT17:18:09+02:00] Data File: AAAA-MM-GG 17:18:09
[AAAA-MM-GGT17:18:09+02:00] ...
[AAAA-MM-GGT17:18:13+02:00] Fine Rapporto di Versamento
```

*Figura 8- Schema XML Rapporto di Versamento ArchiCons*

Nella piattaforma ConSED fx il sistema utilizza il formato XML di seguito descritto:

```

<RdV>
  <RIFERIMENTO_TEMPORALE>[tempo UTC]</RIFERIMENTO_TEMPORALE >
  <AZIENDA DESCRIZIONE=[ragione sociale] PIVA_COD_FISC=[partita iva]>
    <DOC_VERSATI NUM_DOC=[numero documenti]>
      <UNITA_DOCUMENTARIA>
        <DOC>
          <CAMPO nome=[nome metadato_1]> [valore metadato_1] </CAMPO>
          ...
          <CAMPO nome=[nome metadato_n]> [valore metadato_n] </CAMPO>
        </DOC>
      </FILES>
      <FILE>
        <ID>[identificativo file_1]</ID>
        <Path>[path file_1]</Path>
        <Hash function="SHA-256"> [hash file_1] </Hash>
      </FILE>
      ...
      <FILE>
        <ID>[identificativo file_n]</ID>
        <Path>[path file_n]</Path>
        <Hash function="SHA-256"> [hash file_n] </Hash>
      </FILE>
    </FILES>
    <ERRORI>
      <ERRORE> [Errore_1] </ERRORE>
      ...
      <ERRORE> [Errore_n] </ERRORE>
    </ERRORI>
  </UNITA_DOCUMENTARIA >
  ...
  <UNITA_DOCUMENTARIA >
  ...
  </UNITA_DOCUMENTARIA >
</DOC_VERSATI>
</AZIENDA>
</RdV>

```

Figura 9- Schema XML Rapporto di Versamento ConSEDfx

## Descrizione dei nodi

NODO		DESCRIZIONE
<b>Ragione Sociale</b>		Ragione Sociale dell'Ente versante
<b>Numero Documenti</b>		Numero (cardinalità) dei documenti che compongono il PdV
<b>DATA</b>	<b>Campo (1-n)</b>	Identifica i metadati propri della tipologia documentale. Attributi del nodo: nome : nome del campo
<b>DATA</b>	<b>Identificativo File (1-n)</b>	Identifica gli identificativi dei file che compongono ciascuna UD
<b>DATA</b>	<b>Path File (1-n)</b>	Identifica il path di ciascuno dei file che compongono l'UD
<b>DATA</b>	<b>Hash File (1-n)</b>	Identifica l'hash di ciascuno dei file che compongono l'UD
<b>DATA</b>	<b>Errore (1-n)</b>	Identifica gli errori rilevati in fase di versamento per la specifica UD

[Torna al sommario](#)

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

Gli errori gestiti dal SdC in fase di versamento sono:

- errori specifici del contenuto dei metadati (errore nel parametro – dati incongruenti – errore nella numerazione della documentazione fiscalmente rilevante)

- segnalazione che l'unità documentaria di cui si richiede il versamento è già stata versata (warning)
- errore dovuto ad almeno un esito negativo nelle verifiche dei file che compongono il documento oggetto di versamento

Quando, a seguito di un errore una UD viene scartata dal sistema, questa viene spostata nella cartella delle UD scartate.

Lo scarto delle UD viene operato nei seguenti casi:

1. il sistema rileva l'assenza del documento
2. il sistema rileva anomalie sulle firme (come precedentemente descritto)
3. il sistema rileva l'assenza dei metadati obbligatori

Negli altri casi il versamento viene accettato e l'anomalia viene segnalata nel RdV (vedi 7.3.2).

Se in un PdV è presente almeno una UD che viene scartata, il sistema effettua lo scarto della singola UD o dell'intero PdV, sulla base di specifici accordi con il Cliente

Le anomalie sono consultabili all'interno della piattaforma (vedi cap. 7.2.3); vengono elencate nell'operazione di versamento e riportate nel dettaglio su ciascuna UD, in una sezione denominata "Anomalie".

Il sistema tiene traccia in modo automatico delle anomalie rilevate nel corso dei controlli, mentre consente di inserire manualmente la descrizione di eventuali altre anomalie e gli eventi che l'hanno generata.

Ad ogni RdV è associato il Riferimento Temporale, specificato con riferimento al Tempo Universale Coordinato, e registrato nel DB delle operazioni: AAAA-MM-GGT hh:mm:ss

[Torna al sommario](#)

## 7.5 Preparazione e gestione del pacchetto di archiviazione

La preparazione e la gestione del PdA viene effettuata attraverso un processo che consta delle seguenti fasi:



Figura 10 - Schema creazione del PdA

[Torna al sommario](#)

### **7.5.1 Creazione del Pacchetto di Archiviazione**

Il sistema di conservazione gestisce esclusivamente PdA omogenei, ovvero composti da UD della stessa tipologia. I PdA vengono generati secondo criteri e tempistiche definiti nel documento *Specificità del contratto*.

La struttura dell'IPdA è definita in modo univoco per ciascuna tipologia documentale ed è conforme allo standard nazionale SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010).

In fase di setup è possibile stabilire, in accord con il Responsabile della Conservazione e in base alla tipologia documentale oggetto di trattamento, le modalità di aggregazione e le tempistiche di invio in conservazione. La schedulazione avverrà comunque nel rispetto delle prescrizioni normative vigenti.

In un Pacchetto di Archiviazione possono confluire uno o più Pacchetti di Versamento, interamente o o in parte.

Il Pacchetto di Archiviazione è identificato attraverso un identificativo numerico complesso. A ciascun record presente nella base dati relativo a ciascun singolo documento è associato sia l'identificativo del pacchetto di versamento che quello del pacchetto di Archiviazione, in modo da poter seguire l'iter di ciascun singolo documento.

L'evidenza informatica, firmata e marcata temporalmente dal Responsabile del Servizio di Conservazione, unitamente ai documenti, formano il Pacchetto di Archiviazione.

La consultazione dei PdA è possibile attraverso le funzioni di esibizione, accessibili ai soli utenti preventivamente identificati e autorizzati.

