Arancia Innovation **C**onsulting **T**echnology S.r.l.
Via Resuttana Colli, 360 – 90146 Palermo
Tel. 091 774 2579 - Fax 091 619 7327
www.arancia-ict.it - direzione@arancia-ict.pecnp.it

P. IVA e Reg. Imprese di Palermo: 05653800820
C.C.I.A.A. di Palermo R.E.A. 268766
Capitale sociale € 300.000,00

Manuale di Conservazione

di Arancia-ICT S.r.l.

per il servizio "Conservazione No Problem"

Versione 2.10 del 06/07/2018

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	29/06/2018	Antonio Ferraro	RFAC
Verifica	06/07/2018	Nicola Incandela	RSIC
Approvazione	06/07/2018	Filippo Ciaravella	RSC

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	05/10/2010	Nuovo documento	
2.0	24/11/2014	Nuovo documento basato sull'indice pubblicato da AgID il 16/10/2014 e allineato alle specifiche del DPCM 3/12/2013	
2.1	19/03/2015	Inseriti i riferimenti al luogo di conservazione e al provider che fornisce il data center	
2.2	07/05/2015	Inserito indirizzo del server di conservazione dei documenti. Aggiornata la tabella dei profili professionali.	
2.3	17/06/2015	Apportate modifiche e integrazioni segnalate da AgID e basate sullo schema pubblicato il 16/01/2015 ("Schema di manuale di conservazione v.2_1")	
2.4	16/07/2015	Apportate modifiche e integrazioni segnalate da AgID il 14/07/2015	
2.5	20/07/2015	Apportate ultime modifiche e integrazioni segnalate da AgID il 20/07/2015	
2.6	29/01/2016	Apportate ultime modifiche e integrazioni segnalate da AgID con e-mail del 22/12/2015 e basate sullo schema pubblicato il 16/01/2015 ("Schema di manuale di conservazione v.2_1")	
2.7	17/02/2016	Apportate correzioni formali ai paragrafi 4.1, 4.2 e 4.3 sostituendo il termine "delega" con "affidamento"	
2.8	31/01/2018	Apportate modifiche al capitolo 4 e al capitolo 5 per aggiornamento dell'Organigramma aziendale. Apportate modifiche al capitolo 6 e al capitolo 7 per modifiche alle Procedure di acquisizione e verifica dei PdV e alla Procedura per la generazione dei PdA. Apportate modifiche al paragrafo 8.5 'Procedure di gestione ed evoluzione' in relazione ai processi di: • *Audit di revisione della conformità agli standard e normative* • *Change Management* e *Capacity Management*	
2.9	30/04/2018	Apportate modifiche al capitolo "*8 – IL PROCESSO DI CONSERVAZIONE*" circa il	

		controllo crittografico da applicare secondo le specificità del contratto con il cliente. Apportate modifiche al paragrafo 9.6 “Procedure di Monitoraggio”. Apportate modifiche al paragrafo 5.3 “Responsabile del servizio di Conservazione – Soggetto Conservatore”. Apportate modifiche al capitolo 6 “STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE”. Apportate modifiche al Template del Documento: Aggiornato il Capitale Sociale e i loghi RINA della prima pagina del Frontespizio. Aggiornati i riferimenti alla norma UNI EN ISO 9001:2015 (qualità). Aggiornati i riferimenti a tutte le procedure operative e a tutte le istruzioni operative del Sistema di Gestione Integrato (SGI).	
2.10	29/06/2018	Apportate modifiche al paragrafo “8.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori”: dettagliate le modalità di trasferimento dei dati in caso di cessazione dell’Organizzazione. Apportate modifiche al paragrafo “9.5.1.2 Audit di revisione della conformità agli standard e normative e obsolescenza tecnologica”: dettagliate le modalità di conduzione e registrazione delle revisioni di conformità agli standard di riferimento e alle normative applicabili.	

INDICE DEL DOCUMENTO

1 Sommario

2 SCOPO E AMBITO DEL PROGETTO

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti (di seguito anche "Manuale della Conservazione") ai sensi dell'articolo 8 del DPCM 3/12/2013 (G.U. 12/03/2014).

Il Manuale ha lo scopo di documentare il processo di conservazione dei documenti informatici in riferimento alla normativa corrente ed è relativo al Servizio di Conservazione erogato in outsourcing ai Clienti da Arancia-ICT S.r.l. (nel seguito Arancia-ICT). Il documento si applica al servizio denominato *Conservazione No Problem* fornito in modalità ASP (*Application Service Providing*) da Arancia-ICT secondo uno schema di BPO (*Business Process Outsourcing*).

Il Manuale descrive le procedure e le prassi seguite dal Soggetto Produttore (il Cliente), che affida in quanto Responsabile della Conservazione il Servizio di Conservazione in outsourcing al Soggetto Conservatore (*Arancia-ICT*) in qualità di Responsabile del servizio di Conservazione, in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate.

Il documento illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, le procedure, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento nel tempo, del sistema di conservazione.

Il predetto documento e gli eventuali ulteriori documenti rilasciati quali "specifiche forniture del servizio di conservazione" sono custoditi presso la sede del Conservatore *Arancia-ICT SRL*. Il documento è identificato attraverso il livello di revisione e la data di emissione. Il Conservatore esegue periodicamente un controllo di conformità del processo di erogazione del servizio di conservazione e, ove necessario, aggiorna il documento in oggetto anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

Il Manuale della Conservazione, depositato e pubblico presso l'*Agenzia per l'Italia Digitale*, è un documento informatico prodotto nel formato PDF/A, su cui è apposta la firma digitale del Responsabile del Servizio di Conservazione e Rappresentante Legale ed è conservato secondo le disposizioni della normativa vigente, al fine di assicurarne l'origine, la data certa e l'integrità del contenuto dalla sua emissione e per tutto il periodo di conservazione.

In caso di ispezione da parte delle Autorità di Vigilanza o di altri organismi a ciò deputati, il Manuale permette un agevole svolgimento di tutte le attività di controllo e costituisce un'importante dimostrazione dell'impegno del Responsabile della Conservazione al rispetto delle norme.

Il presente Manuale della Conservazione è collegato ai documenti riportati nella successiva tabella, che entrano più nel dettaglio in diversi aspetti del sistema e del servizio di conservazione e costituiscono parti integranti e sostanziali del Manuale della Conservazione.

Documenti collegati	
Condizioni Generali del Servizio **+** **Specificità del Contratto**	Il documento di Condizioni generali di fornitura rappresenta il documento che contiene le specifiche condizioni del servizio di conservazione ("Condizioni Generali Del Servizio"), e insieme all'eventuale documento di "Specificità del Contratto" sono parte integrante e sostanziale del contratto di servizio sottoscritto tra le parti e del Manuale di conservazione: quest'ultimo viene redatto dal Conservatore sulla base

(Scheda Servizio Cliente)	delle informazioni condivise con il Produttore dei documenti, contenente i requisiti essenziali del Servizio, le relative specifiche tecnico-funzionali e procedurali per le varie fase del servizio (attivazione, versamento, conservazione, post-produzione, distribuzione) oltre ai livelli di Servizio (SLA); tale documento è redatto in fase di analisi, prima del collaudo e della produzione del primo processo di conservazione.
Piano per la Sicurezza	Rappresenta il documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici *Conservazione No Problem* da possibili rischi nell'ambito dell'organizzazione.

Nella piena consapevolezza di voler rispondere in maniera efficace ed efficiente alle aspettative del Cliente, *Arancia-ICT* ha deciso di definire un Sistema di Gestione Integrato (SGI) organizzato ed attivato in conformità ai requisiti delle normative UNI EN ISO 9001:2015 (qualità), UNI CEI ISO/IEC 27001:2014 (sicurezza delle informazioni).

Arancia-ICT si impegna ad essere conforme ai requisiti richiesti per garantire un servizio di conservazione a norma, sia esso diretto a Pubbliche amministrazioni o a Privati, tenendolo sempre allineato alle normative vigenti ed ai più elevati standard di qualità ed affidabilità, nonché si impegna ad offrire tale servizio in maniera duratura nel tempo.

Torna al Sommario

3 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Di seguito si riporta la tabella contenente in ordine alfabetico il Glossario dei termini e gli Acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata.

Termine o acronimo	Significato
AgID	È l'acronimo di *Agenzia per l'Italia Digitale*. È una agenzia pubblica italiana istituita dal Governo Monti, ed è sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato. Svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della Pubblica Amministrazione e al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.
AIP	Nel Modello OAIS, Archival Information Package. Rappresenta il Pacchetto di Archiviazione PdA.
Application Service Providing	Si intende il servizio erogato attraverso la fruizione di un'applicazione software su Internet senza alcuna installazione sul computer del cliente. (Fonte: http://it.wikipedia.org/wiki/Application_service_provider)
Archiviazione	È il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.

ASP	Vedi Application Service Providing
BPO	Vedi Business Process Outsourcing
Business Process Outsourcing	Letteralmente "*esternalizzazione di processi amministrativi*".
CA	È l'acronimo di *Certification Authority*, letteralmente Autorità Certificativa, è un ente di terza parte (trusted third party), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conforme alla normativa europea e nazionale in materia.
Conservazione	È il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nel DPCM 03/12/2013.
CNP	Acronimo di ***Conservazione No Problem***, il servizio di conservazione digitale dei documenti erogato da Arancia-ICT ai propri Clienti.
DIP	Nel Modello OAIS, Dissemination Information Package. Rappresenta il Pacchetto di Distribuzione PdD.
Documento analogico originale	Documento analogico, che contrappone al *Documento Informatico* o *Documento Digitale*. Può essere *unico* oppure *non unico.* In questo secondo caso si tratta di un documento cui sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi, tipicamente Fatture, Libri Contabili etc. Il documento analogico unico, invece, è tipicamente identificato con il documento con una o più firme autografe (es. contratti).
Documento digitale	Vedi Documento Informatico.
Documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Evidenza Informatica	sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (all. 1 DPCM 03/12/2013) a partire da un documento informatico o da un insieme di questi.
Firma Digitale	un particolare tipo di firma elettronica basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
FNP	Acronimo di ***Fattura No Problem***, il servizio di emissione e gestione delle fatture elettroniche alle PPAA erogato da Arancia-ICT ai propri Clienti.
Hash	Vedi Evidenza Informatica.
IdC	Indice di Conservazione
IdPA	Indice del Pacchetto di Archiviazione
IdPV	Indice del Pacchetto di Versamento
Impronta informatica	Vedi Evidenza Informatica.

Marca Temporale	il riferimento temporale che consente la validazione temporale di un documento informatico. È l'equivalente della Data Certa che gli Uffici Postali appongono sui documenti cartacei.
NdR	Notifica di Rifiuto
PDF	È l'acronimo di *Portable Document Format*, formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'*International Organization for Standardization* (ISO) con la norma ISO 19005:2005.
PdV	Pacchetto di Versamento
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PEC	Vedi Posta Elettronica Certificata
PNP	Acronimo di ***Protocollo No Problem***, il servizio di protocollo informatico e gestione documentale erogato da Arancia-ICT ai propri Clienti.
Posta Elettronica Certificata	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici. Ha la medesima valenza della Raccomandata postale.
RdV	Rapporto di Versamento
Responsabile della Conservazione	Il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione digitale conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
RSC - Responsabile del Servizio della Conservazione	Responsabile del Servizio di Conservazione. La conservazione può essere affidata ad un soggetto esterno (art. 6, comma 7), che assume il ruolo di *Responsabile del Servizio di Conservazione* e opera nel rispetto del "Manuale della Conservazione". Arancia ICT, alla luce di quanto prescritto dalla normativa, opera come *Responsabile del Servizio di Conservazione*, utilizzando un sistema di conservazione accreditato AgID e descritto nel presente "Manuale della Conservazione" e nel "Piano della Sicurezza" associato.
RSIC	Responsabile dei Sistemi Informativi per la conservazione.
RFAC	Responsabile funzione Archivistica di Conservazione
RSSC	Responsabile per la Sicurezza dei sistemi per la Conservazione
RTDP	Responsabile del Trattamento dei Dati Personali
Riferimento temporale	Vedi Marca Temporale.
SGI	Sistema di Gestione Integrato
SIC	Sistema Informatico di Conservazione

SIP	Nel modello OAIS, Submission Information Package. Rappresenta il Pacchetto di Versamento PdV.
SLA	È l'acronimo di *Service Level Agreement*, letteralmente Accordo sui Livelli di Servizio, nella fattispecie servono a monitorare la qualità del servizio di conservazione in rapporto al contratto sottoscritto con il Cliente.
SSL	Secure Socket Layer
URL	Uniform Resource Locator
XML	È l'acronimo di Extensible Markup Language. Viene utilizzato per definire le strutture dei dati utilizzando dei marcatori (markup tags). È lo standard utilizzato, ad esempio, per l'emissione delle Fatture Elettroniche verso la Pubblica Amministrazione.

Torna al Sommario

4 NORMATIVA E STANDARD DI RIFERIMENTO

4.1 Normativa di riferimento

Il contesto normativo in cui si inquadra la conservazione digitale risale sostanzialmente all'anno 2004 con il Decreto del Presidente del Consiglio dei Ministri del 13/01/2004, le numerose deliberazioni AIPA – poi divenuta CNIPA, ora AgID –, il Decreto Ministero Economia e Finanze 23 gennaio 2004 e il Decreto Legislativo 52 del 20 febbraio 2004, relativi a specifiche tipologie di documenti). Quindi, è stato emanato il "Codice Dell'Amministrazione digitale", il D.Lgs n. 82 del 7 marzo del 2005 (GU 16/05/2005 s.o. n. 93/L) entrato in vigore a partire dal 1 gennaio 2006, che vuole contribuire a rendere ancora più omogeneo il quadro di riferimento; da questa data tutte le disposizioni non riunite e coordinate all'interno del Codice sono state abrogate. Il Codice è stato recentemente rivisto dal D.Lgs. n. 235 del 30 dicembre 2010, allo scopo di rendere il quadro normativo più coerente alle innovazioni tecnologiche occorse negli ultimi anni.

Infine il DPCM 03/12/2013 (GU n. 59 del 12-03-2014) 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, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004.

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.
- DMEF 17 giugno 2014 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto - articolo 21, comma 5, del decreto legislativo n. 82/2005.
- 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

4.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento adottati da Arancia-ICT ed elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione con indicazione delle versioni aggiornate al 1° ottobre 2014:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- UNI CEI ISO/IEC 27001:2014, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1:

Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

- ETSI TR 101 533-2 V1.3.1 (2012-04) Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- UNI ISO 15489-1:2006 (Information and documentation - Records management - Part 1: General, Informazione e documentazione), Gestione dei documenti di archivio - Principi generali sul record management;

Torna al Sommario

5 RUOLI E RESPONSABILITÀ

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei e conservazione informatica.

5.1 Cliente – Soggetto Produttore

Nei Dati Tecnici e Contrattuali allegati al presente Manuale il 'Cliente' è il *Soggetto Produttore* dell'archivio digitale. I recapiti, i riferimenti amministrativi e anagrafici, nonché l'atto di affidamento per lo svolgimento del servizio di conservazione del Cliente/Soggetto Produttore sono tenuti da Arancia-ICT nell'apposito archivio digitale.

5.2 Responsabile della Conservazione - Referente di processo del Soggetto Produttore

Il Referente di processo del Soggetto Produttore è l'incaricato al controllo della creazione dei documenti e dell'invio degli stessi in conservazione. Costui è il *Responsabile della Conservazione* INTERNO all'Ente/Società Cliente (Soggetto Produttore) che affida ad Arancia-ICT gli oneri di cui all'art. 7 del DPCM 03/12/2013, ovvero che affida il Servizio di Conservazione ad Arancia-ICT (Soggetto Conservatore). I relativi recapiti e i riferimenti amministrativi e anagrafici del referente Responsabile della Conservazione presso il Cliente-Soggetto Produttore sono tenuti da Arancia-ICT unitamente a quelli del Cliente/Soggetto Produttore stesso.

5.3 Responsabile del servizio di Conservazione – Soggetto Conservatore

Il Soggetto Produttore, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM 03/12/2013, ha affidato il Servizio di Conservazione al Soggetto Conservatore e ha affidato lo svolgimento delle attività del Responsabile della Conservazione ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle attività di conservazione. Tale soggetto conservatore terzo è Arancia-ICT, *Responsabile del servizio di Conservazione* ovvero il gestore del servizio di conservazione digitale in outsourcing.

L'atto di affidamento del Servizio di Conservazione (per lo svolgimento delle attività del Responsabile del servizio di Conservazione) viene conferito dal Soggetto Produttore ad Arancia-ICT (Soggetto Conservatore) contestualmente alla sottoscrizione del contratto di adesione al servizio.

Arancia-ICT ha affidato lo svolgimento delle attività del *Responsabile del servizio di Conservazione* così come riportate all'art. 7 del DPCM 03/12/2013, ad una o più persone fisiche che, per competenza ed esperienza, garantiscono la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali, nonché dal presente Manuale.

Di seguito è riportata la tabella dei "*Responsabili del servizio di Conservazione*" che elenca le responsabilità soggettivamente identificate ed assegnate a persone incaricate da Arancia-ICT per lo svolgimento del Servizio di Conservazione:

Ruoli	**Nominativo**	**Attività di competenza**	**Periodo nel ruolo**	**Eventuali Deleghe**
Responsabile del Servizio di Conservazione	Filippo Ciaravella (FCI)	Definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità, svolgendo il ruolo di *Responsabile del servizio di Conservazione* ai sensi dell'art. 7 del DPCM 3/12/2013. Svolge in prima persona i seguenti compiti: • assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; • assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza; • definisce le caratteristiche e i requisiti del sistema di conservazione in conformità alla	Dal 1° giugno 2005	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		normativa vigente e verifica periodicamente con il *Responsabile dei sistemi informativi per la conservazione* la conformità alla normativa e agli standard di riferimento; • supervisiona insieme al *Responsabile Servizio Clienti* (area: *Servizi SaaS*) la corretta erogazione del servizio di conservazione all'ente produttore; • assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite; • predispone il presente Manuale di Conservazione insieme al *Responsabile funzione Archivistica di conservazione* e al *Responsabile sistemi informativi per la conservazione* e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti; • gestisce le convenzioni, definisce gli aspetti tecnico-operativi e la validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi		

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		di conservazione (insieme al *Responsabile del Servizio Clienti* – area: *Servizi SaaS*); • presa in carico dei pacchetti di versamento e generazione del rapporto di versamento; • preparazione e gestione del pacchetto di archiviazione; • preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta del Cliente. Delega esplicitamente gli altri compiti previsti dall'art. 7 del DPCM 3/12/2013.		
Responsabile sistemi informativi per la conservazione	Nicola Incandela (NIN)	Svolge i seguenti compiti: • definisce con il *Responsabile del servizio di Conservazione* e con il *Responsabile funzione Archivistica di conservazione* le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, in conformità alla normativa vigente; • gestisce la conduzione del sistema di conservazione ovvero gestisce l'esercizio delle componenti hardware e software del sistema di conservazione; • pianifica lo sviluppo delle infrastrutture	Dal 1° gennaio 2015	Nell'ambito della gestione della conduzione del sistema di conservazione (gestione dell'esercizio delle componenti hardware e software del sistema di conservazione) affida (con Delega del 30/04/2018) a Manfredi Trizzino (MTR) (già designato Amministratore dei Sistemi presso Arancia-ICT da ottobre 2015) il ruolo specifico di *Amministratore di Sistema di Conservazione* (area: *Infrastruttura e Sistemi/IaaS*) con i seguenti compiti: • Monitoraggio Sistemistico componenti hardware e software

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		tecnologiche del sistema di conservazione; • verifica il monitoraggio della corretta funzionalità del sistema di conservazione di concerto con il *Responsabile Servizio Clienti* (area: *Servizi SaaS*) ovvero verifica il monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; • segnala le eventuali difformità degli SLA al *Responsabile del Servizio di conservazione* e individua e pianifica le necessarie azioni correttive; • progetta il change management di concerto con il *Responsabile sviluppo e manutenzione del sistema di conservazione*; • verifica periodicamente con il *Responsabile del servizio di Conservazione* la conformità alla normativa e agli standard di riferimento.		
Responsabile funzione Archivistica di conservazione	Antonio Ferraro (AFE)	Svolge le seguenti funzioni: • analizza il sistema archivistico analogico del Cliente; • acquisisce i requisiti del Cliente; • progetta concettualmente il sistema di conservazione digitale e definisce le specifiche di realizzazione del	Dal 17 ottobre 2006	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		sistema; ● definisce e gestisce il processo di conservazione digitale, 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/e, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; ● definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici; ● monitora il processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione; ● 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.		
Responsabile sviluppo e manutenzione del sistema di conservazione	Nicola Incandela (NIN)	Svolge i seguenti compiti: ● coordina lo sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione ovvero progetta e realizza le funzionalità del sistema di conservazione (pianifica e monitora i progetti di sviluppo del	Dal 1° gennaio 2012	Nell'ambito della gestione della conduzione del sistema di conservazione (gestione dell'esercizio delle componenti hardware e software del sistema di conservazione) affida (con Delega del 30/04/2018) a Manfredi Trizzino (MTR) (già designato Amministratore dei Sistemi presso Arancia-ICT da ottobre 2015) il ruolo specifico di *Amministratore di Sistema di Conservazione* (area:

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		sistema di conservazione) e ne gestisce la conduzione e la manutenzione; • effettua il change management di concerto con il *Responsabile sistemi informativi per la conservazione*; • si occupa di concerto con il *Responsabile Servizio Clienti* (area: *Servizi SaaS*) del monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione • si interfaccia di concerto con il *Responsabile Servizio Clienti* (area: *Servizi SaaS*) 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; • gestisce lo sviluppo di siti web e portali connessi al servizio di conservazione. • al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di		*Infrastruttura e Sistemi/IaaS*) con i seguenti compiti: • Monitoraggio Sistemistico componenti hardware e software

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		memorizzazione e, ove necessario, per ripristinare la corretta funzionalità; ● adotta analoghe misure con riguardo all'obsolescenza dei formati; ● provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione; ● implementa le misure necessarie per la sicurezza fisica e logica del sistema di conservazione. ● Responsabile per la gestione delle Segnalazioni inerenti anomalie, incidenti di sicurezza e vulnerabilità.		
Responsabile Sicurezza dei sistemi per la conservazione	Massimo Perillo (MPE)	Assicura l'efficacia e l'efficienza: ● della qualità aziendale, e verificare la corretta esecuzione dei processi sottoposti a certificazione; ● del sistema di sicurezza nel senso più ampio del termine: sicurezza dei lavoratori, sicurezza informatica, sicurezza nell'accesso ai locali aziendali, adottando in particolare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3/12/2013.	Dal 1° febbraio 2009	

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo	Eventuali Deleghe
		In particolare svolge le seguenti funzioni: ● rispetta e monitora i requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; ● segnala le eventuali difformità al Responsabile del servizio di conservazione e individuando e pianificando le necessarie azioni correttive.		
Responsabile trattamento dati personali (Privacy)	Massimo Perillo (MPE)	Assicura l'efficacia e l'efficienza: ● del trattamento dei dati personali in ottemperanza al Dlgs. 30 giugno 2003, n. 196. In particolare svolge le seguenti funzioni: ● Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; ● garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.	Dal 1° febbraio 2009	

5.3.1 Cronologia dei Responsabili

Responsabile del servizio di conservazione

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Filippo Ciaravella	*Responsabile del Servizio di Conservazione*	01/10/2015	Sino a Revoca

Responsabile dei sistemi informativi per la conservazione

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Francesco Bianco	*Responsabile sistemi informativi per la conservazione*	01/10/2015	Recesso del 27/04/2018 per motivi personali
Nicola Incandela	*Responsabile sistemi informativi per la conservazione*	30/04/2018	Sino a Revoca

Responsabile della funzione archivistica di conservazione

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Antonio Ferraro	*Responsabile funzione Archivistica di conservazione*	01/10/2015	Sino a Revoca

Responsabile sviluppo e manutenzione del sistema di conservazione

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Nicola Incandela	*Responsabile sviluppo e manutenzione del sistema di conservazione*	01/10/2015	Sino a Revoca

Responsabile della sicurezza dei sistemi per la conservazione

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Massimo Perillo	*Responsabile Sicurezza dei sistemi per la*	01/10/2015	Recesso del 31/10/2017 per motivi

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
	conservazione		personali
Letizia Ciuro	*Responsabile Sicurezza dei sistemi per la conservazione*	02/11/2017	Recesso del 06/04/2018 per motivi personali
Massimo Perillo	*Responsabile Sicurezza dei sistemi per la conservazione*	09/04/2018	Sino a Revoca

Responsabile del trattamento dei dati personali

Nome e Cognome	Funzione	Data Nomina	Data Revoca/Recesso
Massimo Perillo	*Responsabile trattamento dati personali (Privacy)*	01/10/2015	Recesso del 31/10/2017 per motivi personali
Letizia Ciuro	*Responsabile trattamento dati personali (Privacy)*	02/11/2017	Recesso del 06/04/2018 per motivi personali
Massimo Perillo	*Responsabile trattamento dati personali (Privacy)*	09/04/2018	Sino a Revoca

5.4 Utente finale

L'Utente finale è una persona o una procedura software che ha la possibilità di accedere al sistema di conservazione dei documenti informatici al fine di fruire delle informazioni di interesse conservate al suo interno nei limiti previsti dalle norme vigenti.

