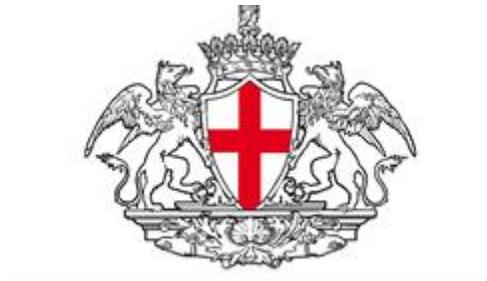


Comune di Genova



Manuale di gestione del protocollo informatico, dei documenti e dell'archivio

Indice

1. PRINCIPI GENERALI	6
1.1 Premessa.....	6
1.2 Riferimenti normativi	6
1.3 Acronimi.....	7
1.4 Definizioni	7
1.5 Aree Organizzative Omogenee.....	7
1.5.1 Accreditamento dell'AOO all'IPA	8
1.6 Ruoli e competenze	8
1.6.1 Servizio per la gestione informatica del protocollo, la gestione dei flussi documentali e degli archivi	8
1.6.2 Conservazione dei documenti informatici	9
1.6.3 Sicurezza delle informazioni	9
1.6.4 Tutela dei dati personali	9
2. I DOCUMENTI DELL'ENTE	10
2.1 Documento informatico	10
2.2 Documento analogico (cartaceo).....	10
2.3 Documento ricevuto	11
2.4 Documento inviato	11
2.5 Documento interno formale	11
2.6 Documento interno informale	12
2.7 Formazione dei documenti: aspetti operativi	12
2.7.1 Modalità di formazione dei documenti informatici.....	12
2.8 Sottoscrizione di documenti informatici	13
2.9 Requisiti degli strumenti informatici di scambio.....	13
2.10 Verifica delle firme digitali nel Sistema di Protocollo	14
2.11 Interoperabilità tra Pubbliche Amministrazioni: posta elettronica certificata.....	14
3. PROCESSO DI GESTIONE DEI DOCUMENTI	15
3.1 Documenti in ingresso	15
3.1.1 Ricezione di documenti informatici sulla casella di posta elettronica certificata istituzionale.....	17

3.1.2	Ricezione di documenti informatici sulla casella di posta elettronica certificata non istituzionale.....	1 7
3.1.3	Ricezione di documenti informatici sulla casella di posta elettronica ordinaria	1 7
3.1.4	Ricezione di documenti informatici su supporti rimovibili o servizi “file transfer”	1 7
3.1.5	Ricezione di documenti informatici con più allegati scorporati in invii successivi	1 7
3.1.6	Ricezione di documenti informatici prodotti in formati non accettati.....	1 8
3.1.7	Ricezione di documenti informatici con anomalie, contenuti illeggibili o instabili	1 8
3.1.8	Ricezione di documenti cartacei a mezzo posta convenzionale.....	1 8
3.1.9	Ricezione di documenti presentati allo sportello di protocollo generale.....	1 8
3.1.10	Ricezione di documenti presentati direttamente alle Strutture.....	1 9
3.1.11	Ricezione dei medesimi documenti pervenuti da sorgenti diverse.....	1 9
3.1.12	Ricezione di documenti analogici indirizzati al personale del Comune di Genova.....	1 9
3.1.13	Ricezione di documentazione non firmata e corrispondenza anonima	1 9
3.1.14	Ricezione di documento analogico erroneamente indirizzato al Comune di Genova....	1 9
3.1.15	Ricezione di documento digitale erroneamente indirizzato al Comune di Genova	1 9
3.1.16	Rilascio di ricevute attestanti la ricezione di documenti informatici.....	2 0
3.1.17	Rilascio di ricevute attestanti la ricezione di documenti cartacei	2 0
3.1.18	Archiviazione dei documenti informatici.....	2 0
3.1.19	Archiviazione delle copie per immagine di documenti cartacei.....	2 0
3.1.20	Assegnazione, presa in carico dei documenti e classificazione	2 1
3.2	Documenti in uscita.....	2 2
3.2.1	Modalità di formazione del documento	2 4
3.2.2	Verifica formale dei documenti	2 4
3.2.3	Classificazione, fascicolazione, segnatura e registrazione di protocollo	2 4
3.2.4	Trasmissione di documenti informatici.....	2 4
3.2.5	Trasmissione di documenti cartacei a mezzo posta	2 5
3.2.6	Inserimento delle ricevute di trasmissione nel fascicolo.....	2 5
3.3	Documenti interni	2 5
3.3.1	Documenti interni formali.....	2 7
3.3.2	Documenti interni informali.....	2 7
4.	PROTOCOLLAZIONE	2 7

4.1	Registro informatico di protocollo	2 8
4.1.1	Registro giornaliero di protocollo	2 8
4.2	Gestione delle registrazioni di protocollo con il Sistema di Protocollo	2 8
4.3	Principali regole per la registrazione di protocollo.....	2 8
4.4	Registrazione di protocollo di documenti informatici.....	2 9
4.5	Registrazione di protocollo di documenti analogici.....	2 9
4.6	Elementi facoltativi delle registrazioni di protocollo.....	2 9
4.7	Segnatura di protocollo dei documenti informatici	3 0
4.8	Segnatura di protocollo dei documenti cartacei.....	3 0
4.9	Annullamento e modifica delle registrazioni di protocollo	3 1
4.10	Livello di riservatezza	3 1
4.11	Protocollo di emergenza	3 1
5.	CLASSIFICAZIONE	3 1
5.1	Il titolare di classificazione.....	3 2
6.	AGGREGAZIONI DOCUMENTALI	3 2
6.1	Fascicolazione dei documenti	3 3
6.2	Apertura del fascicolo	3 3
6.3	Chiusura del fascicolo	3 3
6.4	Processo di assegnazione dei fascicoli	3 3
6.5	Modifica dell'assegnazione dei fascicoli	3 4
7.	GESTIONE ARCHIVI	3 4
7.1	Gestione e organizzazione dei documenti e dei fascicoli nell'archivio corrente.....	3 4
7.2	Archivio di deposito.....	3 5
7.3	Archivio storico	3 5
8.	CONSERVAZIONE A NORMA	3 5
8.1	Regole per il versamento in conservazione	3 5
8.2	Processi di gestione.....	3 5
8.3	Metadati	3 6
9.	SCARTO	3 6
10.	ACCESSO AGLI ATTI	3 6
10.1	Trasparenza	3 7

11. INFRASTRUTTURA INFORMATICA DELL'ENTE.....	3 7
11.1 Strumenti	3 7
11.2 Posta elettronica.....	3 7
11.3 Sicurezza	3 7
12. PRODUZIONE E AGGIORNAMENTO DEL MANUALE.....	3 8
12.1 Modalità creazione, gestione e adozione	3 8
12.2 Pubblicità del presente Manuale.....	3 8
13. ALLEGATI.....	3 8

1. PRINCIPI GENERALI

1.1 Premessa

Le Linee guida sulla formazione, gestione e conservazione dei documenti informatici prevedono, per tutte le amministrazioni di cui al Decreto legislativo 07/03/2005, n. 82, art. 2, comma 2, l'adozione del manuale di gestione documentale.

Il manuale, redatto secondo quanto previsto dalle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" dell'AgID (Agenzia per l'Italia Digitale) (di seguito LLGG), cap. 3.5, *"descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi"*.

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile della gestione documentale, ai sensi del Decreto del Presidente della Repubblica 28/12/2000, n. 445, art. 50 ("Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa").

Il presente manuale è uno strumento operativo che descrive il sistema di produzione e gestione dei documenti, sia digitali che analogici: in esso sono indicate le procedure e sono fornite le istruzioni per la corretta formazione, gestione, tenuta e conservazione della documentazione digitale e analogica. Inoltre, esso descrive le attività di gestione dei flussi documentali e archivistici in relazione ai procedimenti amministrativi del Comune di Genova. Tali disposizioni si applicano a tutte le Direzioni del Comune di Genova.

Il manuale di gestione documentale è destinato alla più ampia diffusione interna ed esterna, in quanto fornisce le istruzioni complete per eseguire correttamente le operazioni di formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione dei documenti. Pertanto, si rivolge non solo agli operatori di protocollo ma in generale a tutti i dipendenti e ai soggetti esterni che si relazionano con l'Amministrazione.

1.2 Riferimenti normativi

Le principali normative di riferimento per la stesura del Manuale sono le seguenti:

- **Legge 07/08/1990, n. 241** - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
- **Decreto del Presidente della Repubblica 28/12/2000, n. 445** - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (TUDA).
- **Decreto legislativo 22/01/2004, n. 42** - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della L. 6 luglio 2002, n. 137.
- **Decreto legislativo 07/03/2005, n. 82**- Codice dell'Amministrazione Digitale (CAD)
- **Decreto del Presidente del Consiglio dei Ministri 03/12/2013** - Regole tecniche per il protocollo informatico ai sensi degli artt. 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione Digitale di cui al D.Lgs 7 marzo 2005, n. 82.
- **Regolamento (UE) n. 910/2014 (eIDAS)** del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

- **Regolamento (UE) n. 679/2016 (GDPR)** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (General Data Protection Regulation)
- **Decreto legislativo 13/12/2017, n. 217** - Modifiche ed integrazioni al Codice dell'Amministrazione Digitale, di cui al D.Lgs 7 marzo 2005, n. 82.
- **Linee guida AgID** sulla formazione, gestione e conservazione dei documenti informatici.