[Torna al sommario](#)

### **7.5.2 Risoluzione delle anomalie o forzatura del processo di conservazione**

In caso di segnalazione di un'anomalia il sistema blocca l'operazione di conservazione. Il RdC, o un suo delegato, attraverso il rapporto di anomalia esposto sull'interfaccia web possono verificare verificare il tipo di errore e attivare le necessarie correzioni.

L'operatore ha la facoltà di forzare la chiusura di un processo di conservazione anche se in presenza di anomalie. Questa possibilità è sempre oggetto di condivisione e autorizzazione da parte del Titolare dell'archivio fiscale oggetto di conservazione e del RDC. Le modalità di comunicazione sono definite a livello contrattuale.

[Torna al sommario](#)

### **7.5.3 Generazione dell'IPdA**

Dopo la conferma o la forzatura del processo di conservazione da parte del RdC, il sistema chiude il Pacchetto di Archiviazione e genera l'Indice del Pacchetto di Archiviazione che, insieme con le UD compone il PdA.

La struttura dell'IPdA è conforme allo standard UNI-11386 SInCRO.

I metadati specifici dei documenti conservati vengono memorizzati attraverso l'impiego del nodo XML <MoreInfo> come di seguito descritto:

```
<MoreInfo XMLSchema="DocumentoFx">
  <EmbeddedData>
    <CustomMetadata>
      <IDENTIFICATIVO xmlns="">[IdDocumento]</IDENTIFICATIVO>
      <OGGETTO xmlns="">[Oggetto]</OGGETTO>
      <DATA xmlns="">[DataDocumento]</DATA>
      <MAIN_FILE xmlns="">[NomeFile] </MAIN_FILE>
      <DATA xmlns="">
        <CAMPO nome=[NomeCampo1]>[Campo1]</CAMPO>
        <CAMPO nome=[NomeCampo2]>[Campo2]</CAMPO>
        ...
      </DATA>
    </CustomMetadata>
  </EmbeddedData>
</MoreInfo>
```

Figura 11 - SInCRO - Sezione metadati documento

#### Descrizione dei nodi

NODO		DESCRIZIONE
IDENTIFICATIVO		Identificativo del documento a cui si fa riferimento
OGGETTO		Descrive l'oggetto del documento
DATA		Data di creazione del documento
MAIN_FILE		Nome del file principale del documento
DATA	Campo (1-n)	Identifica i metadati propri della tipologia documentale. Attributi del nodo: nome : nome del campo

[Torna al sommario](#)

#### 7.5.4 Sottoscrizione dell'IPdA

Sull'Indice del Pacchetto di Archiviazione viene apposta, in formato CADES, la firma digitale del Conservatore, come da delega ricevuta dal Responsabile della Conservazione del Titolare dell'archivio digitale:

- per ciascun indice di conservazione correttamente compilato viene calcolata l'impronta mediante algoritmo di Hashing SHA-256;
- viene apposta la firma sull'impronta dell'IdC mediante uso del certificato elettronico qualificato del responsabile del servizio di conservazione;

Il processo prevede l'utilizzo di un certificate di Firma Digitale secondo lo Standard ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI) - CMS Advanced Electronic Signatures (CadES). I Certificati crittografici utilizzati sono rilasciati da Certification Authority.

IDC utilizza due diverse CA: Actalis e Namirial. I certificati di firma utilizzati sono memorizzati su dispositivi HSM in grado di garantire elevati livelli di sicurezza, affidabilità e performance in termini di velocità di esecuzione delle operazioni di firma. Tale processo permette di rispondere ai requisiti di autenticità, non modificabilità, integrità, staticità.

Nella figura seguente viene mostrata l'architettura di riferimento del Sistema di Firma Remota utilizzato:

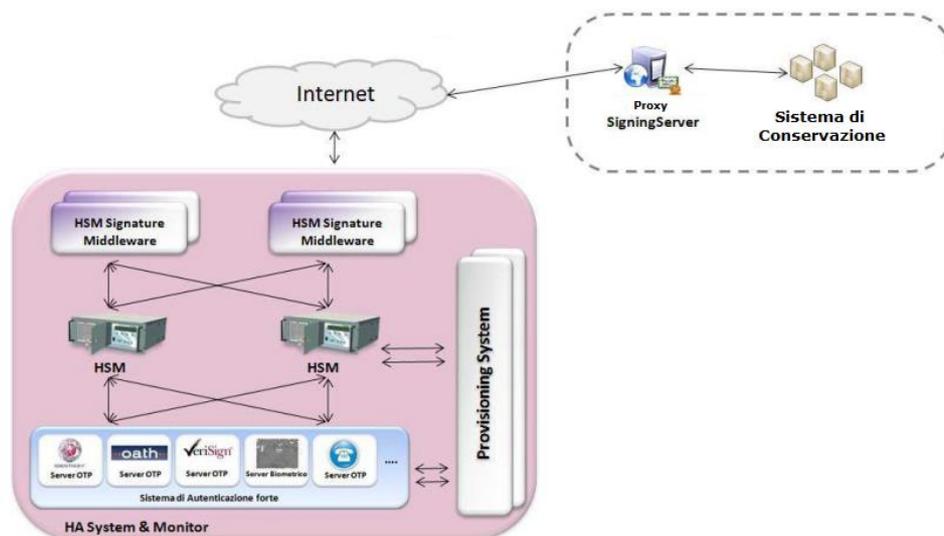


Figura 12 - Architettura Sistema di Firma Remota

Per gestire la firma il sistema si avvale di un componente software (proxy), che su un canale sicuro con mutua autenticazione con i Sistemi della CA.

[Torna al sommario](#)

### 7.5.5 Apposizione della marca temporale

Dopo la sottoscrizione il sistema appone sull'IPdA firmato una marca temporale emessa da una Time Stamp Authority accreditata presso AgID.

Per le Marche Temporalì il riferimento è lo standard RFC 3161 basata su infrastruttura a chiave asimmetrica X.509. Le TSA (Time Stamping Authority) utilizzate nel processo di apposizione del riferimento temporale sono apposte da Certification Authority accreditate AgID (<http://www.agid.gov.it/identitadigitali/firmeelettroniche/certificatori-attivi>).

Le operazioni di apposizione di firma e marcatura temporale vengono effettuate nel rispetto delle normative specifiche in materia di firme e validazione temporale.