Il ruolo dell'Utente si può identificare in relazione a specifici soggetti abilitati, indicati dal Soggetto Produttore stesso, che possono accedere ai documenti conservati o a parte di essi, secondo le politiche di accesso concordate.

Infine si segnala che l'abilitazione e l'autenticazione di tutti i soggetti e gli operatori avviene in base alle procedure di gestione utenze indicate nel Piano della sicurezza del sistema di conservazione, e nel rispetto delle misure di sicurezza previste negli artt. da 31 a 36 del D.Lgs. 30 giugno 2003, n. 196, in particolare di quelle indicate all'art. 34 comma 1 e dal Disciplinare tecnico in materia di misure minime di sicurezza di cui all'Allegato B del medesimo Decreto.

5.5 Mansionario

La tabella che segue riporta la definizione dei ruoli e mansioni previsti nell'ambito delle funzionalità del sistema di conservazione (si tratta della definizione dei diversi livelli di accesso alle informazioni sia per il personale interno al Conservatore che al personale esterno del Cliente o di terze parti), ovvero riporta i ruoli configurati per l'accesso alle funzionalità del sistema di conservazione (**politiche di gestione degli accessi alle informazioni**):

Ruolo	Organizzazione di appartenenza	Descrizione	Accesso ai Log	Note
Amministratore di Sistema	Conservatore (Arancia ICT Srl)	Ha accesso a tutte le configurazioni del Sistema Ha accesso ai log di sistema (log degli accessi, log delle operazioni).	Si (sola lettura)	Non può operare come operatore di basso livello sul sistema
Responsabile del servizio di Conservazione	Conservatore (Arancia ICT Srl)	A questo ruolo è demandata tutta l'operatività del sistema di conservazione ovvero: verifica e presa in carico dei PdV, emissione RdV positivi o negativi, creazione dei PdA e firma digitale e marca temporale dell'IdC, etc... Può delegare tutta o parte dell'operatività del sistema ad altri utenti con ruolo 'Operatore'.	No	Non ha accesso alle configurazioni del sistema, ovvero non ha privilegi amministrativi
Operatore	Conservatore (Arancia ICT Srl)	A questo ruolo è demandata tutta l'operatività del sistema di conservazione ovvero: verifica e presa in carico dei PdV, emissione RdV positivi o negativi, creazione dei PdA e firma digitale e marca temporale dell'IdC, etc...	No	Non ha accesso alle configurazioni del sistema, ovvero non ha privilegi amministrativi
Soggetto Produttore (Proprietario delle Informazioni)	Soggetto Produttore/Resp. della Conservazione/Referenti (Cliente)	È il titolare (proprietario) delle unità documentarie informatiche poste in conservazione: è colui che effettua i versamenti dei documenti da conservare. Ha permessi in sola lettura e accesso alla sezione di distribuzione dei documenti conservati di sua proprietà,	No	

Ruolo	Organizzazione di appartenenza	Descrizione	Accesso ai Log	Note
		ovvero da lui versati: richiesta emissione PdD e Copia Archivi.		
Auditor	Soggetti terzi esterni	Ha piena e globale visibilità su tutti i contenuti: documenti e funzioni (come l'Operatore ma con permessi di sola lettura). Ha accesso ai log di sistema.	Si (sola lettura)	
Terza Parte (Vigilanza)	Soggetti terzi esterni	Ha accesso con visibilità globale alla sezione di distribuzione dei documenti per la visualizzazione di tutti i documenti conservati (richiesta emissione PdD e Copia Archivi)	No	Autorità preposte alla vigilanza con permessi congruenti alle necessità di accesso

Solo al personale che è autorizzato per l'accesso ai log, ovvero con Ruolo "Amministratore" e "Auditor" sulla piattaforma di conservazione, vengono consegnate anche le credenziali (username e password) per l'accesso in sola lettura a tutti i file di log prodotti dal sistema di conservazione.

5.5.1 Procedura di revisione periodica delle politiche di controllo degli accessi

Il personale di Arancia ICT preposto alla gestione e amministrazione del sistema di Conservazione, opera una revisione dei ruoli e dei permessi associati a seguito di modifiche sostanziali al sistema e comunque con periodicità di 1 anno assicurandosi che gli stessi siano coerenti e conformi con la versione software del sistema in uso.

Tali verifiche vengono effettuate al fine di:

- verificare la persistenza delle attuali necessità;
- rilevare eventuali anomalie e problematiche;
- rilevare eventi relativi a utilizzi impropri dei diritti di accesso;
- rilevare se i ruoli risultano ancora corretti a seguito di modifiche al sistema;
- prevedere eventuali azioni correttive alle politiche di controllo degli accessi alle informazioni

A valle delle verifiche sopra elencate, viene prodotto apposito verbale di revisione periodica dei diritti di accesso.

Per ulteriori dettagli fare riferimento alle Procedure Operative "*ARA_PO 7.1.2* ***Gestione del personale***" e "*ARA_PO 7.1.2.1* ***Gestione credenziali accessi a CNP***" del SGI a norma UNI CEI ISO/IEC 27001:2014.

Torna al Sommario

6 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

6.1 Organigramma

La figura che segue riporta le strutture organizzative coinvolte nel servizio di conservazione, ovvero l'organigramma di Arancia-ICT con evidenza delle strutture aziendali e dei ruoli preposti al Servizio di Conservazione Digitale di Arancia-ICT, le cui descrizioni sono riportate nel paragrafo successivo.

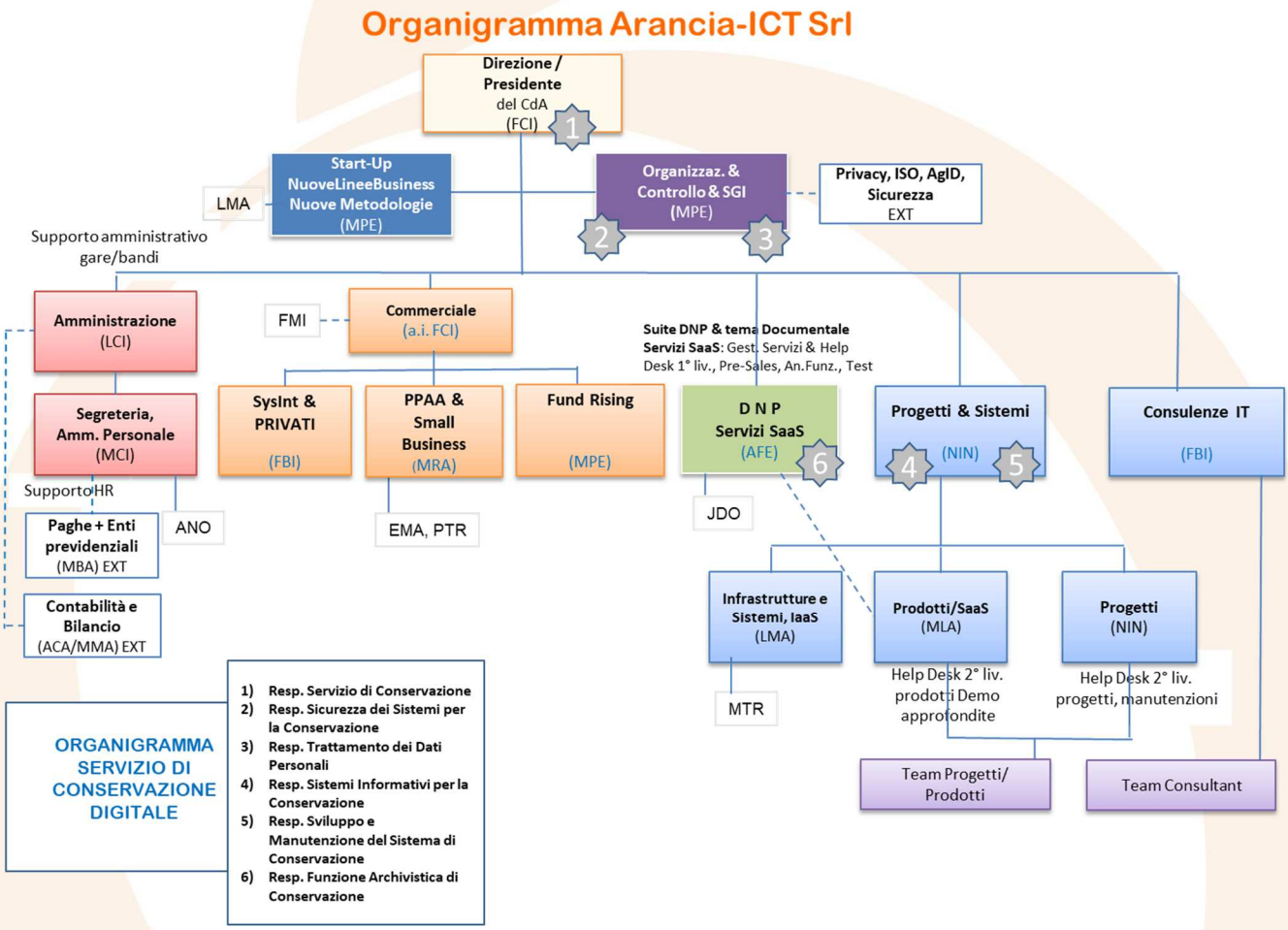

Figura 1 – Organigramma

Torna al Sommario

6.2 Strutture organizzative del Servizio di Conservazione

Di seguito si riportano le descrizioni sintetiche per ciascuna struttura organizzativa coinvolta nel servizio di conservazione:

Direzione/Presidente del CdA: È responsabile della definizione e dell'applicazione delle politiche aziendali

Organizzazione e Controllo / Sistema di Gestione Integrato – SGI (ISO/Qualità/SGQ, Privacy, Sicurezza): Ha lo scopo di definire di concerto con la Direzione la politica per assicurare l'efficacia e l'efficienza:

- della qualità aziendale, e verificare la corretta esecuzione dei processi sottoposti a certificazione;
- del trattamento dei dati personali in ottemperanza al Dlgs. 30 giugno 2003, n. 196;
- del sistema di sicurezza nel senso più ampio del termine: sicurezza dei lavoratori, sicurezza informatica, sicurezza nell'accesso ai locali aziendali;

DNP/Servizi SaaS: è preposta alle seguenti attività:

- gestione servizi e assistenza clienti/help-desk di 1° livello, verifica del rispetto dei livelli di servizio, interazione e verifica della soddisfazione della clientela, verifica e supporto dell'operato dei clienti attraverso la piattaforma informatica di erogazione dei vari servizi della suite *DNP - Digitale No Problem* verso i clienti (tra cui il servizio di conservazione oggetto del presente documento);
- Analisi funzionale e Test sui prodotti facenti parte della piattaforma *DNP – Digitale No Problem* (tra cui il servizio di conservazione oggetto del presente documento);
- Pre-sales e supporto ai commerciali riguardo le tematiche legate ai prodotti della suite *DNP – Digitale No Problem*.

Progetti e Sistemi: è preposta alla progettazione, realizzazione ed esercizio dei sistemi informativi aziendali, e dei sistemi informatici per l'erogazione dei vari servizi verso i clienti (tra cui il servizio di conservazione oggetto del presente documento);

Infrastrutture e Sistemi/IaaS: è preposta allo sviluppo, manutenzione ed esercizio del sistema informatico per l'erogazione dei vari servizi verso i clienti (tra cui il servizio di conservazione oggetto del presente documento);

Prodotti/SaaS: è preposta alla progettazione e implementazione dei vari prodotti informatici in base ai requisiti specifici dei clienti (tra cui il servizio di conservazione oggetto del presente documento).

Nel processo di conservazione digitale intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità. La tabella seguente individua per ciascuna attività e responsabilità che intervengono nelle principali funzioni che riguardano il servizio di conservazione, le strutture organizzative e i ruoli coinvolti:

Strutture e Ruoli	Direzione	Organizzazione e Controllo / SGI		DNP / Servizi SaaS		Progetti e Sistemi	Progetti e Sistemi	Infrastrutture e Sistemi /IaaS
	Responsabile del Servizio di Conservazione Filippo Ciaravella (FCI)	**Responsabile Sicurezza dei Sistemi per la Conservazione** Massimo Perillo (MPE)	**Responsabile trattamento Dati Personali** Massimo Perillo (MPE)	**Responsabile Servizio Clienti** Antonio Ferraro (AFE)	**Responsabile funzione Archivistica di Conservazione** Antonio Ferraro (AFE)	**Responsabile Sistemi informativi per la Conservazione** Nicola Incandela (NIN)	**Responsabile Sviluppo e Manutenzione del Sistema di Conservazione** Nicola Incandela (NIN)	**Amministratore del Sistema di Conservazione** Manfredi Trizzino (MTR)
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)				X				
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico				X				
Generazione del rapporto di versamento	X							
Preparazione e gestione del Pacchetto di archiviazione	X							
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	X			X				
Scarto dei pacchetti di archiviazione				X				
Chiusura del servizio di conservazione (al termine di un contratto)				X				
Conduzione e manutenzione del sistema di conservazione						X	X	X
Monitoraggio del sistema di conservazione				X		X	X	X
Change management				X		X	X	
Verifica periodica di conformità a normativa e standard di riferimento	X	X				X		

Strutture e Ruoli	Direzione	Organizzazione e Controllo / SGI		DNP / Servizi SaaS		Progetti e Sistemi	Progetti e Sistemi	Infrastrutture e Sistemi /IaaS
Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali			X					
Definizione del set di metadati di conservazione e di fascicoli					X			
Aggiornamento del manuale di conservazione	X				X	X		
Definizione delle modalità di trasferimento da parte dell'ente produttore, descrizione archivistica dei documenti e delle aggregazioni documentali					X			

Torna al Sommario

7 OGGETTI SOTTOPOSTI A CONSERVAZIONE

7.1 Oggetti conservati

Il Servizio ***Conservazione No Problem*** offre ai propri Clienti il trattamento di diverse tipologie di documenti da sottoporre a conservazione, in particolare conserva documenti informatici, di natura fiscale, amministrativa e sanitaria, con i metadati ad essi associati e le loro aggregazioni documentali informatiche (aggregazioni), che includono i fascicoli informatici (fascicoli).

Le tipologie di documenti che caratterizzano gli oggetti digitali da versare nel sistema di conservazione sono definite attraverso le attività di analisi e di classificazione documentale nella fase di prevendita ed attivazione del servizio e sono riportate nel documento allegato "Specificità del Contratto". La descrizione delle tipologie documentali, con l'indicazione della loro natura, dei formati, dei metadati obbligatori e dei metadati opzionali, delle regole e della durata di conservazione (piano di conservazione e successivo scarto) sono riportate nel dettaglio in APPENDICE 10 (al paragrafo 10.1 – Elenco tipologie di documenti sottoposti a conservazione, al paragrafo 10.2 – Descrizione categorie/tipologie documentali e metadati associati e al paragrafo 10.3 – Descrizione politiche di conservazione).

Torna al Sommario

7.2 Pacchetto di versamento

Il Pacchetto di Versamento (PdV) viene creato a cura del Soggetto Produttore e trasmesso da quest'ultimo al sistema di conservazione (server) in modo diverso a seconda delle specifiche di contratto (tali modalità sono eventualmente descritte all'interno del documento allegato 'Specificità del Contratto'). In particolare sono previste le modalità di conferimento seguenti:

- Interfaccia applicazione SICWeb /HTTPs – CNP Client (con modalità di comunicazione sFTP sincrono con il server di conservazione – CNP Server, ad esempio per il collegamento automatico del server di conservazione con sistemi informativi interni di Arancia-ICT: *FNP – FatturaNoProblem* e *PNP – ProtocolloNoProblem*)
- sFTP polling asincrono (per collegamento automatico del server di conservazione con sistemi informativi terzi)
- Web-Service /HTTPs (per collegamento automatico del server di conservazione con sistemi informativi terzi)

Si segnala che il *Responsabile del Servizio di Conservazione* (Soggetto Conservatore), non si assume nessuna responsabilità in merito al contenuto dei documenti inviati in conservazione dal Soggetto Produttore. I contenuti del pacchetto di versamento devono infatti essere sottoposti a verifica da parte del soggetto produttore prima dell'invio al sistema di conservazione, quest'ultimo ha la piena responsabilità in merito al contenuto dei documenti inviati in conservazione.

Si individuano tre macro modalità di creazione e trasmissione del PdV in base alla tipologia documentale:

- Fattura Elettronica PA con relative Ricevute (gestione tramite procedure integrate);
- Documenti Amministrativi protocollati/non protocollati (gestione tramite procedure integrate);
- Altre Tipologie di documenti.

In generale il PdV è costituito da una entità logica informativa contenente:

- **i documenti/oggetti da conservare**, eventualmente firmati digitalmente (nello standard di firma CAdES ".p7m" ovvero nello standard PAdES ovvero XAdES) o eventualmente marcati temporalmente (nello standard di validazione temporale CAdES-T ovvero nello standard PAdES-T ovvero XAdES-T);
- **un file Indice IPdV** (**Indice o file di chiusura del Pacchetto di Versamento**) in formato XML, finalizzato alla descrizione dell'oggetto della conservazione e che secondo lo standard ISO 14721:2012 OAIS permette di identificare il produttore, di contenere i dati descrittivi ed informativi sull'impacchettamento ed i dati descrittivi e di rappresentazione (metadati) di ciascun documento contenuto nel pacchetto.

Torna al Sommario

7.2.1 Fattura Elettronica PA con relative Ricevute gestita da procedure integrate sincrone

Il PdV viene conferito attraverso un "*canale sicuro*" implementato tramite collegamento automatico con un sistema di fatturazione elettronica PA, quale ad esempio *FNP-FatturaNoProblem* fornito da

Arancia-ICT (applicazione WEB che funge da CNP Client), o altri sistemi di proprietà del cliente/soggetto produttore per i quali è stata realizzata apposita interfaccia informatica sincrona di collegamento (la comunicazione tra il CNP Client e il server di conservazione CNP Server avviene in questo caso con modalità sFTP sincrono).

Il Soggetto Produttore, in questo caso, è un intermediario cui è stata delegata la funzione di emissione della fattura elettronica, e che gestisce tale sistema memorizzando fatture e ricevute relative all'anno corrente sul proprio sistema. Al termine dell'anno fiscale, in base alla politica di conservazione di cui al paragrafo 10.3 - Descrizione politiche di conservazione, attraverso apposita funzione/procedura informatica automatica schedulata trasmette al sistema di conservazione il PdV costituito dall'insieme delle fatture (in formato xml firmate digitalmente) e dall'insieme delle ricevute (in formato xml) di ogni soggetto cedente/prestatore di beni/servizi.

Nel dettaglio la piattaforma informatica di conservazione produce automaticamente una struttura dati in formato XML (il cosiddetto 'file di chiusura' o 'evidenza informatica' o 'indice' del PdV) che contiene le seguenti informazioni:

- identificativo univoco del PdV;
- data e ora di creazione del PdV;
- autore del PdV (soggetto produttore del PdV);
- identificazione applicativo che ha prodotto il PdV (CNPClient);
- tipologia documentale e metadati associati a ciascun documento (di tipologia Fattura Elettronica PA e relativa Ricevuta) mandato in conservazione (in questo caso i metadati associati a ciascuna fattura elettronica PA o ricevuta da conservare vengono acquisiti ed estratti in automatico direttamente dallo specifico file xml gestito dal sistema di fatturazione sorgente);
- hash/impronta associata a ciascun documento (di tipologia Fattura Elettronica PA e relativa Ricevuta) mandato in conservazione.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato specifico di ciascun contratto ('Specificità del Contratto').

Torna al Sommario

7.2.2 Documento Amministrativo protocollato/non protocollato gestito da procedure integrate sincrone

Il PdV viene conferito attraverso un "*canale sicuro*" implementato tramite collegamento automatico con il sistema di gestione documentale/protocollo informatico, *PNP-ProtocolloNoProblem* fornito da Arancia-ICT (applicazione WEB che funge da CNP Client), o altri sistemi documentali/di protocollo di proprietà del cliente/soggetto produttore per i quali è stata realizzata apposita interfaccia informatica sincrona di collegamento (la comunicazione tra il CNP Client e il server di conservazione CNP Server avviene in questo caso con modalità sFTP sincrono).

Il Soggetto Produttore, in questo caso, è il fruitore del sistema di gestione documentale/protocollo e in base alla politica di conservazione di cui al paragrafo 10.3 - Descrizione politiche di conservazione, attraverso apposite funzioni/procedure informatiche automatiche schedulate o attraverso funzione manuale trasmette al sistema di conservazione i PdV costituiti dall'insieme dei

documenti da conservare organizzati secondo criteri prestabiliti (ad esempio per tipologia documentale).

Nel dettaglio la piattaforma informatica di conservazione produce automaticamente una struttura dati in formato XML (il cosiddetto 'file di chiusura' o 'evidenza informatica' o 'indice' del PdV) che contiene le seguenti informazioni:

- identificativo univoco del PdV;
- data e ora di creazione del PdV;
- autore del PdV (soggetto produttore del PdV);
- identificazione applicativo che ha prodotto il PdV (CNPClient);
- tipologia documentale e metadati associati a ciascun documento mandato in conservazione (in questo caso i metadati associati a ciascun documento da conservare vengono acquisiti ed estratti in automatico direttamente dal sistema documentale/di protocollo sorgente);
- hash/impronta associata a ciascun documento mandato in conservazione.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato specifico di ciascun contratto ("Specificità del Contratto").

Torna al Sommario

7.2.3 Altre Tipologie di Documenti

Le "altre Tipologie di Documenti" sono rappresentate da tutte le tipologie documentali seguenti che possono provenire anche da sistemi terzi (scenario di conferimento per il quale non è stata implementata una interfaccia sincrona di collegamento tra i sistemi del soggetto produttore e il server di conservazione):

- Documento analitico emesso/ricevuto in riferimento ad una transazione (fatture emesse/ricevute, DDT, etc.);
- Documento analogico riepilogativo (libri contabili, registri, dichiarativi, etc.);
- Documento amministrativo;
- Documento sanitario.

Salvo quanto previsto dai contratti specifici, il PdV viene creato a cura del Soggetto Produttore[1] e viene conferito al server di conservazione attraverso le varie modalità previste (vedi paragrafo 7.2 - Pacchetto di versamento).

Di seguito vengono esplicitati i semplici passaggi eseguiti sulla piattaforma informatica web (applicazione SICWeb/HTTPs che funge da CNP Client) che Arancia-ICT mette a disposizione dei propri clienti su richiesta – quelli per i quali non è stata realizzata alcuna interfaccia di collegamento

[1] Si segnala che il *Responsabile del Servizio di Conservazione* (Soggetto Conservatore), non si assume nessuna responsabilità in merito al contenuto dei documenti inviati in conservazione dal Soggetto Produttore. I contenuti del pacchetto di versamento devono infatti essere sottoposti a verifica da parte del soggetto produttore prima dell'invio al sistema di conservazione, quest'ultimo ha la piena responsabilità in merito al contenuto dei documenti inviati in conservazione.

con i propri sistemi (la modalità di comunicazione con il server di conservazione è in questo caso sempre sFTP sincrono):

1. Fase di conferimento:

- **Upload del documento informatico** da sottoporre a conservazione, nel formato file specifico per ogni tipologia di documento (v. paragrafo 10.1 - Elenco tipologie di documenti sottoposti a conservazione);
- **Inserimento dei metadati specifici per tipo documento** (v. paragrafo 10.1 - Elenco tipologie di documenti sottoposti a conservazione). In questo caso la fase di acquisizione dei metadati è a cura del soggetto produttore, che in base alla Categorie documentale e alla Tipologia documentale prescelta procede all'inserimento e alla valorizzazione dei metadati specifici per il singolo documento. (Vi è anche la possibilità di procedere con una acquisizione massiva dei documenti e dei relativi metadati tramite upload di un archivio .zip contenente i documenti da conservare e una distinta in formato .csv dove sono riportati i metadati per ciascun documento).

