COMUNE DI SAN FRATELLO

Provincia di Messina

Copia di Deliberazione della Giunta Comunale

N. 181 del Reg. **Data 26.10.2015**	**OGGETTO: APPROVAZIONE MANUALI PER LA GESTIONE DEL PROTOCOLLO INFORMATICO E PER LA GESTIONE DEL FLUSSO DOCUMENTALE E DELL'ARCHIVIO.**

L'anno **duemilaquindici** il giorno **VENTISEI** del mese di OTTOBRE alle ore **16.30** nella sala delle adunanze del Comune suddetto, convocata, con appositi avvisi, la Giunta Comunale, si è riunita in presenza dei Sigg.:

	Amministratore	Carica	Presenze
1	FULIA Dr. FRANCESCO	Sindaco	SI
2	CARROCCETTO Dr. CIRO	Vice Sindaco	SI
3	SALANITRO Avv. LUIGI	Assessore	SI
4	CARRINI Sig.ra ANTONELLA	Assessore	SI

Presenti 4
Assenti 0

Partecipa il Segretario Comunale Dott.ssa Stancampiano Carmela
Il Sindaco, constatato che gli intervenuti sono in numero legale, dichiara aperta la riunione ed invita i convocati a deliberare sull'oggetto sopra indicato.

LA GIUNTA COMUNALE

Vista la legge 8 giugno 1990, n. 142, come recepita con la L.R. 11.12.1991, n. 48;
Vista la L.R. 3 dicembre 1991, n. 44;
Premesso che sulla proposta della presente deliberazione, ai sensi dell'art. 53 della Legge 8 giugno 1990, n. 142, come recepito con l'art. 1, comma 1, lett. i della L.R. n. 48/1991, come modificato con l'art. 12 della L.R. n. 30/2000:
Il responsabile del servizio interessato, per quanto concerne la regolarità tecnica ha espresso parere: Favorevole.

VISTA la proposta di deliberazione che viene allegata alla presente in parte integrante e sostanziale;

RITENUTA la stessa, così come formulata, meritevole di approvazione;

VISTO lo Statuto Comunale;

VISTE le LL.RR. nn.44/91, 7/92, 26/93, 32/94, 23/97, 23/28 e 30/2000

VISTO l'O.A.EE.LL. vigenti in Sicilia,come integrato con la L.R. 11/12/1991, n.48 e successive modifiche ed integrazioni;

Con voti unanimi favorevoli espressi nei modi di legge;

DELIBERA

- Di approvare, così come formulata, l'allegata proposta di deliberazione intendendosi qui integralmente trascritto, ad ogni effetto di legge, il relativo dispositivo;
- Di dichiarare la presente deliberazione immediatamente esecutiva , stante l'urgenza, ai sensi del 2 comma dell'articolo 12 della Legge regionale n. 44/91.

IL SINDACO
F.to Dott.Francesco Fulia

L'ASSESSORE ANZIANO
F.to Dott. Ciro Carroccetto

IL SEGRETARIO COMUNALE
F.to Dott.ssa Stancampiano Carmela

Il sottoscritto Segretario Comunale, visti gli atti d'ufficio,

ATTESTA

Che la presente deliberazione, in applicazione della legge regionale 3 dicembre 1991,n. 44:

- E' stata pubblicata all'Albo pretorio on-line istituito sul sito informatico istituzionale dell'Ente (art. 32 legge n. 69/2009 e art. 12 L.R. n. 5/2011) il giorno_____per rimanervi per quindici giorni consecutivi (art.11, comma 1):

  E' copia conforme all'originale

  Dalla Residenza Municipale, lì _____

IL SEGRETARIO COMUNALE
*F.to **Dott.ssa Stancampiano Carmela***

Il sottoscritto Segretario Comunale, visti gli atti d'ufficio,

ATTESTA

- Che la presente deliberazione, in applicazione della legge regionale 3 dicembre 1991, n. 44, è stata pubblicata all'Albo pretorio on-line per quindici giorni consecutivi dal _____ al _____ come previsto dall'art.11:

E' DIVENUTA ESECUTIVA IL GIORNO 26.10.2015

- ○ Decorsi 10 giorni dalla pubblicazione (Art. 12, comma 2, L.R. n. 44/1991);
- X Dichiarata immediatamente esecutiva ai sensi dell'art. 12, comma 2, L.R. n. 44/1991;

Dalla Residenza Municipale, lì 26.10 .2015

IL SEGRETARIO COMUNALE
F.to Dott.ssa Stancampiano Carmela

E' COPIA CONFORME ALL'ORIGINALE DA SERVIRE PER USO AMMINISTRATIVO

Dalla Residenza Municipale, lì

IL SEGRETARIO COMUNALE

COMUNE DI SAN FRATELLO

PROVINCIA DI MESSINA

PROPOSTA DI DELIBERAZIONE

DA SOTTOPORRE ALLA GIUNTA COMUNALE

OGGETTO	APPROVAZIONE MANUALI PER LA GESTIONE DEL PROTOCOLLO INFORMATICO E PER LA GESTIONE DEL FLUSSO DOCUMENTALE E DELL'ARCHIVIO.

APPROVATA CON DELIBERAZIONE DEL CONSIGLIO COMUNALE

N. 181 DEL 26-10-2015

IL PRESIDENTE

IL SEGRETARIO COMUNALE

Premesso che è già in funzione in questo Comune il Protocollo informatico istituito ai sensi del DPR n. 445/2000 e s.m.i.,

Visti: la Direttiva del 9/12/2002 del Ministro per l'innovazione e le tecnologie, il DPCM 14/10/2003 e il DPCM 03/12/2013 ad oggetto "Regole Tecniche per il protocollo informatico ai sensi degli articoli 40 – bis, 41, 47, 57 – bis e 71 del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005;

Visto il DPCM 13/11/2014 avente ad oggetto "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 del Codice dell'amministrazione digitale di cui al D.Lgs. n. 82/2005;

Visto il *Manuale di Gestione del protocollo informatico dei flussi documentali e degli archivi,* composto da n. 51 articoli, e ritenutolo meritevole di approvazione;

Ritenuto altresì, che occorre uniformarsi alla direttiva per realizzare la sicurezza dei dati, dei documenti e delle tecnologie sulla base delle disposizioni del DPCM del 03.12.2013.

Visto il manuale per il servizio di conservazione composto da n.10 sezioni, redatto dalla Ditta ARANCIA ICT s.r.l. e ritenutolo meritevole di approvazione;

Dato atto che in esecuzione di dette disposizioni il Dirigente dell'Area Amministrativa con determinazione n.142 del 19/10/2015, ha individuato nell'area Amministrativa (AOO) il Responsabile del servizio di Conservazione ed un vicario, per casi di assenza o impedimento, per la tenuta del Protocollo Informatico, della gestione dei flussi documentali e dell'archivio comunale ai sensi dell'art. 61 del D.P.R. n. 445/2000;

Visto l'O.R.EE.LL. della Regione Sicilia e successive modifiche ed integrazioni;

SI PROPONE CHE LA GIUNTA MUNICIPALE

Deliberi:

Per le motivazioni espresse in parte premessa e che qui si intendono integralmente riportate, quanto appresso:

DI APPROVARE:

1) il Manuale di Gestione del Protocollo informatico composto da n. 51 articoli,
2) il Manuale per la gestione del flusso documentale e dell'archivio, redatto dalla Ditta ARANCIA ICT s.r.l. composto da n.10 sezioni, facenti parte integrante e sostanziale del presente atto, nulla avendo da eccepire né in punto di merito né in punto di legittimità;

2) **DI DARE ATTO** che i suddetti Manuali sono strumento di lavoro necessari e pertanto dovranno essere aggiornati allorquando innovazioni tecnologiche, nuove situazioni organizzative o normative lo richiedano o, comunque, ogni qualvolta si renda necessario;

3) **DI PROVVEDERE** alla pubblicazione dei Manuali sul sito internet del Comune;

4) **DI TRASMETTERE** copia della presente ai Responsabili di Area.

San Fratello 19.10.2015

Il Proponente

SERVIZIO ECONOMICO – FINANZIARIO

Il sottoscritto responsabile del servizio economico – finanziario, a norma dell'art. 1 della L.R. 11.12.1991, n. 48 ed in ordine alla proposta di deliberazione che precede

ATTESTA

La copertura finanziaria della spesa con imputazione della stessa all'intervento in conto competenza/residui del bilancio corrente esercizio indicato nella proposta di deliberazione succitata.

San Fratello, lì _____

Il Responsabile del Servizio Finanziario

_____

Ai sensi dell'art.1, comma 1, lettera i) della L.R. 11.12.1991, n. 48, sulla proposta di deliberazione che precede i sottoscritti esprimono i seguenti pareri:

*Il **RESPONSABILE DELL'AREA AMMINISTRATIVA** per quanto concerne la regolarità tecnica esprime parere* favorevole

Data 19/10/2015

Il Responsabile
Saluto

*Il **RESPONSABILE DELL'AREA ECONOMICO FINANZIARIA** per quanto concerne la regolarità contabile esprime parere* _____

Data ___.___.____

Il Responsabile

_____

Manuale di Conservazione

di Arancia-ICT S.r.l.

per il servizio *"Conservazione No Problem"*

Versione 2.5 del 20/07/2015

ARANCIA ICT

Manuale di Conservazione di Arancia-ICT S.r.l.

per il servizio *"Conservazione No Problem"*

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	20/07/2015	Maria Imburgia Antonio Ferraro	Analista Funzionale CAD/Gestione relazioni Clienti Analista Tecnico CAD/ Responsabile funzione Archivistica di conservazione
Verifica	20/07/2015	Francesco Bianco	Responsabile sistemi informativi per la conservazione
Approvazione	20/07/2015	Filippo Ciaravella	Responsabile del Servizio di Conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	5/10/2010	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 sull'indice pubblicato il 16/01/2015 (versione 2)	
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	

ARANCIA ICT

INDICE DEL DOCUMENTO

1 SCOPO E AMBITO DEL DOCUMENTO

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 e al Servizio di Conservazione erogato in *outsourcing* ai Clienti da Arancia-ICT S.r.l. (nel seguito Arancia-ICT).

Inoltre, descrive le procedure e le prassi seguite dal Soggetto Produttore, identificato dal Cliente che conferisce l'incarico in outsourcing al Soggetto Responsabile del servizio di Conservazione che è Arancia-ICT, in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate.

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 documento si applica al servizio denominato ***ConservazioneNoProblem*** fornito in modalità ASP (Application Service Providing) da Arancia-ICT secondo uno schema di *Business Process Outsourcing* (BPO).

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO E ACRONIMI)

Inserire in ordine alfabetico il Glossario dei termini e Acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata. Di seguito si riporta un esempio di tabella.

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.
Application Service Providing	s'intende il servizio erogato attraverso la fruizione di un'applicazione software su Internet senza alcuna installazione sul computer del cliente. (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
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

Termine o acronimo	Significato
	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
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.
Riferimento temporale	Vedi Marca Temporale.
SIC	Sistema Informatico di Conservazione
SLA	È l'acronimo di *Service Level Agreement*, letteralmente Accordo sui Livelli di

Termine o acronimo	Significato
	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

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 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;
- 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.
- 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.
- Torna al sommario

3.2 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;

ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for

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

ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;

ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

Torna al sommario

4 RUOLI E RESPONSABILITA'

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.

4.1 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 la delega per lo svolgimento del servizio di conservazione del Cliente/Soggetto Produttore sono tenuti da Arancia-ICT nell'apposito archivio digitale.

4.2 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 che delega ad Arancia-ICT gli oneri di cui all'art. 7 del DPCM 03/12/2013. I relativi recapiti e i riferimenti amministrativi e anagrafici del referente sono tenuti da Arancia-ICT unitamente a quelli del Cliente/Soggetto Produttore.

4.3 Responsabile del servizio di Conservazione

Il Soggetto Produttore, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM 03/12/2013, ha delegato 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 terzo è Arancia-ICT, Responsabile del servizio di Conservazione ovvero il gestore del servizio di conservazione digitale in outsourcing.

L'atto di affidamento allo svolgimento delle attività del Responsabile del servizio di Conservazione viene conferito dal Soggetto Produttore ad Arancia-ICT 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
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 normativa vigente e verifica periodicamente con il Responsabile dei sistemi informativi per la conservazione la conformità alla normativa e agli standard di riferimento • supervisiona 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 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 di conservazione; • 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.	Dal 1° giugno 2005

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile sistemi informativi per la conservazione	Francesco Bianco (FBI)	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 tecnologiche del sistema di conservazione; • verifica il monitoraggio della corretta funzionalità del sistema di conservazione di concerto con il Responsabile Servizio Clienti 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 Servizio Clienti; • verifica periodicamente con il Responsabile del servizio di Conservazione la conformità alla normativa e agli standard di riferimento.	Dal 1° gennaio 2012
Responsabile funzione Archivistica di conservazione	Antonio Ferraro (AFE)	Svolge le seguenti funzioni: • analizzare il sistema archivistico analogico del Cliente; • acquisire i requisiti del Cliente; • progettare concettualmente il sistema di conservazione digitale e definire le specifiche di realizzazione del sistema; Definizione e gestione del 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, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; - definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici; - monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove	Dal 17 ottobre 2006

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		funzionalità del sistema di conservazione; - collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.	
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 sistema di conservazione) e ne gestisce la conduzione e la manutenzione; • effettua il change management; • si occupa del monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione • Si interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; - • 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 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.	Dal 1° gennaio 2012
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	Dal 1°febbraio 2009

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3/12/2013. In particolare svolge le seguenti funzioni: - Rispetto e monitoraggio dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; - segnalazione delle eventuali difformità al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive.	
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

4.4 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 Produttore stesso, che possono accedere ai documenti conservati o a parte di essi, secondo le politiche di accesso concordate.