1.3 Acronimi

AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CAD	Codice dell'Amministrazione Digitale
CE	Comunità Europea
eIDAS	electronic IDentification, Authentication and trust Services
GDPR	General Data Protection Regulation
LLGG	Linee guida sulla formazione, gestione e conservazione dei documenti informatici
IPA	Indice delle Pubbliche Amministrazioni
PEC	Posta Elettronica Certificata
PEO	Posta Elettronica Ordinaria
RGD	Responsabile della Gestione Documentale
TUDA	Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
UE	Unione Europea

1.4 Definizioni

Per quanto riguarda la definizione degli elementi specifici utilizzati all'interno del Manuale si rimanda all'*Allegato n. 1 - Glossario*.

1.5 Aree Organizzative Omogenee

Per la gestione dei documenti, ai sensi del TUDA, art. 50, l'Amministrazione ha istituito un'unica Area Organizzativa Omogenea (AOO) dove è presente un unico servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

All'AOO corrisponde un unico registro di protocollo per tutte le Direzioni e le Strutture ad esse afferenti, ed è associato un indirizzo di posta elettronica certificata (PEC) istituzionale ed eventuali ulteriori indirizzi PEC, connessi con il sistema di protocollo informatico e utilizzabili per la gestione dei documenti informatici, sia in uscita che in entrata al Comune di Genova.

1.5.1 Accreditamento dell'AOO all'IPA

L'Amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice dei domicili digitali della Pubblica Amministrazione e dei gestori di pubblici servizi (IPA), tenuto e reso pubblico dallo stesso fornendo le informazioni che individuano l'Amministrazione (identificata tramite codice c_d969) e l'articolazione della sua AOO.

Inoltre, si impegna a comunicare tempestivamente all'IPA eventuali modifiche, variazioni o aggiornamenti delle proprie informazioni e la data in cui la modifica stessa sarà operativa. Con la stessa tempestività l'Amministrazione comunica eventuali variazioni della propria organizzazione, come la soppressione di una AOO.

L'IPA è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati (<https://indicepa.gov.it/ipa-portale/>).

1.6 Ruoli e competenze

Il presente capitolo descrive le responsabilità attribuite ai diversi ruoli individuati e le relative competenze, raggruppate per servizio.

1.6.1 Servizio per la gestione informatica del protocollo, la gestione dei flussi documentali e degli archivi

Nell'AOO è istituito il Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.

Al suddetto Servizio è preposto il Responsabile della Gestione Documentale (di seguito RGD), nominato con Provvedimento del Sindaco. Il RGD è chiamato a conoscere tutte le funzionalità del sistema di protocollo informatico e le regole organizzative dell'AOO, garantendo il buon funzionamento del Servizio e il rispetto delle disposizioni normative e delle procedure concernenti le attività di registrazione di protocollo, di gestione dei flussi documentali, dei documenti e degli archivi.

In relazione alla modalità di fruizione del servizio di protocollo adottata dall'AOO, è compito del servizio:

- predisporre lo schema del “Manuale di gestione del protocollo informatico, dei documenti e dell'archivio dell'ente”, con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla massima diffusione dello stesso, anche attraverso la pubblicazione sul sito istituzionale dell'amministrazione;
- garantire il rispetto delle disposizioni normative vigenti in materia di gestione documentale e protocollo informatico;
- garantire la corretta conservazione della copia del registro giornaliero di protocollo;
- garantire il buon funzionamento degli strumenti interni all'AOO e sollecitare il ripristino del servizio di protocollazione e gestione documentale in caso di indisponibilità del medesimo;
- garantire il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali e le attività di gestione degli archivi;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza nel caso di disservizio del sistema di protocollo.

I compiti del Servizio sono svolti attraverso il supporto del sistema informatico di gestione documentale che garantisce il rispetto dei requisiti normativi nonché dei requisiti relativi alla sicurezza.

1.6.2 Conservazione dei documenti informatici

All'attività di conservazione dei documenti informatici sono preposte due figure:

- Il Responsabile della conservazione
- Il Responsabile del servizio di conservazione, nominato tra soggetti esterni all'Amministrazione dotati di specifica competenza in materia.

Il Responsabile della conservazione ha l'onere di garantire l'integrità e la conservazione dei documenti, oltre che presidiare l'evoluzione tecnologica e normativa del servizio, al fine di individuare tempestivamente eventuali necessità di adeguamento del servizio di conservazione.

In particolare:

- a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, in conformità alla normativa vigente;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive il rapporto di versamento;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione previste dalle regole tecniche;
- i) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- j) predispose il manuale di conservazione di cui alle LLGG, par. 4.7, e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Come previsto nel capitolo 4.5 delle LLGG, il servizio di conservazione è affidato a un conservatore esterno all'Ente, e le attività suddette, ad esclusione della lettera j), sono affidate al Responsabile del servizio di conservazione. Si precisa inoltre che il nominativo e i riferimenti del Responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il conservatore nel quale sono anche riportate le attività affidate al Responsabile del servizio di conservazione.

Per ulteriori informazioni si precisa che è in fase di elaborazione il Manuale di conservazione, e si rimanda poi all'*Allegato 2 – Manuale del servizio di conservazione del fornitore dell'ente*.

1.6.3 Sicurezza delle informazioni

All'attività di sicurezza delle informazioni è preposto il Responsabile della sicurezza, il quale definisce le policy, le regole e le procedure di sicurezza che devono essere implementate dalle Strutture di competenza per la corretta gestione e conservazione dei documenti e delle informazioni trattate.

1.6.4 Tutela dei dati personali

L'Amministrazione, titolare dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa di propria competenza, opera secondo quanto dettato dal General Data Protection Regulation (GDPR, Regolamento UE 2016/679) e dal Regolamento comunale approvato con Deliberazione del Consiglio comunale 21/09/2021, n. 78, in vigore dal 26 ottobre 2021. Alla suddetta attività è proposto il l'Ufficio del Responsabile della Protezione dei dati personali (DPO).

2. I DOCUMENTI DELL'ENTE

Il presente capitolo fornisce indicazioni in merito alle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno e all'esterno dell'AOO.

Nell'ambito del processo di gestione documentale il documento, in termini tecnologici, è così classificabile:

- informatico
- analogico.

L'oggetto di scambio (il documento) in termini operativi è così classificabile:

- ricevuto
- inviato
- interno formale
- interno informale.

2.1 Documento informatico

Il documento informatico è un documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento informatico soddisfa il requisito della forma scritta e ha valore probatorio se:

- è sottoscritto con firma digitale o altro tipo di firma elettronica qualificata o avanzata;
- è formato attraverso un processo in grado di garantire la sicurezza, l'integrità e l'immodificabilità del documento e la sua inequivoca riconducibilità all'autore, secondo i requisiti fissati dall'AgID ai sensi del CAD, art. 71.

In tutti gli altri casi, la valenza probatoria del documento informatico è liberamente valutabile in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità dello stesso.

Si precisa che la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle LLGG.

2.2 Documento analogico (cartaceo)

Il documento analogico è una rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.

All'interno del Manuale, si fa riferimento al documento analogico cartaceo, che può essere prodotto in maniera tradizionale (per esempio, una lettera scritta a mano o a macchina) o con strumenti informatici (per esempio, una lettera prodotta tramite un sistema di videoscrittura o text editor) e poi stampato.

Da un documento analogico è possibile ottenere uno dei seguenti documenti informatici:

- copia informatica di documento analogico = documento informatico avente contenuto identico a quello del documento analogico da cui è tratto, per esempio tramite copiatura manuale tramite sistema di videoscrittura;

- copia per immagine su supporto informatico di documento analogico = documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto, per esempio tramite scansione o fotografia.

Si ricorda che i documenti informatici sopra indicati hanno valore giuridico solo se conformi alle specifiche indicazioni delle LLGG, Allegato 3.

2.3 Documento ricevuto

Il documento ricevuto è un documento prodotto all'esterno dell'Ente e acquisito nell'esercizio delle proprie funzioni dal personale in servizio presso il Comune: tale documento può essere acquisito dall'AOO con diversi mezzi e modalità, in base alla tecnologia di trasporto utilizzata dal mittente.

I documenti informatici possono essere ricevuti:

- a mezzo posta elettronica ordinaria (PEO) o certificata (PEC);
- attraverso sportelli telematici;
- su supporto rimovibile, quale ad esempio cd rom, dvd o pen drive, consegnato direttamente dal mittente agli Uffici comunali o inviato tramite posta convenzionale, corriere o posta raccomandata.

I documenti analogici possono essere ricevuti:

- a mezzo posta convenzionale o corriere;
- a mezzo posta raccomandata;
- per telegramma;
- con consegna diretta da parte dell'interessato, oppure tramite persona dallo stesso delegata, agli Uffici comunali.

Infine, un documento può essere ricevuto anche in formato "ibrido", cioè composto da un documento analogico (per esempio, una lettera di accompagnamento) e da uno o più documenti digitali.

2.4 Documento inviato

Il documento inviato è un documento formale, ossia dal quale possano nascere diritti, doveri o legittime aspettative di terzi, o utile al fine di documentare fatti inerenti all'attività svolta e alla regolarità delle azioni amministrative di competenza, prodotto all'interno dell'Amministrazione e destinato a persone fisiche, giuridiche o altre amministrazioni all'esterno dell'Ente.