Questa fase è iterativa e può protrarsi man mano nel tempo.

2. Fase di avvio in conservazione:

Creazione del PdV attraverso selezione singola/multipla dei documenti precedentemente caricati.

A fronte della creazione del Pacchetto di Versamento (PdV) da parte del Soggetto Produttore, la piattaforma informatica di conservazione produce automaticamente una struttura dati in formato XML (il cosiddetto 'file di chiusura' o 'evidenza informatica' o 'indice' del PdV) che contiene le seguenti informazioni:

- identificativo univoco del PdV;

- data e ora di creazione del PdV;

- autore del PdV (soggetto produttore del PdV);

- identificazione applicativo che ha prodotto il PdV (CNPClient);

- tipologia documentale e metadati associati a ciascun documento mandato in conservazione (per quanto riguarda le modalità di acquisizione dei metadati vedi sopra "**Inserimento dei metadati specifici per tipo documento**");

- hash/impronta associata a ciascun documento mandato in conservazione.

Le eventuali personalizzazioni di tali pacchetti, specifiche di un contratto, sono descritte nell'allegato specifico di ciascun contratto ('Specificità del Contratto').

Infine si segnala che per queste tipologie di documenti il PdV può essere conferito attraverso collegamento automatico con i sistemi informativi esterni del cliente soggetto/produttore (sistema gestionale, sistema documentale, sistemi di protocollo informatico) per i quali è stata realizzata

apposita interfaccia informatica asincrona di collegamento tramite la modalità sFTP polling asincronica o la modalità Web-Service/HTTPs.

Torna al Sommario

7.3 Pacchetto di archiviazione

Il pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema CNP è composto a partire da uno o più Pacchetti di Versamento accettati dal SIC (ovvero che sono stati correttamente ricevuti, presi in carico ed elaborati dal SIC) secondo le modalità riportate nel presente Manuale di Conservazione. La funzione di produzione di un PdA a partire da uno o più PdV accettati è una procedura automatica gestita dal SIC che non prevede alcuna interazione da parte di un operatore, ovvero nessun operatore è in grado di modificare il contenuto informativo del PdA.

Un Pacchetto di Archiviazione (PdA) è un contenitore informativo che contiene:

- **gli oggetti informativi individuati per la conservazione** (quindi i documenti, i fascicoli elettronici o le aggregazioni documentali sottoposti al processo di conservazione a lungo termine);
- **un Indice del Pacchetto di Archiviazione (IPdA)** in formato XML che rappresenta le Informazioni sulla Conservazione.

Il Pacchetto di Archiviazione (PdA), o meglio l'Indice di Conservazione (IPdA o IdC) del PdA viene realizzato in conformità al formato definito nello standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010 che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione), e nell'allegato 4 delle Regole tecniche in materia di sistema di conservazione contenute nel DPCM 3 dicembre 2013, che prevedono l'utilizzo dello schema XML la cui struttura è di seguito riportata:

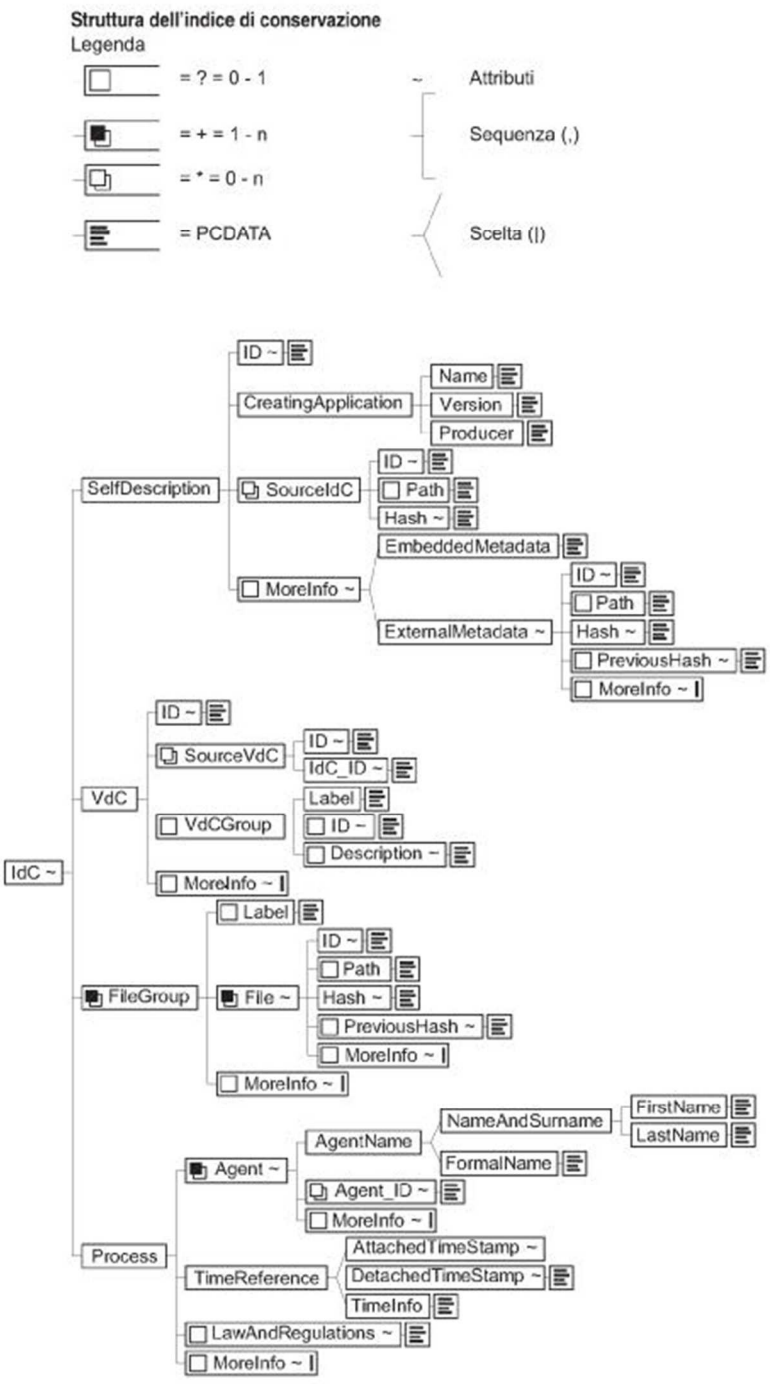

Figura 2 - Struttura dell'Indice di Conservazione (IPdA)

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche, in cui è riportata nel dettaglio la struttura dati prevista.

Su ciascun IPdA viene apposta una marca temporale e la firma digitale del Responsabile del Servizio di Conservazione.

Per quanto riguarda gli elementi *MoreInfo* presenti nella struttura dell'IdC, si segnala che verrà utilizzato l'elemento *MoreInfo* definito a livello di *FileGroup* (che contiene i sotto-elementi *File* da conservare), in modo da consentire di introdurre l'insieme di metadati (specifici per categoria e tipologia documentale e definiti dall'utilizzatore) relativi a tutti i file che costituiscono il *FileGroup*, ovvero relativi alla tipologia documentale dei file contenuti nel PdA e che sono oggetto della conservazione.

Questo elemento sarà valorizzato nella modalità '*ExternalMetadata*', ovvero questi metadati verranno strutturati nel formato XML, utilizzando uno schema XML – xsd – che ne definisce la struttura e la cui localizzazione viene specificata nell'attributo *XMLScheme* dell'elemento; l'insieme di queste informazioni costituisce un corpo che viene inserito all'esterno dell'IdC e specificato nel sub-elemento '*ExtrernalMatedata*' con attributi *encoding* per le informazioni relative al tipo di codifica, *extention* per indicare l'estensione del file e *format* per fornire informazioni sulla struttura dati. In questo caso quindi l'insieme dei metadati cosi definiti individua concretamente un file xml esterno all'IdC (sarebbe lo Schema XML – xsd - istanziato) ma che comunque rimane interno al PdA. Infine l'elemento ExternalMetadata così definito avrà un sotto-elemento ID obbligatorio (che contiene l'identificativo univoco), un sotto-elemento Hash obbligatorio che contiene l'impronta del file esterno xml e un sotto-elemento Path facoltativo che contiene la localizzazione del file xml.

Il contenuto informativo del file xml esterno che contiene i metadati per ciascun documento specifici della tipologia documentale associata al FileGroup, potrà essere di volta in volta definito nel dettaglio in fase contrattuale col Cliente/Produttore: ovvero i contenuti specifici degli elementi "moreinfo" potranno essere esplicitati e descritti nel dettaglio nell'allegato "Specificità del Contratto".

Di seguito si riporta un esempio di struttura dell'elemento FileGroup a titolo esplicativo:

- **FileGroup** (1-n): la tipologia documentale
  - **Label**: Nome della tipologia documentale
  - **File** (1-n): Definizione del file comprensiva di codifica, estensione e formato (MimeType)
    - **ID**: Id del documento (univoco all'interno della tipologia documentale definita per l'azienda)
    - **Path**: Indirizzo logico del file rappresentato da un URI (individua il file all'interno dello storage)
    - **Hash**: Funzione di hash utilizzata e valore restituito dalla funzione applicandola al file oggetto della Conservazione
    - **MoreInfo**: eventuali Metadati Integrati e specifici a livello singolo File
  - **MoreInfo** • eventuali Metadati Integrati a livello di Tipologia documentale (FileGroup) comuni a tutti i File della stessa tipologia

Di seguito un esempio di un estratto del file xml dell'IdC (per quanto riguarda sempre l'elemento FileGroup):

```
<sincro:FileGroup>
  <sincro:Label>XXXX </sincro:Label>
  <sincro:File>
  ...
  </sincro:File>
  <sincro:File>
  ...
  </sincro:File>
  <sincro:File>
  ...
  </sincro:File>
  ...
  <sincro:MoreInfo sincro:XMLScheme="../moreinfo.xsd">
    <sincro:ExternalMetadata         sincro:format="application/xml"         sincro:extention=".xml"
sincro:encoding="binary">
      <sincro:ID>XXXX</sincro:ID>
      <sincro:Path>../XXXX.xml</sincro:Path>
      <sincro:Hash sincro:function="SHA-256">XXXXXXXXXXXXXXXXXXXXXX</sincro:Hash>
    </sincro:ExternalMetadata>
  </sincro:MoreInfo>

</sincro:FileGroup>
```

Di seguito si riporta lo schema xsd della sezione MoreInfo (*moreinfo.xsd*):

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

        <!-- Versamento -->
        <xs:element name="Versamento" type="VersamentoType" />
        <xs:complexType name="VersamentoType">
                <xs:choice>
                        <xs:sequence>
                                <xs:element name="Documenti" type="DocumentiType" />
                                <xs:element name="Fascicoli" type="FascicoliType" minOccurs="0" />
                        </xs:sequence>
                        <xs:sequence>
                                <xs:element name="Fascicoli" type="FascicoliType" />
                        </xs:sequence>
                </xs:choice>
        </xs:complexType>

        <xs:complexType name="DocumentiType">
                <xs:sequence>
                        <xs:element name="Documento" type="DocumentoType" maxOccurs="unbounded" />
                </xs:sequence>
        </xs:complexType>

        <xs:complexType name="DocumentoType">
                <xs:annotation>
                        <xs:documentation>
                                Definizione tipo documento: utilizzato per i
                                documenti di rilevanza fiscale
                        </xs:documentation>
                </xs:annotation>
                <xs:sequence>
                        <xs:element name="Path" type="xs:string" />
                        <xs:element name="Categoria" type="NonBlankString100Type" minOccurs="0" />
                        <xs:element name="TipoDocumento" type="NonBlankString100Type" minOccurs="0" />
```

```
                <xs:element name="Metadati" type="MetadatiType" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="idDocumento" type="xs:string" use="required" />
</xs:complexType>

        <!-- fascicoli contenuti nel PdV -->
<xs:complexType name="FascicoliType">
        <xs:annotation>
                <xs:documentation>
                        Contenitore di tipi FascicoloType
                </xs:documentation>
        </xs:annotation>
        <xs:sequence>
                <xs:element name="Fascicolo" type="FascicoloType" maxOccurs="unbounded" />
        </xs:sequence>
</xs:complexType>

<xs:complexType name="FascicoloType">
        <xs:annotation>
                <xs:documentation>
                        Definizione tipo Fascicolo: utilizzato per definire fascicoli
                        di documenti
                </xs:documentation>
        </xs:annotation>
        <xs:sequence>
                <xs:element name="Categoria" type="NonBlankString100Type" minOccurs="0" />
                <xs:element name="TipoFascicolo" type="NonBlankString100Type" minOccurs="0" />
                <xs:element name="Metadati" type="MetadatiType" minOccurs="0" />
                <xs:element name="Documenti" type="DocumentiType" />
        </xs:sequence>
        <xs:attribute name="idFascicolo" type="xs:string" use="required" />
</xs:complexType>

<!-- METADATI -->

<xs:complexType name="MetadatiType">
        <xs:sequence>
                <xs:element name="Metadato" type="MetadatoType" maxOccurs="unbounded"/>
        </xs:sequence>
</xs:complexType>

<xs:complexType name="MetadatoType">
        <xs:simpleContent>
                <xs:extension base="NonBlankStringSupplementType">
                        <xs:attribute name="id" type="MetadatoIdType" use="required" />
                </xs:extension>
        </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="MetadatoIdType">
        <xs:restriction base="xs:normalizedString">
                <xs:pattern value="[A-Z][A-Z0-9_]{0,99}" />
        </xs:restriction>
</xs:simpleType>

<!-- TIPI STRINGA -->

<xs:simpleType name="NonBlankStringType">
        <xs:restriction base="xs:normalizedString">
                <xs:pattern value="(\p{IsBasicLatin})+" />
        </xs:restriction>
</xs:simpleType>

<!-- tipi stringa supplement -->
```

```
        <xs:simpleType name="NonBlankStringSupplementType">
                <xs:restriction base="xs:normalizedString">
                        <xs:pattern value="([\p{IsBasicLatin}\p{IsLatin-1Supplement}])+" />
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="NonBlankString100Type">
                <xs:restriction base="NonBlankStringType">
                        <xs:maxLength value="100" />
                </xs:restriction>
        </xs:simpleType>

        <xs:simpleType name="NonBlankString255Type">
                <xs:restriction base="NonBlankStringType">
                        <xs:maxLength value="255" />
                </xs:restriction>
        </xs:simpleType>

</xs:schema>
```

Per maggiore chiarezza e completezza viene descritta la modalità di creazione dell'xml relativo all'IdC, ovvero il modo in cui verrà operativamente istanziato l'xsd della norma SInCRO secondo le specifiche esigenze del contesto riferito al servizio CNP di Arancia ICT.

L'elemento padre dell'xml ***IdC*** (con attributi ***url*** per localizzare lo schema xsd di riferimento dello standard SInCRO utilizzato poi per la validazione dell'xml e ***version*** per indicare l'attuale versione dello standard SInCRO) viene popolato con le seguenti strutture:

- ***SelfDescription*** relativa all'indice del pacchetto di archiviazione che si compone di:
  - un identificatore univoco (***ID***) dell'IPdA (alfanumerico) con un attributo ***scheme***,
  - il riferimento all'applicazione che l'ha creato (***CreatingApplication***), che si compone di:
    - ***Name***, ***Version*** e ***Producer*** (Stringhe)
  - eventuali riferimenti ad altri IdC (uno o più di uno) da cui deriva il presente (***SourceIdC***), se il PdA è stato creato a partire da uno esistente o da più esistenti, che si compone di:
    - ***ID*** alfanumerico dell'IdC originario con un attributo ***scheme***, eventuale ***Path*** (percorso relativo URI rispetto all'xml dell'IdC Corrente relativo alla localizzazione dell'IdC originario) ed ***Hash*** del IdC originario con attributi ***canonicalXML*** e ***function*** per identificare la funzione di hash utilizzata;

- ***VdC*** relativa al PdA stesso che si compone di:
  - un identificatore univoco (***ID***) del PdA stesso (alfanumerico) con un attributo ***scheme***,
  - eventuali riferimenti ad altri PdA (uno o più di uno) da cui deriva il presente (***SourceVdC***), se il PdA è stato creato a partire da uno esistente o da più esistenti, che si compone di:
    - ***ID*** alfanumerico del PdA originario con un attributo ***scheme*** e ***IdC_ID*** ovvero l'Identificativo dell'IdC associato al PdA originario con un attributo ***scheme*** (il valore deve essere uguale all'elemento ID contenuto nell'elemento SourceIdC associato – vedi sopra)

- informazioni relative a una eventuale tipologia/aggregazione (di natura logica o fisica) cui il PdA appartiene (***VdCGroup***), che si compone di:
    - ***Label*** (una etichetta/descrizione di tipo stringa ad es: "Fatture elettroniche PA di <Nome Azienda>") ed eventuali ***ID*** alfanumerico con un attributo ***scheme*** e ***Description*** stringa con un attributo ***language***;

– un singolo elemento ***FileGroup*** relativo a un raggruppamento di uno o più file da conservare che sono contenuti nel PdA (come detto sopra nel contesto specifico di CNP ci sarà solamente un elemento FileGroup dato che il PdA sarà sempre relativo ad una unica tipologia documentale) che si compone di:

- Una eventuale ***Label*** (una etichetta/descrizione di tipo stringa)
- Uno o più elementi ***File*** da conservare, con attributi ***encoding*** per le informazioni relative al tipo di codifica, ***extention*** per indicare l'estensione del file e ***format*** per fornire informazioni sulla struttura dati, che si compone di:
    - l'identificativo univoco ***ID*** del file (alfanumerico) con un attributo ***scheme***
    - un eventuale ***Path*** (viene valorizzato con il percorso relativo – URI - del file sul filesystem rispetto all'xml dell'IdC
    - l'impronta attuale dello stesso, ovvero l'***Hash***, ottenuta con l'applicazione di un algoritmo di hash, con attributi ***canonicalXML*** e ***function*** per identificare la funzione di hash utilizzata
    - un'eventuale impronta precedentemente associata ad esso ***PreviousHash*** con attributi ***canonicalXML*** , ***function*** per identificare la funzione di hash utilizzata e ***relatedIdC*** per identificare l'IdC associato alla precedente impronta: in questo modo è possibile ad esempio gestire il passaggio da un algoritmo di hash diventato non più sicuro ad uno più robusto;
- un eventuale elemento "***MoreInfo***" che consente di introdurre metadati definiti dall'utilizzatore relativi a tutti i file che costituiscono il FileGroup, ovvero relativi alla tipologia documentale dei file oggetto della conservazione (sarebbero i metadati 'minimi' definiti nell'allegato 5 del DPCM del 3/12/2013 più altri metadati specifici della tipologia documentale). Questo elemento viene valorizzato nella modalità 'ExternalMetadata' ovvero questi metadati vengono strutturati nel formato XML, utilizzando lo schema XML – xsd – la cui localizzazione viene specificata nell'attributo ***XMLScheme*** dell'elemento, l'insieme di queste informazioni costituisce un corpo che viene inserito all'esterno dell'Idc e specificato nel sub-elemento '***ExtrernalMatedata***' con attributi ***encoding*** per le informazioni relative al tipo di codifica, ***extention*** per indicare l'estensione del file e ***format*** per fornire informazioni sulla struttura dati. In questo caso quindi l'insieme dei metadati cosi definiti individua concretamente un file xml esterno all'IdC ma che comunque deve rimanere interno al PdA, per cui la sua struttura è identica all'elemento ***File*** – vedi sopra;

– ***Process*** relativa al processo di produzione del PdA, che si compone di:

- l'indicazione delle informazioni (nome e ruolo) dei soggetti (***Agent***) che intervengono nel processo di produzione del PdA con attributi ***role*** (deve essere valorizzato con uno

dei seguenti valori: Delegate, Operator, ***PreservetionManager***[2], PublicOfficer, OtherRole), ***otherRole*** da valorizzare nel caso in cui l'attributo role sia valorizzato con 'OtherRole' e ***type*** da valorizzare con '***organization***' o 'person', che si compone di:

- ***AgentName***, nel caso specifico di CNP verrà valorizzato il sotto-elemento ***FormalName*** con la denominazione dell'ente che interviene nel processo di conservazione sostitutiva
- Un eventuale ***AgentID*** identificativo univoco (alfanumerico) dell'Agente coinvolto nel processo di conservazione (per esempio il Codice fiscale se persona fisica o la partita IVA se un ente come nel caso del contesto CNP) con attributi ***scheme*** (i possibili valori sono: NationalHealtCareAuthority,***TaxCode***,VATRegistrationNumber,OtherScheme) e ***otherScheme*** (da valorizzare nel caso in cui l'attributo scheme sia valorizzato con 'OtherScheme')

- il riferimento temporale adottato ***TimeReference*** ovvero le informazioni relative a data e ora di creazione dell'IdC. Nel nostro caso all'IdC viene poi apposta una marca temporale 'Attached' per cui il sotto-elemento ***AttachedTimeStamp*** non viene valorizzato – rimane vuoto in quanto non ha senso indicare l'URI delle marca temporale dato che poi l'IdC viene inserito all'interno di una busta crittografica .tsr - ma è obbligatorio valorizzare l'attributo ***normal*** con la date l'ora di creazione dell'IdC in forma normalizzata di tipo 'datetime' espressa nel formato UNI ISO 8601:2010 nella forma YYYY-MM-DDT00:00:00+-00,
- un'eventuale indicazione delle norme tecniche e giuridiche applicate per l'implementazione del processo di produzione del PdA ***LawAndRegulations***.

Infine si riporta di seguito l'esempio completo del file xml dell'IdC:

```
<?xml version="1.0" encoding="UTF-8"?>
<sincro:IdC            sincro:url="http://www.uni.com/U3011/sincro/"            sincro:version="1.0"
xmlns:sincro="http://www.uni.com/U3011/sincro/"         xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="http://www.uni.com/U3011/sincro/IdC.xsd">
  <sincro:SelfDescription>
    <sincro:ID sincro:scheme="XXXXX">XXXXXXXXXXXXXXXXXXXXXXXXX</sincro:ID>
    <!-- Denominazione cliente -->
      <sincro:CreatingApplication>
      <sincro:Name>CNP</sincro:Name>
      <sincro:Version>1.0</sincro:Version>
      <sincro:Producer>Arancia ICT S.r.l.</sincro:Producer>
    </sincro:CreatingApplication>
  </sincro:SelfDescription>
  <sincro:VdC>
    <sincro:ID sincro:scheme="XXXXX">XXXXXXXXXXXXXXXXXXXXXXX</sincro:ID>
    <!-- ID lotto -->
    <sincro:VdCGroup>
      <sincro:Label>Fatture elettroniche PA di <Nome Azienda></sincro:Label>
      <sincro:ID sincro:scheme="XXXXX">XXXXXXXXXXXXXXXXXXXX</sincro:ID>
      <!-- ID tipologia -->
      <sincro:Description   sincro:language="IT">lotto   di   Fatture   elettroniche   PA   di   <Nome
Azienda></sincro:Description>
    </sincro:VdCGroup>
```

[2] Ruolo corrispondente al Responsabile della conservazione.