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

La figura che segue riporta le strutture organizzative coinvolte nel servizio di conservazione, ovvero l'organigramma del Servizio di Conservazione Digitale di Arancia-ICT, le cui descrizioni sono riportate nel paragrafo successivo.

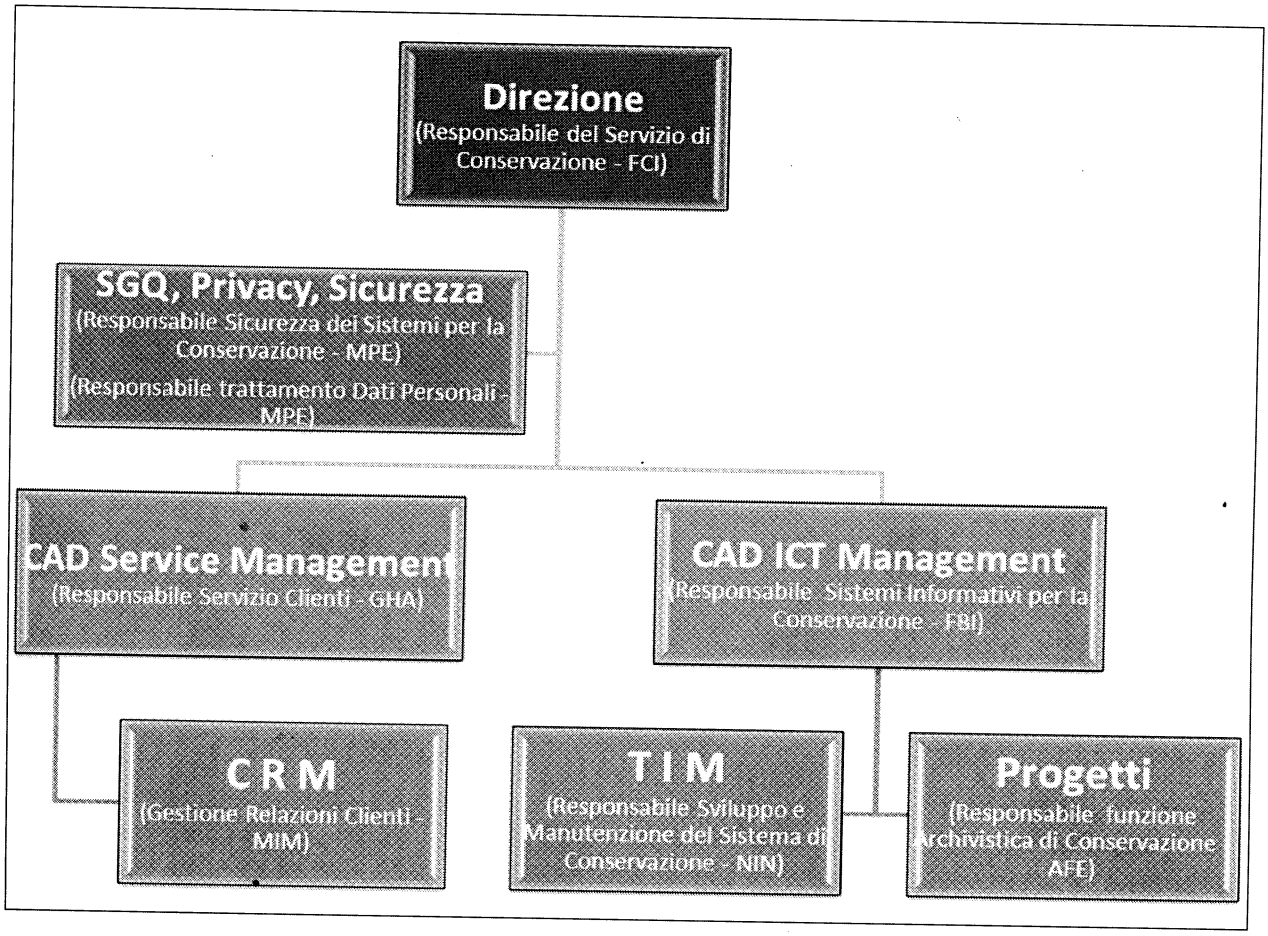

Figura 1 Organigramma

Torna al sommario

5.2 Strutture organizzative del Servizio di Conservazione

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

Direzione: È responsabile della definizione e dell'applicazione delle politiche aziendali

Quality/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;

CAD Service Management: è preposta alla verifica del rispetto dei livelli di servizio e della soddisfazione della clientela, alla verifica dell'operato dei clienti attraverso la piattaforma informatica di erogazione dei vari servizi verso i clienti (tra cui il servizio di conservazione);

CAD ICT Management: 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);

CRM – Customer Relashionship Management: è preposta, insieme al CAD Service Management, all'interazione con la clientela, al supporto dell'operato dei clienti attraverso la piattaforma informatica di erogazione dei vari servizi verso i clienti (tra cui il servizio di conservazione);

TIM – Technology Infrastracture Management: 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);

Progetti: è preposta alla progettazione dei vari sistemi informatici in base ai requisiti specifici dei clienti.

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 RUOLI - PERSONE ATTIVITÀ	Direzione	Quality, Privacy, Sicurezza		CAD Service Management	CAD ICT Management	CRM	TIM	Progetti
	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** - Giulio Hassan (GHA)	**Responsabile Sistemi informativi per la Conservazione** - Francesco Bianco (FBI)	**Gestione Relazioni Clienti** - Maria Imburgia (MIM)	**Responsabile Sviluppo e Manutenzione del Sistema di Conservazione** - Nicola Incandela (NIN)	**Responsabile funzione Archivistica di Conservazione** - Antonio Ferraro (AFE)
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							

STRUTTURE RUOLI - PERSONE / ATTIVITÀ	Direzione	Quality, Privacy, Sicurezza		CAD Service Management	CAD ICT Management	CRM	TIM	Progetti
	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 - Giulio Hassan (GHA)	Responsabile Sistemi informativi per la Conservazione - Francesco Bianco (FBI)	Gestione Relazioni Clienti - Maria Imburgia (MIM)	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione - Nicola Incandela (NIN)	Responsabile funzione Archivistica di Conservazione - Antonio Ferraro (AFE)
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	
Monitoraggio del sistema di conservazione					X		X	

STRUTTURE RUOLI - PERSONE ATTIVITÀ	Direzione	Quality, Privacy, Sicurezza		CAD Service Management	CAD ICT Management	CRM	TIM	Progetti
	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 - Giulio Hassan (GHA)	Responsabile Sistemi informativi per la Conservazione - Francesco Bianco (FBI)	Gestione Relazioni Clienti - Maria Imburgia (MIM)	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione - Nicola Incandela (NIN)	Responsabile funzione Archivistica di Conservazione - Antonio Ferraro (AFE)
Change management					X		X	
Verifica periodica di conformità a normativa e standard di riferimento	X	X			X			
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

STRUTTURE RUOLI - PERSONE ATTIVITÀ	Direzione	Quality, Privacy, Sicurezza		CAD Service Management	CAD ICT Management	CRM	TIM	Progetti
	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 - Giulio Hassan (GHA)	Responsabile Sistemi informativi per la Conservazione - Francesco Bianco (FBI)	Gestione Relazioni Clienti - Maria Imburgia (MIM)	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione - Nicola Incandela (NIN)	Responsabile funzione Archivistica di Conservazione - Antonio Ferraro (AFE)
Change management					X		X	
Verifica periodica di conformità a normativa e standard di riferimento	X	X			X			
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

STRUTTURE RUOLI - PERSONE ATTIVITÀ	Direzione	Quality, Privacy, Sicurezza		CAD Service Management	CAD ICT Management	CRM	TIM	Progetti
	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 - Giulio Hassan (GHA)	Responsabile Sistemi informativi per la Conservazione - Francesco Bianco (FBI)	Gestione Relazioni Clienti - Maria Imburgia (MIM)	Responsabile Sviluppo e Manutenzione del Sistema di Conservazione - Nicola Incandela (NIN)	Responsabile funzione Archivistica di Conservazione - Antonio Ferraro (AFE)
Definizione delle modalità di trasferimento da parte dell'ente produttore, descrizione archivistica dei documenti e delle aggregazioni documentali								X

Torna al sommario

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 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. 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 nelle due tabelle presenti al capitolo *10.1 - Elenco tipologie di documenti sottoposti a conservazione*.

Torna al sommario

6.2 Pacchetto di versamento

Il Pacchetto di Versamento (PdV) viene creato a cura del Soggetto Produttore in modo diverso a seconda delle specifiche di contratto. Si individuano due macro modalità:

- Fattura Elettronica PA e relativa Ricevuta;
- 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 di ciascun documento contenuto nel pacchetto.

Torna al sommario

6.2.1 Fattura Elettronica PA e relativa Ricevuta

Il PdV viene conferito attraverso collegamento automatico con un sistema di fatturazione elettronica PA, quale ad esempio FNP-FatturaNoProblem erogato da Arancia-ICT, Contabilità

Facile erogato da Geritec S.r.l., Fattura-PA erogato da Echo Sistemi S.r.l. o altri sistemi per i quali è stata realizzata apposita interfaccia informatica di collegamento.

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 cap. *10.2-Descrizione politiche di conservazione*, attraverso apposita funzione/procedura informatica automatica trasmette ad Arancia-ICT il PdV costituito dall'insieme delle fatture e dall'insieme delle ricevute 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;

- 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.

Torna al sommario

6.2.2 Altre Tipologie di Documenti

Le "altre Tipologie di Documenti" sono rappresentate da:

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

Salvo quanto previsto dai contratti specifici, il PdV viene creato a cura del Soggetto Produttore attraverso alcuni semplici passaggi eseguiti sulla piattaforma informatica che Arancia-ICT mette a disposizione dei propri clienti:

Fase di conferimento:

- **Upload del documento informatico** da sottoporre a conservazione, nel formato file specifico per ogni tipologia di documento (v. capitolo *10.1 - Elenco tipologie di documenti sottoposti a conservazione);*
- **Inserimento dei metadati specifici per tipo documento** (v. capitolo 10.1 - Elenco tipologie di documenti sottoposti a conservazione).

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

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;
- 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.

Torna al sommario

6.3 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 secondo le modalità riportate nel presente manuale di conservazione.

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:

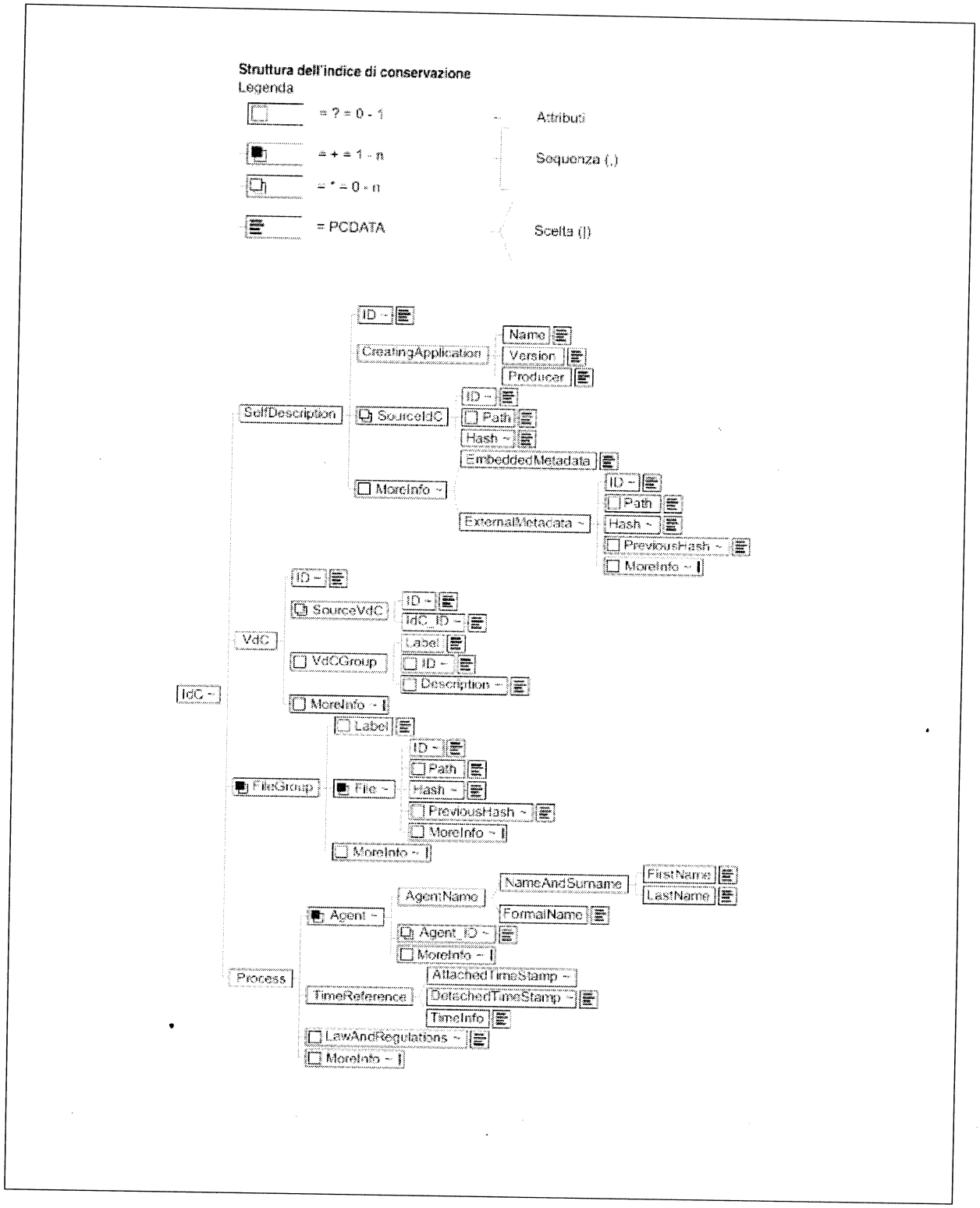

Figura 2 Struttura dell'Indice di Conservazione (IPdA)