[Torna al sommario](#)

### **7.5.6 Memorizzazione del PdA nel Supporto di Conservazione**

Il sistema di conservazione adotta come supporto di conservazione uno storage standard, in linea con i requisiti di sicurezza richiesti dal servizio.

La memorizzazione dei PdA sul supporto di conservazione viene eseguita dal sistema nell'ambito del processo di conservazione prima della chiusura di ciascuna operazione di conservazione.

[Torna al sommario](#)

### **7.6 Predisposizione delle copie di backup**

Il sistema di server di IDC è basato su un ambiente virtuale in modo da rispondere al meglio ai requisiti di resilienza richiesti.

Il sistema viene replicato, come descritto nella politica di BC e DR, su un sistema secondario.

Le copie di backup vengono effettuate in conformità alle politiche ISO 27001 e i metodi per ottenerle vengono adattati in base al progresso tecnologico, in modo da migliorarne le performance e la precisione.

I sistemi di backup sono costantemente sotto monitoraggio da parte dei preposti sistemi automatici.

[Torna al sommario](#)

### **7.7 I log delle operazioni di conservazione**

Tutte le attività eseguite nell'ambito del processo di conservazione digitale vengono registrate nel SdC e sono riportate nella sezione denominata "Storico" dell'operazione di Conservazione, consultabile tramite interfaccia applicativa. In tale sezione è riportato l'elenco delle operazioni che vengono eseguite durante il processo di conservazione. Per ciascuna operazione il sistema riporta:

- la descrizione dell'operazione eseguita;
- l'autore;
- il riferimento temporale;

Tra gli eventi storicizzati il sistema tiene traccia anche delle operazioni di consultazione delle UD e degli annessi associati all'operazione di conservazione.

I log vengono poi esportati come già descritto al precedente punto 7.2.3.

[Torna al sommario](#)

### **7.8 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione**

La predisposizione del PdD viene effettuata dal sistema come ultima fase del processo di conservazione.

Il PdD viene reso disponibile agli utenti preventivamente censiti e abilitati alla sua fruizione.

Il processo di esibizione degli oggetti conservati consente:

- 1) La sottomissione di un criterio di ricerca sui contenuti conservati, potendo definire filtri di selezione sui metadati registrati;

- 2) La consultazione dei documenti che rispondono al criterio di ricerca;
- 3) L'esibizione di detti documenti.

La funzione denominata esibizione effettua le seguenti attività:

- a) identifica l'operazione di conservazione a cui è associato il documento;
- b) verifica la validità della marca temporale apposta sull'IPdA durante l'operazione di conservazione;
- c) verifica la validità della firma digitale del RdC apposta sull'IPdA durante l'operazione di conservazione;
- d) calcola l'impronta (hash) associata al documento oggetto dell'esibizione;
- e) verifica la rispondenza dell'impronta calcolata con quella riportata nell'IPdA
- f) apre una *form web* nella quale mostra all'utente gli esiti dei controlli effettuati e il contenuto dell'IPdA, evidenziando la parte riferita al documento su cui è stata attivata la funzione di esibizione.

Gli esiti degli eventuali errori rilevati dal sistema durante l'operazione di esibizione sono:

- 1) Marca temporale non valida
- 2) Firma del RdC non valida
- 3) Impronta del documento non corrispondente con quella contenuta nell'IPdA

La presenza di tali errori determina l'invalidità del documento esibito.

La consultazione e lo scarico dei PdD sono rese disponibili tramite interfaccia web sicura, per il RDC e per gli utenti appositamente autorizzati.

Il RDC può richiedere al personale IDC la consegna di uno o più PdD attraverso la produzione di supporti fisici trasportabili (es: CD / DVD) o attraverso il deposito in un'area storage sicura. Possibilità e specifiche sono eventualmente regolate attraverso il Contratto di Servizio.

La procedura prevede l'adozione delle seguenti precauzioni:

- i supporti fisici devono essere crittografati e non devono presentare riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.;
- i dati trasmessi in forma telematica devono essere protetti con sistemi crittografici; l'eventuale download degli stessi da parte del cliente avverrà solo mediante canali sicuri, quali HTTPS o SFTP

In caso di accessi ed ispezioni da parte dell'Amministrazione finanziaria, è necessario garantire ai verificatori l'estrazione dal supporto di memorizzazione di un qualsiasi documento conservato, per consentire la verifica della correttezza dell'archivio di conservazione.

E' quindi possibile sottoporre a verifica i seguenti elementi:

- certificato di firma
- firma digitale, del riferimento temporale e della marca temporale
- evidenza informatica
- Impronta di hash
- documento firmato

[Torna al sommario](#)

## **7.9 Produzioni di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti**

L'utente autorizzato ad accedere al sistema di conservazione, tramite le proprie credenziali, può eseguire le ricerche attraverso una interfaccia web e tramite l'ausilio di una serie di chiavi di ricerca (metadati) predefinite.

Una volta ottenuto l'output della ricerca l'utente ha la possibilità di richiedere la produzione di un PdD o più semplicemente può eseguire la richiesta di download dei duplicati dei documenti informatici conservati.

Vi sono casi in cui è necessaria la produzione di una copia informatica con attestazione di conformità da parte di un pubblico ufficiale:

- per adeguare il formato del documento all'evoluzione tecnologica attivando un processo di riversamento sostitutivo a seguito dei controlli da parte del Responsabile del Servizio di Conservazione;
- per far fronte a specifiche esigenze dell'utente.

Il processo richiede la gestione di un riversamento sostitutivo, ovvero il processo che trasferisce uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica, garantendo il mantenimento dell'integrità del contenuto.

Proprio per la garanzia della conformità del contenuto nel passaggio da una rappresentazione informatica ad un'altra rappresentazione, più aggiornata tecnologicamente, è necessario l'intervento del pubblico ufficiale. In questi casi il RSDC, dopo aver contattato il PU di riferimento, mette a disposizione di quest'ultimo tutte le risorse e gli strumenti utili al completamento del processo di certificazione e autenticazione dei documenti conservati.

La procedura prevede la messa a disposizione dei documenti originali e dei documenti copia al PU che, una volta verificata la conformità del contenuto, appone la firma digitale su un file denominato "attestazione di conformità".