```
  </sincro:VdC>
  <sincro:FileGroup>
    <sincro:Label>Fatture elettroniche PA di <Nome Azienda></sincro:Label>
    <!-- ID_tipologia-ID documento -->
    <sincro:File sincro:format="text/xml">
      <sincro:ID sincro:scheme="XXXXX">X-XXXX-X</sincro:ID>
      <!-- ID_tipologia-ID_documento-progressivo -->
      <sincro:Path>fattura1.xml</sincro:Path>
      <sincro:Hash sincro:function="SHA-256">5b9f8490fc3906f836c18c308383fd600e8cd987</sincro:Hash>
    </sincro:File>
    <!-- ID_tipologia-ID documento -->
    <sincro:File sincro:format="text/xml">
    <sincro:ID sincro:scheme="XXXXX">X-XXXX-X</sincro:ID>
    <!-- ID_tipologia-ID_documento-progressivo -->
    <sincro:Path>fattura2.xml</sincro:Path>
    <sincro:Hash sincro:function="SHA-256">0907fc21b679128c892800b98028f8021b5c03cc</sincro:Hash>
    </sincro:File>
    <sincro:MoreInfo sincro:XMLScheme="file:///moreinfo.xsd">
      <sincro:ExternalMetadata           sincro:format="text/xml"           sincro:extention=".xml"
sincro:encoding="binary">
        <sincro:ID sincro:scheme="XXXXX">XXXXXXXXXXXXXXXXXXXXX</sincro:ID>
        <!-- ID tipologia -->
        <sincro:Path>index.xml</sincro:Path>
        <sincro:Hash                                                    sincro:function="SHA-
256">48cd42700403afa309b6344082ca3fd62e65fb53</sincro:Hash>
      </sincro:ExternalMetadata>
    </sincro:MoreInfo>
  </sincro:FileGroup>
  <sincro:Process>
    <sincro:Agent sincro:type="organization" sincro:role="PreservationManager">
      <sincro:AgentName>
        <sincro:FormalName>Arancia ICT S.r.l.</sincro:FormalName>
      </sincro:AgentName>
      <sincro:Agent_ID sincro:scheme="TaxCode">IT:xxxxxxxxxxx</sincro:Agent_ID>
    </sincro:Agent>
    <sincro:TimeReference>
     <sincro:AttachedTimeStamp sincro:normal="xxxx-xx-xxTxx:xx:xx+01:00"/>
    </sincro:TimeReference>
    <sincro:LawAndRegulations               sincro:language="IT">Deliberazione               CNIPA
11/2004</sincro:LawAndRegulations>
  </sincro:Process>
</sincro:IdC>
```

Torna al Sommario

7.4 Pacchetto di distribuzione

Il pacchetto di distribuzione (PdD), distribuito in risposta alla richiesta dell'Utente sarà composto da:

- i documenti conservati dal SIC richiesti (*content*);
- gli indici dei PdA a cui appartengono i documenti, firmati dal Responsabile del servizio di conservazione o da un suo delegato e marcati temporalmente;
- software per la visualizzazione (*viewer*) dei documenti contenuti nel PdD.

Torna al Sommario

8 IL PROCESSO DI CONSERVAZIONE

Il Sistema di conservazione garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità degli oggetti conservati dal momento della loro presa in carico, fino all'eventuale scarto indipendentemente dall'evolversi del contesto tecnologico e organizzativo.

Il processo di conservazione è composto dalle seguenti fasi "sequenziali":

- acquisizione dei pacchetti di versamento per la loro presa in carico;
- verifica dei pacchetti di versamento e degli oggetti in essi contenuti, e conseguente accettazione o rifiuto degli stessi;
- accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico;
- rifiuto dei pacchetti di versamento e generazione del rapporto di versamento con evidenziazione delle anomalie;
- preparazione e gestione del pacchetto di archiviazione;
- firma digitale e marca temporale dell'indice di conservazione del pacchetto di archiviazione da parte del Responsabile del servizio di Conservazione
- preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.

Il processo è completato dalle seguenti altre fasi:

- produzione di duplicati e copie informatiche;
- scarto dei pacchetti di archiviazione;
- trasferimento pacchetti di archiviazione ad altri conservatori.

Nei paragrafi che seguono vengono descritti i singoli passi del processo.

Torna al Sommario

8.1 Acquisizione dei pacchetti di versamento per la loro presa in carico

8.1.1 Fatture Elettroniche PA e relative Ricevute gestite da procedure integrate sincrone

Queste tipologie di documenti vengono generalmente conferiti attraverso un "*canale sicuro*" (sFTP sincrono) implementato tramite collegamento automatico sincrono con uno dei sistemi di fatturazione elettronica PA "integrati" con il servizio ***Conservazione No Problem*** (cfr. *7.2.1 – Fattura Elettronica PA con relative Ricevute gestita da procedure integrate sincrone*).

Il PdV viene creato automaticamente dal sistema di fatturazione elettronica PA su input del responsabile del servizio e viene conferito al Sistema Informatico di Conservazione (SIC).

Il SIC produce contestualmente registrazione su file di log.

Il log riporta:

- Gli estremi identificativi del PdV;
- Gli estremi identificativi dei documenti associati;

- Il dettaglio dell'operazione eseguita;
- L'informazione dell'utente che ha svolto l'operazione;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di conferimento dei PdV.

Il PdV viene preso in carico dal Sistema Informatico di Conservazione (SIC) per le successive elaborazioni.

Durante la fase di presa in carico il SIC procede alla validazione formale del PdV verificando:

- la presenza del **file Indice IPdV** (**Indice o file di chiusura del Pacchetto di Versamento**) in formato XML;
- la coerenza della nomenclatura: il nome del PdV deve essere uguale al nome del file .xml di IPdV.

Torna al Sommario

8.1.2 Documenti Amministrativi protocollati/non protocollati gestiti da procedure integrate sincrone

Queste tipologie di documenti vengono generalmente conferiti attraverso un "*canale sicuro*" (sFTP sincrono) implementato tramite collegamento automatico sincrono con il sistema di gestione documentale/protocollo informatico di Arancia-ICT "integrato" con il servizio ***Conservazione No Problem*** (cfr. 7.2.2 -Documento Amministrativo protocollato/non protocollato gestito da procedure integrate sincrone).

Il PdV viene creato automaticamente dal sistema di gestione documentale/protocollo (sia tramite opportuni task automatici schedulati che tramite funzione manuale) su input del responsabile del servizio e viene conferito al Sistema Informatico di Conservazione (SIC).

Il SIC produce contestualmente registrazione su file di log.

Il log riporta:

- Gli estremi identificativi del PdV;
- Gli estremi identificativi dei documenti associati;
- Il dettaglio dell'operazione eseguita;
- L'informazione dell'utente che ha svolto l'operazione;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di conferimento dei PdV.

Il PdV viene preso in carico dal Sistema Informatico di Conservazione (SIC) per le successive elaborazioni.

Durante la fase di presa in carico il SIC procede alla validazione formale del PdV verificando:

- la presenza del **file Indice IPdV** (**Indice o file di chiusura del Pacchetto di Versamento**) in formato XML;
- la coerenza della nomenclatura: il nome del PdV deve essere uguale al nome del file .xml di IPdV.

8.1.3 Altre Tipologie di Documenti

Il sistema dispone di un'interfaccia web SICWeb (HTTPs) che viene fornita su richiesta ai clienti (quelli per i quali non è stata realizzata alcuna interfaccia di integrazione) e che funge da CNP Client tramite la quale il Cliente o Soggetto Produttore procede alla composizione del pacchetto di versamento caricando sul sistema, attraverso operazione di *upload* su canale sicuro i documenti in uno dei formati previsti (cfr. *10.1 – Elenco tipologie di documenti sottoposti a conservazione*) e compilando manualmente i metadati associati a seconda della categoria e della tipologia documentale (Utilizzo di un canale di comunicazione sFTP sincrono con il server di conservazione, mentre l'autenticazione e identificazione del cliente/soggetto produttore sull'applicazione web avviene tramite credenziali personali username e password).

(È prevista anche una modalità di *upload* massivo di documenti e metadati tramite caricamento di un archivio .zip che contiene i documenti da conservare e una distinta .csv con l'insieme dei metadati associati a ciascun documento).

Una volta completato il PdV (la composizione del PdV può essere effettuata in momenti diversi), il Cliente procede alla ***chiusura*** dello stesso tramite apposita funzionalità che seleziona i singoli file/cartelle oggetto del versamento (fine fase di conferimento).

Alla chiusura del PdV viene generata una registrazione su file di log del SIC.

Il log riporta:

- Gli estremi identificativi del PdV;
- Gli estremi identificativi dei documenti associati;
- Il dettaglio dell'operazione eseguita;
- L'informazione dell'utente che ha svolto l'operazione;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di preparazione e di gestione dei PdV.

Il PdV quindi viene preso in carico dal Sistema Informatico di Conservazione (SIC) per le successive elaborazioni.

Durante la fase di presa in carico il SIC procede alla validazione formale del PdV verificando:

- la presenza del **file Indice IPdV** (**Indice o file di chiusura del Pacchetto di Versamento**) in formato XML;

- la coerenza della nomenclatura: il nome del PdV deve essere uguale al nome del file .xml di IPdV.

Specifici contratti possono prevedere il conferimento tramite sistemi diversi dall'upload tramite interfaccia web (sFTP polling asincrono, Web-Service/HTTPs), utilizzati per l'integrazione con sistemi informativi (gestionali e documentali) esterni:

- **sFTP polling asincrono**

  In questa modalità il cliente/Soggetto Produttore, una volta che il contratto è stato definito, comunica al Soggetto Conservatore un proprio indirizzo IP da abilitare, quest'ultimo abilita il canale sicuro (protetto) e fornisce le credenziali personali per l'accesso tramite protocollo FTP sicuro (username e password) e il certificato di autenticazione univoco (file di licenza del client) associato al cliente (identificazione in modo certo del soggetto produttore).

- **Web-Service/HTTPs**

  In questa modalità al cliente/Soggetto Produttore, a seguito della definizione del contratto, viene fornito il certificato di autenticazione univoco (file di licenza del client) associato al cliente, che sarà utilizzato per la generazione del Token di autenticazione (limitato o operativo) e l'apertura del canale di comunicazione HTTP sicuro (protetto). In questo modo il cliente/soggetto produttore viene identificato in modo certo.

Su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare, nell'ambiente di storage, una crittografia a livello di folder "***password-protected with 256-bit AES encryption***".

Torna al Sommario

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

Il PdV conferito/ricevuto e preso in carico, viene posto in una coda di elaborazione e viene sottoposto alle seguenti verifiche/controlli sul PdV stesso e sugli oggetti (documenti e Fascicoli da conservare) in esso contenuti:

1. Validazione del file xml di Indice del Pacchetto di Versamento (IPdV) con lo schema .XSD (*spilling.xsd*)

Di seguito si riporta lo schema xsd (*spilling.xsd*) per la validazione dell'IPdV:

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" version="1.0">

	<!-- elementi relativi al PdV -->
	<xs:element name="Versamento" type="VersamentoType" />
	<xs:complexType name="VersamentoType">
		<xs:sequence>

			<xs:element name="CNPClient" type="CNPClientType" />
			<xs:element name="Organizzazione" type="OrganizzazioneType" />
```

```
                        <xs:element name="SoggettoProduttore" type="AnagraficaType" />
                        <xs:element name="DataCreazione" type="xs:date" />
                        <xs:element name="AnnoCompetenza" type="xs:gYear" />
                        <xs:element name="Descrizione" type="NonBlankStringSupplement255Type" />

                        <xs:element name="Metadati" type="MetadatiType" minOccurs="0" />

                        <xs:choice>
                                <xs:sequence>
                                        <xs:element name="Documenti" type="DocumentiType" />
                                        <xs:element name="Fascicoli" type="FascicoliType" minOccurs="0" />
                                </xs:sequence>
                                <xs:sequence>
                                        <xs:element name="Fascicoli" type="FascicoliType" />
                                </xs:sequence>
                        </xs:choice>

                        <!-- Sezione valorizzata da CNP SERVER per rapporto di versamento -->
                        <xs:element name="IdentificativoRapporto" type="NonBlankString255Type" minOccurs="0"
/>
                        <xs:element name="DataCreazioneRapporto" type="xs:date" minOccurs="0" />
                        <xs:element name="HashVersamento" type="HashVersamentoType" minOccurs="0" />
                        <xs:element name="Esito" type="VersamentoEsitoType" minOccurs="0" />
                        <xs:element name="ResponsabileConservazione" type="AnagraficaType" minOccurs="0" />
                        <xs:element name="Errori" type="ErrorsType" minOccurs="0" maxOccurs="1" />
                </xs:sequence>
                <xs:attribute name="idVersamento" type="NonBlankString255Type" use="required" />
                <xs:attribute name="versione" type="VersioneType" use="required" />
        </xs:complexType>

        <!-- versione del versamento -->
        <xs:simpleType name="VersioneType">
                <xs:restriction base="xs:string">
                        <xs:enumeration value="V_2_0">
                                <xs:annotation>
                                        <xs:documentation>Versione 2.0</xs:documentation>
                                </xs:annotation>
                        </xs:enumeration>
                </xs:restriction>
        </xs:simpleType>

        <!-- hash versamento -->
        <xs:simpleType name="HashVersamentoType">
                <xs:restriction base="xs:string">
                        <xs:pattern value="[0-9A-Fa-f]{64}"></xs:pattern>
                </xs:restriction>
        </xs:simpleType>

        <!--  -->
        <xs:complexType name="ConservabileType">
                <xs:annotation>
                        <xs:documentation>
                                Contenuto conservabile
                        </xs:documentation>
                </xs:annotation>
                <xs:sequence>
                        <xs:element name="Nome" type="NonBlankString255Type" />
                        <xs:element name="Categoria" type="NonBlankString100Type" />
                        <xs:element name="Tipologia" type="NonBlankString100Type" />
                        <xs:element name="Metadati" type="MetadatiType" minOccurs="0" />
                        <!-- Campi valorizzato da CNP SERVER per rapporto di versamento -->
                        <xs:element name="Errori" type="ErrorsType" minOccurs="0" maxOccurs="1" />
                </xs:sequence>
```

```
        <xs:attribute name="id" type="ConservabileIdType" use="required" />
</xs:complexType>

<xs:simpleType name="ConservabileIdType">
        <xs:restriction base="NonBlankStringType">
                <xs:maxLength value="45" />
        </xs:restriction>
</xs:simpleType>

<!-- documenti contenuti nel PdV -->
<xs:complexType name="DocumentiType">
        <xs:annotation>
                <xs:documentation>
                        Contenitore di tipi DocumentoType
                </xs:documentation>
        </xs:annotation>
        <xs:sequence>
                <xs:element name="Documento" type="DocumentoType" maxOccurs="unbounded" />
        </xs:sequence>
</xs:complexType>

<xs:complexType name="DocumentoType">
        <xs:annotation>
                <xs:documentation>
                        Definizione tipo Documento: utilizzato per tutte le
                        categorie di documenti
                </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
                <xs:extension base="ConservabileType">
                        <xs:sequence>
                                <xs:element name="Hash" type="HashVersamentoType" />
                                <xs:element name="URI" type="NonBlankString255Type" />
                        </xs:sequence>
                </xs:extension>
        </xs:complexContent>
</xs:complexType>

<!-- fascicoli contenuti nel PdV -->
<xs:complexType name="FascicoliType">
        <xs:annotation>
                <xs:documentation>
                        Contenitore di tipi FascicoloType
                </xs:documentation>
        </xs:annotation>
        <xs:sequence>
                <xs:element name="Fascicolo" type="FascicoloType" maxOccurs="unbounded" />
        </xs:sequence>
</xs:complexType>

<xs:complexType name="FascicoloType">
        <xs:annotation>
                <xs:documentation>
                        Definizione tipo Fascicolo: utilizzato per definire fascicoli
                        di documenti
                </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
                <xs:extension base="ConservabileType">
                        <xs:sequence>
                                <xs:element name="Documenti" type="DocumentiType" />
                        </xs:sequence>
                </xs:extension>
        </xs:complexContent>
```

```
	</xs:complexType>

	<!-- esiti del versamento -->
	<xs:simpleType name="VersamentoEsitoType">
		<xs:restriction base="xs:string">
			<xs:enumeration value="ES01">
				<xs:annotation>
					<xs:documentation>Esito verifica positivo</xs:documentation>
				</xs:annotation>
			</xs:enumeration>
			<xs:enumeration value="ES02">
				<xs:annotation>
					<xs:documentation>Esito verifica positivo con warning
					</xs:documentation>
				</xs:annotation>
			</xs:enumeration>
			<xs:enumeration value="ES03">
				<xs:annotation>
					<xs:documentation>Esito verifica negativo</xs:documentation>
				</xs:annotation>
			</xs:enumeration>
		</xs:restriction>
	</xs:simpleType>

	<!-- organizzazione e divisione -->
	<xs:complexType name="OrganizzazioneType">
		<xs:sequence>
			<xs:element name="Descrizione" type="NonBlankString90Type" />
			<xs:element name="IdFiscale" type="IdFiscaleType" />
			<xs:element name="Divisione" type="DivisioneType" minOccurs="0" maxOccurs="1" />
		</xs:sequence>
	</xs:complexType>

	<xs:complexType name="DivisioneType">
		<xs:sequence>
			<xs:element name="Descrizione" type="NonBlankString90Type" />
			<xs:element name="Identificativo" type="NonBlankString30Type" />
			<xs:element name="IdFiscale" type="IdFiscaleType" minOccurs="0" />
		</xs:sequence>
	</xs:complexType>

	<!-- client CNP -->
	<xs:complexType name="CNPClientType">
		<xs:sequence>
			<xs:element name="Codice" type="CNPClientIdType" />
			<xs:element name="Descrizione" type="String255Type" />
		</xs:sequence>
	</xs:complexType>

	<xs:simpleType name="CNPClientIdType">
		<xs:restriction base="NonBlankStringType">
			<xs:maxLength value="50" />
		</xs:restriction>
	</xs:simpleType>

	<!-- Anagrafica -->

	<xs:complexType name="AnagraficaType">
		<xs:sequence>
			<xs:element name="Denominazione" type="NonBlankString150Type" minOccurs="0" />
			<xs:element name="IdFiscaleIVA" type="IVAType" minOccurs="0" />
			<xs:element name="Nome" type="NonBlankString150Type" minOccurs="0" />
			<xs:element name="Cognome" type="NonBlankString150Type" minOccurs="0" />
			<xs:element name="CodiceFiscale" type="CodiceFiscaleType" minOccurs="0" />
```

```
        </xs:sequence>
    </xs:complexType>

    <!-- Codice Fiscale -->

    <xs:simpleType name="CodiceFiscaleType">
        <xs:restriction base="NonBlankStringType">
            <xs:pattern value="[A-Za-z0-9]{1,28}"></xs:pattern>
        </xs:restriction>
    </xs:simpleType>

    <!-- Partita IVA -->

    <xs:complexType name="IVAType">
        <xs:sequence>
            <xs:element name="IdPaese" type="NazioneType" default="IT" />
            <xs:element name="IdCodice" type="IVACodiceType" />
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="NazioneType">
        <xs:restriction base="NonBlankStringType">
            <xs:pattern value="[A-Z]{2}" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="IVACodiceType">
        <xs:restriction base="NonBlankStringType">
            <xs:minLength value="1" />
            <xs:maxLength value="28" />
        </xs:restriction>
    </xs:simpleType>

    <!-- Partita IVA o Codice Fiscale -->

    <xs:simpleType name="IdFiscaleType">
        <xs:restriction base="NonBlankStringType">
            <xs:pattern value="[A-Z0-9]{1,28}" />
        </xs:restriction>
    </xs:simpleType>

    <!-- Metadati -->

    <xs:complexType name="MetadatiType">
        <xs:sequence>
            <xs:element name="Metadato" type="MetadatoType" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="MetadatoType">
        <xs:simpleContent>
            <xs:extension base="NonBlankStringSupplementType">
                <xs:attribute name="id" type="MetadatoIdType" use="required" />
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:simpleType name="MetadatoIdType">
        <xs:restriction base="xs:normalizedString">
            <xs:pattern value="[A-Z][A-Z0-9_]{0,99}" />
        </xs:restriction>
    </xs:simpleType>

    <!-- tipi stringa -->
```

```
<xs:simpleType name="StringType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin})*" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankStringType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin})+" />
	</xs:restriction>
</xs:simpleType>

<!-- tipi stringa supplement -->
<xs:simpleType name="StringSupplementType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="([\p{IsBasicLatin}\p{IsLatin-1Supplement}])*" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankStringSupplementType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="([\p{IsBasicLatin}\p{IsLatin-1Supplement}])+" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankString30Type">
	<xs:restriction base="NonBlankStringType">
		<xs:maxLength value="30" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankString90Type">
	<xs:restriction base="NonBlankStringSupplementType">
		<xs:maxLength value="90" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankString100Type">
	<xs:restriction base="NonBlankStringType">
		<xs:maxLength value="100" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankString150Type">
	<xs:restriction base="NonBlankStringSupplementType">
		<xs:maxLength value="150" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="String255Type">
	<xs:restriction base="StringSupplementType">
		<xs:maxLength value="255" />
	</xs:restriction>
</xs:simpleType>

<xs:simpleType name="NonBlankString255Type">
	<xs:restriction base="NonBlankStringType">
		<xs:maxLength value="255" />
	</xs:restriction>
</xs:simpleType>

	<xs:simpleType name="NonBlankStringSupplement255Type">
	<xs:restriction base="NonBlankStringSupplementType">
		<xs:maxLength value="255" />
```

```
            </xs:restriction>
        </xs:simpleType>

        <!-- Errori rilevati in fase di verifica del versamento -->
        <xs:complexType name="ErrorsType">
            <xs:sequence>
                <xs:element name="Errore" type="ErrorType" minOccurs="0" maxOccurs="unbounded" />
            </xs:sequence>
        </xs:complexType>

        <xs:complexType name="ErrorType">
            <xs:simpleContent>
                <xs:extension base="NonBlankStringType">
                    <xs:attribute name="livello" type="ErrorLevelType" use="required" />
                    <xs:attribute name="tag" type="NonBlankStringSupplementType" />
                </xs:extension>
            </xs:simpleContent>
        </xs:complexType>

        <xs:simpleType name="ErrorLevelType">
            <xs:restriction base="NonBlankStringType">
                <xs:enumeration value="CRITICO" />
                <xs:enumeration value="ERRORE" />
                <xs:enumeration value="AVVISO" />
            </xs:restriction>
        </xs:simpleType>

</xs:schema>
```

Se questa validazione non va a buon fine e il file di chiusura del PdV risulta non valido (controllo bloccante) viene prodotto un Errore 'Critico' da parte del SIC (si tratta di un errore di sistema bloccante) e il PdV non viene accettato.

Terminata con esito positivo la validazione con lo schema .XSD, il PdV viene sottoposto ad un ulteriore insieme di controlli:

2. Presenza di PdV duplicato, ovvero univocità dell'identificativo associato al PdV: presenza di altro PdV con lo stesso Id, all'interno del Sistema di Conservazione;
3. Identificazione del soggetto produttore (corrispondenza con quanto configurato nel sistema di conservazione);
4. Presenza e coerenza di tutti i documenti referenziati dal file xml di IPdV:
    a. il Numero di files presenti nel PdV deve corrispondere al numero di files dichiarati nel file di chiusura xml;
    b. i Nomi dei files presenti nel PdV devono corrispondere ai nomi dei files definiti nel file di chiusura xml;
    c. Presenza di files nel file xml di chiusura con lo stesso Id documento;
    d. Presenza di files nel file xml di chiusura con Id documento non specificato;
5. Presenza di oggetti (documenti/fascicoli) duplicati (univocità degli identificativi contenuti nel file di chiusura xml: presenza di documenti con lo stesso Id documento, all'interno del Sistema di Conservazione);
6. Controllo di coerenza con gli hash dei documenti: gli hash (impronte) dei documenti calcolati dal conservatore devono corrispondere con gli hash dichiarati nel file xml di chiusura originato dal PdV del produttore;
7. Controlli di merito sui formati dei singoli files:

a. Tipo MIME dichiarato nel file di chiusura xml risulta tra quelli ammessi per la conservazione dei files;
b. Le estensioni dichiarate nel file di chiusura xml risultano tra quelle ammesse per la conservazione dei files;

8. Controlli di merito sulle tipologie documentali e sui metadati associati ai file:
   a. Le tipologie documentali configurate nel sistema di conservazione devono essere corrispondenti a quelle definita e dichiarata nel file xml di chiusura;
   b. I metadati configurati per la specifica tipologia documentale nel sistema di conservazione corrispondono a quelli dichiarati nel file xml di chiusura: Il nome e l'ordine dei metadati configurati per la specifica tipologia documentale nel sistema di conservazione corrispondono a quelli dichiarati nel file xml di chiusura;
9. Verifica della validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati è opzionale ed attivabile solo sui documenti firmati.