I documenti informatici, compresi di eventuali allegati, sono inviati di norma attraverso un messaggio di posta elettronica certificata.

Per quanto riguarda i documenti analogici, questi possono essere trasmessi al destinatario con i consueti mezzi di trasmissione postale, altresì consegnati a mano, a seconda della tipologia di documento.

2.5 Documento interno formale

Il documento interno formale è un documento prodotto nell'esercizio delle proprie funzioni dal personale in servizio presso il Comune e scambiato tra Direzioni/Strutture/Uffici dell'Ente, anche appartenenti alla stessa Direzione/Struttura.

I documenti interni formali sono prodotti in formato digitale con le opportune tecnologie informatiche. Essi sono sottoscritti con firma digitale al fine di garantirne rilevanza amministrativa giuridico-probatoria. Tale tipologia di documenti è inoltre soggetta a registrazione di protocollo e conservazione.

Si ricorda che la trasmissione di tali documenti interni formali tra Direzioni/Strutture avviene esclusivamente attraverso il Sistema di Protocollo.

2.6 Documento interno informale

Il documento interno informale è un documento prodotto nell'esercizio delle proprie funzioni dal personale in servizio presso il Comune e scambiato tra Direzioni/Strutture/Uffici dell'Ente, anche appartenenti alla stessa Direzione/Struttura, che abbia carattere meramente informativo, equivalente a una comunicazione verbale, un appunto, ecc.

Per questi documenti non sono obbligatorie le operazioni di sottoscrizione, protocollazione e conservazione.

2.7 Formazione dei documenti: aspetti operativi

I documenti dell'Amministrazione sono prodotti in originale attraverso strumenti informatici, come previsto dal CAD, art. 23.

Ogni documento prodotto per essere inoltrato formalmente:

- deve trattare un unico argomento, indicato in maniera sintetica ed esaustiva nell'oggetto;
- deve essere identificato univocamente da un solo numero di protocollo;
- deve essere classificato secondo il titolario di classificazione;
- può fare riferimento a più fascicoli.

Le firme (in caso di documento analogico, le sottoscrizioni autografe), necessarie al perfezionamento sotto il profilo giuridico del documento in partenza, devono essere apposte prima della sua protocollazione.

Il documento deve consentire l'identificazione dell'Amministrazione del Comune di Genova attraverso le seguenti informazioni:

- denominazione e logo dell'Amministrazione;
- indicazione completa dell'AOO, della Direzione e della Struttura che ha prodotto il documento;
- indirizzo completo dell'Amministrazione (via, numero civico, CAP, città, provincia);
- riferimenti telefonici e indirizzo mail della Direzione/Struttura.

Il documento deve inoltre recare almeno le seguenti informazioni:

- luogo di redazione;
- data (giorno, mese, anno);
- oggetto;
- numero degli allegati, se presenti;
- riferimenti del firmatario;
- in caso di documento digitale, firma elettronica qualificata (digitale) del responsabile;
- in caso di documento analogico, sottoscrizione autografa del responsabile.

2.7.1 Modalità di formazione dei documenti informatici

I documenti informatici sono formati mediante una delle seguenti modalità:

- redazione tramite l'utilizzo di appositi strumenti software;
- acquisizione per via telematica o su supporto informatico;
- acquisizione della copia per immagine su supporto informatico di un documento analogico;
- acquisizione della copia informatica di un documento analogico;
- registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente, per esempio tramite sportello telematico;

- generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica, per esempio registro giornaliero di protocollo.

Nel caso di documento informatico redatto tramite l'utilizzo di appositi strumenti software, le caratteristiche di immodificabilità e di integrità sono determinate da una o più delle seguenti operazioni:

- sottoscrizione con firma digitale o con firma elettronica qualificata;
- apposizione di una validazione temporale;
- trasferimento a soggetti terzi con posta elettronica certificata (PEC) con ricevuta completa;
- memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza;
- versamento ad un sistema di conservazione.

2.8 Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.

La firma digitale, strumento utile a soddisfare i requisiti di integrità e immodificabilità dei documenti con valenza giuridico-probatoria:

- deve riferirsi in maniera univoca ad un solo soggetto e al documento o all'insieme di documenti cui è apposta o associata;
- per la sua generazione si deve utilizzare una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa a opera del soggetto pubblico o privato che l'ha certificata;
- attraverso di essa si devono poter rilevare gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.

Prima della sottoscrizione con firma digitale, i documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, sono eventualmente convertiti in uno dei formati standard previsti dalla normativa vigente in materia di gestione documentale e conservazione (LLGG, Allegato 2) ed elencati nell'*Allegato 3 – Formati* al fine di garantire la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

2.9 Requisiti degli strumenti informatici di scambio

Gli strumenti informatici di scambio dei documenti e gli standard di composizione dei messaggi di posta elettronica certificata garantiscono sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- il non ripudio del messaggio;
- la riservatezza del messaggio;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno dell'AOO;
- l'interconnessione tra le Direzioni e le Strutture, in caso di documenti interni formali e informali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

2.10 Verifica delle firme digitali nel Sistema di Protocollo

I documenti sottoscritti con firma digitale sono sottoposti a verifica di validità: questo processo si realizza con modalità conformi a quanto prescritto dalla normativa vigente in materia.

Nel Sistema di Protocollo sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti. La sequenza delle operazioni previste dal Sistema è la seguente:

- apertura della busta "virtuale" contenente il documento firmato;
- verifica della validità del certificato, attività realizzata tramite verifica on-line delle Certificate Revocation List (CRL);
- durante l'apposizione della firma, verifica dell'utilizzo di un certificato emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati;
- segnalazione all'operatore dell'esito della verifica.

2.11 Interoperabilità tra Pubbliche Amministrazioni: posta elettronica certificata

La trasmissione ad altre Pubbliche Amministrazioni di documenti informatici soggetti a registrazione di protocollo è effettuato mediante messaggi, codificati in formato XML, conformi ai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME definito nelle specifiche pubbliche RFC 821-822, RFC 2045-2049 e successive modificazioni o integrazioni.

Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei Sistemi di Protocollo tra Pubbliche Amministrazioni.

Allo scopo di effettuare la trasmissione di un documento dal Comune di Genova ad un'altra Pubblica Amministrazione utilizzando l'interoperabilità dei Sistemi di Protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno: denominazione, indirizzo, casella di posta elettronica);
- convertire il documento in uno dei formati elencati nell'*Allegato 3 – Formati*;
- firmare il documento (ed eventualmente associare il riferimento temporale al documento firmato);
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato digitalmente alla casella di posta istituzionale del destinatario.

L'utilizzo della PEC consente di:

- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre amministrazioni.

La data e l'ora di trasmissione o di ricezione di un documento informatico tramite posta elettronica certificata sono opponibili ai terzi. La trasmissione del documento informatico per via telematica, con una modalità che assicuri l'avvenuta consegna, equivale alla notifica per mezzo della posta nei casi consentiti dalla legge.

3. PROCESSO DI GESTIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, inviati o interni, oltre che le regole di gestione documentale dell'Ente. Per descrivere i flussi di lavorazione dei documenti all'interno dell'AOO si fa riferimento ai diagrammi di flusso riportati nei sottocapitoli successivi.

Essi si riferiscono a:

- Documenti ricevuti da soggetti esterni all'AOO;
- Documenti inviati a soggetti esterni all'AOO;
- Documenti interni all'AOO.