Questo documento viene posto in conservazione nel sistema come allegato integrativo all'operazione di conservazione della copia conforme.

Le operazioni di Riversamento vengono registrate nel "*Prospetto di riversamento*", allegato alla scheda "Specificità del Contratto".

[Torna al sommario](#)

## **7.10 Scarto dei pacchetti di archiviazione**

Alla scadenza dei termini di conservazione relativi alla specifica tipologia documentale e comunque definiti in sede contrattuale con il Cliente e riportati nel documento *Specificità del contratto*, avviene lo scarto del Pacchetto di Archiviazione dal sistema di conservazione a norma.

Sei mesi prima della scadenza del termine di conservazione viene inviata una comunicazione al Titolare dell'archivio, con il riepilogo dei documenti prossimi al termine del loro ciclo di archiviazione.

Il Titolare dovrà, entro 3 mesi dalla comunicazione, confermare la cancellazione o richiedere il prolungamento del periodo di conservazione; in entrambi i casi dovrà specificare se l'ordine di cancellazione o prolungamento debba essere applicato all'intero archivio in scadenza o solo a parte di esso. In quest'ultima ipotesi il Titolare dovrà comunicare l'elenco dettagliato dei documenti compresi, o esclusi, dalla comunicazione.

Il suddetto scambio di informazioni dovrà avvenire per iscritto; sia il verbale che la risposta del cliente dovranno essere firmati digitalmente dal RdC e dal Titolare dell'archivio

Con riferimento ad archivi di Enti Pubblici o di particolare interesse storico, le operazioni di scarto dovranno essere preventivamente autorizzate dal Ministero dei Beni e delle attività culturali e del turismo.

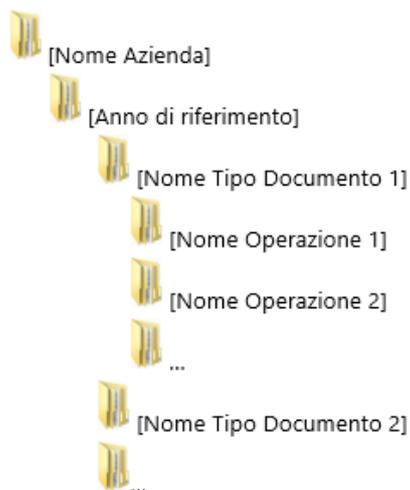
Tale autorizzazione, che dovrà pervenire per iscritto, verrà richiesta a cura del RDC, dietro segnalazione del RSDC.

[Torna al sommario](#)

### **7.11 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori**

Su richiesta del RdC è possibile esportare l'intero archivio di conservazione.

L'archivio viene organizzato in una gerarchia di folder che presentano la seguente struttura:



*Figura 13 - Esempio struttura di archiviazione*

Le operazioni di conservazione riferite a una tipologia di conservazione, sono ordinate in modo cronologico per periodo di riferimento. Dentro ciascun folder associato ad un'operazione di conservazione risulta memorizzato il relativo PdA.

L'adozione dello standard UNI 11386:2010 Standard SInCRO per l'IPdA garantisce il pieno supporto all'interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali

[Torna al sommario](#)

## 8 IL SISTEMA DI CONSERVAZIONE

Il sistema di conservazione dispone di numerose funzionalità, atte a gestire un obiettivo fondamentale come la sicurezza dei dati, le cui caratteristiche sono evidenziate di seguito:

Obiettivo	Caratteristiche del prodotto
Auditing (tracciamento delle attività)	Tutte le operazioni eseguite vengono storicizzate, registrando i riferimenti dell'utente che ha effettuato l'operazione, la data e la descrizione dell'operazione eseguita. In caso di modifica e/o cancellazione di un dato, il sistema è in grado di riproporre la storia delle singole operazioni e di risalire al contenuto del dato originale.
Sicurezza accesso alle funzionalità proposte	Tutte le funzionalità a disposizione degli utenti sono subordinate al processo di autenticazione e vengono gestite in base ad una lista di controllo accessi (elenco competenze).
Visibilità ed integrità delle informazioni registrate	L'accesso in modifica e la visibilità delle informazioni registrate sono subordinati a: Livello di accesso dell'utente collegato Grado di riservatezza della documentazione Politica di smistamento dei documenti Competenze specifiche (es. Responsabile del servizio di conservazione della Conservazione, Delegato ecc.)
Integrità e riservatezza dei file Allegati	Il sistema garantisce l'integrità dei documenti registrati: grazie a politiche di sicurezza sull'accesso ai dati mediante il controllo dell'impronta dei documenti registrati nel sistema, che viene generata e memorizzata all'atto della registrazione grazie alla firma digitale e marcatura temporale eventualmente apposta sui file è possibile garantire la riservatezza dei documenti imponendo la crittografia dei file archiviati

Nei paragrafi a seguire verranno descritte le componenti tecnologiche logiche e fisiche coinvolte nel sistema di conservazione, con particolare risalto agli aspetti di sicurezza ed alle procedure adottate per garantire la massima qualità del servizio erogato.

[Torna al sommario](#)

## 8.1 Componenti Logiche del Sistema ConSEDFx

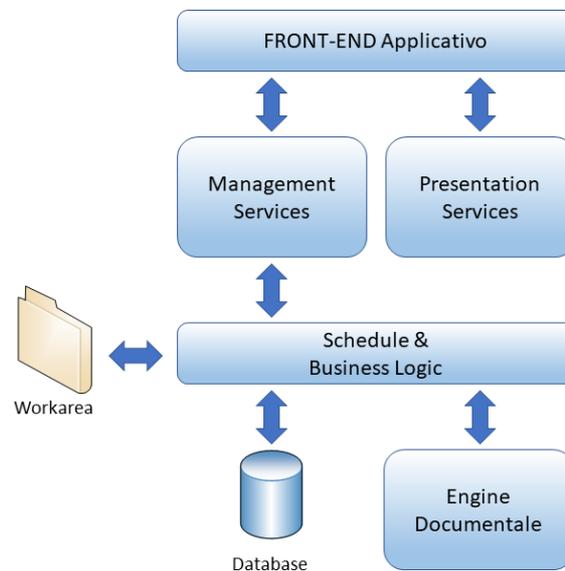


Figura 14 – Schema grafico component logiche

[Torna al sommario](#)

### 8.1.1 Front/end applicativo

Il front end applicativo è articolato in due sub-componenti:

#### **Management services**

È l'interfaccia web di amministrazione del sistema con la quale interagisce il Responsabile del servizio di conservazione di Conservazione e i suoi delegati per la fruizione delle funzionalità di gestione e monitoraggio dei processi di versamento e di conservazione.