Si segnala che le verifiche sul formato dei documenti e sui metadati aggiuntivi dei documenti contenuti nel PdV vengono eventualmente personalizzate per cliente a valle della contrattualizzazione del servizio (possono essere eventualmente inserite nell'allegato al contratto "Specificità del Contratto").

I metadati minimi del documento Informatico e Amministrativo (compreso il Registro giornaliero di protocollo) e quelli del Fascicolo (aggregazione documentale) sono quelli previsti dalla normativa esplicitati nell'Allegato 5 al DPCM del 3/12/2013, per quanto riguarda l'obbligatorietà, i valori ammessi e il tipo di dato si veda Appendice 10 (paragrafo 10.1). I metadati aggiuntivi previsti per ciascuna categoria/tipologia documentale sono esplicitati sempre in Appendice 10 (paragrafo 10.2).

Al termine delle elaborazioni il PdV viene impostato nello stato 'Nuovo' (elaborato), e vengono eventualmente segnalati gli errori/problemi riscontrati, che possono essere bloccanti o non bloccanti, eliminabili dall'utente o meno secondo la seguente tabella:

LIVELLO	BLOCCANTE **(si/no)**	CLASSIFICAZIONE **(Utente/Eliminabile oppure Sistema/Non Eliminabile)**	DESCRIZIONE
Critico	Si (PdV rifiutato/verifica negativa)	Di Sistema (Non Eliminabile)	- PdV non conforme allo schema .XSD
Error	Si (PdV rifiutato/verifica negativa)	Utente (Eliminabile)	- Errori sui metadati
Error	Si (PdV rifiutato/verifica negativa)	Di Sistema (Non Eliminabile)	- Firma corrotta o revocata o scaduta - File corrotto - File duplicato - File non presente

			- Formato file non conforme
Warning	no	Utente (Eliminabile)	- Errori sui metadati
Warning	no	Di Sistema (Non Eliminabile)	- Firma revocata ma con controllo alla data valido - Certificato di Firma Scaduto ma con controllo alla data valido

Torna al Sommario

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

Superate le verifiche, il PdV può essere accettato dal SIC se non sono presenti errori oppure a discrezione dell'operatore se sono presenti warning (avvisi non bloccanti), viene quindi generato il Rapporto di Versamento (RdV) positivo – in formato XML - in cui sono indicati tutti i contenuti informativi del PdV. In particolare contiene una serie di informazioni che permettono di identificare il pacchetto di versamento a cui si riferisce, nonché il dettaglio dei documenti contenuti e gli esiti dei controlli (l'esito dei controlli sarà OK in caso di RdV di accettazione – verifica positiva, oppure sarà KO con l'eventuale codice dell'anomalia riscontrata/motivazione di rifiuto - in caso di rifiuto/verifica negativa – vedi paragrafo successivo):

- Numero identificativo univoco del RdV;
- Data RdV;
- Esito RdV (Positivo-OK / Negativo-KO + Codice Anomalia/motivazione rifiuto);
- Riferimenti del Produttore (denominazione azienda e id fiscale);
- Riferimenti del Responsabile del Servizio di Conservazione;
- Tipologia documentale di riferimento;
- Metadati della tipologia documentale;
- Riferimento temporale;
- Impronta (hash) riferita al contenuto del PdV;
- Elenco dei documenti (file) che lo compongono:
    - Nome dei file contenuti;
    - Impronta di hash (SHA256) di ogni file contenuto;
    - Valore dei metadati di ogni file contenuto;

- Descrizione eventuali anomalie risultanti dai controlli effettuati per ogni file.

Il RdV viene etichettato con un identificativo univoco, associato ed archiviato nel SIC insieme al PdV. Al RdV viene associato un riferimento temporale (campo UTC – Tempo Universale Coordinato) e viene firmato digitalmente[3] dal Responsabile del servizio di Conservazione se previsto dal contratto stipulato con il cliente (documento "Specificità del Contratto"); il Cliente tramite l'applicazione Web può consultare il RdV e scaricarlo (Viene inviata una notifica email automatica al cliente/soggetto produttore contenente un link per la consultazione del RdV).

Il SIC produce contestualmente registrazione su file di log dell'operazione di accettazione del PdV; inoltre i PdV accettati insieme ai RdV associati che vengono opportunamente archiviati vanno a comporre il registro dei PdV accettati (registro dei Rapporti di Versamento positivi). Il sistema in sostanza consente la memorizzazione su Storage e/o su DB dei PdV ricevuti e accettati correttamente e dei relativi RdV.

Il log riporta:

- Gli estremi identificativi del Rapporto di Versamento prodotto a valle del processo di verifica;
- Gli estremi identificativi del PdV associato;
- L'esito del controllo;
- L'eventuale motivo di scarto;
- L'informazione dell'utente che ha svolto l'operazione;
- Data e ora dell'attività di verifica.

Il log tiene traccia di tutti gli eventuali errori occorsi durante le operazioni di accettazione del PdV.

Per ciascun PdV in verifica positiva il SIC può procedere con la successiva fase di Archiviazione, ovvero formazione dei PdA.

Torna al Sommario

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

Il PdV che non supera le verifiche in presenza di errori bloccanti (oppure a discrezione dell'operatore anche in presenza di warning non bloccanti) viene rifiutato dal SIC che provvede alla generazione di un Rapporto di versamento negativo di rifiuto ovvero di una notifica di rifiuto (NdR) – in formato XML - in cui vengono descritte le anomalie riscontrate.

La struttura dei dati e i contenuti informativi della NdR sono quelli previsti per il RdV di accettazione descritti nel paragrafo precedente. In particolare l'esito dei controlli effettuati sul PdV

[3] articolo 9, comma 1, lettere e) del DPCM 3 dicembre 2013, "Regole tecniche in materia di sistema di conservazione": eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione

sarà KO e all'interno dell'XML che costituisce la NdR saranno indicati anche i codici delle anomalie riscontrate (la motivazione del rifiuto).

Le possibili anomalie che determinano il rifiuto del PdV sono per comodità elencate nuovamente di seguito (vedi paragrafo 8.2 - Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti):

- PdV non contiene il file xml di chiusura ed i documenti;
- File xml di chiusura non valido rispetto allo schema XSD;
- Identificazione del Produttore dei documenti e non corrispondenza con quanto configurato nel sistema di conservazione;
- Nel sistema di conservazione non è configurato il Responsabile della Conservazione per il Produttore dei documenti a cui il PdV si riferisce;
- Numero di files presenti nel PdV non corrispondente al numero di files dichiarati nel file di chiusura xml;
- Nomi dei files presenti nel PdV non corrispondenti ai nomi files definiti nel file di chiusura xml;
- Tipo MIME dichiarato nel file di chiusura xml non previsto tra quelli ammessi per la conservazione dei files;
- Estensioni dichiarate nel file di chiusura xml non previste tra quelle ammesse per la conservazione dei files;
- Presenza di files nel file xml di chiusura con Id documento non specificato;
- Presenza di files nel file xml di chiusura con lo stesso Id documento;
- Tipologia documentale configurata nel sistema di conservazione non corrispondente a quella definita e dichiarata nel file xml di chiusura;
- I metadati configurati per la specifica tipologia documentale nel sistema di conservazione non corrispondono a quelli dichiarati nel file xml di chiusura;
- Il nome e l'ordine dei metadati configurati per la specifica tipologia documentale nel sistema di conservazione non corrispondono a quelli dichiarati nel file xml di chiusura;
- Presenza di documenti con lo stesso Id documento, all'interno del Sistema di Conservazione;
- Mancata corrispondenza degli hash (impronte) dei documenti calcolati dal conservatore con l'hash dichiarato nel file xml di chiusura originato dal PdV del produttore;
- Verifica della validità della firma sul singolo documento. Il controllo della verifica sui documenti firmati è opzionale ed attivabile solo sui documenti firmati.

La NdR viene firmata digitalmente[4] dal Responsabile del servizio di Conservazione se previsto dal contratto stipulato con il cliente (documento "Specificità del Contratto").

Il Cliente tramite l'applicazione Web può consultare il NdR e scaricarlo (Viene inviata una notifica email automatica al cliente/soggetto produttore contenente un link per la consultazione del NdR) .

Il SIC produce specifica registrazione su file di log dell'operazione di rifiuto del PdV riportandone il motivo nella sezione Motivo dello Scarto (il log tiene traccia di tutti gli eventuali errori occorsi durante le operazioni di rifiuto del PdV); inoltre i PdV rifiutati insieme alle NdR associate vengono opportunamente archiviate/conservate e vanno a comporre il registro dei PdV rifiutati (registro dei Rapporti di Versamento negativi). Il sistema in sostanza consente la memorizzazione su Storage e/o su DB dei PdV ricevuti e rifiutati e delle relative NdR.

Ciascun PdV in verifica negativa può essere re-inviato dal cliente/Soggetto Produttore al SIC previa correzione degli errori segnalati.

Torna al Sommario

8.5 Preparazione e gestione del pacchetto di Archiviazione

Il pacchetto di Archiviazione (PdA) generato nel processo di conservazione del sistema CNP è composto a partire da uno o più Pacchetti di Versamento accettati in 'verifica positiva' dal SIC (ovvero che sono stati correttamente ricevuti, presi in carico ed elaborati dal SIC) secondo le modalità riportate nel presente manuale di conservazione. La funzione di produzione di un PdA a partire da uno o più PdV accettati è una procedura automatica gestita dal SIC che non prevede alcuna interazione da parte di un operatore, ovvero nessun operatore è in grado di modificare il contenuto informativo del PdA.

Il PdA o meglio l'Indice di Conservazione (IdC) del PdA viene realizzato in conformità al formato XML definito nello standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (UNI 11386:2010)(che è lo standard nazionale riguardante la struttura dell'insieme dei dati a supporto del processo di conservazione), e nell'allegato 4 delle Regole tecniche in materia di sistema di conservazione contenute nel DPCM 3 dicembre 2013; esso viene firmato digitalmente dal Responsabile del Servizio di Conservazione e sottoposto a marcatura temporale.

L'indice del PdA (IdPA o IdC) contenente i metadati e le impronte (hash - SHA256) dei file contenuti nel PdA, insieme agli stessi file, viene archiviato/conservato dal SIC nel Repository.

Per la struttura dati e il contenuto informativo si veda il paragrafo 7.3 - Pacchetto di archiviazione.

L'accesso al Repository, per le richieste di distribuzione degli oggetti conservati e per le richieste delle copie degli archivi, è garantito al Cliente/Soggetto Produttore con soluzione di continuità 24 X 7, nelle modalità previste e descritte nel presente Manuale:

[4] articolo 9, comma 1, lettere e) del DPCM 3 dicembre 2013, "Regole tecniche in materia di sistema di conservazione": eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione

- attraverso collegamento web (applicazioni/interfacce WEB) su canale sicuro (HTTPs) con credenziali di accesso private (username e password personali).
- attraverso modalità sFTP polling
- attraverso Web-Service in modalità REST

Il SIC assicura il monitoraggio e il tracciamento dei PdA tramite la registrazione di tutte le operazioni svolte sul PdA (azioni svolte sia in maniera automatica dal sistema che in maniera manuale dagli operatori): in particolare viene data indicazione dell'utente, dello stato/operazione svolta e della data (funzionalità di "Storico Stati").

Il SIC produce anche apposita registrazione sul file di log di tutti gli accessi in visualizzazione ai PdA e di tutte le operazioni effettuate per quanto riguarda la preparazione e la gestione del PdA e dell'IdC ad esso associato. In particolare il log riporta:

- Gli estremi identificativi del PdA (e dell'IdPA);
- Gli estremi identificativi del o dei PdV associati;
- Il dettaglio dell'operazione eseguita;
- L'informazione dell'utente che ha svolto l'operazione;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di preparazione e di gestione dei PdA.

La gestione del PdA assicura la conservazione nel tempo delle informazioni (*long term preservation*) e include la verifica di congruenza e di integrità degli archivi contenuti (vedi par. 9.7 - Verifica dell'integrità degli archivi). Alla presenza di anomalie, il controllo viene esteso a tutte le copie disponibili (Storage primario e secondario di backup, copie su supporti fisici rimovibili custodite dal Responsabile dei servizi di conservazione) del PdA in esame, la copia danneggiata viene quindi sostituita da una copia integra del pacchetto.

Il Servizio di Conservazione di Arancia-ICT non utilizza allo stato attuale metodi di crittografia per la creazione dei Pacchetti di Archiviazione.

Su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare, nell'ambiente di storage, una crittografia a livello di folder "***password-protected with 256-bit AES encryption***".

Torna al Sommario

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

Per quanto riguarda le modalità di richiesta di esibizione ovvero per l'attività di ricerca e l'esibizione a norma dei documenti conservati (anche a fronte di una verifica ispettiva da parte delle Autorità competenti) lo strumento di accesso all'archivio documentale a norma del Cliente/Soggetto Produttore (solo personale autorizzato del soggetto Produttore in possesso di credenziali di autenticazione personali) è rappresentato dal servizio CNP stesso.

In particolare l'accesso al Repository del SIC, per le richieste di distribuzione degli oggetti conservati e per le richieste delle copie degli archivi, è garantito al Cliente/Soggetto Produttore con soluzione di continuità 24 X 7, nelle modalità previste e descritte nel presente Manuale:

- attraverso collegamento web (applicazioni/interfacce WEB) su canale sicuro (HTTPs) con credenziali di accesso private (username e password personali).
- attraverso modalità sFTP polling
- attraverso Web-Service in modalità REST

In risposta ad un ordinativo (richiesta dell'Utente) tramite l'apposita interfaccia web di ricerca documenti di CNP, il sistema di conservazione fornisce all'Utente richiedente tutto o parte o una raccolta di Pacchetti di Archiviazione, sotto forma di Pacchetto di Distribuzione (PdD).

L'Utente (solo personale autorizzato del soggetto Produttore in possesso di credenziali di autenticazione personali) può ricercare da interfaccia web, attraverso l'inserimento di apposite chiavi di ricerca, i documenti come output della ricerca, su cui poi richiedere la distribuzione del relativo PdD.

Il Cliente, tramite le interfacce Web, può pertanto richiedere l'esibizione ovvero la visualizzazione di tutti i documenti conservati dal Responsabile del servizio di Conservazione per:

- visionare e scaricare il documento direttamente;
- verificare l'eventuale firma digitale apposta dall'emittente sul documento originale;
- visionare e scaricare il documento conservato all'interno dell'archivio a norma;
- richiedere e scaricare l'intero PdD in formato ZIP o ISO – in particolare una volta che l'utente richiede un PdD il sistema restituisce tramite canale sicuro crittografato (protocollo HTTPS) il pacchetto PdD in formato di cartella compressa .zip o .iso dove all'interno l'utente ha a disposizione tutti i file necessari;
- richiedere eventualmente un supporto fisico esterno rimovibile contenente uno o più PdD tenuto conto che:
    - i supporti fisici non presenteranno riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia;
    - in questo caso i dati trasmessi saranno protetti con sistemi crittografici. Nello specifico, su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare a livello di folder del supporto fisico rimovibile una crittografia "***password-protected with 256-bit AES encryption***".

Si segnala che l'utente può richiedere la generazione di più PdD e ogni azione di richiesta e messa a disposizione del PdD viene tracciata con un identificativo univoco all'interno del sistema di Log e con la registrazione di un riferimento temporale. Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di preparazione e di gestione dei PdD.

Il PdD prima di essere messo a disposizione dell'utente richiedente, viene sottoposto a controlli di congruenza e di integrità, utilizzando una procedura analoga a quella citata nel paragrafo precedente per il PdA. (descritta al par. 9.7 - Verifica dell'integrità degli archivi).

Qualora l'utente dovesse riscontrare delle anomalie non individuate dalla procedura di controllo, o verificatesi nella trasmissione degli archivi, può segnalare l'anomalia attraverso il sistema di *trouble-ticketing* adottato da Arancia-ICT, che consente una gestione completa delle anomalie, tracciando l'owner (chi è incaricato della risoluzione dell'anomalia), le azioni intraprese e l'evoluzione dello stato del problema fino alla completa risoluzione.

Eventuali altri canali di gestione delle anomalie e di comunicazione, richiesti dal Soggetto Produttore, saranno descritti nello specifico contratto con il Cliente (allegato 'Specificità del Contratto').

Torna al Sommario

8.7 Produzione di duplicati e copie informatiche

In alternativa alla richiesta di esibizione di uno o più PdD, il Cliente può più semplicemente in modo del tutto similare, eseguire una richiesta di download dei duplicati dei documenti informatici conservati, questa operazione predispone una copia del documento nel formato richiesto apponendo le corrette indicazioni di conformità al documento in conservazione come previsto dalla normativa vigente.

La produzione di duplicati dei pacchetti di archiviazione (PdA) è una funzione self-service che il Cliente (solo personale autorizzato del soggetto Produttore) può attivare in qualunque momento tramite interfaccia web di CNP e attraverso collegamento al Repository mediante autenticazione con le proprie credenziali personali (username e password) e attivazione del download del PdA. Il download avverrà tramite un canale crittografato (protocollo HTTPS).

Oltre alla modalità di richiesta da interfaccia web è possibile richiedere la copia degli Archivi (PdA) anche tramite la modalità Web-Service/REST.

In alternativa, il Cliente (o la *Pubblica Autorità*) può richiedere ad Arancia-ICT la fornitura di un supporto fisico esterno rimovibile contenente una o più copie informatiche di un PdA. Solo in questo caso i dati trasmessi saranno protetti con sistemi crittografici (nello specifico su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare a livello di folder del supporto fisico rimovibile una crittografia "***password-protected with 256-bit AES encryption***").

Per quanto riguarda l'eventuale adeguamento del formato dei file all'evoluzione tecnologica il *Responsabile del Servizio di Conservazione*, secondo un piano preventivo di controlli, esegue le verifiche di integrità, di leggibilità e di adeguatezza della rappresentazione informatica dei documenti all'evoluzione tecnologica (vedi par. 9.5.1.2 - Audit di revisione della conformità agli standard e normative). Si evidenzia che la strategia di conservazione relativa agli oggetti conservati ha portato alla scelta di formati idonei, previsti e consigliati dalla normativa vigente (ad esempio il formato PDF/A), in ottemperanza all'Allegato 2 sui Formati del DPCM del 3/12/2013, è la

scelta/strategia adottata proprio come prevenzione e minimizzazione dei rischi legati all'obsolescenza tecnologica.

Il processo di produzione di duplicati, realizzato mediante strumenti che assicurino la corrispondenza del contenuto della copia alle informazioni del documento informatico di origine adottando tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia, si conclude con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti, del riferimento temporale e della firma digitale da parte del Responsabile del Servizio della Conservazione, salvi i casi previsti dalla legge secondo i quali risulti indispensabile la presenza di un Pubblico Ufficiale a chiusura del processo di conservazione.

Si segnala che anche in questo caso, ogni volta che l'utente richiede la produzione di duplicati e copie informatiche ogni azione di richiesta viene tracciata con un identificativo univoco all'interno del sistema di Log e con la registrazione di un riferimento temporale. Il log tiene traccia di tutti gli eventuali errori occorsi durante le procedure di preparazione e di gestione delle copie degli archivi.

Torna al Sommario

8.8 Scarto dei pacchetti di archiviazione

Se non diversamente concordato e a meno di documenti che rivestono interesse storico particolarmente importante, i **PdA di natura fiscale** vengono scartati automaticamente allo scadere del decimo anno di archiviazione.

I PdA di altra natura (amministrativa, sanitaria) vengono conservati fino a quando lo prevede lo specifico contratto con il Cliente.

(Si veda il paragrafo 10.3 - Descrizione politiche di conservazione).

Per entrambi i casi di cui sopra, prima della scadenza prevista, a partire dall'ultimo anno di conservazione e con una frequenza via via crescente (inizio anno, metà anno, inizio ultimo mese, inizio ultima settimana) viene inviata una PEC informativa al Cliente.

Infine, lo scarto dei PdA avverrà secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettera k) e comunque sempre previa autorizzazione del Cliente opportunamente informato dal Conservatore (tramite notifiche PEC di cui sopra). Si segnala inoltre che, per i documenti delle PA le procedure di scarto avverranno invece previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

Torna al Sommario

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

Il Servizio di conservazione erogato da Arancia-ICT genera PdA conformi alla norma UNI SInCRO 11386:2010. La conformità del file di indice del Pacchetto di archiviazione a tale Standard garantisce l'interoperabilità con tutti gli altri sistemi di conservazione aderenti alle disposizioni del DPCM 3 dicembre 2013.

Nel caso di versamento dell'archivio conservato in altro sistema di conservazione a norma o restituzione dell'archivio al Soggetto Produttore (Cliente) e comunque in tutti i casi di interruzione dei rapporti contrattuali con il Cliente, Arancia-ICT restituirà i documenti conservati e i relativi pacchetti di archiviazione tramite l'interfaccia web di esposizione dei documenti conservati (richiesta Pacchetti di Distribuzione e/o copie degli archivi) oppure su esplicita richiesta del cliente su supporto fisico esterno rimovibile e in quest'ultimo caso i dati così trasmessi saranno protetti con sistemi crittografici (nello specifico su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare a livello di folder del supporto fisico rimovibile una crittografia "***password-protected with 256-bit AES encryption***").

Piano di Cessazione

Per il caso di cessazione dell'attività di conservazione, anche a seguito della modifica della mission dell'Organizzazione, è in atto una **procedura che consente la restituzione di tutti i dati conservati ai Produttori cui appartengono**.

Nello specifico, è previsto che preliminarmente alla cessazione delle attività, il *Responsabile del Servizio di Conservazione*:

- si assicuri che tutte le Funzioni dell'Organizzazione deputate al controllo e alla gestione del Servizio di Conservazione siano formalmente informate mediante comunicazione e-mail;
- si assicuri che siano generati – per ciascun Soggetto Produttore – i Pacchetti di Distribuzione (PdD) e/o le copie degli Archivi secondo le modalità previste dal presente Manuale;
- si assicuri che i PdD e/o le copie degli Archivi siano distribuiti a tutti i Soggetti Produttori a mezzo del canale già attivo per la ricezione dei PdV. Nello specifico il sistema consente al Cliente tramite apposita funzionalità di esposizione dell'interfaccia web di procedere alla richiesta dei PdD o alle copie degli Archivi. Sarà possibile procedere allo scaricamento dei PdD o delle copie degli Archivi per i successivi 3 mesi dalla cessazione del servizio. Inoltre su esplicita richiesta del Cliente i documenti conservati e i relativi archivi potranno essere restituiti tramite riversamento su supporto fisico esterno rimovibile e in quest'ultimo caso i dati così trasmessi saranno protetti con sistemi crittografici (nello specifico su richiesta del produttore e in accordo con quanto previsto nelle specificità del contratto, è possibile attivare a livello di folder del supporto fisico rimovibile una crittografia "***password-protected with 256-bit AES encryption***");
- si assicuri che sia inviata specifica comunicazione PEC all'Agenzia per l'Italia Digitale (AgID) nella quale, per altro, sia identificata specifica tempistica di esecuzione delle attività sopra evidenziate.

Compito del *Responsabile del Servizio di Conservazione* è, in ogni caso, quello di garantire che siano rispettati tutti i requisiti per l'interoperabilità dei pacchetti informativi generati, secondo le specifiche tecniche e le norme al momento vigenti.

Il Servizio di Conservazione, per il tramite di tutte le Funzioni Responsabili nominate dal presente Manuale, assicura che le informazioni, i dati, i documenti trasferiti mediante la generazione dei pacchetti informativi sopra citati, siano resi comunque disponibili per un tempo sufficientemente congruo – almeno 3 mesi e comunque da concordare con l'Agenzia per l'Italia Digitale o con le

competenti Autorità preposte alla Vigilanza per i servizi di conservazione – ai fini dell'eventuale produzione di prove nell'ambito di procedimenti giudiziari.

Infine la cessazione del Servizio di Conservazione, implica, in funzione degli accordi contrattuali specifici per il Cliente – Soggetto Produttore, la dismissione delle utenze appositamente generate per il Cliente in fase di Start-Up sull'applicativo.
Il *Responsabile del Servizio di Conservazione* o suo delegato provvede difatti, una volta che tutti i PdD contenenti i documenti conservati o che tutti gli archivi sono stati distribuiti al Cliente, o comunque allo scadere delle tempistiche prestabilite, mediante l'applicativo a disattivare l'accesso delle utenze Web (e anche gli eventuali accessi/canali SFTP e Web-Service) per il Cliente in oggetto.
Torna al Sommario

9 IL SISTEMA DI CONSERVAZIONE

9.1 Luogo di conservazione dei documenti informatici

L'infrastruttura sottesa all'erogazione del servizio di conservazione si avvale di strutture ed impianti tecnologici di ultima generazione.