L'IPdA è l'evidenza informatica nel formato XML associata ad ogni PdA, contenente un insieme di informazioni descritte nelle regole tecniche in materia, 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 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, sarà di volta in volta definito nel dettaglio in fase contrattuale col Produttore: ovvero i contenuti degli elementi "moreinfo" verranno 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:

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

    <xs:complexType name="DocumentiType">
        <xs:annotation>
            <xs:documentation>
                Contenitore 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 i
                    documenti di rilevanza fiscale
                </xs:documentation>
            </xs:annotation>

            <xs:sequence>
                <xs:element name="NomeFile" type="xs:string" />
                <xs:element name="Categoria" type="CategoriaEnumType" minOccurs="0" />
                <xs:element  name="TipoDocumento"  type="TipoDocumentoEnumType"  minOccurs="0"
/>
                <xs:element name="Numero" type="String20Type" minOccurs="0" />
                <xs:element name="DataChiusura" type="xs:date" minOccurs="0" />
                <xs:element name="OggettoDocumento" type="xs:string" minOccurs="0" />
                <xs:element name="SoggettoProduttore" type="AnagraficaType" minOccurs="0" />
                <xs:element name="Destinatario" type="AnagraficaType" minOccurs="0" />
                <xs:element name="Protocollo" type="ProtocolloType" minOccurs="0" />
                <xs:element name="AnnoCompetenza" type="xs:gYear" />
            </xs:sequence>
            <xs:attribute name="idDocumento" type="xs:string" use="required" />
        </xs:complexType>

        <xs:simpleType name="CategoriaEnumType">
            <xs:restriction base="xs:string">
                <xs:enumeration value="privato">
                    <xs:annotation>
                        <xs:documentation>Documenti                    Operatori
Economici</xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
                <xs:enumeration value="amministrativo">
                    <xs:annotation>
                        <xs:documentation>Documenti Pubbliche Amministrazioni
                        </xs:documentation>
                    </xs:annotation>
                </xs:enumeration>
            </xs:restriction>
        </xs:simpleType>
```

```
<xs:complexType name="AnagraficaType">
        <xs:sequence>
                <xs:element name="Denominazione" type="xs:string" minOccurs="0" />
                <xs:element name="IdFiscaleIVA" type="IdFiscaleType" minOccurs="0" />
                <xs:element name="Nome" type="xs:string" minOccurs="0" />
                <xs:element name="Cognome" type="xs:string" minOccurs="0" />
                <xs:element name="CodiceFiscale" type="xs:string" minOccurs="0" />
        </xs:sequence>
</xs:complexType>
<xs:complexType name="IdFiscaleType">
        <xs:sequence>
                <xs:element name="IdPaese" type="NazioneType" default="IT" />
                <xs:element name="IdCodice" type="CodiceType" />
        </xs:sequence>
</xs:complexType>
<xs:simpleType name="CodiceType">
        <xs:restriction base="xs:string">
                <xs:minLength value="1" />
                <xs:maxLength value="28" />
        </xs:restriction>
</xs:simpleType>
<xs:simpleType name="NazioneType">
        <xs:restriction base="xs:string">
                <xs:pattern value="[A-Z]{2}" />
        </xs:restriction>
</xs:simpleType>
<xs:simpleType name="CodiceFiscaleType">
        <xs:restriction base="xs:string">
                <xs:pattern value="[A-Z0-9]{16}" />
        </xs:restriction>
</xs:simpleType>
<!-- String types -->
<xs:simpleType name="String10Type">
        <xs:restriction base="xs:normalizedString">
                <xs:pattern value="(\p{IsBasicLatin}{1,10})" />
        </xs:restriction>
</xs:simpleType>
<xs:simpleType name="String15Type">
        <xs:restriction base="xs:normalizedString">
                <xs:pattern value="(\p{IsBasicLatin}{1,15})" />
        </xs:restriction>
```

```
</xs:simpleType>
<xs:simpleType name="String20Type">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin}{1,20})" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String35Type">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin}{1,35})" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String60Type">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin}{1,60})" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String80Type">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin}{1,80})" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String100Type">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="(\p{IsBasicLatin}{1,100})" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String60LatinType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="[\p{IsBasicLatin}\p{IsLatin-1Supplement}]{1,60}" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String80LatinType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="[\p{IsBasicLatin}\p{IsLatin-1Supplement}]{1,80}" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String100LatinType">
	<xs:restriction base="xs:normalizedString">
		<xs:pattern value="[\p{IsBasicLatin}\p{IsLatin-1Supplement}]{1,100}" />
	</xs:restriction>
</xs:simpleType>
<xs:simpleType name="String200LatinType">
```

```
            <xs:restriction base="xs:normalizedString">
                <xs:pattern value="[\p{IsBasicLatin}\p{IsLatin-1Supplement}]{1,200}" />
            </xs:restriction>
        </xs:simpleType>
        <xs:simpleType name="String1000LatinType">
            <xs:restriction base="xs:normalizedString">
                <xs:pattern value="[\p{IsBasicLatin}\p{IsLatin-1Supplement}]{1,1000}" />
            </xs:restriction>
        </xs:simpleType>
        <!-- Pubblica Amminitrazione Types -->
        <xs:complexType name="AmministrazioneType">
            <xs:sequence>
                <xs:element ref="CodiceAmministrazione" />
                <xs:element ref="CodiceAOO" />
            </xs:sequence>
        </xs:complexType>
        <xs:element name="Amministrazione" type="AmministrazioneType" />

        <xs:complexType name="ProtocolloType">
            <xs:sequence>
                <!-- Set previsto D.P.C.M. 31 ottobre 2000 art.9 -->
                <xs:element ref="Amministrazione" />
                <xs:element ref="CodiceRegistro" />
                <xs:element ref="NumeroRegistrazione" />
                <xs:element ref="DataRegistrazione" />

                <!-- Set previsto D.P.C.M. 31 ottobre 2000 art.19 -->
                <xs:element ref="Mittente" />
                <xs:element ref="Destinatario" minOccurs="0" maxOccurs="unbounded" />
            </xs:sequence>
        </xs:complexType>

        <xs:element name="CodiceAmministrazione" type="xs:string" />
        <xs:element name="CodiceAOO" type="xs:string" />
        <xs:element name="CodiceRegistro" type="xs:string" />
        <xs:element name="NumeroRegistrazione" type="xs:string" />
        <xs:element name="DataRegistrazione" type="xs:date" />

        <xs:complexType name="ProtocolloAnagraficaType">
            <xs:choice>
                <xs:element ref="Amministrazione" />
                <xs:element name="Anagrafica" type="AnagraficaType" />
```

```
        </xs:choice>
    </xs:complexType>
    <xs:element name="Mittente" type="ProtocolloAnagraficaType" />
    <xs:element name="Destinatario" type="ProtocolloAnagraficaType" />

    <xs:simpleType name="TipoDocumentoEnumType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="FattureElettronicheEmesse" />
            <xs:enumeration value="FattureElettronicheRicevute" />
            <xs:enumeration value="FattureEmesse" />
            <xs:enumeration value="FattureRicevute" />
            <xs:enumeration value="NotaVariazioneAumento" />
            <xs:enumeration value="NotaVariazioneDiminuzione" />
            <xs:enumeration value="DocumTrasporto" />
            <xs:enumeration value="Scontrino" />
            <xs:enumeration value="Ricevuta" />
            <xs:enumeration value="Bolla" />
            <xs:enumeration value="LibroGiornale" />
            <xs:enumeration value="LibroInventari" />
            <xs:enumeration value="LibroMastro" />
            <xs:enumeration value="RegistroCronologico" />
            <xs:enumeration value="LibroCespiti" />
            <xs:enumeration value="RegistroIrpef" />
            <xs:enumeration value="RegistroFattureAcquisto" />
            <xs:enumeration value="RegistroAcquistiAgenzieViaggio" />
            <xs:enumeration value="RegistroFattureEmesse" />
            <xs:enumeration value="RegistroFattureInSospeso" />
            <xs:enumeration value="RegistroCorrispettivi" />
            <xs:enumeration value="GiornaleFondo" />
            <xs:enumeration value="RegistroCorrispettiviAgenzieViaggio" />
            <xs:enumeration value="RegistroEmergenzaIva" />
            <xs:enumeration value="Bollettario" />
            <xs:enumeration value="RegistroPrimaNota" />
            <xs:enumeration value="RegistroUnicoIva" />
            <xs:enumeration value="RegistroRiepilogativoIva" />
            <xs:enumeration value="RegistroSezionaleIvaAcquisitiIntraUe" />
            <xs:enumeration value="RegistroAcquistiIntraUeNonComm" />
            <xs:enumeration value="RegistroTrasferimentiIntraUe" />
            <xs:enumeration value="RegistroDichIntentiEmesse" />
            <xs:enumeration value="RegistroDichIntentiRicevute" />
            <xs:enumeration value="RegistroOmaggi" />
            <xs:enumeration value="RegistroMemoriaProdContrassegno" />
```

```
<xs:enumeration value="RegistroLavorazioneProdContrassegno" />
<xs:enumeration value="RegistroCaricoProdContrassegno" />
<xs:enumeration value="RegistroScaricoProdContrassegno" />
<xs:enumeration value="RegistroBeniInDeposito" />
<xs:enumeration value="RegistroBeniInContoLavorazione" />
<xs:enumeration value="RegistroBeniComodato" />
<xs:enumeration value="RegistroBeniProva" />
<xs:enumeration value="RegistroSezionaleIvaInterno" />
<xs:enumeration value="RegistroCaricoStampatiFiscali" />
<xs:enumeration value="RegistroSocControllantiControllate" />
<xs:enumeration value="RegistroCaricoScaricoRegimeMargineMetodoAnalitico" />
<xs:enumeration value="RegistroAcquistiRegimeMargineMetodoGlobale" />
<xs:enumeration value="RegistroVenditeRegimeMargineMetodoGlobale" />
<xs:enumeration value="RegistroCaricoCentriElabDati" />
<xs:enumeration value="RegistroScaricoCentriElabDati" />
<xs:enumeration value="RegistroSommeRicevuteDeposito" />
<xs:enumeration value="RegistroEditori" />
<xs:enumeration value="LibroSoci" />
<xs:enumeration value="LibroObbligazioni" />
<xs:enumeration value="LibroAdunanzeDelibAssemblee" />
<xs:enumeration value="LibroAdunanzeDelibConsiglioAmministrazione" />
<xs:enumeration value="LibroAdunanzeDelibCollegioSindacale" />
<xs:enumeration value="LibroAdunanzeDelibComitatoEsecutivo" />
<xs:enumeration value="LibroAdunanzeDelibAssembleeAzionisti" />
<xs:enumeration value="AltriRegistri" />
<xs:enumeration value="UnicoPersoneFisiche" />
<xs:enumeration value="UnicoSocietaPersone" />
<xs:enumeration value="UnicoSocietaCapitale" />
<xs:enumeration value="UnicoEntiNonCommerciali" />
<xs:enumeration value="IrapPersoneFisiche" />
<xs:enumeration value="IrapSocietaPersone" />
<xs:enumeration value="IrapSocietaCapitale" />
<xs:enumeration value="IrapEntiNonCommercialiEdEquiparati" />
<xs:enumeration value="IrapAmministrazioniEdEntiPubblici" />
<xs:enumeration value="Modello730" />
<xs:enumeration value="ModelloConsolidatoNazionaleEMondiale" />
<xs:enumeration value="ModelloIva" />
<xs:enumeration value="ModelloIvaVrRichiestaRimborsoCreditoIva" />
<xs:enumeration value="ModelloIva26Lp2006ProspettoLiquidazioniPeriodiche" />
<xs:enumeration value="ModelloIva74Bis" />
<xs:enumeration value="ComunicazioneAnnualeDatiIva" />
<xs:enumeration value="ModelloRichiestaRimborsoCreditoIvaTrimestrale" />
```

```
                    <xs:enumeration value="ModelloDatiContenutiDichiarazioneIntentoRicevute" />
                    <xs:enumeration value="Modello770Semplificato" />
                    <xs:enumeration value="Modello770Ordinario" />
                    <xs:enumeration value="ModelloCertificazioneCud" />
                    <xs:enumeration value="ModelloF23" />
                    <xs:enumeration value="ModelloF24" />
                    <xs:enumeration value="ModelliAllegatiDichiarazioneRedditiModelloUnico" />
                    <xs:enumeration value="ModelliAnnotazioneSeparata" />
                    <xs:enumeration value="RicevutaPresentazioneModelliDichiarazione" />
                    <xs:enumeration value="AltriDocumenti" />
                </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:

  - 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, ovverol'***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 rimanare 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***[1], 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

[1] Sarebbe il ruolo corrispondente al Responsabile della conservazione.