Al servizio di management è delegata la gestione, l'impostazione, e la consultazione delle informazioni relative alla conservazione digitale, fungendo anche da cruscotto operativo del sistema.

#### **Presentation services**

Rappresenta la parte documentale di accesso ai documenti della gestione digitale è più generalmente di tutti i documenti a disposizione secondo il proprio profilo di accesso.

[Torna al sommario](#)

### 8.1.2 Schedule & Business Logic

È la parte responsabile della gestione dei processi correlati al servizio di conservazione:

- Processi di versamento
- Controlli di congruenza sulle unità documentarie versate e sui pacchetti di conservazione

- Processi di conservazione
- Processi di riversamento

[Torna al sommario](#)

### 8.1.3 Database

È il motore RDBMS preposto alla conservazione dei metadati dei documenti e di tutte le informazioni relative ai pacchetti versati, sia dal punto di vista dello stato, sia della composizione, sia delle azioni effettuate, che alla locazione fisica e logica di conservazione e che consente di riepilogare e tracciare tutte le informazioni relative al sistema di catalogazione.

[Torna al sommario](#)

### 8.1.4 Workarea

Area di lavoro che consiste nell'unica zona storage condivisa con l'esterno, ove il sistema può ricevere i pacchetti di versamento e su cui il sistema di conservazione memorizza i rapporti di versamento e i rapporti di conservazione.

[Torna al sommario](#)

### 8.1.5 Engine documentale

È il sistema che provvede alla fruizione della documentazione in senso generale e memorizzandola e presentandola in maniera omogenea rispetto alla generale documentazione aziendale.

[Torna al sommario](#)

## 8.2 Componenti Logiche del Sistema ArchiCons

L'infrastruttura è così composta:

- Sito primario c/o Datacenter Naquadria - Via Orsi, 39, 29122 Piacenza) – certificato ISO 27001:2013
- Sito primario presso il quale viene esercitato il servizio di conservazione documentale (società esterna)
- Sito secondario c/o Datacenter GTT Communication Inc. – Via Caldera, 21, 20153, Milano) – certificato ISO 27001:2013
- Sito secondario presso il quale viene esercitato il servizio di Disaster Recovery (società esterna)

L'applicazione ArchiCons consiste essenzialmente in tre moduli applicativi:

- Versamento
- Conservazione

- Esibizione

I moduli Versamento e Conservazione sono finalizzati alla Conservazione Digitale a Norma, pertanto prevedono l'acquisizione dei documenti con la relativa indicizzazione per la ricerca e l'archiviazione documentale secondo le normative di riferimento. L'Esibizione è il modulo che permette invece la generazione dei documenti preventivamente conservati per un loro utilizzo secondo i termini di legge.

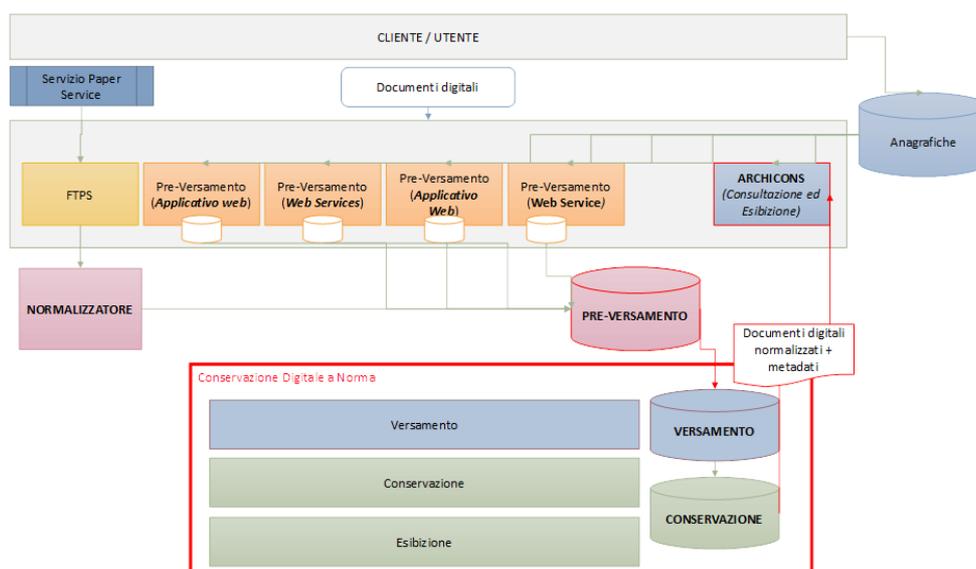


Figura 15 Struttura modulo di Versamento – Conservazione

Ogni modulo risponde ad una logica di struttura multi tier:

Livello di Presentazione Front End e Componenti Logico Applicative atte allo svolgimento di tutte le fasi del processo di conservazione: insieme delle interfacce attraverso le quali gli utenti interagiscono con il sistema nelle diverse fasi del processo di conservazione utilizzando le componenti logiche sottostanti.

Livello di Gestione Dati: rappresentato dai differenti DB di gestione-omogenizzazione dati, versamento, conservazione e gestione anagrafiche-modelli documentali (la gestione database è esplicitata poco più avanti)

Livello Repository per lo storage dei documenti e dei pacchetti informativi gestiti, versati e conservati

L'infrastruttura relativa ad ArchiCons ha una componente centrale, per l'elaborazione e presentazione delle informazioni, ospitata nel Datacenter primario. In particolare, gli utenti hanno a disposizione diversi Servizi Web che consentono loro di caricare i documenti oggetto di Conservazione Digitale a Norma. Il primo modulo "Versamento e Conservazione" emette un Report di versamento per confermare l'avvenuta presa in carico dei documenti.

I dati sono trasferiti dalla postazione utente al Servizio centralizzato attraverso il protocollo HTTPS (o FTPS) che garantisce un trasferimento sicuro delle informazioni.