Il Data Center dove sono memorizzati i dati e i documenti informatici del Cliente è localizzato fisicamente sul territorio nazionale: in particolare il sito di conservazione primario (datacenter principale) si trova presso la sede di Palermo della società Arancia ICT Srl, fornitore del servizio di Conservazione (*Soggetto Conservatore*), mentre il sito di conservazione di Backup/Disaster Recovery (datacenter secondario in 'Housing') si trova a Milano.

Ubicazione del data center principale	Ubicazione del data center secondario
Arancia-ICT S.r.l. **Via Resuttana Colli 360** **90146 Palermo – Italia**	**SoftLayer Technologies Italia S.r.l.** **Campus DATA4 Italy** **Via Monzoro 103** **20010 Cornaredo (MI) – Italia**

Le caratteristiche del Data Center secondario sono del tutto assimilabili a quelle del Data Center primario, e consentono l'erogazione del servizio di conservazione nel caso non fosse disponibile il sito primario.

Le diverse componenti critiche e significative ("sensitive") del sistema di conservazione sono isolate da altri ambienti, organizzativamente, fisicamente e logicamente. Per ulteriori dettagli si faccia riferimento al paragrafo "*6.4 – Ambienti di installazione di CNP*", documentato nel "**Manuale di Installazione e configurazione**".

Torna al Sommario

9.2 Componenti Logiche

Il Sistema di Conservazione (SIC) di Arancia-ICT è costituto da tre componenti principali così come mostrato nella figura seguente (in particolare il sistema server di conservazione oggetto del presente Manuale – CNP Server - è costituito dai componenti *SICEngine* e *SICStorage*, mentre il componente SICWeb è un componente Web aggiuntivo fornito da Arancia-ICT, su richiesta dei propri clienti, che può essere utilizzato per la creazione e il conferimento e la gestione dei PdV, la visualizzazione dei RdV (positivi o negativi) prodotti dal server, le richieste di esposizione dei documenti conservati ovvero la visualizzazione dei PdD e la copia degli Archivi):

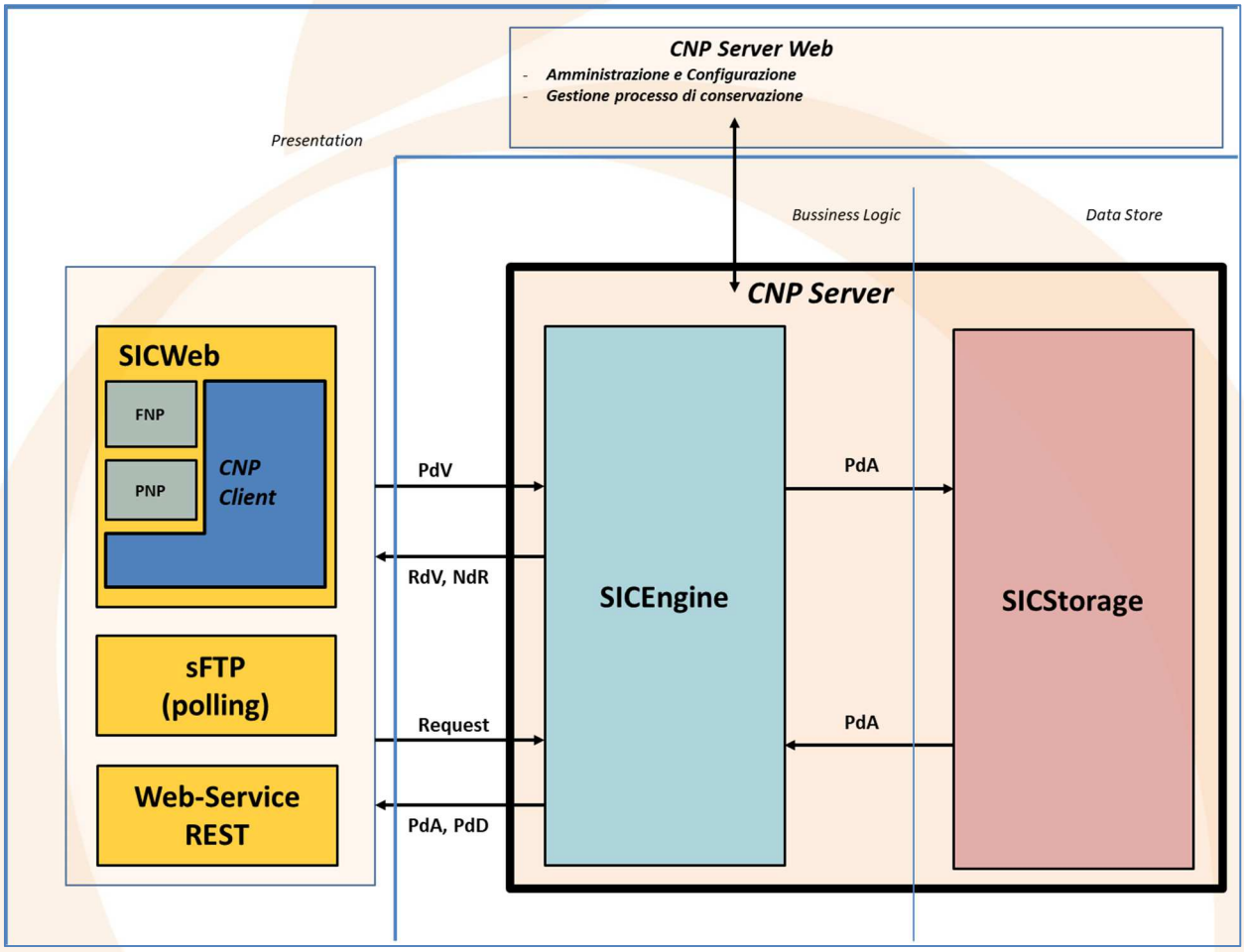

Figura 3 - Componenti logiche del SIC

La soluzione è basata su una struttura *multi-tier* e più livelli (*layer*).

Presentation:

La soluzione è stata progettata per garantire una veloce scalabilità, il livello *Presentation* costituisce l'interfaccia dove i produttori e gli amministratori di sistema possono operare e gestire il sistema di conservazione, di seguito il dettaglio delle singole componenti:

- **SFTP** asincrono, il servizio di FTP polling che ha il compito di ricevere i PdV da parte dei produttori: processo asincrono che consente ai produttori tramite l'integrazione con i loro sistemi (esterni) di trasferire direttamente i PdV con processi asincroni.
- **Web Services**, l'interfaccia web HTTPs esposta su protocollo REST che consente ai produttori tramite l'integrazione con i loro sistemi (esterni) di trasferire direttamente i PdV con processi sincroni. Il Web Services inoltre espone le funzionalità di ricerca dei documenti e le funzionalità di generazione copia degli archivi e di generazione dei PdD.
- **Web Applications**:
    - Il componente **SICWeb** rappresenta il *layer* di presentazione aggiuntivo del sistema. Esso è costituito dal sottosistema CNP Client (Conservazione No Problem Client) che rappresenta il modulo di *Front End* aggiuntivo. Quest'ultimo costituisce il client di gestione web del sistema di conservazione riservato ai soli *clienti/soggetti produttori* che ne fanno richiesta: è un componente Web aggiuntivo fornito da Arancia-ICT che può essere utilizzato per la creazione e il conferimento e la gestione dei PdV, la visualizzazione dei RdV (positivi o negativi) prodotti dal server, le richieste di esposizione dei documenti conservati ovvero la visualizzazione dei PdD e la copia degli Archivi. È a sua volta integrato all'interno delle applicazioni FNP – FatturaNoProblem e PNP – ProtocolloNoProblem di Arancia-ICT.
    - Il modulo di *Front End* principale è invece costituito dalla applicazione web CNP Server (Conservazione No Problem Server): in questa web application è possibile gestire da parte degli *amministratori* la configurazione del sistema di conservazione, la definizione dei soggetti produttori, la configurazione dei soggetti per i processi di conservazione, definire le classi documentali e i rispettivi metadati, definire le policy di accesso o gli utenti che dovranno consultare i documenti, mentre è possibile gestire da parte degli *operatori* e del *Resp. del Servizio di Conservazione* l'intero processo di conservazione fino alla creazione e gestione dei PdA. Infine anche i *clienti/soggetti produttori* possono accedere alla web application del server di Conservazione per procedere alla richiesta di esibizione dei documenti conservati (richiesta PdD e copia degli Archivi).

Bussiness Logic:

SICEngine costituisce il livello di *business* del Sistema, esso è preposto alla ricezione e verifica dei PdV, alla trasformazione in PdA e allo *storage* attraverso il sottosistema SICStorage.

Data Store:

SICStorage rappresenta il livello dati del sistema, è costituito da uno Storage primario locale, gestito da Arancia ICT presso la propria sede di Palermo, e da uno storage secondario di Backup (servizio in housing). Quest'ultimo oltre ad avere la funzione di *Disaster Recovery Site* garantisce anche la Business Continuity. In particolare dalla struttura di erogazione del servizio (struttura primaria), è previsto un collegamento diretto, cifrato e privato, verso la struttura di Disaster Recovery. Tale struttura è logicamente suddivisa, come la struttura primaria.

Arancia ICT ha implementato una infrastruttura IT in grado di fare fronte a situazioni di disastro ("Disaster Recovery") e capace di garantire la continuità nell'erogazioni dei servizi agli Utenti del SIC ("Business Continuity Management").

Il Data center di Arancia ICT fornisce una infrastruttura di storage altamente affidabile, progettata per immagazzinare dati primari e mission-critical: effettua un'archiviazione ridondante dei dati su più strutture e su dispositivi diversi all'interno di ogni struttura.

Torna al Sommario

9.3 Componenti Tecnologiche

Il software si sviluppa all'interno dell'affermato *framework Spring*, l'utilizzo di tale *framework* consente una strutturazione solida del progetto ma garantisce al contempo performance elevate grazie alla semplicità del modello.

Il modello dati (database relazionale) è mappato attraverso le più recenti specifiche JPA (*Java Persistence API*), completamente transazionale e confacente allo standard ORM (*Object-Relational Mapping*), ovvero del tutto disaccoppiato dal RDBMS (*Relational DataBase Management System*).

La struttura di progetto è arricchita dall'uso di un database non relazionale orientato ai documenti (MongoDB), che consente performance elevate in fase di reperimento della significativa mole di informazioni a corredo dei file gestiti.

L'autenticazione e la sicurezza all'interno del software sono sviluppate con particolare cura e garantiscono protezione contro gli attacchi come: *session fixation, cross site request forgery, SQL injection*.

L'interazione con il sistema avviene attraverso un'interfaccia utente semplice e ricca di contenuti visivi che migliorano l'esperienza d'uso dell'utente. La fruizione dei contenuti del portale web è possibile attraverso tutte le categorie di dispositivi mobili.

La comunicazione con i sistemi esterni avviene in modalità completamente criptata e utilizza lo standard *HTTPS/SSL*

I sistemi che accolgono il software sono *Unix-like* e sono configurati per avere appositi controlli sugli accessi e una valutazione a grana sottile dei tentativi di *handshake*.

I dati inseriti sono garantiti da *backup* incrementali con ampia profondità di storico e dalla presenza di monitoraggi automatici sullo stato delle macchine.

Torna al Sommario

9.4 Componenti Fisiche

Arancia-ICT Srl è garante di tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione, comprensivo delle copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni.

Arancia-ICT Srl garantisce che gli strumenti informatici in dotazione sono di ultima generazione e che sono sempre aggiornati, con la tecnologia e la normativa di tutela della privacy, per garantire il corretto funzionamento contro il "malicious code" e contro gli accessi non autorizzati sia logici che fisici. Per quanto riguarda le politiche di sicurezza dell'organizzazione con incluse le politiche per l'utilizzo degli strumenti informatici si rimanda alla documentazione relativa al sistema di gestione della sicurezza informatica, certificato UNI CEI ISO/IEC 27001:2014.

Nella figura di seguito riportata è schematizzata l'architettura fisica che ospita il Sistema di Conservazione di Arancia-ICT (siti di conservazione: datacenter principale e datacenter secondario – Disaster Recovery) in tutte le sue componenti:

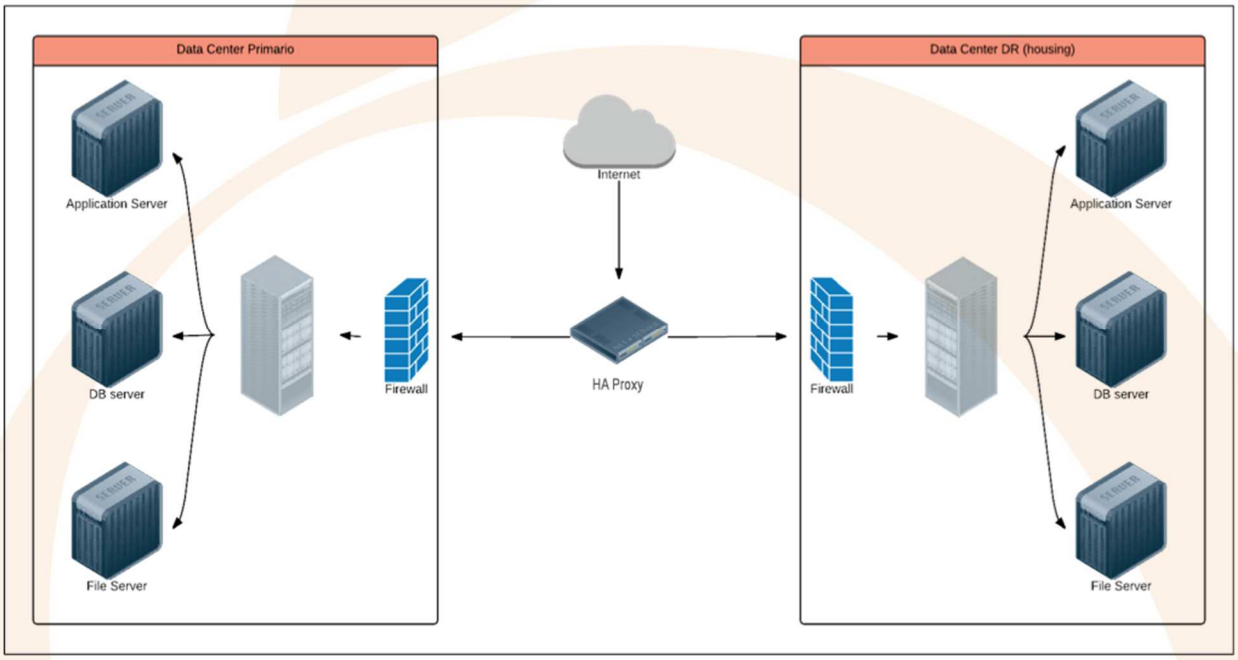

Figura 4 - Architettura fisica SIC

Nella tabella seguente sono riepilogate tutte le componenti fisiche (componenti hardware e software) utilizzate dal sistema di conservazione, tutte le componenti sono collocate presso il Data Center del Conservatore:

Nome	Descrizione
Application Server	Server che fornisce l'infrastruttura e le funzionalità di supporto, sviluppo ed esecuzione delle applicazioni FNP e CNP
DataBase Server	Server dedicato ad ospitare fisicamente il database che ospita i dati e le informazioni dei documenti sottoposti a conservazione
File Server	Server che mette a disposizione dello spazio disco su un filesystem, per permettere il salvataggio, la lettura, la modifica, la creazione

Nome	Descrizione
	dei documenti/file e cartelle
Firewall	componente per la difesa della sotto-rete informatica, che garantisce una protezione in termini di sicurezza informatica della rete stessa
HA Proxy	Questo componente si occupa dei Servizi di HA: se uno dei due nodi del cluster non funziona l'altro nodo comincia a erogare il servizio.

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 UNI CEI ISO/IEC 27001:2014.

Torna al Sommario

9.5 Procedure di gestione e di evoluzione

L'unità operativa *Servizi SaaS* è incaricata alla operatività del servizio e alla conduzione del sistema di conservazione: attività quali generazione dei rapporti di versamento e dei pacchetti di archiviazione, verifica degli esiti, gestione delle anomalie e supporto al cliente, quotidianamente svolte dagli incaricati per l'erogazione del servizio.

L'unità operativa *Produzione ICT* è incaricata allo sviluppo e alla manutenzione del sistema di conservazione e ha cura di mantenere le versioni aggiornate del Software e degli altri strumenti informatici utilizzati per la realizzazione del Sistema di Conservazione di Arancia-ICT.

A tale scopo, tutto il software realizzato per il processo di conservazione digitale e per i processi ad esso collegati si trova all'interno di un sistema di gestione del software in grado di mantenere il *versioning* del codice sorgente sviluppato.

Le operazioni effettuate dai vari componenti tecnologici del Sistema di Conservazione, al fine di facilitare la diagnosi di eventuali comportamenti anomali del sistema, sono soggette a *tracking* su appositi file di log. Ogni record informativo scritto sul log contiene il *timestamp* dell'operazione ed altre informazioni legate al componente e al tipo di attività effettuata. I file di log sono sottoposti a backup periodici con una adeguata retention e profondità storica dei dati archiviati. I file di log vengono conservati per il periodo di almeno 1 anno (come esplicitato ai paragrafi 7.3 "Gestione dei log" e 7.5 "Politiche di conservazione dei log" del documento "Piano della Sicurezza del Sistema di Conservazione - ISPD").

Le attività di monitoraggio riguardano sia aspetti applicativi che di infrastruttura. Le prime sono in carico all'unità operativa *Servizi SaaS*, e sono finalizzate a rilevare eventuali problemi relativi al processo di conservazione nelle sue componenti applicative. Tali attività rientrano a tutti gli effetti nell'ambito della conduzione del servizio descritta precedentemente. Le eventuali anomalie

riscontrate sono tracciate tramite il sistema di tracking *Mantis* e sono condivise e assegnate al personale dell'unità *Produzione ICT*, che si occuperà della loro gestione e risoluzione.
Le seconde sono finalizzate alla rilevazione di problemi a livello infrastrutturale e vengono gestite direttamente dal reparto *Produzione ICT* che, fra le proprie funzioni, ha il compito di gestire anche gli incidenti di sicurezza e di vulnerabilità.

I sistemi che concorrono alla composizione del Sistema di Conservazione, sia fisici / di infrastruttura (c.a. *Server*, *Network*) sia applicativi (c.a. *Application Server*, *RDBMS*) sono sottoposti a monitoraggio automatico effettuato dal sistema di controllo *Nagios* che esegue dei controlli sulle risorse fisiche delle singole macchine e monitoraggio *http* delle applicazioni esistenti sui predetti sistemi.
Torna al Sommario

9.5.1 Change Management

La gestione del cambiamento è in carico alle figure professionali che rivestono i vari ruoli previsti nell'ambito della conservazione e nello specifico al *Responsabile del Servizio di Conservazione* insieme al *Responsabile dei Sistemi Informativi per la Conservazione* (unità operativa "Produzione ICT") e al *Responsabile del Servizio Clienti* (unità operativa "Servizi SaaS"). Tali figure hanno il compito di seguire le evoluzioni tecnologiche e normative, analizzare i feedback ricevuti dalle attività di monitoraggio o innescate dai processi di '*incident management*' e '*vulnerability assessment*', e collaborare nella definizione delle soluzioni idonee a garantire che le funzionalità del sistema di conservazione siano costantemente adeguate.

Il processo di *Change Management* è finalizzato a identificare, analizzare e valutare i cambiamenti ritenuti utili o necessari per i processi critici, che potrebbero potenzialmente impattare il sistema di conservazione.

Il processo di *Change Management* può essere determinato da:

- Cambiamenti interni (ad esempio, di tipo organizzativo) ed esterni (ad esempio, di tipo normativo) che possono impattare sul servizio;
- Piani e/o azioni di miglioramento che scaturiscono dal processo di Monitoraggio (cfr. capitolo 9 'MONITORAGGIO E CONTROLLI' del presente Manuale della Conservazione).

Tali cambiamenti possono essere, ad esempio, relativi ai processi di versamento, archiviazione e distribuzione dei pacchetti, ai processi e alle modalità di gestione degli accessi, alla architettura infrastrutturale ed applicativa del sistema, alla sicurezza, ecc.

9.5.1.1 Procedura per la gestione delle modifiche al sistema di Conservazione

A seguito di una richiesta/esigenza di cambiamento (1. ***Request for Change***), dopo una prima fase di identificazione ed analisi dei cambiamenti e/o definizione dei Piani/Azioni di miglioramento (2. ***Impact Analysis***), l'*Owner* (ossia chi ha intercettato e identificato l'esigenza di cambiamento)

identifica i ruoli da coinvolgere nella gestione, definisce e condivide il piano di Change Management/Release-Plan (vedi Modello "*ARA_Mod. 8.5 CM_RP_[SOFTWARENAME]_v.XX.XX.XX.XLSX*" allegato alla presente procedura) con i principali soggetti coinvolti (produce adeguata documentazione di progetto: documento/verbale di analisi e progettazione delle Change Request – CR) e tiene traccia delle nuove Feature/Azioni da implementare tramite il sistema di tracking *Mantis*. Queste ultime, una volta che il documento/verbale di analisi/progettazione delle CR (documento di 'Richiesta di Modifiche al Sistema di Conservazione' - vedi Modello "*ARA_Mod. 8.5 CM_MOD[NUM]_[SOFTWARENAME]_[DESC].docx*" allegato alla presente procedura) viene valutato e approvato dal *Responsabile del Servizio di Conservazione* e dal *Responsabile dei Sistemi Informativi per la Conservazione* (3. ***Approve/Deny***), vengono poi assegnate dal *Responsabile dello sviluppo e manutenzione del sistema di conservazione* al personale tecnico che si occuperà della loro implementazione. Una volta che le modifiche approvate vengono implementate dal personale tecnico (4. ***Implement Change***) il *Responsabile dello sviluppo e manutenzione del sistema di conservazione* produce e condivide le relative *Release Notes* (vedi Modello "*ARA_Mod. 8.5 CM_[SOFTWARENAME] - Release Notes - V.XX.XX.XX.DOCX*" allegato alla presente procedura) e procede con il rilascio della nuova versione del software contenente le modifiche in ambient di test. Le *Release Notes* sono utilizzate dal *Responsabile del Servizio Clienti* e dal *Test Manager* per procedere alla fase di test in ambiente di test di tutte le funzionalità implementate (vedi Modello Piani/Casi di test "*ARA_Mod. 8.5 CM_Piano di test [SOFTWARENAME] v.XX.XX.XX.XLSX*" allegato alla presente procedura): durante la fase di test vengono aggiornati i Piani/Casi di Test e prodotti i relativi Test Report, ovvero i report contenenti gli esiti positivi o negativi dei test. Una volta che la fase di Test (cicli di test) risulta completata e tutti i test delle nuove funzionalità hanno esito positivo (5. ***Review/Reporting***), il *Responsabile dello sviluppo e manutenzione del sistema di conservazione* procede con la schedulazione del rilascio della nuova versione del software in ambiente di produzione: in particolare viene prodotto il documento di "Rilascio di una nuova versione del software" (vedi Modello "*ARA_Mod. 8.5 CM_REL_[SOFTWARENAME]_[V. xx.xx.xx].docx*" allegato alla presente procedura) che contiene le informazioni di pianificazione circa il rilascio in produzione (es. nome versione e data e ora rilascio) e deve essere approvato sia dal *Responsabile del Servizio di Conservazione* che dal *Responsabile dei Sistemi Informativi per la Conservazione*.

Per i dettagli relativi alla fase di Test e Rilascio di nuove versioni del software si faccia riferimento alla Istruzione Operativa "*ARA_IO 8.5* ***Gestione Test e rilasci SW***" del SGI a norma UNI CEI ISO/IEC 27001:2014.

L'implementazione delle singole azioni è effettuata dalle relative Funzioni e dal personale tecnico coinvolto, le quali si impegnano a produrre e fornire ai propri responsabili la reportistica delle attività svolte (5. **Review/*Reporting***).