- 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">XXXXXXXXXXXXXXXXXXXXX</sincro:ID>
   <!-- ID tipologia -->
```

```
      <sincro:Description sincro:language="IT">lotto di Fatture elettroniche PA di <Nome Azienda></sincro:Description>
    </sincro:VdCGroup>
  </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

6.4 Pacchetto di distribuzione

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

- i documenti 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

7 IL PROCESSO DI CONSERVAZIONE

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

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

7.1.1 Fatture Elettroniche PA e relative Ricevute gestite da procedure integrate

Queste tipologie di documenti vengono conferiti attraverso collegamento automatico con uno dei sistemi di fatturazione elettronica PA "integrati" con il servizio ***Conservazione No Problem*** (cfr. *6.2.1-Fattura Elettronica PA e relativa Ricevuta*).

Il PdV viene creato automaticamente dal sistema di fatturazione elettronica PA su input del responsabile del servizio e viene preso in carico dal Sistema Informatico di Conservazione (SIC) per le successive elaborazioni. 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;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

Torna al sommario

7.1.2 Altre Tipologie di Documenti

Il sistema dispone di un'interfaccia web tramite la quale il Cliente o Soggetto Produttore procede alla composizione del pacchetto di versamento caricando sul sistema, attraverso operazione di *upload*, i documenti in uno dei formati previsti (cfr.*10.1-Elenco tipologie di documenti sottoposti a conservazione*) e compilando manualmente i metadati associati. Specifici contratti possono prevedere il conferimento tramite sistemi diversi dall'upload (stampante virtuale, web-service, FTP, etc.).

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.

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;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

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

Torna al sommario

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

Il PdV ricevuto viene sottoposto alle seguenti verifiche:

1. identificazione del soggetto produttore;
2. verifica del formato dei documenti contenuti nel PdV mediante attivazione della specifica routine di controllo, eventualmente personalizzata per cliente a valle della contrattualizzazione del servizio.

Torna al sommario

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

Superate le verifiche, il PdV è considerato accettato dal SIC, viene quindi generato il Rapporto di Versamento (RdV) – 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 (sarà OK in caso di RdV di accettazione) con l'eventuale codice dell'anomalia riscontrata (in caso di rifiuto – vedi paragrafo successivo):

- Numero identificativo univoco del RdV;
- Data RdV;
- Esito RdV (Positivo-OK / Negativo-KO + Codice Anomalia);
- 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[2] dal Responsabile del servizio di Conservazione se previsto dal contratto stipulato con il cliente; viene reso disponibile al Cliente tramite l'applicazione Web per la consultazione ed inviato allo stesso tramite e-mail/PEC se previsto dallo specifico contratto.

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. 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;

[2] 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

- Data e ora dell'attività di verifica.

Torna al sommario

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

Il PdV che non supera le verifiche viene rifiutato dal SIC che provvede alla generazione di un Rapporto di versamento 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 sarà KO e all'interno dell'XML che costituisce la NdR saranno indicati anche i codici delle anomalie riscontrate.

Le possibili anomalie che determinano il rifiuto del PdV sono elencate di seguito:

- 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[3] dal Responsabile del servizio di Conservazione se previsto dal contratto stipulato con il cliente.

Tale notifica viene resa disponibile al Cliente tramite l'applicazione Web per la consultazione e inviata via e-mail/PEC se previsto dallo specifico contratto. Il PdV rifiutato viene riaperto dal Sistema in modo che il Cliente possa apportare le necessarie modifiche.

Il SIC produce specifica registrazione su file di log dell'operazione di rifiuto del PdV riportandone il motivo nella sezione Motivo dello Scarto; inoltre i PdV rifiutati insieme alle NdR associate vengono opportunamente archiviate/conservate e vanno a comporre il registro dei PdV rifiutati. Il sistema in sostanza consente la memorizzazione su Storage e/o su DB dei PdV ricevuti e rifiutati e delle relative NdR.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di Archiviazione

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 della Conservazione (firma digitale di tipo 'attached') e sottoposto a marcatura temporale (marca temporale di tipo 'attached').

L'indice del PdA (IdPA o IdC) contenente i metadati e le impronte (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 6.3 Pacchetto di archiviazione.

L'accesso al Repository è garantito al Cliente senza soluzione di continuità 24 X 7, attraverso collegamento web con credenziali private.

Il SIC produce registrazione sul file di log 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;

[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

- Il dettaglio dell'operazione eseguita;
- Il riferimento temporale dell'inizio e del termine dell'operazione.

La gestione del PdA include la verifica di congruenza e di integrità degli archivi contenuti. 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.

Torna al sommario

7.6 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 (solo personale autorizzato del soggetto Produttore in possesso di credenziali di autenticazione personali) è rappresentato dal servizio FNP o CNP.

In risposta ad un ordinativo (richiesta dell'Utente) tramite l'interfaccia 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 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 un media – supporto fisico rimovibile- (DVD/M-DISC) 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;
    - i dati trasmessi saranno protetti con sistemi crittografici.

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 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 descritta nel paragrafo precedente per il PdA.

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.

Torna al sommario

7.7 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).

In alternativa, il Cliente (o la *Pubblica Autorità*) può richiedere ad Arancia-ICT la fornitura di un *media* - supporto fisico rimovibile - (DVD/M-DISC) contenente una o più copie informatiche di un PdA. In questo caso i dati trasmessi saranno protetti con sistemi crittografici.

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. Si evidenzia che la scelta di formati idonei, previsti e consigliati dalla normativa vigente (ad esempio il formato PDF/A) è la scelta 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 richiedere 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.

Torna al sommario

7.8 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.

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

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

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 su supporto ottico (CD/DVD) e i dati così trasmessi saranno protetti con sistemi crittografici.

La conformità del file di indice del Pacchetto di archiviazione allo standard UNI 11386:2010 – SInCRO ne garantisce l'interoperabilità con tutti gli altri sistemi di conservazione aderenti alle disposizioni del DPCM 3 dicembre 2013.

Si segnala che il sistema *ConservazioneNoProblem* di Arancia ICT è in grado di acquisire ovvero prendere in carico pacchetti di versamento coincidenti con i pacchetti di archiviazione di altri conservatori purchè conformi con la struttura UNI SINCRO 11386:2010 e secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettera h) nel caso di subentro su archivi gestiti da altro conservatore che abbia adottato tale standard per la generazione dell'IPdA.

Torna al sommario

8 IL SISTEMA DI CONSERVAZIONE

8.1 Luogo di conservazione dei documenti informatici

L'infrastruttura sottesa all'erogazione del servizio 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, mentre il sito di conservazione di Backup/Disaster Recovery (datacenter secondario in 'Housing') si trova a Milano.

Torna al sommario

8.2 Componenti Logiche

Il Sistema di Conservazione (SIC) di Arancia-ICT è costituto da tre componenti principali così come mostrato nella figura seguente.

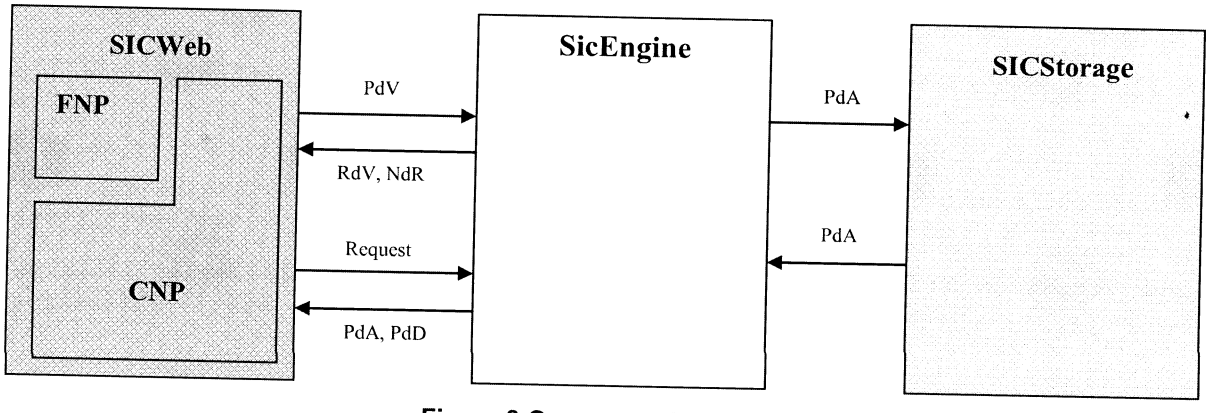

Figura 3 Componenti logiche

Il componente **SICWeb** rappresenta il *layer* di presentazione del sistema, esso a sua volta è costituito dal sottosistema FNP (Fattura No Problem) per la fatturazione elettronica alla P.A. e dal sottosistema CNP (Conservazione No Problem) che rappresenta il modulo di *Front End* principale.

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.

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.

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

8.3 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 ed confacente allo standard ORM (*Object-Relational Mapping*), ovvero del tutto disaccoppiato dal RDBMS (*Relational DataBase Management System*).

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

8.4 Componenti Fisiche

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:

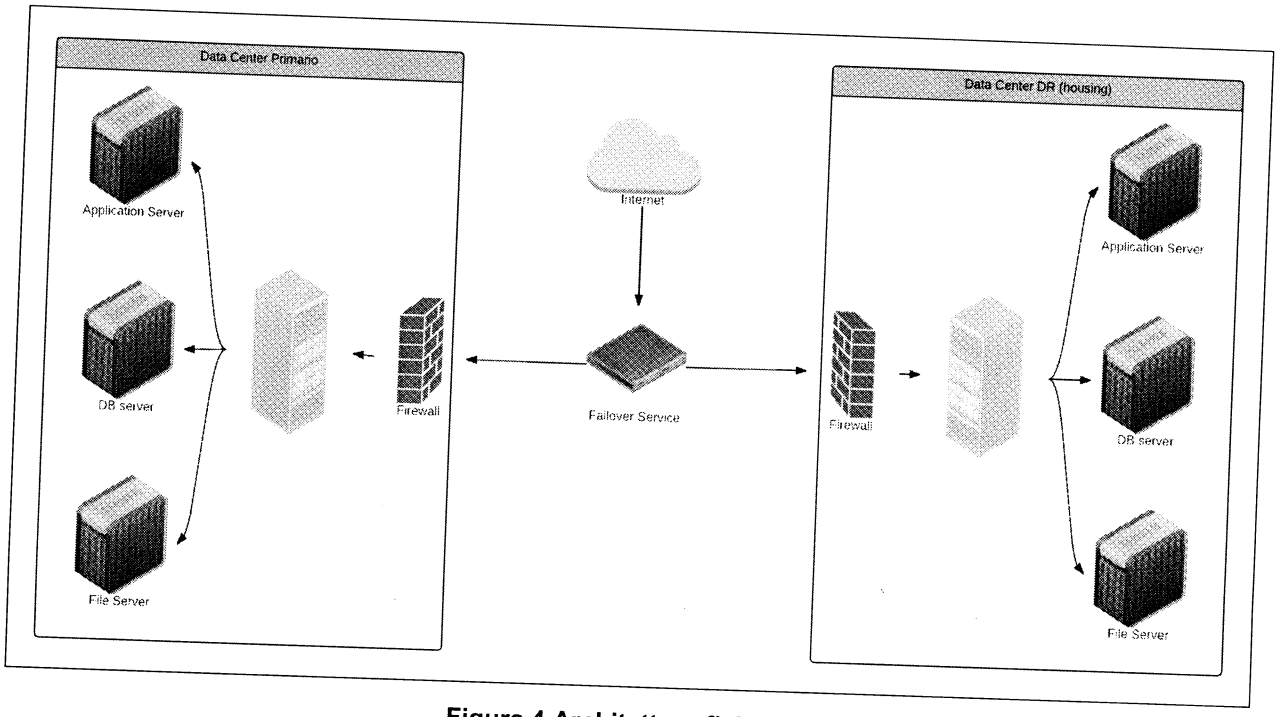

Figura 4 Architettura fisica

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 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
Failover Service	Questo componente di occupa dei Servizi di failover: 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 ISO/IEC 27001:2014.

Torna al sommario

8.5 Procedure di gestione e di evoluzione

L'unità operativa *CAD/ICT Management* 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 sistemi che concorrono alla composizione del Sistema di Conservazione, sia fisici (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.