3.1 Documenti in ingresso

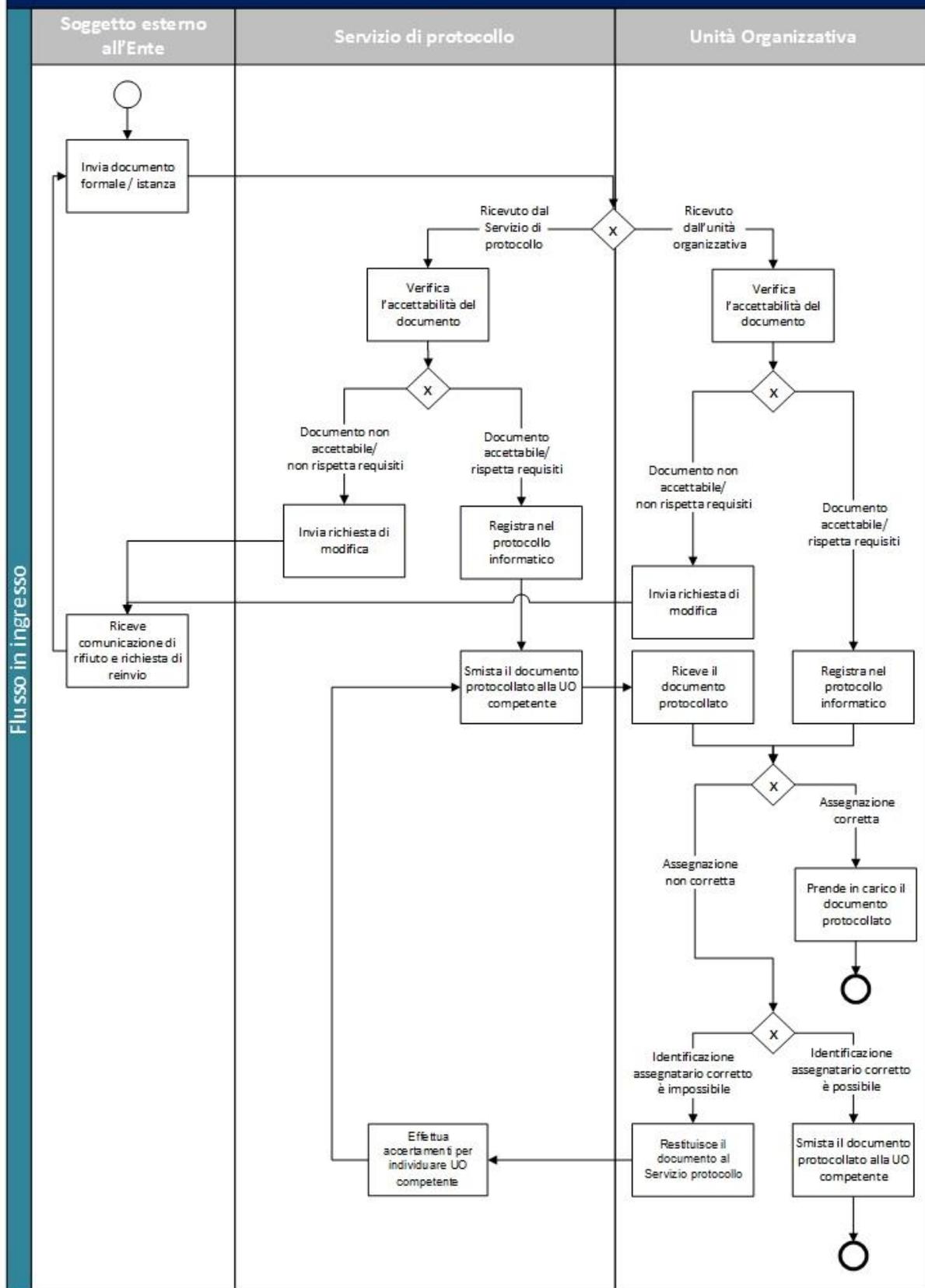
Il presente sotto capitolo descrive il flusso di lavorazione dei documenti inviati da soggetti esterni all'AOO e le regole di registrazione dei documenti pervenuti tramite diversi canali di ricezione: per "sorgente esterna dei documenti" si intende un soggetto mittente, esterno all'Amministrazione, che invia corrispondenza all'AOO nelle forme e con i mezzi descritti nel presente Manuale.

Presso l'Amministrazione è presente un servizio centrale di protocollazione, utile alla gestione centralizzata della documentazione in ingresso, sia in formato cartaceo ricevuta attraverso lo sportello di protocollo generale, sia in formato digitale ricevuta attraverso la casella PEC istituzionale.

A ogni Direzione compete la registrazione a protocollo e la gestione dei documenti ricevuti mezzo posta elettronica sulle caselle e-mail di Direzione, sia certificate che ordinarie, oltre che dell'eventuale documentazione cartacea ricevuta direttamente presso gli uffici delle singole Strutture, purché attinenti a procedimenti amministrativi di propria competenza.

Il flusso dei documenti in ingresso è rappresentato graficamente in Figura 1.

Figura 1: Processo documentale in ingresso



3.1.1 Ricezione di documenti informatici sulla casella di posta certificata istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella PEC istituzionale. Il personale del servizio centrale di protocollazione controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale. Quando i documenti informatici pervengono all'AOO, il servizio centrale di protocollazione, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo e all'assegnazione alle Direzioni/Strutture di competenza. Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente senza registrazione a protocollo.

3.1.2 Ricezione di documenti informatici sulla casella di posta elettronica certificata non istituzionale

I documenti informatici ricevuti tramite messaggi e-mail sulle caselle di posta elettronica certificata delle Direzioni devono essere inseriti nel flusso di lavorazione del Protocollo Informatico. Le Direzioni/Strutture si fanno carico di tale attività, procedendo con la protocollazione, segnatura, classificazione e assegnazione dei documenti ricevuti.

3.1.3 Ricezione di documenti informatici sulla casella di posta elettronica ordinaria

Tenuto conto che il canale ordinario di trasmissione informatica dei documenti formali è la casella PEC istituzionale dell'Ente e delle varie Direzioni/Strutture, nel caso di documenti informatici ricevuti tramite caselle PEO riferite a Strutture o personale dell'Ente, il destinatario valuta l'opportunità di protocollazione dell'e-mail ricevuta e di eventuali allegati, procedendo direttamente all'operazione e suggerendo al mittente di non utilizzare questo canale di trasmissione per le future comunicazioni, indicando inoltre il riferimento corretto.

3.1.4 Ricezione di documenti informatici su supporti rimovibili o servizi "file transfer"

Nel caso di ricezione di documenti informatici su supporti rimovibili (dvd, usb, dischi esterni rimovibili, ecc.) o servizi "file transfer", l'AOO si riserva la facoltà di acquisire e trattare solo i documenti informatici che riesce a decodificare e interpretare con le tecnologie a propria disposizione, di cui all'*Allegato 3 - Formati*. Superata questa fase il documento viene scaricato e inserito all'interno del sistema di protocollo, anche quale allegato della eventuale lettera di accompagnamento debitamente registrata a protocollo, e sottoposto a tutti i controlli e gli adempimenti del caso.

3.1.5 Ricezione di documenti informatici con più allegati scorporati in invii successivi

Qualora il mittente faccia pervenire il documento principale e parte degli allegati con un primo invio e poi faccia seguire altri eventuali allegati in uno o più invii aggiuntivi, tutte le e-mail ricevute devono essere protocollate. Sarà cura delle Direzioni/Strutture di competenza utilizzare come riferimento dell'istanza il primo numero di protocollo in ordine cronologico, al quale verranno collegati i successivi invii, e di darne

eventuale notizia al mittente, vista la pluralità di numeri di protocollo, con le modalità ritenute più opportune.

3.1.6 Ricezione di documenti informatici prodotti in formati non accettati

Per i documenti informatici è fondamentale preoccuparsi sin dal momento della loro acquisizione che gli stessi siano prodotti in formati il più possibile stabili e codificati, così da consentire la trasmissione al servizio di conservazione e la conseguente decifrabilità a distanza di tempo.

Qualora pervengano documenti informatici in formati non congruenti con l'elenco riportato nel presente Manuale, il servizio centrale di protocollazione inoltra il documento alla Direzione/Struttura competente, affinché questa possa tempestivamente contattare il mittente per richiedere un nuovo invio di files in formati accettati.

3.1.7 Ricezione di documenti informatici con anomalie, contenuti illeggibili o instabili

Qualora il documento informatico, o i suoi allegati, risultino illeggibili perché deteriorati o qualora il documento contenga campi variabili, non stabili nel tempo (es. collegamenti ipertestuali, link a pagine web ecc.) il servizio centrale di protocollazione non procede alla protocollazione, ma inoltra mezzo mail il documento alla Direzione/Struttura di riferimento. Quest'ultima, dopo aver esaminato il documento, se lo ritiene opportuno, procede alla protocollazione o si attiva nei confronti del mittente perché proceda ad effettuare un nuovo invio sanando le anomalie o le situazioni di illeggibilità/instabilità dei contenuti che non hanno consentito la protocollazione.

3.1.8 Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta convenzionale sono gestiti dal servizio centrale di protocollazione e dalle segreterie di Direzione. Le buste, o contenitori, sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario apposti sugli stessi. A seguito di tale verifica preliminare, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione. La corrispondenza in ingresso viene, di norma, aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata e assegnata. La busta viene allegata al documento per la parte recante i timbri postali.

Si precisa che la corrispondenza relativa a bandi di gara, per le procedure ancora svolte in forma cartacea, non viene aperta, ma viene protocollata in arrivo con l'apposizione del numero di protocollo e della data e ora di registrazione direttamente sulla busta, plico o simili, e inviata alla Struttura interessata. Dopo l'apertura delle buste sarà cura della Struttura che gestisce la gara riportare gli estremi di protocollo su tutti i documenti in esse contenuti.

La corrispondenza ricevuta via telegramma, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo.

3.1.9 Ricezione di documenti presentati allo sportello di protocollo generale

I documenti presentati direttamente allo sportello di protocollo generale sono di norma registrati a protocollo, segnati e assegnati alle Direzioni/Strutture destinatarie, per competenza o conoscenza, entro la giornata di ricezione. Qualora fossero competenti più Direzioni/Strutture in relazione allo stesso documento, viene individuata la Struttura capofila quale prima assegnataria: ad essa è consegnato il documento ricevuto, la quale si occupa di trasmetterne copia in formato digitale agli altri destinatari.

3.1.10 Ricezione di documenti presentati direttamente alle Strutture

I documenti recapitati direttamente alle Strutture sono da queste registrati a protocollo, segnati, classificati e assegnati. Quando le Strutture ricevono direttamente dei documenti di competenza di una Struttura differente, i documenti sono inoltrati o al servizio competente, se di pronta individuazione, per la protocollazione e presa in carico, o al servizio centrale di protocollo, che si occuperà della trasmissione o assegnazione alla Struttura di competenza, previa protocollazione.

3.1.11 Ricezione dei medesimi documenti pervenuti da sorgenti diverse

Qualora un medesimo documento pervenisse all'AOO più di una volta, ovvero ricevuto da più fonti diverse (es. prima via PEC, poi cartaceo), verrà registrato a protocollo il primo documento ricevuto. Ai medesimi documenti ricevuti successivamente saranno attribuiti lo stesso numero e la stessa data di protocollo già assegnati, purché ne sia possibile il collegamento.