Tutte le modifiche apportate al sistema di conservazione sono tracciate e reperibili tramite accesso al software di *versioning* in uso. In particolare:

- è possibile risalire alla versione attuale del software in esercizio;
- le modifiche sono identificata in modo univoco in tale SW di *versioning*, specificando la data in cui tale modifica è stata eseguita e il/i soggetti che hanno applicato la modifica;

- è riferita e disponibile sia la versione di SW precedente a quella attualmente in esercizio, sia la versione in campo del codice relativo al SW che recepisce la modifica attuata.

Eccezioni e procedure in caso di emergenza

In casi di emergenza urgenti, che possono determinare ad esempio un grave disservizio, si procederà direttamente con l'implementazione delle modifiche e con il rilascio in produzione (senza procedere alla autorizzazione formale da parte del management e senza procedere con i relativi test in ambiente di test o effettuandone solo una parte), mentre al *Responsabile del Servizio di Conservazione* e al *Responsabile dei Sistemi Informativi per la Conservazione* verrà data comunque comunicazione della esigenza di eseguire i cambiamenti, ovvero verranno informati senza attivare il processo autorizzativo formale. In questo caso il personale coinvolto dovrà fornire motivazioni convincenti circa la necessità di non eseguire parte o tutti i test previsti dai Piani di test in ambiente di test (come stabilito della presente procedura) le quali dovranno poi essere approvate da un responsabile.

Istruzioni per il ripristino/roll-back alla condizione precedente l'applicazione delle modifiche

Infine è prevista specifica procedura di *roll-back* all'interno del processo di cambiamento, per ripristinare il sistema alla condizione precedente l'applicazione delle modifiche.

In particolare le misure di ripristino richiedono la produzione di un apposito documento/verbale di ripristino/roll-back (vedi Modello "*ARA_Mod. 8.5 CM_ROL_[SOFTWARENAME]_[V. xx.xx.xx].docx*" allegato alla presente procedura) che deve contenere la schedulazione e l'autorizzazione di un *roll-back* del sistema di Conservazione ad una versione software precedente alla attuale in ambiente di test o produzione. Il documento deve contenere anche una descrizione delle motivazioni e delle valutazioni eseguite (ad esempio a seguito di test funzionali sul sistema in campo) per giungere alla conclusione di operare il ripristino allo stato di partenza e devono essere opportunamente approvate dal *Responsabile del Servizio di Conservazione* e dal *Responsabile dei Sistemi Informativi per la Conservazione*.

La figura di sotto descrive le macro-fasi del processo di *Change Management* applicato al sistema di conservazione di Arancia-ICT, che sono state descritte sopra:

Figura 5 - Change Management Process

Tutte le operazioni di gestione, monitoraggio, change management e verifica sono descritte dettagliatamente nelle procedure operative e nelle istruzioni operative certificate e garantite dalla norma ISO/IEC 27001 (Nello specifico si faccia riferimento alla Istruzione Operativa "*ARA_IO 8.5* ***Gestione delle modifiche del SW (Change Management)***" del SGI a norma UNI CEI ISO/IEC 27001:2014).

Torna al Sommario

9.5.1.2 Audit di revisione della conformità agli standard e normative e obsolescenza tecnologica

Il monitoraggio e la conformità alla normativa e agli standard di riferimento, elencati nel capitolo "*4 – NORMATIVA E STANDARD DI RIFERIMENTO*" di questo documento, viene verificata con periodicità annuale, dal *Responsabile del Servizio di Conservazione* di concerto con la funzione *Servizi Saas*, e, in collaborazione con la funzione *Produzione ICT,* ne progetta l'eventuale *change management* (evoluzione del sistema). Nell'ambito dei processi *change management* e di verifica periodica di conformità alla normativa e agli standard di riferimento, vengono considerate ed analizzate anche le possibili implicazioni derivanti dall'obsolescenza tecnologica.

Nel dettaglio, con periodicità annuale il *Responsabile del Servizio di Conservazione*, effettua un riesame normativo-tecnico del servizio per accertare la conformità del sistema rispetto alla normativa attualmente in vigore o eventuali standard che modificano le regole tecniche del processo. Attraverso un *Preservation Plan*, vengono pianificati processi di audit che coinvolgono aspetti normativi, di processo, organizzativi, tecnologici e logistici, per essere adesi alle nuove metodologie e alla compliance normativa. Ai fini della verifica di conformità sono periodicamente effettuati degli audit interni applicando procedure appositamente definite che stabiliscono il processo di verifica, attività, ruoli e responsabilità. 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 previsto una programmazione delle verifiche (sulla base di una serie di elementi tra cui le non conformità riscontrate, gli obiettivi ed i piani di miglioramento) in modo che venga verificata l'efficacia del Sistema di Gestione Integrato e che tutti i processi di rilievo siano visti di norma una volta l'anno;
2) Assegnazione: il *Responsabile del Servizio di Conservazione* sceglie il personale responsabile che si occuperà di svolgere la verifica, sulla base di peculiari criteri di formazione e qualificazione, per tipologia di norma da verificare;
3) Accordo di audit: viene fissata la data di audit con il responsabile da valutare richiedendo la potenziale documentazione necessaria;
4) Esecuzione: viene eseguita la verifica dei requisiti del Sistema previsti sulle attività proprie del responsabile esaminato, comparando le evidenze delle attività svolte con le procedure previste per quelle attività;
5) Verifica chiusura non conformità: il responsabile verifica e valuta le correzioni effettuate e ne dichiara la (eventuale) risoluzione;
6) Riepilogo delle non conformità: viene redatto il riepilogo delle non conformità (indirizzato, nei momenti pianificati, al riesame della Direzione).
7) Azioni ProAttive delle non conformità: vengono svolte azioni correttive rispetto alle problematiche evidenziate.

Torna al Sommario

9.5.2 Capacity Management

Al fine di garantire che la capacità dei servizi (erogati ai Clienti) e dell'infrastruttura IT (facente parte del SIC) sia in grado di fornire in modo efficace e tempestivo gli obiettivi di livello di servizio concordati in sede di contratto a seguito dei monitoraggi delle varie risorse (continuo monitoring dell'utilizzo delle risorse e delle prestazioni dell'infrastruttura IT) è definito un apposito *Capacity Plan* che tiene conto delle previsioni sull'uso delle risorse del SIC al fine di assicurare un dimensionamento adeguato alle risorse di ogni servizio.
Tutte le operazioni di gestione, monitoraggio, verifica e capacity management sono descritte dettagliatamente nelle procedure operative e nelle istruzioni operative certificate e garantite dalla norma ISO/IEC 27001 (nello specifico fare riferimento alle Istruzioni Operative "*ARA_IO 8.5* ***CNP Capacity Planning***" e "*ARA_IO 8.5* ***Gestione delle modifiche del SW (Change Management)***" del SGI a norma UNI CEI ISO/IEC 27001:2014).

Torna al Sommario

MONITORAGGIO E CONTROLLI

Il sistema di conservazione digitale di Arancia-ICT è sottoposto a diverse procedure di monitoraggio e di controllo secondo quanto previsto dalle Regole Tecniche: art. 8, comma 2, lettera h, allo scopo di assicurare che gli oggetti conservati restino leggibili e usabili dagli utenti (fruibili).

Tutte le operazioni di gestione, monitoraggio, verifica e i conseguenti processi di change management e capacity management sono descritti dettagliatamente nelle procedure operative e nelle istruzioni operative certificate e garantite dalla norma ISO/IEC 27001 (Nello specifico si faccia riferimento alla "*ARA_IO 8.5* ***Gestione delle modifiche del SW (Change Management)***" e alla "*ARA_IO 8.5* ***CNP Capacity Planning***" del SGI a norma UNI CEI ISO/IEC 27001:2014).

Torna al Sommario

9.6 Procedure di monitoraggio

Si descrivono di seguito le procedure di monitoraggio del sistema di conservazione digitale di Arancia-ICT effettuate sia sul funzionamento del software applicativo e di sistema, sia sulle componenti hardware secondo diversi livelli di monitoraggio che prevedono la produzione di apposite notifiche agli Amministratori:

- **Monitoraggio hardware**

I nodi sono sottoposti ad un monitoraggio attivo attraverso l'istallazione di apposite sonde su ogni nodo. I dati raccolti comprendono gli stati delle singole risorse *hardware* e delle istanze di connessione alle macchine (*SSH, http, ftp …*)
Il sistema centrale di monitoraggio raccoglie i dati delle sonde eseguendo *handler* di correzione delle anomalie e avvisando tempestivamente gli amministratori di sistema tramite produzione di apposite notifiche. È prevista inoltre l'estrazione di *report* su base oraria, giornaliera, mensile e annuale dell'andamento delle risorse occupate e dell'affidabilità e raggiungibilità dei singoli nodi.

- **Monitoraggio servizi**

Tutti i servizi esposti sono controllati da un sistema di monitoraggio interno, che esegue tutto il set di controlli necessari e che ne garantisce appieno la continuità e la completezza.
I *report*, estratti con cadenza giornaliera/settimanale/mensile, comprendono i più significativi parametri di valutazione dei servizi (*uptime, reponse time, failure number, Avg values*).

- **Monitoraggio software applicativo**

Sono previste verifiche del corretto funzionamento del sistema di Conservazione nel suo insieme attraverso l'esecuzione di test di sistema, tali verifiche sono pianificate almeno con cadenza annuale utilizzando il Piano di test globale di tutte le funzionalità implementate nel sistema (Vedi *CNP_Piano_di_Test_v1.0.doc* e *CNP_Allegato_Piano_di_test_v1.0.xls*). Al termine dei test vengono prodotti appositi Test Report che danno evidenza dei risultati.

- **Monitoraggio e gestione dei log**

È previsto il tracciamento degli accessi e delle attività/operazioni svolte per tutti gli account utenti che accedono al sistema, nei vari ruoli previsti.

Attraverso script di sistema, tutti i log vengono periodicamente, compressi e conservati in una cartella dello storage, utilizzata per il backup e di esclusivo accesso degli amministratori di sistema.
Tutti i log del SIC di Arancia-ICT vengono archiviati e conservati per un periodo non inferiore a 1 anno (come esplicitato ai paragrafi 7.3 "Gestione dei log" e 7.5 "Politiche di conservazione dei log" del documento "Piano della Sicurezza del Sistema di Conservazione - ISPD").

➢ **Verifica presenza di virus o malware**

Tutti i documenti immessi nel SIC sono sottoposti ad una scansione per la rilevazione di virus o malware. Tale scansione, eseguita ad intervalli periodici, viene eseguita attraverso un software (ClamAV) che individua virus e malware, appoggiandosi ad un database che viene aggiornato periodicamente con un processo automatico.

➢ **Prevenzione attacchi**

La prevenzione dagli attacchi è garantita attraverso appositi controlli sugli accessi e una valutazione a grana sottile dei tentativi di *handshake*. Sono applicate politiche di inibizione all'accesso su base temporale per i fruitori che generano traffico anomalo o ripetute richieste non autorizzate.
Inoltre il sistema di autenticazione dell'applicazione garantisce protezione contro gli attacchi come: *session fixation*, *cross site request forgery*, *SQL injection*.

➢ **Raccolta e Classificazione dei Dati di Monitoraggio**

Arancia-ICT definisce e applica un processo di Quality Assurance applicato ai sistemi hardware e software gestiti. Il sistema adottato è "*Mantis BT*", uno dei più noti e diffusi strumenti web di *issue tracking* open source presenti sul mercato. "*Mantis BT*", in questa accezione, viene usato per raccogliere e classificare i dati di monitoraggio a seguito di notifiche inviate dalle sonde *Nagios*, di anomalie rilevate da *ClamAV* (software per la rilevazione della presenza di Virus e Malware) e di notifiche inviate dal servizio *Monitor.us* circa lo stato dei servizi web. Inoltre, quando i dati di monitoraggio sono relativi ad eventuali "Incidenti di Sicurezza", permette di tracciare e di classificare opportunamente queste segnalazioni (per maggiori dettagli fare riferimento all'Istruzione Operativa "*ARA_IO 8.5* ***Gestione Anomalie e Incidenti di Sicurezza***"). "*Mantis BT*" permette di classificare le segnalazioni arricchendole con printscreen dei tool di monitoraggio, log e analisi dei team che verranno coinvolti nella gestione e risoluzione delle stesse. "*Mantis BT*" inoltre, grazie alle sue funzionalità di reportistica, garantisce un valido strumento di supporto al "*Capacity Management*" (per maggiori dettagli fare riferimento all'istruzione operativa "*ARA_IO 8.5* ***CNP Capacity Planning***).
Un buon *Capacity Plan* viene prodotto tenendo in considerazione diversi scenari per le previsioni di richieste di business e le relative opzioni con le stime dei costi per fornire i livelli di servizio concordati. Esempi di capacità sono:

- spazio su disco per l'archiviazione di file;
- potenza di elaborazione;
- memoria;
- banda minima garantita;
- etc…

Sono previste e pianificate, a livello aziendale, le necessità future in termini di capacità operativa al fine di evitare pericolosi "colli di bottiglia" nei processi di implementazione o di upgrading dei

sistemi; per quanto riguarda la gestione della capacità de sistemi, per il monitoraggio interno dei server e delle applicazioni viene utilizzato il già citato, software *Nagios*, versione Core - rel. 3. *Nagios* si occupa di effettuare un monitoraggio costante di tutti quei servizi/risorse presenti in ogni singolo server fisico e/o virtuale, tramite l'installazione in locale del servizio NRPE (*Nagios Remote Plugin Executor*). Effettua il monitoraggio dello spazio disco, delle risorse disponibili (CPU, RAM, etc…), del numero di utenti connessi, del numero di processi attivi e dello stato degli applicativi presenti. Il monitoraggio avviene in real time e prevede l'invio di notifiche tramite email, per segnalare sia lo stato di alert che quello di ripristino dei servizi interessati.
In questo modo è possibile mantenere sotto controllo i sistemi e di effettuare le dovute stime e proiezioni per assicurare sempre le prestazioni richieste.

Torna al Sommario

9.7 Verifica dell'integrità degli archivi

Il SIC prevede una pianificazione ed esecuzione di un processo di verifica che assicuri l'integrità, la correttezza, la completezza e leggibilità nel tempo (conservazione nel tempo) degli oggetti conservati.
Il Processo di verifica esegue i seguenti controlli:

- Verifica del formato dichiarato e della leggibilità del documento per ogni documento digitale conservato all'interno del PdA oggetto della verifica;
- Verifica dell'integrità dei metadati associati ad ogni documento digitale conservato all'interno del PdA oggetto della verifica;
- Calcolo dell'impronta attraverso algoritmo di Hash-256 per ogni documento digitale conservato all'interno del PdA oggetto della verifica: ottenute tutte le impronte dei documenti presenti nel PdA vengono confrontate con quelle dichiarate nell'IdC al fine di verificarne la coerenza;
- Per ciascun IdC viene verificata la validità della Firma Digitale e della Marca Temporale apposta.

Questi controlli periodici di validità nel tempo delle informazioni, si aggiungono ai controlli di verifica delle informazioni in ingresso al SIC (verifiche previste durante la fase di acquisizione dei PdV); il controllo viene effettuato attraverso la verifica del mantenimento nel tempo delle caratteristiche di ingresso degli oggetti poi conservati e gestiti dal sistema.
Ogni ciclo di verifica viene registrato sul sistema di CNP riportante i dati di riferimento temporale e l'oggetto del processo di verifica, legato all'identificativo univoco dell'archivio e del suo PdA. Il processo di verifica dei PdA viene eseguito almeno annualmente ed ha per oggetto i documenti conservati non oltre i cinque anni. Attraverso le informazioni memorizzate all'interno del DataBase di CNP vengono stabilite le date di scadenza entro le quali eseguire i controlli di verifica di leggibilità per ogni archivio conservato. La rilevazione di anomalie viene segnalata attraverso l'invio di un report contenente gli specifici elementi affetti da anomalia e i riferimenti all'identificativo univoco dell'archivio e del suo PdA.
Inoltre il Responsabile del servizio di Conservazione Digitale con cadenza annuale effettuerà un ciclo di verifica degli Archivi di conservazione ovvero controllerà la consistenza e l'integrità dei

PdA (indici e documenti) eseguendo in prima persona o delegando l'esecuzione di una procedura di controllo che interesserà un adeguato campione di Pacchetti sottoposti a Conservazione Digitale.

La procedura di verifica sarà effettuata sui dati presenti all'interno del sistema, sia sulle copie memorizzate nel sito di conservazione /datacenter principale sia sulle copie di sicurezza custodite nel sito di conservazione/datacenter secondario (copie di Backup), sia sulle eventuali copie memorizzate all'interno di supporti fisici rimovibili - (DVD/M-DISC) e custodite dal *Responsabile del servizio di conservazione*.

Si segnala che tutte le operazioni effettuate per la verifica di integrità degli Archivi, sono opportunamente tracciate all'interno di un file di log e che in caso di errori vengono inviati degli alert al personale responsabile. In particolare, al verificarsi di eventuali errori viene mandata una comunicazione via email al *Responsabile del servizio di conservazione* e ai suoi delegati e all'amministratore di sistema contenente i dettagli dell'errore riscontrato.

Tutti i log del SIC di Arancia-ICT, compreso quello derivante dalle operazioni di verifica di integrità, vengono archiviati e conservati per un periodo non inferiore a 1 anno (come esplicitato ai paragrafi 7.3 "Gestione dei log" e 7.5 "Politiche di conservazione dei log" del documento "Piano della Sicurezza del Sistema di Conservazione - ISPD").

Torna al Sommario

9.8 Soluzioni adottate in caso di anomalie

Le eventuali anomalie riscontrate dal sistema di monitoraggio sono classificate in due macro categorie:

1. **Anomalia di Sistema:**
    a. ***tecnica*** (problemi dovuti a *bug del software* o malfunzionamento dei sistemi software e hardware):
        i. Bug software: l'anomalia presa in carico dall'area *Servizi SaaS* viene tracciata nel sistema di *trouble-ticketing* di Arancia-ICT, viene impostata una priorità ed assegnata all'area di competenza per la risoluzione: la struttura *Servizi SaaS* prende in carico la segnalazione dell'*incident*, che può provenire dal Soggetto produttore o dai sistemi di monitoraggio, tracciandolo sul sistema di *Trouble Ticketing*, classifica l'incident secondo i parametri di criticità segnalati o rilevati e lo assegna/inoltra al secondo livello specialistico (applicativo o infrastrutturale – *Produzione ICT*). Quest'ultimo procede con la risoluzione dell'*incident* producendo una risposta con una descrizione dettagliata circa le cause e la sua risoluzione. Infine il cliente viene notificato dell'avvenuta risoluzione dell'anomalia;
        ii. Guasto Hardware dello Storage: l'ambiente operativo utilizzato dal Conservatore è stato progettato e sviluppato in modo da garantire la sicurezza

dei dati e delle informazioni conservate, anche a fronte di guasti improvvisi e imprevedibili. Il sistema di storage composto dal datacenter principale (unità di produzione) e dal datacenter secondario (unità di *Backup - Disaster Recovery*) garantisce un'elevata affidabilità (fare riferimento ai piani BCP e DRP del sistema di conservazione "M.2.1 CNP-BCP Business Continuity Plan" e "M.2.1 CNP-DRP Disaster Recovery Plan"). Per massimizzare la sicurezza del Sistema, la copia di backup dell'archivio viene memorizzata su specifico e distinto hardware rispetto alla copia in esercizio dell'Archivio Informatico. Ulteriore elemento di sicurezza, per minimizzare gli effetti di un possibile guasto all'hardware, consiste nell'effettuare costanti ed ininterrotte operazioni di backup;

iii. Guasto del SIC: il Sistema Informatico utilizzato per la conservazione è governato, monitorato e gestito da Arancia ICT, sotto il controllo del *Responsabile del servizio di Conservazione* e il *Responsabile dei Sistemi Informativi per la Conservazione*. La struttura hardware del SIC in esercizio risponde ai requisiti di alta affidabilità e di ridondanza in modo da garantire un esercizio continuativo. In caso di guasto, la versione in esercizio può essere ripristinata in tempo reale utilizzando le componenti ridondanti dell'architettura del Sistema. Se ciò non fosse possibile si dovrà ricorrere al ripristino delle copie originali del Software e provvedere alla relativa installazione e *deploy* sui nuovi apparati;

iv. Guasto ai dispositivi di firma: in caso di guasto ai dispositivi di firma utilizzati dal *Responsabile del servizio di conservazione* occorre procedere alla individuazione della tipologia di guasto e provvedere immediatamente alla sua riparazione;

v. Problemi con il sito della Certification Authority per la marca temporale: l'indisponibilità del sito della *Time Stamping Authority* per il rilascio della marca temporale da apporre sull'evidenza informatica a chiusura del processo di conservazione, è un evento molto remoto (SLA di alto livello).

b. **funzionale** (evoluzione della normativa): il nuovo requisito viene recepito dal Service desk – *Servizi SaaS* - di Arancia ICT, tracciato e analizzato; la nuova funzionalità viene progettata, sviluppata, testata e integrata nel sistema di conservazione.

2. **Anomalia Dati**

L'anomalia viene recepita dal Service desk – *Servizi SaaS* - e tracciata nel sistema di *trouble-ticketing* di Arancia-ICT, viene impostata una priorità ed assegnata all'area di competenza per la risoluzione.

Le anomalie dati interessano l'integrità dei PdA conservati (vedi paragrafo precedente 9.7 - Verifica dell'integrità degli archivi); a seguito di un'anomalia di questo tipo il controllo di integrità viene esteso a tutte le copie (Storage primario e secondario di backup, copie su supporti fisici rimovibili custodite dal *Responsabile dei servizi di conservazione*) del PdA in esame, la copia danneggiata viene quindi sostituita da una copia integra del pacchetto.

Il Sistema di *trouble-ticketing* adottato da Arancia-ICT, consente una gestione completa delle anomalie, tracciando l'*owner* (chi è incaricato della risoluzione dell'anomalia), le azioni intraprese e l'evoluzione dello stato del problema fino alla completa risoluzione.

Torna al Sommario

10 APPENDICE

10.1 Elenco tipologie di documenti sottoposti a conservazione

Vengono di seguito elencate e descritte le tipologie di documenti sottoposti a conservazione, con le relative politiche di conservazione, nonché descritti i relativi metadati[5].

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
Fiscale	Fattura Elettronica PA (attiva e passiva)	Fattura emessa o ricevuta, inviata o ricevuta dal Sistema d'Interscambio	Conservazione Documenti Fiscali (v. cap. 10.3-DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO INFORMATICO (All. 5 DPCM 3/12/2013), intendendo come Soggetto Produttore il cedente/prestatore di beni/servizi (fattura attiva) o il committente (fattura passiva) + metadati minimi del documento informatico avente rilevanza tributaria: - Anno Fiscale - Numero Fattura - Data Fattura	xml.p7m xml (XML signed - firmato digitalmente con firma di tipo 'attached' signature CAdES o XAdES)
Fiscale	Ricevute Fattura Elettronica PA	Notifica ricevuta dal Sistema d'Interscambio	Conservazione Documenti Fiscali (v. cap. 10.3-DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO INFORMATICO (All. 5 DPCM 3/12/2013), intendendo come Soggetto Produttore il cedente/prestatore di beni/servizi (fattura attiva) o il committente (fattura passiva) + metadati minimi del documento informatico avente rilevanza tributaria: - Anno Fiscale - Numero Fattura cui si riferisce la ricevuta - Data Fattura cui si riferisce la ricevuta	xml (XML signed – con firma digitale di tipo xml signature - XAdES)
Fiscale	Documento analitico emesso/ricevuto in riferimento ad una transazione	Fattura Ricevuta, Fattura Emessa, Documento di Trasporto Emesso, Documento di Trasporto	Conservazione Documenti Fiscali (v. cap. 10.3-DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO INFORMATICO (All. 5 DPCM 3/12/2013), intendendo come Soggetto Produttore il cedente/prestatore di beni/servizi + - Anno Fiscale	.pdf (PDF o PDF/A)

[5] Quanto ai metadati per la conservazione, il SIC utilizza quelli minimi indicati e definiti nell'allegato 5 del D.P.C.M. 3 dicembre 2013 con riferimento al documento informatico, al documento amministrativo informatico e al fascicolo informatico o aggregazione documentale informatica.