Infine gli utenti, mediante la propria postazione di lavoro e attraverso lo stesso canale di comunicazione per l'acquisizione dei dati, possono accedere alla componente centrale di ArchiCons per la visualizzazione ed elaborazione dei dati (Esibizione).

Il Servizio è erogato su un'infrastruttura situata presso il sito primario – certificato ISO27001. La soluzione prevede adeguati presidi tecnologici e infrastrutturali volti a garantire misure di alta affidabilità e disaster recovery in linea con le indicazioni della normativa in materia e con le prassi adottate sul mercato.

Attraverso l'implementazione dei Processi di "Business Continuity e Disaster Recovery" è stata predisposta una infrastruttura aggiuntiva rispetto a quella ubicata nel sito primario, attraverso cui poter erogare i servizi relativi all'ambiente di esercizio dell'applicazione ArchiCons. Questa infrastruttura, ubicata a Milano presso il datacenter GTT Communication Inc, diventa operativa in caso di eventi di interruzione non pianificati dei servizi sul sito primario.

L'infrastruttura relativa all'ambiente di esercizio dell'applicazione ArchiCons presente nel sito secondario è speculare a quella nel sito primario, in modo da garantire l'assenza di degni prestazionali.

Nell'architettura è prevista una separazione fisica e logica degli ambienti di sviluppo e produzione.

Nell'erogazione del Servizio di conservazione ArchiCons, gli aspetti della sicurezza rispettano i principi espressi dalle policies aziendali di IDC e dei Datacenter presso i quali risiedono la farm principale e secondaria di Archivium. Entrambi i datacenter detengono le certificazioni ISO 27001 a garanzia del rispetto delle misure e dei principi di sicurezza richiesti.

[Torna al sommario](#)

### **8.3 Componenti Fisiche della piattaforma ConSEDFx**

L'architettura proposta è organizzata su due datacenter dei quali il principale posto in un locale c/o la Sede di IDC a Milano e l'altro ad Arezzo, in questo modo viene pienamente rispettata la raccomandazione di DIGITPA relative alle distanze fra DC.

L'architettura generale del sistema può essere così schematizzata:

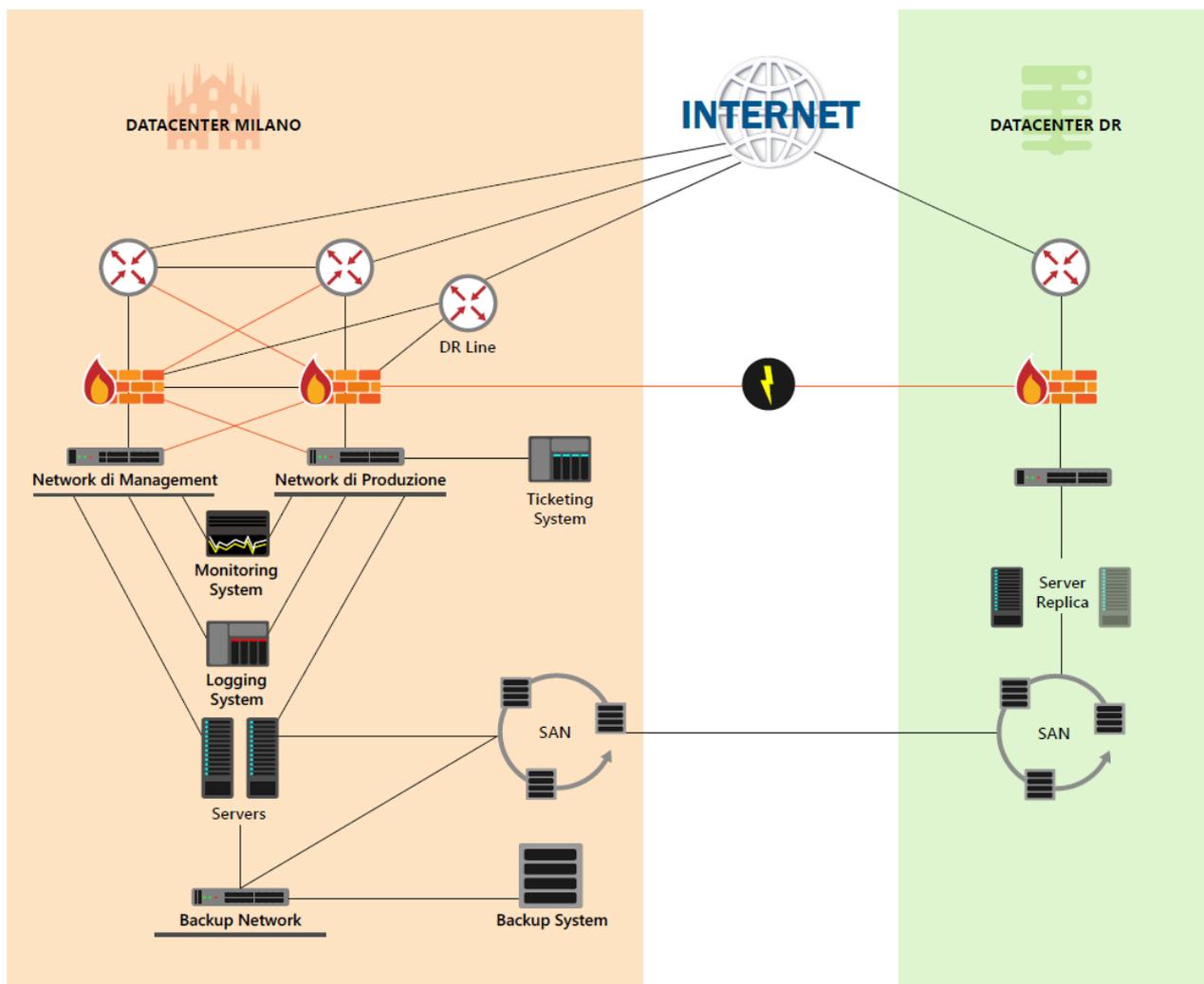


Figura 16 - Schema grafico architettura di sistema

[Torna al sommario](#)

### 8.3.1 Procedure di gestione e di evoluzione

All'interno delle proprie politiche ISO 27001 IDC ha definito le linee guida relative allo sviluppo, alla manutenzione e alla conduzione dei SI, sempre e comunque in conformità alle prescrizioni di legge e agli impegni contrattuali, al fine di proteggere sia il proprio patrimonio informativo che quello dei propri Clienti.