Qualora i documenti siano stati protocollati con numeri diversi, ai fini del calcolo dei tempi del procedimento amministrativo si tiene conto della data archivistica di quello protocollato per primo.

3.1.12 Ricezione di documenti analogici indirizzati al personale del Comune di Genova

La posta indirizzata nominativamente al personale dell'AOO viene regolarmente aperta e registrata nel Sistema di Protocollo, a meno che sulla busta non sia riportata la dicitura "riservata" e/o "personale". In tal caso viene recapitata in busta chiusa al destinatario il quale, dopo aver preso visione del contenuto e verificato che il documento non è personale, procede con le opportune attività di protocollazione.

3.1.13 Ricezione di documentazione non firmata e corrispondenza anonima

Le lettere anonime e/o i documenti non firmati non sono registrate nel Sistema di Protocollo, ma inoltrate alla Direzione/Struttura competente, che valuta l'opportunità di dare seguito alle comunicazioni se contengono informazioni o dati di interesse per l'Amministrazione, individuando le eventuali procedure da sviluppare. In caso di particolare rilevanza per l'Amministrazione, la Direzione/Struttura competente procede con la protocollazione.

3.1.14 Ricezione di documento analogico erroneamente indirizzato al Comune di Genova

Nel caso in cui il servizio centrale di protocollazione ritenga ci sia la certezza che il documento è indirizzato effettivamente al Comune di Genova, procede d'ufficio alla protocollazione. Qualora invece il documento sia ricevuto per errore dal Comune di Genova, il documento è protocollato ed è comunicato al mittente l'errore di invio.

3.1.15 Ricezione di documento digitale erroneamente indirizzato al Comune di Genova

Nel caso in cui pervengano sulla casella di posta elettronica certificata istituzionale dell'AOO, altresì su ulteriori PEC non istituzionali, messaggi dal cui contenuto si rileva che siano stati erroneamente destinati

all'AOO, l'operatore, previa protocollazione, spedisce un messaggio al mittente recante la dicitura "Messaggio erroneamente indirizzato al Comune di Genova - non di competenza dell'Ente".

3.1.16 Rilascio di ricevute attestanti la ricezione di documenti informatici

La ricezione di documenti comporta l'invio al mittente di due tipologie diverse di ricevute: una legata al servizio di posta certificata, l'altra al servizio di protocollazione informatica.

La notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti e se ritenuto opportuno, può provvedere alla formazione e all'invio al mittente di uno dei seguenti messaggi:

- messaggio di conferma di protocollazione: un messaggio che contiene la conferma dell'avvenuta protocollazione in ingresso di un documento ricevuto. Si differenzia da altre forme di ricevute di recapito generate dal servizio di posta elettronica dell'AOO in quanto segnala l'avvenuta protocollazione del documento, e quindi l'effettiva presa in carico. Vengono indicati anche il numero di protocollo, la data e l'ora;
- messaggio di notifica di eccezione: un messaggio che notifica la rilevazione di una anomalia in un messaggio ricevuto;
- messaggio di annullamento di protocollazione: un messaggio che contiene una comunicazione di annullamento di una protocollazione in ingresso di un documento ricevuto in precedenza;
- messaggio di aggiornamento di protocollazione: un messaggio che contiene una comunicazione di aggiornamento riguardante un documento protocollato ricevuto in precedenza.

3.1.17 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Quando il documento cartaceo è consegnato direttamente dal mittente, o da altra persona incaricata, al servizio centrale di protocollazione o alla segreteria di Direzione, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'operatore che lo riceve è autorizzato a:

- fotocopiare gratuitamente la prima pagina del documento;
- apporre gli estremi della segnatura se contestualmente alla ricezione avviene anche la protocollazione;
- apporre sulla copia così realizzata il timbro dell'Amministrazione, con la data e l'ora d'arrivo e la sigla dell'operatore.

3.1.18 Archiviazione dei documenti informatici

I documenti informatici ricevuti dall'AOO sono archiviati nel Sistema di Protocollo, contestualmente alle operazioni di registrazione e segnatura. Tali documenti sono resi disponibili alle Direzioni/Strutture di competenza attraverso il medesimo Sistema a seguito dell'operazione di assegnazione.

3.1.19 Archiviazione delle copie per immagine di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione, segnatura e assegnazione, devono essere acquisiti in formato PDF/A a cura della Direzione/Struttura destinataria, attraverso un processo di scansione.

Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento del file delle immagini alle rispettive registrazioni di protocollo, in modo non modificabile;
- memorizzazione del file delle immagini su supporto informatico, in modo non modificabile.

Qualora il documento abbia degli allegati, questi possono essere scansionati con il documento stesso costituendo un unico file, oppure scansionati separatamente (soprattutto in caso di più allegati) e collegati come "allegati" alla rispettiva registrazione di protocollo. I documenti analogici dopo l'operazione di scansione vengono inviati alle Direzioni/Strutture destinatarie per le operazioni di classificazione, fascicolazione e conservazione.

Si ricorda che questa operazione non sostituisce l'originale e la relativa necessità della sua conservazione fisica.

3.1.20 Assegnazione, presa in carico dei documenti e classificazione

L'assegnazione consiste nella identificazione e selezione della Direzione/Struttura competente a cui attribuire il documento protocollato, oltre che la contestuale trasmissione della eventuale documentazione cartacea.

L'assegnazione dei documenti protocollati avviene utilizzando una specifica funzionalità del Sistema di Protocollo, che agevola il processo di selezione dell'assegnatario tramite la navigazione dell'organigramma dell'AOO.

Gli operatori delle Direzioni/Strutture hanno notizia dell'assegnazione dei documenti tramite il Sistema di Protocollo e sono in grado di visualizzare i documenti, ove presenti, attraverso le funzionalità del Sistema stesso. Nel dettaglio gli operatori delle Direzioni/Strutture:

- eseguono una verifica in merito all'effettiva competenza della documentazione;
- in caso di errore restituiscono il documento al servizio centrale di protocollazione;
- in caso di verifica positiva, eseguono l'operazione di presa in carico, riassegnando, se necessario, la documentazione all'ufficio competente;
- eseguono la classificazione e fascicolazione del documento sulla base del titolare di classificazione.

Il Sistema di Protocollo memorizza tutti i passaggi conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione, al fine di individuare i tempi del procedimento amministrativo.

Ciascun Dirigente di Direzione, attraverso i propri Funzionari/Responsabili deve organizzare una corretta gestione del Sistema di Protocollo, garantendo l'accesso quotidiano e la regolare presa in carico, o rifiuto, dei documenti ricevuti per assegnazione. I tempi di smistamento interno, presa in carico o rifiuto devono necessariamente essere tempestivi per garantire il rispetto delle tempistiche procedurali. È fondamentale che la Direzione/Struttura di destinazione gestisca correttamente il documento nel Sistema di Protocollo, per dare traccia di chi effettivamente prende in carico la pratica e ne garantisce pertanto l'evasione. Documenti assegnati e non gestiti dalle Direzioni/Strutture competenti vanificano l'obiettivo di trasparenza e tracciabilità del flusso documentale.

3.2 Documenti in uscita

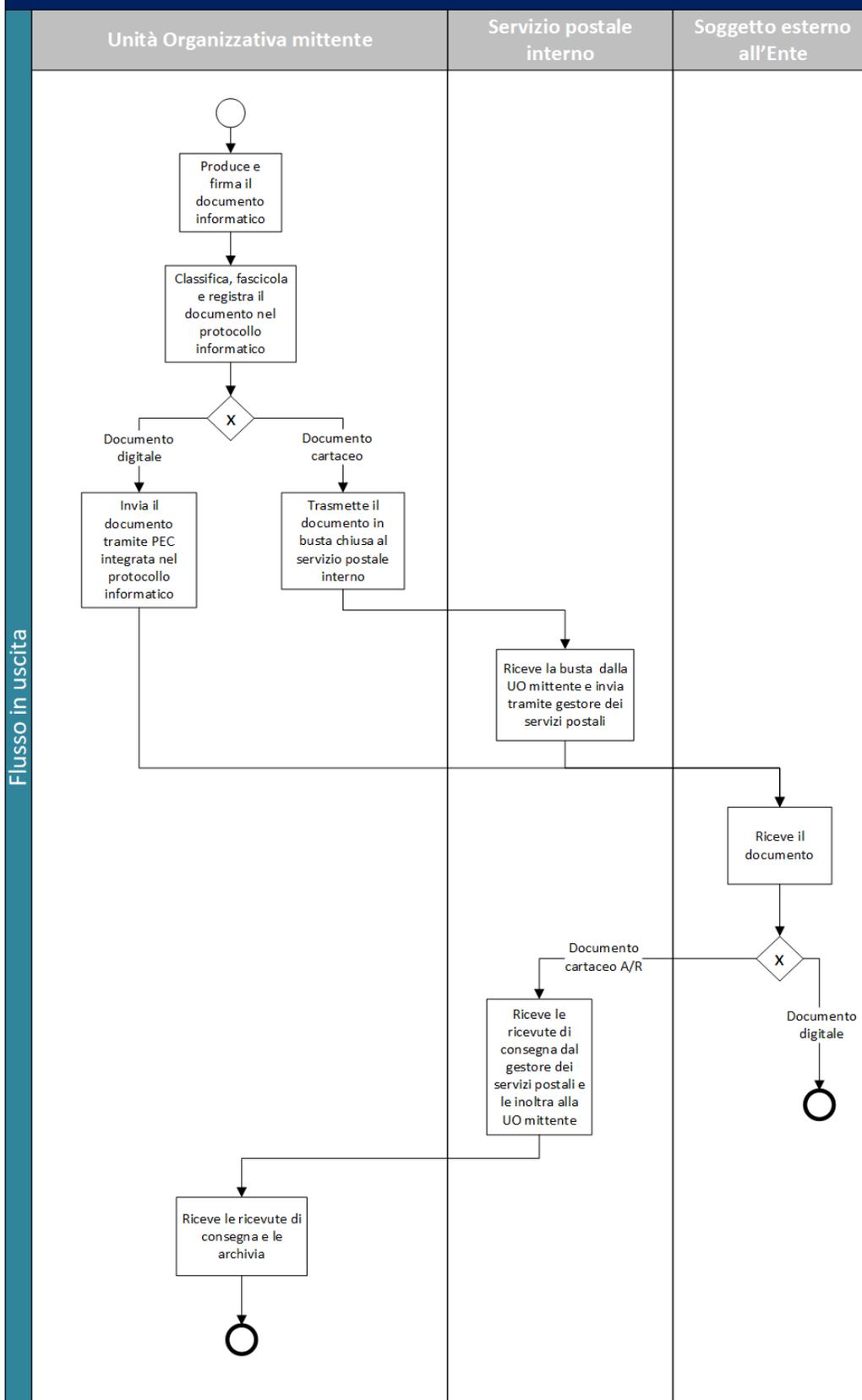
Il presente sottocapitolo descrive il flusso di lavorazione dei documenti inviati a soggetti esterni all'AOO e le regole di trasmissione dei documenti in uscita.