La conformità alla normativa e agli standard di riferimento viene verificata periodicamente dal Responsabile della Conservazione di concerto con la funzione *CAD/ICT Management*, che in collaborazione con la funzione *CAD Service Management* ne progetta l'eventuale *change management*.

Torna al sommario

9 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.

Torna al sommario

9.1 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:

- **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. 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*).

- **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*.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

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.
In particolare il SIC prevede una pianificazione ed esecuzione di un processo di verifica che assicuri l'integrità, e leggibilità 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.

Ad ogni ciclo di verifica periodica dell'integrità degli Archivi di Conservazione viene generato un report attestante l'esito della verifica effettuata. Ogni ciclo di verifica viene registrato sul sistema di CNP riportante i dati di riferimento temporale e l'oggetto del processo di Verifica, ovvero l'identificativo univoco dell'archivio e del suo PdA. Il processo di verifica viene eseguito annualmente ed ha per oggetto i documenti conservati non oltre i cinque anni. Attraverso le informazioni memorizzate all'interno del DB di CNP vengono stabilite le date di scadenza entro le quali eseguire i controlli di verifica di leggibilità per ogni archivio conservato.

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. In particolare, al verificarsi di eventuali errori viene mandata una comunicazione via email al Responsabile del servizio di conservazione e ai suoi delegati contenente i dettagli dell'errore riscontrato. Tutti i log del SIC di Arancia, compreso quello derivante dalle operazioni di verifica di integrità vengono archiviati/conservati nel sistema stesso.

Torna al sommario

9.3 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 dal CRM[4] viene tracciata nel sistema di *trouble-ticketing* di Arancia-ICT, viene impostata una priorità ed assegnata all'area di competenza per la risoluzione;
        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. 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. 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).

[4] il CRM prende in carico la segnalazione dell'*incident*, che può provenire dal Soggetto produttore o dai sistemi, 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). 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.

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

2. Anomalia Dati

L'anomalia viene recepita dal Service desk 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: 9.2 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, 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	Fattura emessa o ricevuta, inviata o ricevuta dal Sistema d'Interscambio	Conservazione Documenti Fiscali (v. cap. 10.2- 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 - Numero Fattura - Data Fattura	xml.p7m (XML signed - firmato digitalmente con firma di tipo 'attached' signature)
Fiscale	Ricevute Fattura Elettronica PA	Notifica ricevuta dal Sistema d'Interscambio	Conservazione Documenti Fiscali (v. cap. 10.2- 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 - Numero Fattura cui si riferisce la ricevuta - Data Fattura cui si riferisce la ricevuta	xml (XML signed – con firma digitale di tipo xml signature)

[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
Fiscale	Documento analitico emesso/ricevuto in riferimento ad una transazione	Fattura Ricevuta, Fattura Emessa, Documento di Trasporto Emesso, Documento di Trasporto Ricevuto, Quietanza Modello F24	Conservazione Documenti Fiscali (v. cap. 10.2- 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 - Numero Fattura (o documento) - Data Fattura (o documento)	.pdf (PDF o PDF/A)
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,	Conservazione Documenti Fiscali (v. cap. 10.2- DESCRIZIONE POLITICHE DI CONSERVAZIONE)	- METADATI MINIMI DEL DOCUMENTO INFORMATICO (All. 5 DPCM 3/12/2013) + - Anno Fiscale	.pdf (PDF o PDF/A)
Amministrativa	Documento analogico	Lettera, comunicazione, corrispondenza in	Conservazione Documenti Amministrativi	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM	.pdf (PDF o PDF/A)

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
	non unico	ingresso o in uscita	(v. cap. 10.2- DESCRIZIONE POLITICHE DI CONSERVAZIONE	3/12/2013)	
Amministrativa	Documento digitale non unico	Lettera, comunicazione, corrispondenza in ingresso o in uscita	Conservazione Documenti Amministrativi (v. cap. 10.2- Descrizione politiche di conservazione	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	.pdf (PDF o PDF/A)
Amministrativa	Documento analogico unico	Contratti, delibere 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. 10.2- Descrizione politiche di conservazione	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	pdf.p7m (PDF o PDF/A signed - firmato digitalmente con firma di tipo 'attached' signature)

Natura	Tipologia Documento	Note ed esempi documentali	Politica di conservazione	Metadati	Formato file
Amministrativa	Documento digitale unico	Contratti , delibere e simili a firma digitale	Conservazione Documenti Amministrativi (v. cap. 10.2- DESCRIZIONE POLITICHE DI CONSERVAZIONE	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	pdf.p7m (PDF o PDF/A signed - firmato digitalmente con firma di tipo 'attached' signature)
Amministrativa	Messaggio di Posta Elettronica Certificata – PEC + notifiche: accettazione e avvenuta consegna		Conservazione Documenti Amministrativi (v. cap. 10.2- DESCRIZIONE POLITICHE DI CONSERVAZIONE	- METADATI MINIMI DEL DOCUMENTO AMMINISTRATIVO (All. 5 DPCM 3/12/2013)	.eml
Fiscale **Amministrativa**	Fascicolo	Aggregazione documentale informatica (documenti di natura Fiscale o Amministrativa)	Conservazione Documenti Fiscali (v. cap. 10.2- DESCRIZIONE POLITICHE DI CONSERVAZIONE) Conservazione Documenti Amministrativi (v. cap. 10.2- 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 Pacchetti 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	ISO32000-1
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	Vari	EML	n.d.	.eml	message/rfc822	RFC2822

[6] Nel caso di formato PDF e comunque In tutti i casi riportati in tabella, il produttore dei documenti si impegna a versare al 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.

elettronica che supportano la visualizzazione di file eml		(Email)				RFC 5322

Torna al sommario

10.2 Descrizione politiche di conservazione

Codice Politica di conservazione	Descrizione Politica di conservazione
Conservazione Documenti Fiscali	L'insieme dei documenti omogeneo per Tipologia di un soggetto cedente/prestatore di beni/servizi relativi ad un anno fiscale viene mandato in conservazione in unica soluzione entro il termine di tre mesi dalla scadenza prevista per la presentazione della dichiarazione annuale, e comunque dopo richiesta del Soggetto Produttore.
Conservazione Documenti Amministrativi	L'insieme dei documenti omogeneo per Tipologia di un soggetto giuridico viene mandato in conservazione a richiesta del Soggetto Produttore tramite composizione di un Pacchetto di Versamento.

Torna al sommario

COMUNE DI SAN FRATELLO

Manuale di gestione del protocollo informatico dei flussi documentali e degli archivi

Indice

PREMESSA

Il presente manuale recepisce le indicazioni contenute nel D.P.R. 445/2000, Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, e rappresenta la sintesi del lavoro progettuale compiuto dall'amministrazione.

Nell'ambito della normativa vigente l'Amministrazione per motivi organizzativi ed economici ha ritenuto opportuno procedere alla realizzazione del protocollo informatico ed alla gestione documentale per gradi, soprassedendo, durante una prima fase di avvio del servizio informatizzato, sia sull'archiviazione ottica sostitutiva che sulla gestione automatica dei documenti ricevuti e spediti direttamente in formato elettronico.

In considerazione di quanto premesso i documenti che saranno archiviati in forma ufficiale continueranno ad essere cartacei anche se la circolazione degli stessi all'interno degli uffici, nonché la loro produzione, gestione e protocollazione avverrà attraverso l'uso del sistema informatico.

Di conseguenza, finchè l'intero servizio non sarà completamente informatizzato e non sarà adottato l'utilizzo della firma digitale per gli adempimenti ad essa connessi, i documenti pervenuti attraverso la casella di posta elettronica certificata istituzionale adibita alla protocollazione dei messaggi ricevuti (ed il cui indirizzo è riportato nell'indice delle amministrazioni pubbliche), eventualmente anche firmati digitalmente, saranno accettati mediante provvedimento del responsabile del servizio di protocollo che firmerà per l'autenticità una stampa degli stessi. Allo stesso modo eventuali documenti elettronici firmati digitalmente e pervenuti a caselle di posta elettronica a disposizione dei vari settori di attività, saranno stampati e protocollati solo se debitamente autorizzati sia dal responsabile di settore che dal responsabile del protocollo.

In un prossimo futuro, dopo che i nuovi meccanismi di gestione saranno stati assimilati e verificati, l'Amministrazione si riserva di operare un ulteriore sforzo organizzativo ed economico per proseguire sulla strada dell'automazione optando per la definitiva eliminazione della carta. Contestualmente si renderà necessario apportare le opportune modifiche al presente Manuale.

CAPO I

Definizioni ed ambito di applicazione

Art. 1 Definizioni

a. ***documento amministrativo:*** ogni rappresentazione informatica, grafica, fotocinematografica, elettromagnetica, o di qualunque altra specie del contenuto di atti, anche interni, prodotti e acquisiti ai fini dell'attività amministrativa.

b. ***gestione documentale:*** l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'amministrazione comunale.

c. ***Registro di protocollo:*** atto pubblico che fa fede dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, perciò è idoneo a produrre effetti giuridici a favore o a danno delle parti.

d. ***sistema di protocollo informatico:*** l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzate dal Comune per la gestione dei documenti.

e. ***segnatura di protocollo:*** l'apposizione o l'associazione, all'originale' del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso.

f. ***autenticazione informatica:*** la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

g. ***documento analogico:*** documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia.

h. ***documento analogico originale:*** documento analogico che puo' essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.

i. ***documento informatico:*** la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

j. ***originali non unici:*** i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.

k. ***supporto ottico di memorizzazione:*** mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD).

l. ***memorizzazione:*** processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'Articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, cosi' come modificato dall'Articolo 6 del decreto legislativo 23 gennaio 2002, n. 10.

m. ***archiviazione elettronica:*** processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, cosi' come individuati nella precedente lettera f), univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione.

n. ***documento archiviato:*** documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica;

o. ***conservazione sostitutiva***: processo effettuato con le modalità di cui agli articoli 3 e 4 della presente deliberazione.

p. ***documento conservato:*** documento sottoposto al processo di conservazione sostitutiva.

q. ***esibizione:*** operazione che consente di visualizzare un documento conservato e di ottenerne copia.

r. ***riversamento diretto:*** processo che trasferisce uno o piu' documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità.

s. ***riversamento sostitutivo:*** processo che trasferisce uno o piu' documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica

t. ***riferimento temporale:*** informazione, contenente la data e l'ora, che viene associata ad uno o piu' documenti informatici.

u. ***pubblico ufficiale:*** il notaio, salvo quanto previsto dall'Articolo 5, comma 4 della deliberazione CNIPA 19 febbraio 2004 n. 11 e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'Articolo 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

v. ***evidenza informatica:*** una sequenza di simboli binari (bit) che puo' essere elaborata da una procedura informatica.

w. ***impronta:*** la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

x. ***funzione di hash:*** una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresi' risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

y. ***firma elettronica:*** l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

z. ***firma elettronica qualificata:*** la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

aa. ***firma digitale:*** un particolare tipo di firma elettronica qualificata basata 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.

bb. ***fruibilità di un dato:*** la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione.

cc. ***gestione informatica dei documenti:*** l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici.

dd. ***validazione temporale:*** il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Art. 2 Oggetto della disciplina

Il presente manuale disciplina, nell'ambito dell'ordinamento normativo vigente, la gestione del sistema per la tenuta del protocollo informatico e dei flussi documentali del Comune.

Art. 3 Finalità

Il protocollo informatico è l'insieme delle risorse tecnologiche necessarie alla realizzazione di un sistema automatico di gestione elettronica dei flussi documentali. Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti e di archiviazione dei documenti, realizza condizioni operative per il miglioramento del flusso informativo e documentale all'interno del Comune, anche ai fini dello snellimento e della trasparenza dell'azione amministrativa.

Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

Il registro di protocollo, unico per tutto l'Ente, che si configura dunque come un'unica Area Organizzativa Omogenea (AOO), si apre il primo gennaio e si chiude il 31 dicembre di ogni anno.

Art. 4 Il servizio di protocollo

Alla tenuta del protocollo informatico è preposto apposito servizio, chiamato altresì a svolgere un ruolo di coordinamento e di indirizzo nei confronti delle strutture dell'Ente, al fine di garantire l'uniformità dell'attività di protocollazione e di gestione documentale.

L'Ufficio di Protocollo è inserito nella struttura organizzativa del Comune nell'ambito del Settore Affari Generali.

CAPO II

IL DOCUMENTO

Art. 5 Tipologia dei documenti

I documenti si distinguono in :

- documenti in entrata
- documenti in uscita
- documenti interni

I documenti vanno di norma protocollati e gestiti secondo le disposizioni e le eccezioni previste nel presente manuale.

Tutti i documenti ricevuti o spediti dall'Amministrazione ed oggetto di registrazione sono protocollati con un'unica numerazione, sicché ogni documento entrato o uscito dal Comune è individuato da un numero progressivo unico nell'anno solare e da una data di protocollazione.

Art. 6 Documenti interni

I documenti interni sono quelli scambiati tra uffici della stessa amministrazione e si distinguono in:

- documenti di preminente carattere informativo
- documenti aventi rilevanza giuridica.

I primi sono di norma memorie informali, appunti, brevi comunicazioni di rilevanza meramente informativa scambiate tra gli uffici.