[Torna al sommario](#)

### **8.3.2 Gestione e conservazione dei log**

IDC considera i log di sistema facenti parte del proprio patrimonio informativo meritevole di protezione da tutto ciò che è in grado di minacciarlo; per tale motivo ha definito i log come dati *confidenziali*, meritevoli del massimo livello di protezione.

I dati, prodotti come descritto al precedente punto 7.2.3, vengono mantenuti per 10 anni.

[Torna al sommario](#)

### **8.3.3 Monitoraggio del sistema**

Il monitoraggio dei sistemi viene effettuato con le seguenti modalità:

- monitoraggio istantaneo (monitoring system): strumenti automatici che vengono utilizzati per una rapida ed efficace gestione degli eventi e che inviano segnalazioni ad un sistema di ticketing. Maggiori dettagli sul monitoraggio verranno forniti al successivo capitolo 9.
- monitoraggio manuale periodico per verificare i tempi di elaborazione e prendere visione dell'andamento delle risorse ai fini di un corretto Capacity Planning.

[Torna al sommario](#)

### **8.3.4 Change management**

IDC per assicurare completezza ed efficienza nella gestione delle richieste di cambiamento al servizio erogato, ha definito delle politiche in ambito ISO 27001 che regolamentano le modalità di presa in carico, valutazione ed autorizzazione delle richieste di change.

[Torna al sommario](#)

### **8.3.5 Verifica periodica di conformità a normativa e standard di riferimento**

Il RSDC ha, tra i suoi compiti, quello di definire le caratteristiche ed i requisiti del sistema di conservazione in conformità alla normativa vigente e monitorarne l'attuazione.

Ai fini della verifica di conformità sono periodicamente effettuati degli audit interni, così come previsto sia nel SGQ ISO 9001 che nella ISO 27001. Le verifiche ispettive sono eseguite sui documenti e/o prodotti delle attività esaminate e sulle registrazioni risultanti dallo svolgimento delle attività.

Il processo di audit si compone dei seguenti passi:

1. Pianificazione: è predisposto il Piano delle verifiche ispettive
2. Accordo di visita: l'ispettore concorda la data di visita con il responsabile da esaminare richiedendo l'eventuale documentazione necessaria

3. Esecuzione visita ispettiva: l'ispettore esegue la verifica dei requisiti del Sistema che fanno capo al responsabile esaminato, confrontando le evidenze delle attività svolte con le procedure previste per quelle attività.
4. Verifica chiusura non conformità: l'ispettore verifica e valuta le correzioni effettuate e ne dichiara la (eventuale) risoluzione
5. Riepilogo delle non conformità: viene redatto il riepilogo delle non conformità (indirizzato, nei momenti pianificati, al riesame della Direzione)

[Torna al sommario](#)

## 8.4 Componenti Fisiche della piattaforma ArchiCons

Schema e descrizione dei siti di conservazione e delle connessioni tra i diversi siti e tra i diversi attori del sistema, con riferimento alle componenti tecnologiche del paragrafo precedente.

Schema e descrizione delle componenti fisiche presenti in ciascuno dei siti di conservazione.

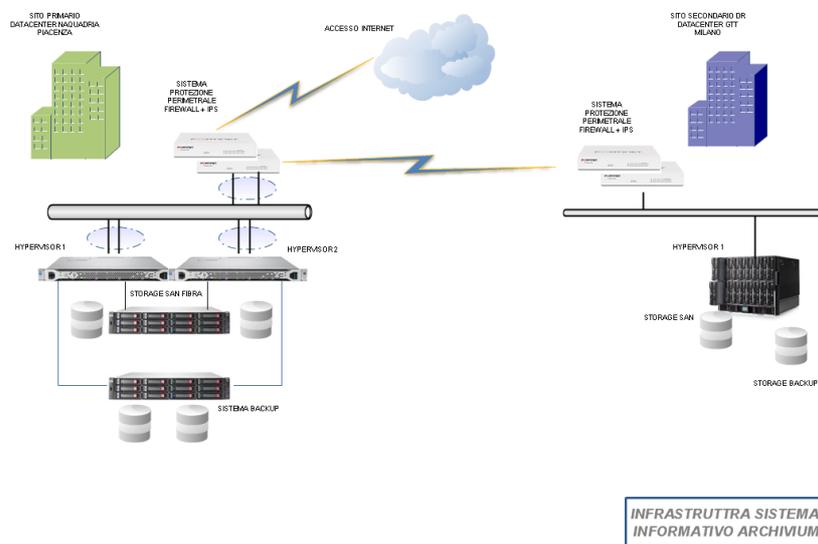


Figura 17 - Schema delle componenti fisiche

Nel Datacenter primario sono presenti i seguenti elementi:

- VPS di sviluppo con ambiente controllato rispetto all'ambiente di produzione;
- VPS di test con ambiente controllato ed omogeneo rispetto all'ambiente di produzione;
- VPS di produzione per la gestione dei DB di gestione documentale

- VPS di produzione che si occupa di ospitare gli applicativi che ricevono dati e immagini i quali necessitano di una procedura di normalizzazione. Gli stessi applicativi, inoltre, organizzano i documenti al fine di creare un pacchetto di versamento. Una procedura di invio del pacchetto viene attivata per il trasferimento del pacchetto ad un altro server.
- VPS che riceve i dati da qualsiasi sistema terzo in grado di generare un pacchetto di versamento come da standard ArchiCons, che effettua la presa in carico ed i controlli sul pacchetto di versamento, scrivendo sul DB AZI\_VE i metadati. All'interno di questo server vengono espletate tutte le funzioni di conservazione ed esibizione.
- Numero 2 VPS ad uso solo storage collegate alla VPS di produzione contenenti ognuna 3 filesystem.
- DB AZI\_GE: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB AZI\_VE: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB AZI\_CO: è il data base che memorizza le informazioni gestite ed elaborate dal Web Service
- DB ANAGRAFICHE: è il database che contiene i dati relativi ai Clienti, agli utenti e ai Modelli Documentali. Inoltre, gestisce i token per gli accessi – nonché le relazioni tra di essi.