Per "sorgente interna dei documenti" si intende la Direzione/Struttura mittente, interna all'AOO, che invia nelle forme e nelle modalità più opportune la corrispondenza a soggetti esterni all'Amministrazione.

Per "documenti in uscita" si intendono quelli prodotti dal personale delle Direzioni/Strutture dell'AOO nell'esercizio delle proprie funzioni, aventi rilevanza giuridica e destinati ad essere trasmessi ad altra Amministrazione o ad altri soggetti esterni all'AOO.

Il flusso dei documenti in uscita è rappresentato graficamente in Figura 2.

Figura 2: Processo documentale in uscita



3.2.1 Modalità di formazione del documento

Ogni documento prodotto dall'Amministrazione deve essere di tipo informatico, come previsto dalla vigente normativa. Solo in casi particolari e motivati il documento può essere prodotto in formato analogico (cartaceo), il quale dovrà comunque essere archiviato nel Sistema di Protocollo, come documento informatico generato da copia informatica di documento analogico.

Ogni documento da inviare a destinatari esterni all'Amministrazione, a prescindere dal formato, deve essere redatto sul modello di "carta intestata" e deve contenere i dati esposti nel presente Manuale al capitolo 2.7.

3.2.2 Verifica formale dei documenti

Tutti i documenti originali da spedire devono, siano essi in formato digitale o analogico, devono essere previste opportune verifiche di conformità della documentazione allo standard formale richiamato nel presente Manuale. Solo se il documento è completo viene registrato nel protocollo generale.

3.2.3 Classificazione, fascicolazione, segnatura e registrazione di protocollo

Il sistema di protocollazione in uscita è totalmente decentralizzato: le operazioni di registrazione di protocollo e di apposizione della segnatura dei documenti in uscita sono effettuate dalle Direzioni, o Strutture afferenti, responsabili dei documenti stessi.

Tutti i documenti in uscita sono, per obbligo normativo, oggetto di protocollazione.

In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili.

I documenti in originale analogico (da utilizzarsi esclusivamente nei casi in cui non sia possibile produrre il documento informatico) sono sempre acquisiti in formato PDF/A attraverso un processo di scansione e allegati alla rispettiva registrazione di protocollo.

I documenti in uscita vengono classificati sulla base del titolario di classificazione, oltre che fascicolati, a cura dell'unità organizzativa che li ha prodotti, protocollati ed eventualmente scansionati.

3.2.4 Trasmissione di documenti informatici

La trasmissione di documenti informatici, a seguito della loro protocollazione, avviene per mezzo della posta elettronica certificata integrata al sistema di protocollo. Ogni Direzione, o Struttura afferente, è responsabile della trasmissione dei documenti informatici prodotti nello svolgimento delle proprie funzioni.

I documenti informatici sono quindi trasmessi all'indirizzo elettronico dichiarato dai destinatari.

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla normativa vigente. Per la spedizione dei documenti informatici, infatti, il Comune di Genova si avvale del servizio di posta elettronica certificata, conforme a quanto previsto dal Decreto del Presidente della Repubblica 11/02/2005, n. 68, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.

Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono duplicare o cedere a terzi a qualsiasi titolo informazioni, anche in forma sintetica o per estratto, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa

indicazione del mittente sono destinate ad essere rese pubbliche.

3.2.5 Trasmissione di documenti cartacei a mezzo posta

L'ufficio del servizio postale del Comune di Genova provvede direttamente a tutte le operazioni di spedizione della corrispondenza compresa l'affrancatura dei documenti in partenza già protocollati dalle Direzioni/Strutture mittenti. Nel dettaglio:

- consegna all'ufficio postale tutta la corrispondenza;
- predispone le ricevute di invio e di ritorno per le raccomandate, unitamente alla distinta delle medesime da rilasciare all'ufficio postale;
- predispone la lista di restituzione degli esiti di invio per le Direzioni/Strutture.

3.2.6 Inserimento delle ricevute di trasmissione nel fascicolo

La copia del documento cartaceo spedito e le ricevute delle raccomandate sono conservate all'interno del relativo fascicolo.

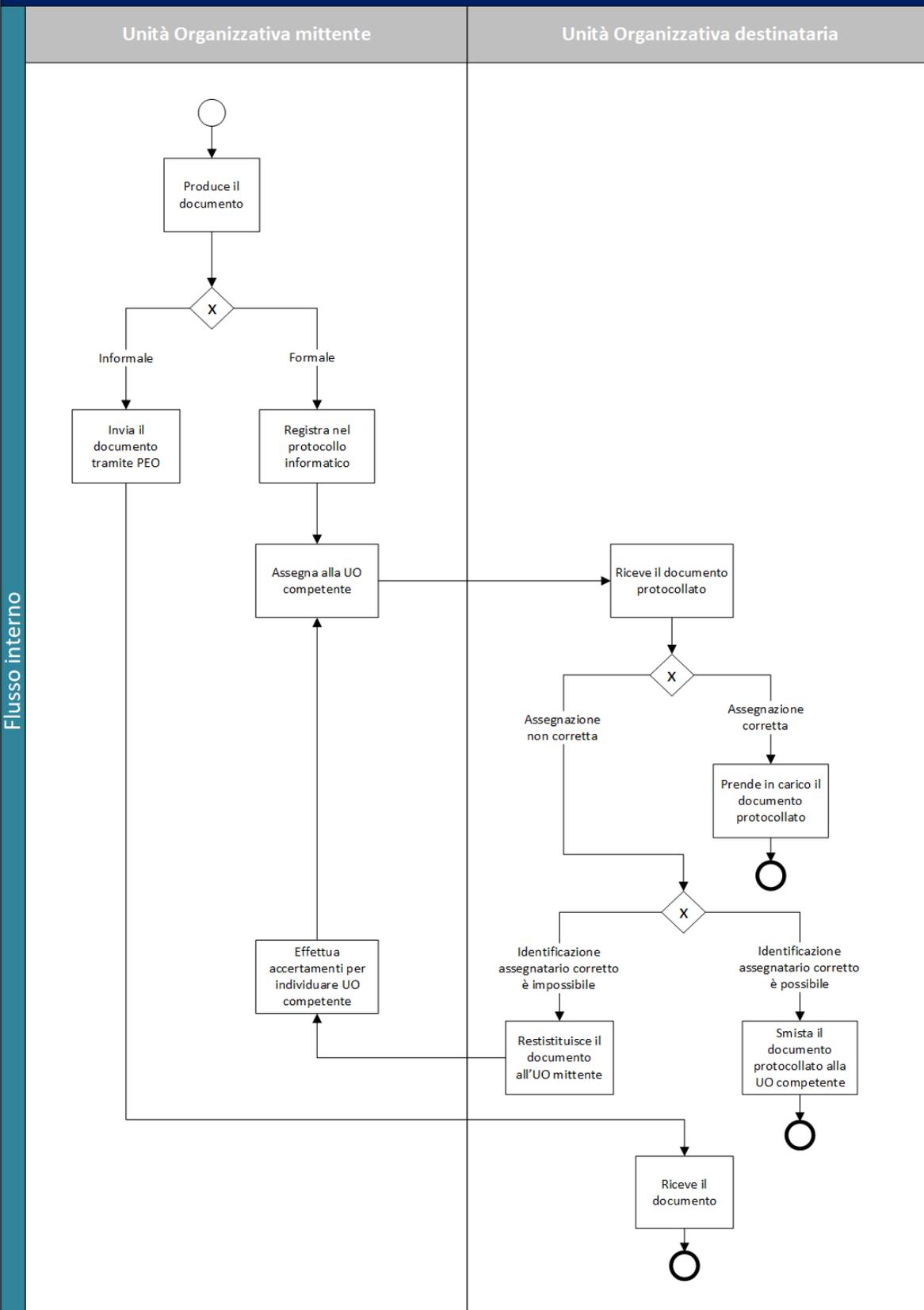
Tale attività è svolta dalle Direzioni, o Strutture afferenti, in quanto responsabili del fascicolo stesso.