I documenti interni aventi rilevanza giuridica sono quelli redatti dal personale nell'esercizio delle proprie funzioni ed al fine di documentare fatti inerenti all'attività svolta ed alla regolarità delle azioni amministrative o qualsiasi altro documento dal quale possano nascere diritti, doveri o legittime aspettative di terzi. Essi sono soggetti alla stessa numerazione dei documenti di preminente carattere informativo per quanto riguarda l'identificazione, inoltre, in funzione della loro tipologia, possono essere assoggettati al repertorio di competenza (es. Deliberazioni di Consiglio o di Giunta, verbali, contratti, determinazioni, ordinanze, circolari ecc.)

Art. 7 Documenti esclusi dalla registrazione di protocollo

Sono escluse, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000, dalla registrazione di protocollo le seguenti tipologie di documenti:

- Gazzette ufficiali, Bollettini ufficiali P.A.
- Notiziari P.A.
- Giornali, Riviste, Libri , Manuali
- Materiali pubblicitari
- Note di ricezione circolari, Note di ricezione, altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte/preventivi di terzi non richieste
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni,).

Sono altresì escluse le seguenti tipologie di documenti secondo le indicazioni contenute negli allegati al manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle pubbliche amministrazioni del CNIPA:

- Richieste ferie
- Richieste permessi
- Richieste di rimborso spese e missioni
- Verbali e delibere del Consiglio Comunitario
- Verbali e delibere della Giunta Esecutiva
- Determinazioni
- Le ricevute di ritorno delle raccomandate A.R.
- Documenti che per loro natura non rivestono alcuna rilevanza giuridica amministrativa presente o futura
- Gli allegati se accompagnati da lettera di trasmissione, ivi compresi gli elaborati tecnici
- Corsi di aggiornamento
- Certificati di malattia
- Variazione sedi ed anagrafe ditte fornitrici
- Convocazioni ad incontri o riunioni e corsi di formazione interni
- Pubblicità conoscitiva di convegni
- Pubblicità in generale
- Offerte e Listini prezzi (spontanei)
- Solleciti di pagamento (salvo che non costituiscano diffida)
- Comunicazioni da parte di Enti di bandi di concorso, di domande da presentare entro....
- Deliberazioni del Consiglio Comunale
- Deliberazioni della Giunta comunale
- Richieste di copia/visione di atti amministrativi
- Non saranno registrate a protocollo le certificazioni anagrafiche rilasciate direttamente al richiedente, le richieste e/o trasmissioni di certificati e tutta la corrispondenza dell'anagrafe,stato civile e leva diretta agli uffici comunali
- Richieste di affissione all'albo pretorio e conferma dell'avvenuta pubblicazione
- Comunicazioni di cessione di fabbricato ex L. 191/78
- Assicurazioni di avvenuta notifica

Art. 8 Documenti soggetti a protocollo riservato e documenti soggetti a registrazione particolare

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto un registro di ***protocollo riservato***, non disponibile alla consultazione dei soggetti non espressamente abilitati.
Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.
Qui di seguito è riportato l'elenco dei documenti soggetti a particolari forme di riservatezza per la registrazione e l'accesso:

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- Corrispondenza legata a vicende di persone o a fatti privati o particolari;
- Le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241
- Documenti di cui all'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.

Documenti soggetti a registrazione particolare in ambito comunale

- **Affari generali ed istituzionali**

  • Atti rogati o autenticati dal segretario comunale (registrazione informatica e cartacea)
  • Contratti e convenzioni (registrazione informatica e cartacea)
  • Verbali delle adunanze del Consiglio Comunale (registrazione informatica)
  • Verbali delle adunanze della Giunta comunale (registrazione informatica)
  • Verbali degli organi collegiali del Comune (registrazione informatica)
  • Autorizzazioni commerciali (registrazione cartacea)
  • Autorizzazioni artigiane (registrazione cartacea)
  • Autorizzazioni turistiche (registrazione cartacea)
  • Autorizzazioni di pubblica sicurezza (registrazione cartacea)
  • Autorizzazioni di polizia mortuaria (registrazione informatica)
  • Autorizzazioni igienico sanitaria e veterinaria (registrazione cartacea)
  • Licenze di pesca (registrazione cartacea)
  • Certificati di iscrizione all'anagrafe canina
  • Atti di stato civile (registrazione informatica)

- Pubblicazioni di matrimonio (registrazione informatica)
- Carte d'identità (registrazione informatica)
- Certificati anagrafici
- Tessere elettorali (registrazione informatica)
- Rapporti incidenti (registrazione informatica)
- Verbali oggetti smarriti
- Verbali C.d.S. (registrazione informatica)
- Richieste permessi transito ZTL

- **Servizi finanziari**

- Fatture attive (registrazione informatica)
- Liquidazioni (registrazione informatica)
- Mandati di pagamento (registrazione informatica)
- Reversali (registrazione informatica)
- Dichiarazioni I.C.I. (registrazione informatica)

- **Polizia municipale**

- registro verbali di violazione regolamenti e leggi varie
- fatture emesse registri IVA
- autorizzazioni sanitarie registro (autorizzazioni sanitarie)
- autorizzazioni commerciali (registro autorizzazioni commerciali)
- autorizzazioni di pubblico esercizio (registro autorizzazioni di pubblico)
- I verbali di violazione del codice della strada ed i verbali di violazioni amministrative

- **Affari culturali, educativi e sociali**

- Dichiarazioni per la certificazione Isee – Riccometro (registrazione cartacea)

- **Altri documenti**

- deliberazioni di consiglio comunale (registro delle deliberazioni del consiglio comunale)
- deliberazioni di giunta comunale (registro delle deliberazioni della giunta comunale)
- determinazioni dei responsabili dei servizi (registro delle determinazioni)
- decreti protocollati al protocollo generale
- ordinanze (registro delle ordinanze)
- contratti in forma pubblica amministrativa
- repertorio dei contratti
- documenti anonimi o non firmati (non soggetti ad alcuna registrazione)
- documenti totalmente illeggibili nel testo (non soggetti ad alcuna registrazione)
- documenti con mittente non riconoscibile (non soggetti ad alcuna registrazione)
- fatture senza lettera di trasmissione (registrazione a cura dell'ufficio ragioneria)
- documenti di competenza di altre amministrazioni protocollati e successivamente inoltrati in copia alle amministrazioni di competenza
- permessi di costruire (registro dei permessi di costruire)
- verbali di violazione codice della strada (registro dei verbali di violazione codice della strada)
- atti pubblicati all'albo pretorio (registro pubblicazioni albo pretorio)
- atti depositati nella casa comunale (registro deposito atti alla casa comunale)
- notifiche (registro notifiche)

- verbali di violazione regolamenti comunali e leggi varie (escluso il c.d.s.)
- Le denunce di variazioni ai fini I.C.I
- la T.A.R.S.U. ,
- L'occupazione di suolo pubblico ed altri tributi ed entrate dell'Amministrazione.

Art. 9 Uso del telefax

Il fax ufficiale dell'Ente, avente rilevanza giuridica, è gestito dall'Ufficio Protocollo.

I documenti pervenuti a mezzo fax vanno di norma protocollati e gestiti secondo le disposizioni ed eccezioni previste nel presente manuale.

I documenti recapitati via fax poi confermati per altre vie vengono protocollati solo la prima volta.

Art. 10 Uso della posta elettronica e della PEC (posta elettronica certificata)

Al fine di velocizzare lo scambio di informazioni con enti pubblici, cittadini ed imprese, gli uffici possono fare uso della posta elettronica.

Il documento ricevuto o trasmesso mediante posta elettronica viene stampato ed archiviato in modo conforme ai documenti originariamente cartacei, sino a quando la gestione e l'archiviazione dei documenti non sarà completamente informatizzata come detto in premessa al presente Manuale.

L'Amministrazione istituisce una casella di posta elettronica certificata per la ricezione e l'invio dei documenti informatici e ne pubblica l'indirizzo sul sito internet istituzionale e sull'Indice delle Pubbliche Amministrazioni.
Tale casella è quella adibita alla protocollazione dei messaggi ricevuti; i messaggi ricevuti che siano stati spediti da una casella di posta elettronica certificata vengono protocollati con la normale procedura e la notifica al mittente dell'avvenuto recapito è assicurata dal servizio di posta elettronica certificata utilizzata dall'amministrazione comunale.

I documenti pervenuti alla casella di posta elettronica certificata istituzionale da caselle di posta elettronica ***non*** certificata vengono accettati solo se firmati digitalmente.

I messaggi, comunque firmati digitalmente, che pervengono ad altre caselle di posta elettronica sono acquisite al protocollo generale solo su richiesta del dirigente responsabile del settore interessato che deve dichiarare che tali e-mail possono essere utilizzate nell'ambito dei procedimenti amministrativi e dare comunicazione al mittente dell'avvenuta o meno protocollazione del documento.

Per la spedizione dei documenti informatici l'Amministrazione si avvale del servizio di posta elettronica offerto da un soggetto in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e consegna dei documenti

attraverso una procedura di rilascio di ricevute di ritorno elettroniche che verranno opportunamente archiviate.

La comunicazione di documenti tra le PA avviene normalmente mediante l'utilizzo della posta elettronica ed è valida ai fini del procedimento amministrativo se ne sia stata verificata la provenienza.

A tal fine sono valide le comunicazioni le quali:

1) siano sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
2) ovvero siano dotate di protocollo informatizzato;
3) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71 del decr. legls. N. 82/2005
4) ovvero siano trasmesse attraverso sistemi di posta elettronica certificata di cui al D.P.R. n.68 dell' 11 febbraio 2005.

CAPO III

Registrazione dei documenti: regole e modalità

Art. 11 Il Responsabile del Protocollo

Il Responsabile del servizio per il Protocollo Informatico, per la gestione dei flussi documentali e degli archivi è un dirigente (ovvero un funzionario) in possesso di idonei requisiti professionali di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti in base alle procedure descritte dalla disciplina vigente.
E' nominato altresì un vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile.

Il Responsabile della tenuta del protocollo, di concerto con il C.E.D. provvede a:

a. pubblicare il presente Manuale di gestione del protocollo informatico anche su internet;
b. predisporre il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
c. individuare gli utenti ed attribuire loro un livello di autorizzazione per l'uso delle funzioni della procedura informatica;
d. individuare gli uffici, diversi dall'ufficio protocollo, che hanno accesso alle varie funzionalità ed, in particolare, gli uffici che possono procedere alla protocollazione in uscita;
e. garantire che le operazioni di registrazione e segnatura di protocollo si svolgano nel rispetto della normativa vigente;
f. autorizzare le operazioni di annullamento della registratura di protocollo;
g. garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
h. garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso esterno o da altre Amministrazioni e le attività di gestione degli archivi, quali, il trasferimento dei documenti all'archivio di deposito, le disposizioni per la conservazione degli archivi e gli archivi storici;
i. verificare che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro 24 ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
j. autorizzare lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza ogni qual volta per cause tecniche non sia possibile utilizzare la normale procedura informatica;

k. conservare copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti;
l. garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;
m. controllare l'osservanza delle presenti norme da parte del personale addetto;
n. promuovere la formazione e l'aggiornamento degli operatori;
o. promuovere, periodicamente, opportune verifiche sulle tipologie di documenti protocollati.

Art. 12 Funzionalità minime del sistema di protocollo informatico

La registrazione di protocollo è effettuata di norma mediante sistema informatico automatizzato.

Il sistema di gestione informatica dei documenti deve:
a. garantire la sicurezza e l'integrità dei dati memorizzati;
b. garantire la corretta e puntuale registrazione dei documenti in entrata e in uscita, generando automaticamente ed in modo non modificabile i numeri e le date di registrazione senza vuoti o dilazioni;
c. consentire la ricerca dei documenti registrati in base a qualsiasi informazione prevista;
d. fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
e. garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato;
f. consentire in condizioni di sicurezza l'accesso alle informazioni del sistema da parte degli interessati, nel rispetto delle disposizioni in materia di trattamento dei dati personali.

Art. 13 Elementi della registrazione di protocollo

La registrazione di protocollo si effettua mediante la memorizzazione di informazioni, delle quali alcune costituiscono elementi obbligatori la cui registrazione è giuridicamente rilevante contenendo le indicazioni minime per l'univoca, certa, efficace ed immediata identificazione dei documenti.

La registrazione degli elementi accessori è rilevante sul piano organizzativo-gestionale.

Art. 14 Elementi obbligatori della registrazione di protocollo

Gli elementi obbligatori della registrazione di protocollo sono registrati in forma non modificabile. Essi sono:

1) il numero di protocollo, generato automaticamente dal sistema;
2) la data di registrazione di protocollo assegnata automaticamente dal sistema;
3) il destinatario (per i documenti spediti) ed il mittente (per i documenti ricevuti);
4) l'oggetto del documento;
5) l'impronta del documento informatico, se trasmesso per via telematica.

Se disponibili devono essere altresì registrati la data ed il protocollo del documento ricevuto.

Il numero di protocollo è progressivo costituito da almeno 7 cifre numeriche e la numerazione è rinnovata ogni anno solare.

L'oggetto deve essere indicato in modo da rendere il documento distinguibile da altri.