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
		Ricevuto, Quietanza Modello F24, etc… (In relazione all'elenco completo dei documenti rilevanti ai fini tributari si veda tabella allegata al provvedimento N.2010/143663 del 25.10.2010 dell'Agenzia delle Entrate)		- Numero Fattura (o documento) - Data Fattura (o documento)	
Fiscale	Documento sintetico o riepilogativo	Libro Inventari, Libro Giornale, Libro Mastro, Libro Cespiti, Registro Fatture emesse, Registro Fatture ricevute, Libro Unico del Lavoro (LUL) UNICO Persone Fisiche, UNICO Società Persone, UNICO Società Capitale, UNICO Enti non commerciali, Modello 730, Modello 770 ordinario e semplificato, etc… (In relazione all'elenco completo dei documenti rilevanti ai fini tributari si veda tabella allegata al provvedimento N.2010/143663 del 25.10.2010 dell'Agenzia delle Entrate)	Conservazione Documenti Fiscali (v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO INFORMATICO (All. 5 DPCM 3/12/2013) + metadati minimi del documento informatico avente rilevanza tributaria: - Anno Fiscale	.pdf (PDF o PDF/A) eventualmente firmato (CAdES pdf.p7m o PAdES)
Amministrativa	Documento analogico non unico	Lettera, comunicazione, corrispondenza in ingresso o in	Conservazione Documenti Amministrativi (v. cap. 10.3-	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5	.pdf (PDF o PDF/A) eventualmente firmato (CAdES pdf.p7m o

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
		uscita	DESCRIZIONE POLITICHE DI CONSERVAZIONE)	DPCM 3/12/2013)	PAdES)
Amministrativa	Documento digitale non unico	Lettera, comunicazione, corrispondenza in ingresso o in uscita	Conservazione Documenti Amministrativi (v. cap. 10.3- Descrizione politiche di conservazione)	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	.pdf (PDF o PDF/A) eventualmente firmato (CAdES pdf.p7m o PAdES)
Amministrativa	Documento analogico unico	Contratti, delibere, determine e simili a firma autografa. **Il Servizio *Conservazione No Problem* accetta la conservazione di questa natura a condizione che l'attestazione di conformità venga svolta dal Cliente (soggetto Produttore) che abbia provveduto all'origine a trasformare l'analogico in digitale attraverso l'intervento di un Pubblico Ufficiale.**	Conservazione Documenti Amministrativi (v. cap. 10.3- Descrizione politiche di conservazione)	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	pdf.p7m pdf (PDF o PDF/A signed - firmato digitalmente con firma di tipo 'attached' signature - CAdES o PAdES)
Amministrativa	Documento digitale unico	Contratti , delibere e determine e simili a firma digitale	Conservazione Documenti Amministrativi (v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	pdf.p7m pdf (PDF o PDF/A signed - firmato digitalmente con firma di tipo 'attached' signature - CAdES o PAdES)
Amministrativa	Messaggio di Posta Elettronica Certificata – PEC + notifiche: accettazione e avvenuta consegna		Conservazione Documenti Amministrativi (v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	.eml
Amministrativa	Registro giornaliero di protocollo		Conservazione Documenti Amministrativi	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5	.pdf.p7m .pdf

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
			(v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE) Il Registro giornaliero deve essere inviato al sistema di conservazione entro la giornata lavorativa successiva a quella della sua produzione	DPCM 3/12/2013) - METADATI DEL REGISTRO GIORNALIERO DI PROTOCOLLO (Documento AgID: Istruzioni per la PRODUZIONE E CONSERVAZIONE DEL REGISTRO GIORNALIERO DI PROTOCOLLO)	(PDF o PDF/A signed - firmato digitalmente con firma di tipo 'attached' signature CAdES o PAdES) .xml.p7m .xml (XML signed – con firma digitale di tipo xml signature - XAdES)
Fiscale **Amministrativa**	Fascicolo	Aggregazione documentale informatica (documenti di natura Fiscale o Amministrativa)	Conservazione Documenti Fiscali (v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE) Conservazione Documenti Amministrativi (v. cap. 10.3- DESCRIZIONE POLITICHE DI CONSERVAZIONE	-METADATI MINIMI DEL FASCICOLO INFORMATICO O DELLA AGGREGAZIONE DOCUMENTALE INFORMATICA (All. 5 DPCM 3/12/2013)	Tutti i formati descritti nella TABELLA FORMATI DI CONSERVAZIONE PREVISTI

I formati dei files contenuti nel Pacchetto di Versamento devono essere conformi all'elenco dei formati previsti dall'Allegato 2 del DPCM 3 Dicembre 2013. I formati associati alla tipologia documentale sottoposta a conservazione sono dichiarati nella tabella precedente.

Nella tabella seguente vengono descritti i formati (comprensivi della relativa versione) dei file accettati e utilizzati per la conservazione (il produttore dei documenti deve adeguarsi al seguente elenco di formati ammessi che il sistema di conservazione verifica nella fase di presa in carico per l'accettazione dei pacchetti di versamento):

TABELLA FORMATI DI CONSERVAZIONE PREVISTI

Visualizzatore	Proprietario/ produttore	Formato del file	Versione del formato	Estensione	Tipo Mime	Standard
Adobe Reader	Adobe Systems - www.adobe.com	PDF[6]	vers. PDF 1.4	.pdf	application/ pdf	ISO 32000-1

[6] Nel caso di formato PDF e comunque In tutti i casi riportati in tabella, il produttore dei documenti si impegna a versare nel sistema di conservazione documenti privi di codici eseguibili o macro istruzioni o privi di qualsiasi causa, anche non visibile all'utente, che ne possa alterare il contenuto.

Adobe Reader	Adobe Systems - www.adobe.com	PDF/A	vers. PDF 1.4 vers. PDF 1.7	.pdf	application/ pdf	ISO 19005-1:2005 (vers. PDF 1.4) ISO 19005-2:2011 (vers. PDF 1.7)
Qualunque lettore di file di testo e qualunque browser	W3C	XML	n.d.	.xml	application/ xml text/xml	http://www.w3.org/XML/
Client di posta elettronica che supportano la visualizzazione di file eml	Vari	EML	n.d.	.eml	message/rfc822	RFC2822 RFC 5322

Torna al sommario

10.2 Descrizione categorie/tipologie documentali e metadati associati

All'interno del file xml IPdV la struttura prevista per i metadati è una struttura dinamica (vedi schema XSD '*spilling.xsd*'), ovvero all'interno del tag *<Metadati>* (contenitore dei tag *<Metadato>* riguardanti gli eventuali metadati specifici aggiuntivi del singolo documento/fascicolo) è possibile definire un numero illimitato di metadati dinamici associati alla categoria e alla tipologia documentale specifica. Ciascun tag *<Metadato>* possiede un attributo "*id*" che è la chiave che identifica univocamente il metadato. In questo modo la gestione dei metadati diventa estremamente semplificata e flessibile, permettendo l'aggiunta e la gestione in un qualsiasi momento di metadati a fronte ad esempio di specifiche richieste dei clienti/soggetti produttori (eventualmente esplicitate nel documento "Specificità del Contratto") oppure di modifiche normative o di gestione di nuove categorie/tipologie documentali.

Procedura di revisione delle modalità di acquisizione dei metadati

In particolare a fronte di eventi quali modifiche normative o gestione di nuove categorie di documenti le procedure/modalità di acquisizione e gestione dei metadati associati agli oggetti conservati sono soggette a revisione da parte del personale di Arancia ICT preposto alla gestione e amministrazione del sistema di Conservazione. A seguito di tali revisioni vengono prodotti opportuni verbali di "Richiesta di aggiornamento e di modifiche al Sistema di conservazione" (nello specifico di aggiornamento e modifica delle modalità di acquisizione dei metadati associati agli oggetti conservati) che devono essere approvati e firmati dai Responsabili.

Categoria documento: Informatico

Di seguito sono elencati i metadati da associare ad un documento di categoria "informatico" (in particolare sono riportati gli attributi "id" del tag <metadato>). Tutti i metadati sono opzionali, a meno dei metadati per i quali è indicata l'obbligatorietà:

NUMBER
CLOSE_DATE (obbligatorio)
SUBJECT (obbligatorio)
ISSUER_DENOMINATION (obbligatorio se non valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
ISSUER_IVA_CODE_ID (obbligatorio se valorizzato ISSUER_DENOMINATION)

ISSUER_IVA_COUNTRY_ID (obbligatorio se valorizzato ISSUER_IVA_CODE_ID)
ISSUER_FIRST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_LAST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_FISCAL_CODE (obbligatorio se valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
RECEIVER_DENOMINATION
RECEIVER_IVA_CODE_ID
RECEIVER_IVA_COUNTRY_ID
RECEIVER_FIRST_NAME
RECEIVER_FISCAL_CODE
RECEIVER_LAST_NAME

Si riporta un esempio di xml IPdV:

```
<Versamento idVersamento="3a3a3a3a3-4155-2a62-8141-bfddcada38e4" versione="V_2_0">
        <CNPClient>
                <Codice>POLLTEST01</Codice>
                Descrizione></Descrizione>
        </CNPClient>
        <Organizzazione>
                <Descrizione> Test Company</Descrizione>
                <IdFiscale>48542692547</IdFiscale>
        </Organizzazione>
        <SoggettoProduttore>
                <Denominazione> Test Company</Denominazione>
                <IdFiscaleIVA>
                        <IdPaese>IT</IdPaese>
                        <IdCodice>48542692547</IdCodice>
                </IdFiscaleIVA>
        </SoggettoProduttore>
        <DataCreazione>2017-05-26+02:00</DataCreazione>
        <AnnoCompetenza>2017+01:00</AnnoCompetenza>
        <Descrizione>test informatico</Descrizione>
        <Documenti>
                <Documento id="a78cde-87cccb">
                        <Nome>01-E-2017.pdf</Nome>
                        <Categoria>INFORMATICO</Categoria>
                        <Tipologia>FATTURE_EMESSE</Tipologia>
                        <Metadati>
                                </Metadato>NUMBER">01/E/2017</Metadato>
                                </Metadato>CLOSE_DATE">11/10/2017</Metadato>
                                </Metadato>SUBJECT">Fattura Elettronica 01/E/2017 Emessa in data:
                        11/10/2017</Metadato>
                                </Metadato>ISSUER_DENOMINATION">AUTOSERVICE</Metadato>
                                </Metadato>ISSUER_IVA_COUNTRY_ID">IT</Metadato>
                                </Metadato>ISSUER_IVA_CODE_ID">98745696586</Metadato>
                                </Metadato>ISSUER_FIRST_NAME">GIUSEPPE</Metadato>
                                </Metadato>ISSUER_LAST_NAME">VERDI</Metadato>
                                </Metadato>ISSUER_FISCAL_CODE">DNSJSC88M65B602K</Metadato>
                                </Metadato>RECEIVER_DENOMINATION">AZIENDA</Metadato>
                                </Metadato>RECEIVER_IVA_CODE_ID">12365895774</Metadato>
                                </Metadato>RECEIVER_IVA_COUNTRY_ID">IT</Metadato>
                                </Metadato>RECEIVER_FIRST_NAME">MARIO</Metadato>
                                </Metadato>RECEIVER_FISCAL_CODE">AAABBB99H22G273P</Metadato>
                                </Metadato>RECEIVER_LAST_NAME">ROSSI</Metadato>
                        </Metadati>
                        <Hash>06754922EA4B1BE00316948317E5FB62F02C422E898C6C66C70F53696B25CFE0</
                Hash>
                        <URI>01-E-2017.pdf</URI>
                </Documento>
        </Documenti>
</Versamento>
```

Categoria documento: Amministrativo

Di seguito sono elencati i metadati da associare ad un documento di categoria "amministrativo" (in particolare sono riportati gli attributi "id" del tag <metadato>). Tutti i metadati sono opzionali, a meno dei metadati per i quali è indicata l'obbligatorietà:

NUMBER
CLOSE_DATE (obbligatorio)
SUBJECT (obbligatorio)
ISSUER_DENOMINATION (obbligatorio se non valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
ISSUER_IVA_CODE_ID (obbligatorio se valorizzato ISSUER_DENOMINATION)
ISSUER_IVA_COUNTRY_ID (obbligatorio se valorizzato ISSUER_IVA_CODE_ID)
ISSUER_FIRST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_LAST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_FISCAL_CODE (obbligatorio se valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
RECEIVER_DENOMINATION
RECEIVER_IVA_COUNTRY_ID
RECEIVER_IVA_CODE_ID
RECEIVER_FISCAL_CODE
RECEIVER_FIRST_NAME
RECEIVER_LAST_NAME
PROTOCOL_ADMIN_CODE
PROTOCOL_AOO_CODE
PROTOCOL_REG_CODE
PROTOCOL_REGISTRATION_CODE
PROTOCOL_REGISTRATION_DATE
PROTOCOL_SENDER_ADMIN_CODE
PROTOCOL_SENDER_AOO_CODE
PROTOCOL_SENDER_FIRST_NAME
PROTOCOL_SENDER_LAST_NAME
PROTOCOL_SENDER_FISCAL_CODE
PROTOCOL_SENDER_DENOMINATION
PROTOCOL_SENDER_IVA_CODE_ID
PROTOCOL_SENDER_IVA_COUNTRY_ID
PROTOCOL_RECEIVER_ADMIN_CODE
PROTOCOL_RECEIVER_AOO_CODE
PROTOCOL_RECEIVER_FIRST_NAME
PROTOCOL_RECEIVER_LAST_NAME
PROTOCOL_RECEIVER_FISCAL_CODE
PROTOCOL_RECEIVER_DENOMINATION
PROTOCOL_RECEIVER_IVA_CODE_ID
PROTOCOL_RECEIVER_IVA_COUNTRY_ID

Si riporta un esempio di xml IPdV:

```
<Versamento idVersamento="2a2a2a2a2-2a2a2a2a2-2a62-8141-bfddcada38e4" versione="V_2_0">
        <CNPClient>
                <Codice>POLLTEST01</Codice>
                <Descrizione></Descrizione>
        </CNPClient>
        <Organizzazione>
                <Descrizione> Test Company</Descrizione>
                <IdFiscale>48542692547</IdFiscale>
        </Organizzazione>
        <SoggettoProduttore>
                <Denominazione> Test Company</Denominazione>
                <IdFiscaleIVA>
                        <IdPaese>IT</IdPaese>
                        <IdCodice>48542692547</IdCodice>
                </IdFiscaleIVA>
        </SoggettoProduttore>
        <DataCreazione>2017-10-10+02:00</DataCreazione>
```

```
        <AnnoCompetenza>2017+01:00</AnnoCompetenza>
        <Descrizione>test amministrativo v.2</Descrizione>
        <Documenti>
                <Documento id="21a85bcc7892">
                        <Nome>doc_amministrativo.pdf</Nome>
                        <Categoria>AMMINISTRATIVO</Categoria>
                        <Tipologia>ALTRI_DOCUMENTI</Tipologia>
                        <Metadati>
                                <Metadato id="NUMBER">12</Metadato>
                                <Metadato id="CLOSE_DATE">26/10/2017</Metadato>
                                <Metadato id="SUBJECT">Registro Protocollo del 26-10-2017</Metadato>
                                <Metadato id="ISSUER_FIRST_NAME">GIUSEPPE</Metadato>
                                <Metadato id="ISSUER_LAST_NAME">VERDI</Metadato>
                                <Metadato id="ISSUER_FISCAL_CODE">dnjdfr88p69p305t</Metadato>
                                <Metadato id="PROTOCOL_SENDER_IVA_CODE_ID">12345678999</Metadato>
                                <Metadato id="PROTOCOL_SENDER_IVA_COUNTRY_ID">IT</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_ADMIN_CODE">ADMIN5PA1</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_AOO_CODE">AOO5PA1</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_FIRST_NAME">MARIO</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_LAST_NAME">ROSSI</Metadato>
                                <Metadato
                        id="PROTOCOL_RECEIVER_FISCAL_CODE">dnjdfr88p69p305t</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_DENOMINATION">ARANCIA-
                        ICT</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_IVA_CODE_ID">12345678999</Metadato>
                                <Metadato id="PROTOCOL_RECEIVER_IVA_COUNTRY_ID">IT</Metadato>
                        </Metadati>
                        <Hash>346B5E5C2B0A95531679464C55379B0CE732E99D934A8579EFC41BCEC75D2A95<
                /Hash>
                        <URI>doc_amministrativo.pdf</URI>
                </Documento>
        </Documenti>
</Versamento>
```

Categoria documento: Registro Protocollo

Di seguito sono elencati i metadati da associare ad un documento di categoria “registro protocollo” (in particolare sono riportati gli attributi “id” del tag <metadato>). Tutti i metadati sono opzionali, a meno dei metadati per i quali è indicata l’obbligatorietà:

NUMBER
CLOSE_DATE (obbligatorio)
SUBJECT (obbligatorio)
ISSUER_DENOMINATION (obbligatorio se non valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
ISSUER_IVA_CODE_ID (obbligatorio se valorizzato ISSUER_DENOMINATION)
ISSUER_IVA_COUNTRY_ID (obbligatorio se valorizzato ISSUER_IVA_CODE_ID)
ISSUER_FIRST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_LAST_NAME (obbligatorio se non valorizzato ISSUER_DENOMINATION)
ISSUER_FISCAL_CODE (obbligatorio se valorizzati ISSUER_FIRST_NAME e ISSUER_LAST_NAME)
RECEIVER_DENOMINATION
RECEIVER_IVA_COUNTRY_ID
RECEIVER_IVA_CODE_ID
RECEIVER_FISCAL_CODE
RECEIVER_FIRST_NAME
RECEIVER_LAST_NAME
PROTOCOL_REGISTER_ADMINISTRATION_NAME (obbligatorio)
PROTOCOL_REGISTER_ADMIN_CODE (obbligatorio)
PROTOCOL_REGISTER_AOO_CODE
PROTOCOL_REGISTER_RESPONSIBLE_FIRST_NAME (obbligatorio)
PROTOCOL_REGISTER_RESPONSIBLE_LAST_NAME (obbligatorio)
PROTOCOL_REGISTER_RESPONSIBLE_FISCAL_CODE (obbligatorio)
ROTOCOL_REGISTER_SOFTWARE_PRODUCER
PROTOCOL_REGISTER_CODE

PROTOCOL_REGISTER_NUMBER
PROTOCOL_REGISTER_YEAR (obbligatorio)
PROTOCOL_REGISTER_FIRST_REGISTRATION_NUMBER (obbligatorio)
PROTOCOL_REGISTER_LAST_REGISTRATION_NUMBER (obbligatorio)
PROTOCOL_REGISTER_FIRST_REGISTRATION_DATE (obbligatorio)
PROTOCOL_REGISTER_LAST_REGISTRATION_DATE (obbligatorio)

Si riporta un esempio di xml IPdV:

```
<Versamento idVersamento="A1a1a1a1a1-1a1a1a1a1-2a62-8141-bfddcada38e4" versione="V_2_0">
	<CNPClient>
		<Codice>POLLTEST01</Codice>
		<Descrizione></Descrizione>
	</CNPClient>
	<Organizzazione>
		<Descrizione>Test Company</Descrizione>
		<IdFiscale>48542692547</IdFiscale>
	</Organizzazione>
	<SoggettoProduttore>
		<Denominazione>Test Company</Denominazione>
		<IdFiscaleIVA>
			<IdPaese>IT</IdPaese>
			<IdCodice>48542692547</IdCodice>
		</IdFiscaleIVA>
	</SoggettoProduttore>
	<DataCreazione>2017-10-10+02:00</DataCreazione>
	<AnnoCompetenza>2017+01:00</AnnoCompetenza>
	<Descrizione>test registro protocollo</Descrizione>
	<Documenti>
		<Documento id="123456789798">
		<Nome>protocollo20171006081037.pdf</Nome>
		<Categoria>REGISTRO_PROTOCOLLO</Categoria>
		<Tipologia>REGISTRO_PROTOCOLLO</Tipologia>
		<Metadati>
			<Metadato id="NUMBER">12</Metadato>
			<Metadato id="CLOSE_DATE">26/10/2017</Metadato>
			<Metadato id="SUBJECT">Registro Protocollo del 26-10-2017</Metadato>
			<Metadato id="ISSUER_FIRST_NAME">GIUSEPPE</Metadato>
			<Metadato id="ISSUER_LAST_NAME">VERDI</Metadato>
			<Metadato id="ISSUER_FISCAL_CODE">dnjdfr88p69p306t</Metadato>
			<Metadato id="ISSUER_DENOMINATION">ARANCIA-ICT</Metadato>
			<Metadato id="ISSUER_IVA_COUNTRY_ID">IT</Metadato>
			<Metadato id="ISSUER_IVA_CODE_ID">12345678999</Metadato>
			<Metadato id="RECEIVER_DENOMINATION">ARANCIA-ICT</Metadato>
			<Metadato id="RECEIVER_IVA_COUNTRY_ID">IT</Metadato>
			<Metadato id="RECEIVER_IVA_CODE_ID">12345678999</Metadato>
			<Metadato id="RECEIVER_FISCAL_CODE">AAABBB99H22G273P</Metadato>
			<Metadato id="RECEIVER_FIRST_NAME">MARIO</Metadato>
			<Metadato id="RECEIVER_LAST_NAME">ROSSI</Metadato>
			<Metadato id="PROTOCOL_REGISTER_ADMINISTRATION_NAME">ARANCIA-
		ICT</Metadato>
			<Metadato id="PROTOCOL_REGISTER_ADMIN_CODE">ARA_2</Metadato>
			<Metadato id="PROTOCOL_REGISTER_AOO_CODE">AOO99</Metadato>
			<Metadato id="PROTOCOL_REGISTER_RESPONSIBLE_FIRST_NAME">LUCA</Metadato>
			<Metadato id="PROTOCOL_REGISTER_RESPONSIBLE_LAST_NAME">BIANCHI</Metadato>
			<Metadato
		id="PROTOCOL_REGISTER_RESPONSIBLE_FISCAL_CODE">DNSJSC88M65B602K</Metadato>
			<Metadato id="PROTOCOL_REGISTER_SOFTWARE_PRODUCER">PNP - PROTOCOLLO NO
		PROBLEM</Metadato>
			<Metadato id="PROTOCOL_REGISTER_CODE">GH98Y</Metadato>
			<Metadato id="PROTOCOL_REGISTER_NUMBER">98</Metadato>
			<Metadato id="PROTOCOL_REGISTER_YEAR">2015</Metadato>
```

```
                    <Metadato id="PROTOCOL_REGISTER_FIRST_REGISTRATION_NUMBER">17</Metadato>
                    <Metadato id="PROTOCOL_REGISTER_LAST_REGISTRATION_NUMBER">25</Metadato>
                    <Metadato
                id="PROTOCOL_REGISTER_FIRST_REGISTRATION_DATE">26/10/2017</Metadato>
                    <Metadato
                id="PROTOCOL_REGISTER_LAST_REGISTRATION_DATE">26/10/2017</Metadato>
                </Metadati>
                <Hash>9546BE4BEF5117EB5F245A21C33ECAF6F38A19E0BEB8EB53AA066DFE99583DF2</Hash>
                <URI>protocollo20171006081037.pdf</URI>
                </Documento>
        </Documenti>
</Versamento>
```


10.3 Descrizione politiche di conservazione

Codice Politica di conservazione	Descrizione Politica di conservazione
Conservazione Documenti Fiscali	L'insieme dei documenti omogeneo per Tipologia relativi ad un anno fiscale di un soggetto cedente/prestatore di beni/servizi (documenti attivi emessi) o di un soggetto committente (documenti passivi ricevuti) viene conservato entro il termine di tre mesi dalla scadenza prevista per la presentazione della dichiarazione dei redditi annuale (una volta all'anno), e comunque dopo richiesta del Soggetto Produttore. La durata della conservazione dipende dalla tipologia documentale (vedi TABELLA 10.1 Elenco tipologie di documenti sottoposti a conservazione) ed è esplicitata all'interno dell'allegato 'Specificità del Contratto'.
Conservazione Documenti Amministrativi	L'insieme dei documenti omogeneo per Tipologia di un soggetto giuridico viene conservato a richiesta del Soggetto Produttore a seguito della composizione di un Pacchetto di Versamento. Le tempistiche periodiche di conservazione (formazione del Pacchetto di Archiviazione) e la durata della conservazione dipendono strettamente dalla tipologia documentale (vedi TABELLA 10.1 Elenco tipologie di documenti sottoposti a conservazione) e sono esplicitate all'interno dell'allegato 'Specificità del Contratto'. In generale sono in accordo al DPR 445/2000 "Testo Unico sulla documentazione amministrativa" o ai contesti normativi specifici.

Torna al sommario