3.3 Documenti interni

Il presente sottocapitolo descrive il flusso di lavorazione dei documenti interni all'AOO, siano essi formali che informali.

Il flusso dei documenti interni è rappresentato graficamente in Figura 3.

Figura 3: Processo documentale interno



3.3.1 Documenti interni formali

I documenti interni formali sono redatti con tecnologie informatiche sul modello di “carta intestata” e devono contenere i dati esposti nel presente Manuale al capitolo 2.7. Essi devono essere informatici e sottoscritti con firma digitale: possono essere cartacei solo in casi particolari e motivati.

Le fasi di produzione, classificazione, fascicolazione, registrazione e segnatura di protocollo si attengono a quanto previsto nel presente Manuale. Il responsabile del documento effettua la sua protocollazione; la trasmissione del documento avviene attraverso il Sistema di Protocollo, con l’assegnazione dello stesso al destinatario.

I documenti formali informatici, redatti da una UO nello svolgimento delle proprie funzioni, nell’ambito dei procedimenti da essa gestiti e non indirizzati a specifiche Direzioni, dovranno essere protocollati ai sensi del TUDA, art. 53, comma 5.

3.3.2 Documenti interni informali

I documenti interni informali sono redatti, di norma, con tecnologie informatiche. Lo scambio dei documenti interni informali avviene, per prassi, utilizzando l’account e-mail personale assegnato a ciascun dipendente. Nel caso in cui il documento, o eventuali allegati associati, superino la dimensione massima consentita dal sistema di posta elettronica la trasmissione al destinatario avviene tramite il sistema di condivisione file adottato dall’AOO (servizio invio file grandi dimensioni nella rete informatica del Comune di Genova). Inoltre, se si ritiene opportuno ai fini della tracciabilità del procedimento, anche i documenti interni informali possono essere archiviati e fascicolati nel sistema di gestione documentale del Comune di Genova.

4. PROTOCOLLAZIONE

Il presente capitolo illustra le modalità di produzione e di conservazione delle registrazioni di protocollo informatico, nonché le modalità di registrazione delle informazioni annullate o modificate nell’ambito di ogni sessione di attività di registrazione.

In conformità con quanto indicato nel TUDA, art. 53, comma 5, sono esclusi dalla registrazione di protocollo tutti i seguenti documenti:

- le gazzette ufficiali
- i bollettini ufficiali
- i notiziari della Pubblica Amministrazione
- le note di ricezione delle circolari e altre disposizioni
- i materiali statistici
- gli atti preparatori interni
- i giornali, le riviste, i libri
- i materiali pubblicitari
- gli inviti a manifestazioni
- tutti i documenti già soggetti a registrazione particolare dell’Amministrazione.

A titolo di esempio, le Delibere di Giunta e di Consiglio, le ordinanze sindacali, i contratti in forma pubblica e amministrativa, nonché i mandati, le reversal, e documenti contabili come le fatture.

4.1 Registro informatico di protocollo

Il registro di protocollo è l'atto pubblico che certifica il ricevimento e la spedizione di documenti ad una certa data, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti. Tale registro è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

4.1.1 Registro giornaliero di protocollo

Il registro giornaliero di protocollo è costituito dall'elenco di tutte le registrazioni di protocollo effettuate dall'AOO nell'arco di uno stesso giorno. Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo, il sistema di protocollazione automaticamente provvede, in fase di chiusura dell'attività di protocollo giornaliera, all'estrazione delle registrazioni di protocollo del giorno corrente. Inoltre, per garantire la non modificabilità delle operazioni di registrazione, il registro giornaliero di protocollo è riversato, al termine della giornata lavorativa, nel sistema di conservazione.

4.2 Gestione delle registrazioni di protocollo con il Sistema di Protocollo

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate solo ed esclusivamente attraverso il Sistema di Protocollo, che è unico per l'AOO.

Inoltre, il sistema di sicurezza garantisce la protezione di tali informazioni sulla base della relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

4.3 Principali regole per la registrazione di protocollo

Di seguito sono illustrate le principali regole di registrazione del protocollo, valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi e interni formali, siano essi informatici o analogici). Su ogni documento ricevuto e spedito dall'AOO, altresì per i documenti interni formali, è effettuata una registrazione di protocollo con il Sistema di Protocollo, consistente nella memorizzazione dei dati obbligatori. Tale registrazione è eseguita in un'unica operazione, senza possibilità, per l'operatore, di inserire quelle che sono informazioni obbligatorie in fasi successive. Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- numero di protocollo, generato automaticamente dal Sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal Sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, destinatario per i documenti spediti oggetto del documento;
- impronta del documento informatico, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, assegnata automaticamente dal Sistema e registrata in forma non modificabile;
- classificazione e fascicolazione, per i documenti in uscita e interni.

Le variazioni su "oggetto", "mittente" o "destinatario", "documento principale" ed "allegati" vengono mantenute con un criterio di storicizzazione dal Sistema di Protocollo, evidenziando data, ora, motivazione e utente che ha effettuato la modifica.

Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.

4.4 Registrazione di protocollo di documenti informatici

I documenti informatici sono ricevuti e trasmessi, in modo formale, attraverso la casella di posta elettronica certificata istituzionale dell'AOO. La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore abilitato alle attività di protocollo ne ha accertato l'autenticità, la provenienza, l'integrità e ha verificato la validità della firma.

Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto o inviato.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere a ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio che a uno dei file ad esso allegati che può assumere la veste di documento principale. Tali documenti sono memorizzati nel Sistema di protocollo, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

4.5 Registrazione di protocollo di documenti analogici

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.

La registrazione di protocollo di un documento cartaceo ricevuto viene sempre eseguita in quanto l'AOO ha la funzione di registrarne l'avvenuta ricezione, ovvero la sequenzialità, la data e l'ora di ricezione di un determinato documento. Nel caso in cui al documento ricevuto non sia connesso alcun procedimento amministrativo di competenza dell'AOO, si procederà a riferire al mittente che la comunicazione ricevuta non avrà alcun seguito.

Nel caso di corrispondenza in uscita, gli operatori incaricati di ogni Direzione/Struttura eseguono la registrazione di protocollo solo dopo che il documento ha superato tutti i controlli formali.

4.6 Elementi facoltativi delle registrazioni di protocollo

Di seguito vengono riportati gli elementi facoltativi in fase di registrazione di protocollo, finalizzati alla conservazione e gestione della documentazione:

- ulteriori informazioni sul mittente/destinatario (es. indirizzo completo del mittente/destinatario: via, numero civico, CAP, città, provincia, stato);
- collegamento a registrazioni precedenti e susseguenti;
- data e ora di ricezione;
- eventuale numero e data di protocollo originario, assegnato da altro soggetto diverso dal Comune di Genova;
- tipologia di documento;
- mezzo di ricezione/spedizione;
- livello di riservatezza.

La registrazione degli elementi facoltativi del protocollo, comprese eventuali modifiche, integrazioni e cancellazioni, in base alle effettive esigenze delle Direzioni/Strutture responsabili dei documenti protocollati, non viene tracciata dal Sistema di Protocollo.

4.7 Segnatura di protocollo dei documenti informatici

La segnatura di protocollo è l'apposizione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti la registrazione di protocollo del documento stesso. Essa consente di individuare ciascun documento in modo univoco e certo.

L'operazione di segnatura di protocollo di documenti informatici viene effettuata, in maniera automatica, dal Sistema di Protocollo contestualmente all'operazione di registrazione di protocollo. La segnatura di protocollo apposta ai documenti informatici registrati nel registro di protocollo riporta almeno le seguenti informazioni obbligatorie:

- codice identificativo dell'Amministrazione;
- codice identificativo dell'AOO;
- codice identificativo del registro di protocollo;
- data di protocollo;
- numero progressivo di protocollo.

In caso di documento firmato digitalmente, la segnatura di protocollo viene apposta a una copia del documento associata al numero di protocollo e archiviata nel Sistema di Protocollo insieme al documento firmato digitalmente.

Nel caso di documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo comprendono anche:

- oggetto del documento;
- mittente;
- destinatario o destinatari.

Eventualmente, anche:

- indicazione della persona o dell'ufficio all'interno della struttura destinataria a cui si presume verrà affidato il trattamento del documento;
- indice di classificazione;
- identificazione degli allegati;
- informazioni sul procedimento a cui si riferisce e sul trattamento da applicare al documento.

Nel caso di documenti informatici trasmessi ad altre Pubbliche Amministrazioni, i dati relativi alla segnatura di protocollo devono essere associati al documento stesso e contenuti nel messaggio in un file conforme alle specifiche dell'Extensible Markup Language (XML), compatibile con un file XML Schema e/o DTD (Document Type Definition), definito e aggiornato periodicamente da AgID.

Le modifiche periodiche di AgID sono da applicare al Sistema di Protocollo dell'Ente nel più breve tempo tecnico/amministrativo possibile, senza che questo comporti la necessità di revisione del presente Manuale. Lo stesso vale anche qualora sia necessario trasmettere maggiori informazioni per lo scambio di documenti con altre Amministrazioni, ai sensi del Decreto del Presidente del Consiglio dei Ministri, 03/12/2013, art. 21, comma 3, e nel rispetto delle indicazioni tecniche stabilite da AgID.