Art. 15 Inalterabilità ed annullamento di una registrazione di protocollo

La registrazione degli elementi obbligatori del protocollo, ad eccezione di quelli di cui al numero 3) dell'articolo precedente, non può essere modificata o integrata, né cancellata, ma soltanto annullata mediante un'apposita procedura.

In caso di errore materiale nella registrazione, la procedura deve consentire l'annullamento dell'operazione registrata. Le informazioni relative devono comunque rimanere memorizzate ed essere sottoposte alle elaborazioni previste dalla procedura. In tale ipotesi la procedura riporta la dicitura " annullato" in posizione visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie, nonché la data, l'identificativo dell'operatore e gli estremi del provvedimento di autorizzazione.

L'annullamento di una registrazione può essere disposto solo dal responsabile del protocollo.

Il numero di protocollo utilizzato per la registrazione del documento poi di seguito annullata non sarà più utilizzabile ed il sistema provvederà automaticamente alla produzione di un nuovo numero.

Art. 16 Individuazione degli elementi accessori della registrazione di protocollo

Gli elementi accessori della registrazione di protocollo sono gestiti ed integrati in forma modulare con gli elementi obbligatori e sono legati alle seguenti funzioni:

a. gestione degli affari e dei procedimenti amministrativi;
b. gestione dell'archivio;
c. gestione delle banche dati.

Gli elementi accessori del protocollo legati alla gestione degli affari e dei procedimenti amministrativi sono i seguenti:

a. data del documento ricevuto;
b. numero di protocollo mittente del documento ricevuto;
c. ora e minuto di registrazione;
d. estremi del provvedimento di differimento dei termini di registrazione;
e. tipo di spedizione (ordinaria, espressa, corriere, raccomandata a/r, fax, email, ecc.);
f. collegamento a documento susseguente o precedente;
g. indicazione del tipo di supporto per gli allegati (cartaceo o informatico);
h. nominativo dei destinatari per conoscenza;
i. ufficio responsabile del procedimento amministrativo;
j. nominativo del responsabile del procedimento ;
k. oggetto del procedimento amministrativo (fascicolo);
l. termine di conclusione del procedimento;
m. stato e tempi parziali del procedimento (scadenzario);
n. tipologia del documento, con indicazione esplicita di sottrazione ad accesso o differimento;
o. immagine informatica del documento.

Gli elementi accessori del protocollo legati alla gestione dell'archivio sono i seguenti:

a. classificazione del documento attraverso il titolario allegato al presente manuale;
b. data di istruzione del fascicolo;
c. numero del fascicolo;
d. numero del sottofascicolo;
e. data di chiusura del fascicolo;
f. numero di repertorio della serie (deliberazioni, determinazioni, verbali circolari e contratti);
g. tipologia del documento con l'indicazione dei termini di conservazione e di scarto.

Gli elementi accessori del protocollo legati alla gestione delle banche dati sono le ulteriori informazioni sul mittente/destinatario (indirizzo completo, telefono, email, partita I.V.A., codice fiscale, chiave pubblica della firma digitale, ecc.).

Art. 17 Riservatezza delle informazioni

Per i procedimenti amministrativi per i quali si renda necessaria la riservatezza delle informazioni, temporanea o senza limiti di tempo, l'accesso sarà riservato ai soli responsabili della pratica.

Il responsabile dei dati deve indicare contestualmente alla registrazione di protocollo anche la data dalla quale le informazioni riservate divengono di pubblico dominio.

Per la registrazione dei documenti di cui all'articolo 8 secondo capoverso di questo manuale si potrà operare in due modalità:

- *il sindaco può disporre la registrazione su un protocollo riservato che dovrà essere definito in quanto a modalità di conservazione e consultazione;*
- *ovvero il responsabile della tenuta del protocollo dispone la registrazione informatica senza digitalizzazione del contenuto e curando che i documenti, dopo*

le operazioni di protocollazione, vengano inseriti in una busta opportunamente chiusa ed inviati ai destinatari.

Art. 18 Segnatura di protocollo

Con l'operazione di segnatura di protocollo si procede all'apposizione o all'associazione all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

Le informazioni minime previste dalla legge sono:

1) il numero di protocollo
2) la data di protocollo
3) l'indicazione in forma sintetica dell'amministrazione.

L'operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione.
Operativamente,gestendo al momento l'amministrazione i documenti in forma cartacea così come detto in premessa, dopo la fase di registrazione, il sistema stampa una o più etichette da incollare sulla prima pagina del documento ed eventualmente degli allegati.

L'operazione di segnatura di protocollo può includere il codice identificativo dell'ufficio cui il documento è assegnato o il codice dell'ufficio che ha prodotto il documento, l'indice di classificazione del documento e ogni altra informazione utile o necessaria, qualora tali informazioni siano disponibili già al momento della registrazione di protocollo.

Quando il documento è indirizzato ad altre amministrazioni ed è formato e trasmesso con strumenti informatici, la segnatura di protocollo può includere tutte le informazioni di registrazione del documento. L'amministrazione che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

Art. 19 Registro giornaliero di protocollo

Si provvede quotidianamente alla stampa del registro di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno. Il responsabile del protocollo appone la propria firma in calce alla stampa.

Entro il mese di gennaio di ogni anno il responsabile del protocollo provvede alla rilegatura delle stampe del registro giornaliero di protocollo dell'anno precedente.

Art. 20 Procedure di salvataggio e conservazione delle informazioni del sistema

Il Responsabile della tenuta del protocollo dispone i tempi e le modalità per la corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile.

Oggetto di salvataggio sono l'intero archivio, le ricevute di ritorno dell'autorità di certificazione della posta elettronica, i documenti originali ricevuti con firma digitale.

Le informazioni trasferite sono sempre ripristinabili. A tal fine il Responsabile della tenuta del protocollo dispone per la corretta conservazione dei supporti.

Responsabile della corretta esecuzione dei salvataggi è il Responsabile informatico del sistema.

Art. 21 Responsabile informatico della sicurezza dei dati del protocollo informatico

Con atto del Segretario Generale, su proposta del dirigente del settore di riferimento, è nominato il Responsabile Informatico della sicurezza dei dati del protocollo.

Il responsabile informatico svolge i seguenti compiti:

a. garantisce la funzionalità del sistema digestione del protocollo informatico;
b. provvede a ripristinare al più presto le funzionalità del sistema in caso di interruzioni o anomalie;
c. garantisce la correttezza delle fasi di salvataggio e ripristino.

Art. 22 Registro di emergenza

Il responsabile del servizio per la tenuta del protocollo o, in caso di sua assenza, il suo vicario, o altri eventualmente incaricati dal responsabile stesso, autorizza lo svolgimento manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la procedura informatica.

Il registro di emergenza, così come quello informatico, si apre il 1° gennaio e si chiude il 31 dicembre di ogni anno.

Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora di ripristino della funzionalità del sistema.

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione.

Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente.

Nel registro di emergenza sono protocollati in via prioritaria i documenti per i quali riveste rilevanza l'effettiva data di ricevimento o di partenza. Per gli altri documenti, il responsabile del protocollo può autorizzare il differimento delle operazioni di registrazione, facendo constare ciò in apposito verbale.

Nel momento in cui viene ripristinato il normale funzionamento del sistema dovranno essere inseriti i documenti protocollati sul registro di emergenza prima di riprendere la normale attività di protocollazione.

Art. 23 Accesso interno

Gli utenti, secondo l'ufficio di appartenenza, hanno abilitazioni di accesso differenziate, secondo le tipologie di operazioni autorizzate.

I profili di utente che vengono attivati sono quelli di:

a. Responsabile del protocollo;
b. Operatore del protocollo
c. Supervisore (sindaco, segretario generale, direttore generale);
d. Responsabile di settore;
e. Addetto di settore;
f. Direttore di ragioneria (caso particolare di responsabile di settore necessario per i pareri contabili);

ad ogni operatore è assegnata una *"login"* ed una *"password"* di accesso al sistema informatico di gestione del protocollo. Ogni operatore, identificato dalla propria login, è responsabile della corrispondenza dei dati desunti dal documento protocollato con quelli immessi nel sistema informatico di gestione del protocollo, compresa la corrispondenza del numero di protocollo archiviato nel sistema con quello segnato sul documento cartaceo. Il sistema garantisce, attraverso l'autenticazione di login e password, la riconoscibilità di ogni operatore in relazione alle operazioni dallo stesso compiute.

Le passwords devono essere cambiate almeno ogni 3 mesi, ciascun operatore sceglie la propria password e non la comunica a nessuno.

I livelli di autorizzazione sono assegnati dal responsabile del protocollo.

CAPO IV

NORME ORGANIZZATIVE

Art. 24 Disposizioni sull'apertura della corrispondenza in arrivo

La corrispondenza in arrivo va aperta di norma nel medesimo giorno lavorativo di ricezione e contestualmente protocollata.

La corrispondenza non viene aperta nei seguenti casi:

a. corrispondenza recante diciture da cui si evinca la partecipazione ad una gara;
b. corrispondenza indirizzata nominativamente oppure riportante l'indicazione ***"riservata" , "personale", "confidenziale" o simili,*** o comunque dalla cui confezione si evinca il carattere di corrispondenza privata.

La corrispondenza di gara prevista dal comma precedente è soggetta a registrazione di protocollo senza acquisizione digitale; le altre tipologie vanno consegnate agli interessati senza alcun tipo di azione, saranno gli stessi destinatari ad attivarsi nel caso i documenti debbano essere sottoposti ad attività di protocollazione.

Art. 25 Protocollazione della corrispondenza in arrivo

L'Ufficio di Protocollo provvede alla registrazione del documento in arrivo e contestualmente all'assegnazione degli elementi obbligatori di cui all'articolo 14.

L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.

E' fatto assoluto divieto agli addetti all'ufficio l'attribuzione del numero di protocollo a documenti non presenti materialmente nell'ufficio.

Contestualmente alla registrazione deve essere effettuata la segnatura così come previsto dall'articolo 18.

Art. 26 Protocollo differito

Nel caso di temporaneo ed eccezionale carico di lavoro che non permette di evadere la corrispondenza ricevuta nella medesima giornata lavorativa e qualora dalla mancata registrazione nel medesimo giorno lavorativo di ricezione possa venire meno un diritto di terzi (es. in caso di arrivo di un numero consistente di domante di partecipazione ad un concorso in scadenza), con provvedimento motivato del responsabile del servizio di protocollo, si differiscono i termini di registrazione a protocollo, ma i documenti devono essere in ogni caso timbrati e datati per ricevuta.

Il protocollo differito consiste semplicemente nel differimento dei termini di registrazione, cioè nel provvedimento con il quale vengono individuati i documenti da ammettere alla

registrazione differita, le cause e il termine entro il quale la registrazione di protocollo deve comunque essere effettuata.

Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il responsabile del servizio di protocollo deve descrivere nel provvedimento.

Art. 27 Email prive di firma

La corrispondenza elettronica (email) priva di firma è inoltrata al dirigente responsabile del settore interessato che deve dichiarare che l'e-mail può essere utilizzata nell'ambito del procedimento amministrativo e dare comunicazione al mittente dell'avvenuta o meno protocollazione del documento.

Sarà compito del Responsabile del Servizio assegnatario del documento valutare caso per caso se la lettera priva di firma è da ritenersi valida ai fini di un determinato affare o procedimento amministrativo.

Art. 28 Digitalizzazione della corrispondenza in arrivo

Dopo le fasi di registrazione e segnatura, i documenti analogici in arrivo che non sono oggetto di apertura differita (come ad es. quelli relativi alle gare) vengono digitalizzati tramite scannerizzazione.
La digitalizzazione può riguardare, a discrezione dell'ufficio, l'intero documento o una parte di esso nel caso di allegati voluminosi o di difficile formato (come i progetti edili) che possono rimanere in formato cartaceo.

La digitalizzazione inserisce nel sistema informatico l'impronta elettronica del documento che resta immutata ed immutabile rispetto all'originale cartaceo.

Art. 29 Assegnazione e classificazione della corrispondenza in arrivo

La corrispondenza in arrivo viene registrata dagli addetti alla protocollazione. La registrazione si completa con le fasi di classificazione e di assegnazione.

La classificazione consiste nell'attribuire al documento un titolo ed una classe secondo il titolario di classificazione adottato ed allegato al presente manuale.

Strettamente connessa alla classificazione è l'assegnazione di un documento ad un servizio ed ad un responsabile di procedimento per la conseguente gestione. Il sistema informatico garantisce la massima flessibilità operativa; infatti, gli addetti alla protocollazione possono:

a. eseguire solo l'assegnazione, anche indicando semplicemente l'utente a cui è assegnata la corrispondenza, sarà poi compito di quest'ultimo procedere alla classificazione;
b. eseguire solo la classificazione, spedendo il documento al supervisore (Segretario, Direttore Generale) per l'assegnazione;
c. eseguire classificazione ed assegnazione;
d. spedire il documento al supervisore senza eseguire la classificazione.

Nel caso in cui un documento venga inviato ad un supervisore quest'ultimo può decidere di assegnarlo e/o classificarlo, eventualmente anche correggendo i dati di classificazione e/o assegnazione attribuiti dall'operatore di protocollo, ed impostare delle direttive attraverso specifiche annotazioni.