Nel sito primario l'unità di storage è collegata con adapter in fibra ridondati ai server fisici. I server fisici sono gestiti da Hypervisor Vmware in cluster con funzioni HA. La struttura lan è supportata da switch ethernet ridondati con porte da 10 GB. Gli Hypervisor ospitano i server virtuali, gestiscono e concedono gli accessi allo storage ed alle specifiche vlan. Per gli approfondimenti ed il dettaglio in relazione alle componenti fisiche ed alla continuità operativa si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato ISO/IEC 27001:2017.

Di seguito lo schema degli ambienti Archivium dedicati alla piattaforma di Indicom eDocument Care Srl:

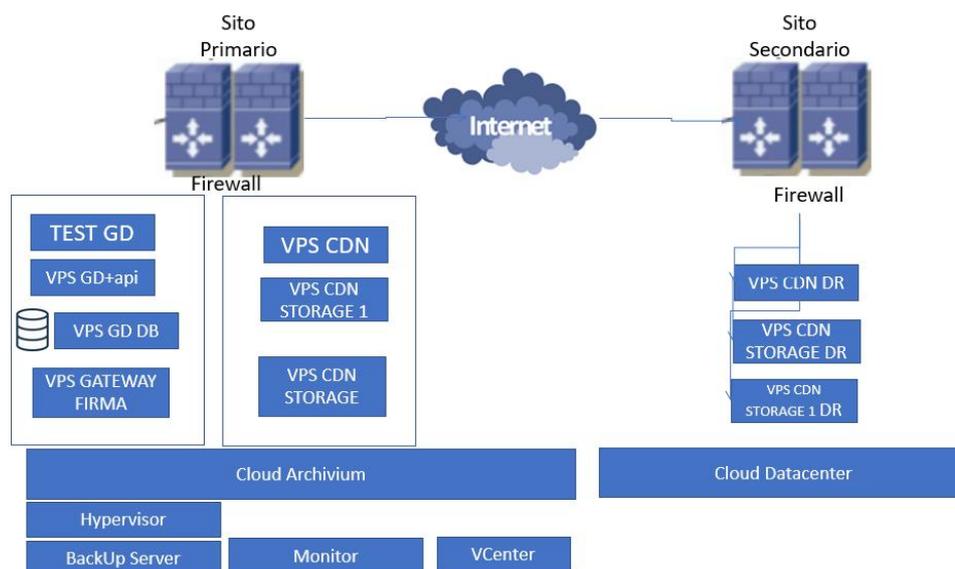


Figura 18 - Schema delle componenti fisiche/logiche di IDC

## 9 MONITORAGGIO E CONTROLLI

In questo capitolo sono descritte le procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi.

Le procedure di monitoraggio si dividono in:

- Monitoraggio dell'infrastruttura
- Verifica dell'integrità degli archivi

[Torna al sommario](#)

### 9.1 Procedure di monitoraggio

Viene effettuato monitoraggio per tutte le macchine virtuali e fisiche delle seguenti grandezze:

- Sistema
  - Storage
    - occupazione disco
  - Cpu
    - carico cpu di picco nei 5 minuti e nell'ora
  - Stato dei processi di sistema 5 min (RDBMS, Indexing, Web server)
  - Esito e durata dei processi di backup
  - Memoria
  - Rete (solo per le macchine fisiche)
    - raggiungibilità dei sistemi fisici e virtuali
    - traffico di rete giornaliero e mensile (volume dati scambiati)
    - max traffico picco banda su su base 15 min
- RDBMS
  - spazio occupato dal DB
  - query wait on lock
  - idle in transaction status
- Procedura di conservazione
  - Stato ed esito dei processi di conservazione

Ognuno di questi valori è soglia su due livelli, nel caso di raggiungimento dei valori di soglia stabiliti il sistema è configurato per inviare una richiesta di ticket all'helpdesk di supporto.

Per quanto riguarda la piattaforma ArchiCons, il monitoraggio è effettuato a livello sistemistico ed applicativo su tutti i moduli che costituiscono il sistema, dal preversamento, al versamento, al modulo di conservazione ed infine quello di esibizione. A livello sistemistico viene monitorato l'uptime delle macchine, nonché l'utilizzo delle loro risorse e le disponibilità residue.

Il software utilizzato è Zabbix:



Figura 19 - Software di monitoraggio

[Torna al sommario](#)

## 9.2 Verifica dell'integrità degli archivi

Il Responsabile del servizio di conservazione, a norma dell'art. 7 lettera f) del DPCM 03 dicembre 2013, verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati, provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Le verifiche periodiche vengono svolte annualmente su tutto l'archivio da una procedura automatizzata che effettua il ricalcolo dell'hash del PdA, generando un report di output che viene firmato da RSDC e conservato a sua volta.

In presenza di eventuali Non Conformità il Responsabile del Servizio di conservazione, in sinergia con i responsabili di funzione interessati e, ove necessario, coinvolgendo il Responsabile della Conservazione del Cliente, definirà le necessarie azioni correttive.

Qualora la segnalazione riguardasse la leggibilità o integrità dei file, è prevista l'attivazione della procedura di riversamento diretto, utilizzando le copie di sicurezza.

L'allerta preventiva è implementata a livello di infrastruttura fisica e logica. Il sistema di monitoraggio controlla in tempo reale se tutti i componenti del sistema di conservazione sono disponibili e se le relative performance sono soddisfacenti. In caso di malfunzionamento e/o degrado, il sistema di monitoraggio effettua la segnalazione via e-mail. La mail consente al gruppo tecnico di verificare e di intervenire secondo l'apposito processo da instradare (rimozione del malfunzionamento, apertura di una richiesta di cambiamento per migliorare le performance, ecc).

Anomalie e azioni correttive vengono registrate nel registro delle anomalie

[Torna al sommario](#)

### **9.3 Soluzioni adottate in caso di anomalie**

Il software utilizzato per la conservazione digitale è governato e gestito dal Responsabile del servizio di conservazione, per le sole funzioni a loro attribuite, dai delegati.

Tutte le attività emerse in relazione a guasti e/o malfunzionamenti, sono da considerarsi attività gestite attraverso il processo di Incident Management. In caso di inaccessibilità al sistema primario, l'operatività è regolata dalle politiche di BC e DR adottate in ambito ISO 27001.

[Torna al sommario](#)