Nel sistema informatico la classificazione è messa in relazione alla struttura dei servizi e all'organigramma funzionale degli stessi, pertanto generalmente la sola fase di classificazione è sufficiente ad indicare il servizio a cui il documento viene assegnato.

Normalmente viene trasmessa al Sindaco, dopo la registrazione di protocollo e fatto salvo quanto previsto a proposito della riservatezza di cui agli articoli 8 e 17, la corrispondenza relativa a :

a. atti concernenti questioni generali o di particolare rilevanza riguardanti il Comune;
b. atti politici;
c. atti inerenti alla politica del personale e la materia finanziaria;
d. richieste di contributi particolarmente onerosi;
e. atti riguardanti i rapporti con altri enti, istituzioni, società a capitale pubblico, ecc.;
f. proposte di punti da inserire all'ordine del giorno del Consiglio Comunale e della Giunta.

Il Sindaco, nella sua qualità di supervisore, può successivamente assegnare i documenti, di cui al precedente comma, ai funzionari, eventualmente aggiungendovi note o direttive.

In caso di incertezza sull'assegnazione di competenza di un documento il servizio protocollo invia il documento al direttore generale.

Art. 30 Lettere erroneamente pervenute

Qualora venga erroneamente registrato un documento di competenza di terzi (altro ente, o persona fisica o giuridica) la registrazione deve essere annullata ed un nuovo numero sarà utilizzato per la trasmissione a chi di competenza.

Qualora un documento analogico non sia stato ancora aperto, un nuovo numero sarà comunque utilizzato per la trasmissione della busta chiusa a chi di competenza. Sulla busta dovrà essere apposta la data ai fini dell'attestazione dell'arrivo.

Art. 31 Erronea assegnazione di competenza

Qualora un servizio riceva un documento relativo a materie estranee alla propria competenza, oppure a causa di un disguido o errore un documento indirizzato ad altri, lo deve recapitare al servizio protocollo o al supervisore che ha assegnato il documento per l'invio al servizio competente.

Il servizio di protocollo provvede ad attribuire una nuova assegnazione ed a correggere l'assegnazione errata sulla registrazione di protocollo.

Art. 32 Creazione dei documenti interni

I documenti interni descritti all'articolo 6 vengono creati dai funzionari, nell'esercizio delle proprie prerogative e competenze, utilizzando i normali strumenti di produttività individuale (word processor, fogli di calcolo, ecc.).

Un documento interno è gestito dal sistema informatico e, pertanto, risiede sul sistema server. Un qualsiasi elaborato, prima di diventare un documento interno ed essere quindi assoggettato a numerazione e sottoposto a gestione centralizzata, viene predisposto in forma di bozza da chi lo crea e gestito sul client di questi fini quando non diventa documento a tutti gli effetti.

Art. 33 Smistamento e gestione dei documenti

I documenti, sia interni che pervenuti dall'esterno, vengono gestiti all'interno degli uffici comunali.

Ciascun responsabile di servizio individua uno o più utenti che possono fungere da responsabili per tipologie omogenee di procedimenti.

Il responsabile di ciascun servizio ha la possibilità di assegnare documenti ad altro componente della struttura del servizio, mantenendone la visibilità.

Il responsabile del procedimento che ha prodotto il documento, o al quale il documento è stato assegnato, ha la facoltà di operare sullo stesso secondo le necessità previste dall'iter del procedimento. La gestione di un documento termina con la sua chiusura.

Art. 34 Fascicoli

Normalmente i documenti, sia provenienti dall'esterno che prodotti dall'interno, entrano a far parte dei fascicoli.

Il responsabile di un procedimento cura la formazione e la gestione di un fascicolo fino alla sua chiusura, inserendovi tutti i documenti che ritiene necessari.

Ogni fascicolo è individuato da un titolo ed una classe e de una numerazione progressiva all'interno della classe, numerazione che si rinnova ogni anno.

Un fascicolo può avere uno o più sottofascicoli individuati da una sottonumerazione.

Attributi obbligatori di un fascicolo sono altresì l'*oggetto* e le *date di creazione di chiusura.*

Art. 35 Smistamento della corrispondenza in arrivo

La corrispondenza in arrivo, esclusa quella riservata, dopo essere stata registrata e segnata subisce il seguente trattamento:

a. la parte elettronica è immediatamente visibile per l'ufficio destinatario e/o il supervisore ed è soggetta alle fasi di assegnazione, classificazione e gestione;
b. la parte cartacea viene trattenuta dall'ufficio protocollo fino a quando non è pronta per essere ritirata dall'ufficio destinatario.

In fase di inoltro verso i destinatari, l'ufficio protocollo stampa una distinta di consegna che viene sottoscritta dal rappresentante dell'ufficio che materialmente la riceve.

Art. 36 Protocollazione della corrispondenza in partenza

La protocollazione della corrispondenza in partenza viene di norma effettuata dall'Ufficio per la tenuta del protocollo.

In caso di corrispondenza cartacea, i direttori di settore fanno pervenire a tale ufficio il documento da protocollare, congiuntamente alla busta ed alla eventuale ricevuta di ritorno eventualmente compilate.

E' assolutamente vietato da parte degli addetti all'Ufficio per la tenuta del protocollo informatico attribuire telefonicamente, o con qualsiasi altro mezzo, numeri di protocollo, dal momento che, per procedere alle operazioni di registrazione e segnatura del documento in uscita, deve essere materialmente disponibile il documento stesso.

Qualora vi sia più di un destinatario del documento in partenza il sistema prevede la registrazione di tutti.

Il responsabile del protocollo può attribuire ai responsabili di settore la possibilità di procedere direttamente alla protocollazione dei documenti in partenza. Tale possibilità è raccomandata dal momento che il sistema è in grado di effettuare la segnatura di protocollo direttamente in forma elettronica, senza la stampa e la conseguente incollatura delle etichette, sgravando l'ufficio protocollo di una considerevole mole di lavoro.

Il documento in partenza per via elettronica, firmata digitalmente, viene accodata all'ufficio del protocollo che provvede ad inviarla tramite la casella di posta certificata.

Art. 37 Spedizione della corrispondenza cartacea

L'affrancatura della posta cartacea è effettuata, di norma, presso l'ufficio protocollo che provvede a:

a. affrancare le lettere ordinarie
b. pesare ed affrancare le lettere soprappeso
c. affrancare le lettere fuori formato
d. procedere alla ricezione ed alla verifica delle distinte di raccomandate compilate dagli uffici
e. pesare ed affrancare le raccomandate estere.

Altri uffici possono essere autorizzati alla spedizione tramite affrancatrice propria o tramite agenzia autorizzata.
Per le operazioni postali urgenti e telegrafiche provvede il servizio commessi.
La spedizione cartacea di avvisi, o comunque di corrispondenza, per conto di un ufficio, qualora essa sia quantitativamente rilevante, deve avvenire con modalità da concordare in via preventiva con il responsabile del protocollo.

CAPO V

ARCHIVIO E PIANO DI CONSERVAZIONE DEI DOCUMENTI

ART. 38 Archivi cartacei e archivio informatico

L'archivio, creato e conservato per scopi politici, giuridici e culturali, è la raccolta ordinata degli atti spediti, ricevuti o comunque prodotti e pubblicati da un ente per il conseguimento dei propri fini o l'espletamento delle proprie funzioni.

Gli atti essendo documenti collegati tra loro con rapporto di causa effetto, devono essere ordinati, strutturati e conservati in modo coerente e devono essere accessibili alla consultazione per usi amministrativi, legali o storici.

L'archivio si suddivide in archivio corrente, di deposito, storico.

L'*archivio corrente* comprende i documenti necessari allo svolgimento delle attività correnti.
L'*archivio di deposito* comprende i documenti relativi degli affari conclusi ma ancora recenti e che possono essere oggetto di ricerca per motivi amministrativi e/o legali.
L'archivio storico (sezione separata) contiene i documenti selezionati per la conservazione permanente.

Temporaneamente l'archivio legalmente riconosciuto sarà quello cartaceo, anche se contemporaneamente all'entrata in vigore del protocollo informatico si dovrà procedere alla formazione di un archivio informatico e l'attività degli uffici verrà quasi interamente svolta basandosi sul sistema informatico.
Una volta introdotte le misure tecniche e informatiche necessarie (es. firma digitale, riversamento diretto, riversamento sostitutivo, conservazione sostitutiva, ecc.), l'archivio informatico sarà valido e rilevante a tutti gli effetti legali e si potrà provvedere alla completa eliminazione della carta con le modalità previste dalle norme tecniche.

Ciascun ufficio organizza l'archivio corrente dei procedimenti ad esso assegnati, in modalità informatica e temporaneamente anche cartacea.

Art. 39 Trasferimento dei documenti all'archivio di deposito

La chiusura di una pratica coincide con il passaggio della stessa all'archivio di deposito. La chiusura di un fascicolo informatico consiste nell'attribuzione di una data di chiusura, mentre in caso di fascicolo cartaceo esso viene trasferito all'ufficio archivio che contestualmente potrà aggiungere sulla pratica informatica le informazioni riguardanti l'archiviazione.

Periodicamente, e in ogni caso almeno una volta ogni anno il responsabile del servizio per la gestione dei flussi documentali e degli archivi provvede a trasferire fascicoli e serie documentarie relativi a procedimenti conclusi in un apposito archivio di deposito.
Per la conservazione degli archivi informatici il responsabile per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi può avvalersi del supporto del responsabile del centro elaborazione dati.

Il responsabile del servizio per la gestione dei flussi documentali e degli archivi deve formare e conservare un elenco dei fascicoli e delle serie trasferite nell'archivio di deposito.

Dei documenti prelevati dagli archivi deve essere tenuta traccia del movimento effettuato e della richiesta di prelevamento.

Art. 40 Archivio storico

Documenti selezionati per la conservazione permanente sono trasferiti contestualmente agli strumenti che ne garantiscono l'accesso, nell'Archivio di Stato competente per territorio o nella separata sezione di archivio secondo quanto previsto dalle vigenti disposizioni in materia di tutela dei beni culturali.

Art. 41 Il fascicolo informatico

L'unità basilare dell'archiviazione è il fascicolo che deve avere un collegamento con il titolario di classificazione.

Il Comune adotta il titolario di classificazione allegato a questo Manuale.

All'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, l'amministrazione comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.

Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento.

Il fascicolo informatico deve recare l'indicazione:

a. dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b. delle altre amministrazioni partecipanti;
c. del responsabile del procedimento;
d. dell'oggetto del procedimento;
e. dell'elenco dei documenti contenuti, salvo quanto disposto dal comma successivo.

Il fascicolo informatico può contenere aree cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990.

Art. 42 Conservazione dei documenti informatici

Il sistema di conservazione dei documenti informatici deve garantire:

a. l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione;
b. l'integrità del documento;
c. la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
d. il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Art. 43 Conservazione sostitutiva dei documenti informatici

Il processo di conservazione sostitutiva di documenti informatici, anche sottoscritti con firma digitale, avviene mediante memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o piu' impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.

Il processo di riversamento sostitutivo di documenti informatici conservati avviene mediante memorizzazione su altro supporto ottico e termina con l'apposizione sull'insieme dei documenti o su un'evidenza informatica contenente una o piu' impronte dei documenti o di insiemi di essi del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo. Qualora il processo riguardi documenti informatici sottoscritti con firma digitale e' inoltre richiesta l'apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d'origine.

Art. 44 Conservazione sostitutiva di documenti analogici

Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su un'evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta così il corretto svolgimento del processo.

Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.

La distruzione di documenti analogici, di cui e' obbligatoria la conservazione, e' consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo quanto previsto al comma 4 dell'articolo 6 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Il processo di riversamento sostitutivo di documenti analogici conservati avviene mediante memorizzazione su altro supporto ottico. Il responsabile della conservazione, al termine del riversamento, ne attesta il corretto svolgimento con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti o su una evidenza informatica contenente una o piu' impronte dei documenti o di insiemi di essi. Qualora il processo riguardi documenti originali unici, e' richiesta l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformita' di quanto riversato al documento d'origine.

I documenti informatici saranno conservati anche presso gestore autorizzato Agid nei tempi previsti per Legge

Art. 45 Responsabile della conservazione

Il responsabile per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi è altresì responsabile conservazione.

Il responsabile del procedimento di conservazione sostitutiva:

1. definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilita' che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;

2. archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
    a. descrizione del contenuto dell'insieme dei documenti;
    b. estremi identificativi del responsabile della conservazione;
    c. estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
    d. indicazione delle copie di sicurezza;

3. mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
4. verifica la corretta funzionalità del sistema e dei programmi in gestione;
5. adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
6. richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
7. definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
8. verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti

Il responsabile del procedimento di conservazione sostitutiva puo' delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o piu' persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.
Il procedimento di conservazione sostitutiva puo' essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione.

Art. 46 Obbligo di esibizione

Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo.

Il documento conservato puo' essere esibito anche per via telematica.

Qualora un documento conservato venga esibito su supporto cartaceo fuori dall'ambiente in cui e' installato il sistema di conservazione sostitutiva, deve esserne dichiarata la conformità da parte di un pubblico ufficiale se si tratta di documenti per la cui conservazione e' previsto il suo intervento.