4.8 Segnatura di protocollo dei documenti cartacei

La segnatura di protocollo di un documento cartaceo in entrata avviene attraverso l'apposizione di un timbro da parte dell'utente che effettua la protocollazione, sul quale sono riportate le seguenti informazioni minime relative alla registrazione di protocollo:

- denominazione dell'AOO
- data e numero di protocollo del documento.

Per quanto concerne invece i documenti in uscita, l'operazione di segnatura viene eseguita dalla Direzione/Struttura che redige il documento, in fase di protocollazione dello stesso e consistente

nell'apposizione del numero e della data di registrazione.

4.9 Annullamento e modifica delle registrazioni di protocollo

L'annullamento anche di una sola delle informazioni generate o assegnate automaticamente dal Sistema di Protocollo e registrate in forma immodificabile, quali numero e data di protocollo, determina l'automatico e contestuale annullamento dell'intera registrazione di protocollo. Il Sistema di Protocollo tiene traccia dell'annullamento tramite una dicitura o un segno. Inoltre, consente la lettura di tutte le informazioni originarie, unitamente alla data, all'identificativo dell'operatore e agli estremi del provvedimento d'autorizzazione dell'operazione di annullamento.

Altresi, la modifica anche di un solo campo delle altre informazioni obbligatorie registrate, quali mittente/destinatario, oggetto, documento principale e allegati, necessaria alla correzione di errori intercorsi in sede di immissione dei dati, comporta la rinnovazione del campo stesso con i dati corretti e la contestuale memorizzazione a sistema, in modo permanente, del valore precedentemente attribuito unitamente a data, ora, autore e motivazione della modifica.

Diversamente, le operazioni di rettifica dei dati di una registrazione nel registro di protocollo, necessarie a sanare un mero errore materiale, sono effettuate dagli operatori abilitati a tali funzioni.

4.10 Livello di riservatezza

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal Sistema di Protocollo.

In modo analogo, in sede di apertura di un nuovo fascicolo viene definito il livello di riservatezza dello stesso. Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

4.11 Protocollo di emergenza

Qualora per cause tecniche non sia possibile utilizzare il Sistema di Protocollo per un periodo di tempo significativo, il Responsabile del Servizio di Protocollo autorizza lo svolgimento delle operazioni di protocollazione su un registro di emergenza, ai sensi del TUDA, art. 63.

Il Responsabile del Servizio di Protocollo provvede successivamente ad impartire le disposizioni per il riversamento dei dati nel Sistema di Protocollo tramite le procedure previste dal manuale operativo del Sistema Informatico e dalla guida all'attivazione del registro di emergenza (*Allegato 4 – Registro di emergenza*).

5. CLASSIFICAZIONE

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO, finalizzata all'organizzazione logica di tutti i documenti prodotti o ricevuti dall'Ente nell'esercizio delle sue funzioni per la tracciabilità e il reperimento degli stessi.

L'attività di classificazione si avvale del titolare di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente: per la consultazione dello stesso si rimanda all'*Allegato 5 – Titolare di classificazione*.

Sono soggetti a classificazione tutti i documenti informatici, sia quelli protocollati che quelli che fanno parte di eventuali registri particolari, a prescindere dal loro stato di trasmissione e dal supporto utilizzato. In quanto strumento di prima organizzazione dei documenti, la classificazione si applica contestualmente allo svolgimento delle attività correnti e mai a posteriori in archivi già formati secondo criteri diversi. Le operazioni di classificazione devono essere svolte interamente dalle Direzioni/Strutture destinarie o istruttorie di atti.

5.1 Il titolario di classificazione

Il titolario (o piano) di classificazione è lo schema logico astratto utilizzato per organizzare i documenti d'archivio secondo una struttura ad albero definita sulla base delle funzioni proprie del Comune di Genova, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi, a prescindere dalla struttura organizzativa dell'Ente.

Il titolario di classificazione si suddivide in titoli, classi e sottoclassi, o più in generale in voci di I livello, II livello, III livello: non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito della Giunta Comunale.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'Ente (macrofunzioni), le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero, secondo lo schema riportato nell'*Allegato 5 – Titolario di classificazione*.

Il titolario può essere soggetto ad aggiornamenti, dato che descrive le funzioni e le competenze dell'Ente, suscettibili di modifiche in forza delle leggi e dei regolamenti statali e regionali. L'aggiornamento del titolario compete esclusivamente alla Giunta Comunale, su proposta del Responsabile del Servizio di Protocollo. Dopo ogni modifica, il Responsabile del Servizio di Protocollo provvede ad informare tutti i soggetti abilitati all'operazione di classificazione dei documenti e a dare loro le istruzioni per il corretto utilizzo delle nuove classifiche.

Il titolario non è retroattivo, cioè non si applica ai documenti protocollati prima della sua introduzione.

Il Sistema di protocollo garantisce la storicizzazione delle differenti versioni di titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.

6. AGGREGAZIONI DOCUMENTALI

L'AOO documenta la propria attività utilizzando funzionalità del sistema di gestione informatica dei documenti, finalizzate alla produzione, alla gestione e all'uso delle seguenti aggregazioni documentali:

- fascicolo = aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico affare/procedimento;
- serie di documenti = costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento;
- serie di fascicoli = costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

Il sistema di gestione informatica dei documenti dell'AOO permette la gestione, formazione, utilizzo di serie secondo il piano di classificazione o di fascicolatura.

Si precisa inoltre che fascicoli appartenenti a serie diverse possono essere collegati tra loro. I criteri di fascicolazione sono indicati all'interno dell'*Allegato 6 – Piano di fascicolazione*.

6.1 Fascicolazione dei documenti

La fascicolazione è l'attività di riconduzione logica di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla pratica relativa.

Tutti i documenti registrati e classificati nel sistema di gestione documentale sono inseriti in fascicoli di riferimento, indipendentemente dal formato.

I documenti sono archiviati all'interno di ciascun fascicolo o sottofascicolo secondo l'ordine cronologico di registrazione.

6.2 Apertura del fascicolo

Se un documento avvia un nuovo affare e/o procedimento amministrativo, si provvede all'apertura di un nuovo fascicolo.

La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione a sistema di alcune informazioni essenziali:

- indice di classificazione, cioè titolo, classe, sottoclasse di appartenenza;
- numero del fascicolo;
- oggetto del fascicolo (stringa di testo che descrive compiutamente l'affare o il procedimento amministrativo);
- data di apertura del fascicolo;
- AOO e Unità Organizzativa Responsabile;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo deve essere aperto all'ultimo livello della struttura gerarchica del titolario.

6.3 Chiusura del fascicolo

Il fascicolo deve essere chiuso al termine dell'affare o del procedimento amministrativo: la data di chiusura è quella dell'ultimo documento prodotto. Esso viene archiviato rispettando l'ordine di classificazione e la data di chiusura.

6.4 Processo di assegnazione dei fascicoli

Quando un documento viene ricevuto dall'AOO, la Direzione/Struttura responsabile, abilitata a effettuare la fascicolazione, con l'ausilio delle funzioni di ricerca del sistema documentale, effettua una delle seguenti operazioni:

- se il documento deve essere ricollegato a un affare o procedimento in corso ed è necessario inserirlo in un fascicolo o sottofascicolo già esistente, procede come segue:
 - seleziona il relativo fascicolo;
 - collega la registrazione di protocollo del documento al fascicolo selezionato.
- Se il documento si riferisce a un nuovo affare o procedimento ed è necessario aprire un nuovo fascicolo o sottofascicolo, procede come segue:

- esegue l'operazione di apertura del fascicolo, secondo quanto indicato nell'*Allegato 6 – Piano di fascicolazione*
- collega la registrazione di protocollo del documento al nuovo fascicolo aperto.

6.5 Modifica dell'assegnazione dei fascicoli

Quando si verifica un errore nell'assegnazione di un fascicolo, è prevista la possibilità di correzione delle informazioni inserite nel Sistema di Protocollo, al fine di procedere con la corretta attribuzione.

Il Sistema di Protocollo tiene traccia di eventuali modifiche di assegnazione.

7. GESTIONE ARCHIVI

Gli archivi e i singoli documenti degli enti pubblici sono beni culturali inalienabili. I singoli documenti sopra richiamati (analogici e informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'AOO, mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

Tradizionalmente, la prassi archivistica prevede tre tipologie di archivi:

- archivio corrente, composto da fascicoli e documenti che riguardano gli affari in corso
- archivio di deposito, composto da documenti che non fanno più parte di un affare in corso, non più necessari per l'operatività corrente
- archivio storico, composto da documenti conservati a tempo indefinito, per esempio documenti di importanza a livello culturale oppure utili per motivi di studio o di ricerca.

Si precisa che questa suddivisione viene trattata automaticamente all'interno del sistema informatico di gestione dei documenti informatici.

L'archivio non può essere smembrato, e deve essere conservato nella sua organicità. L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della Direzione responsabile degli archivi, previa consultazione della Sovrintendenza dei Beni Culturali. L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza tale autorizzazione. Altresì lo scarto dei documenti dell'archivio è subordinato ad autorizzazione.

Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

7.1 Gestione e organizzazione dei documenti e dei fascicoli nell'archivio corrente

Ciascuna Direzione/Struttura è tenuta alla organizzazione e gestione dei fascicoli informatici di propria competenza (corretta classificazione, apertura e chiusura di fascicoli ed eventuali sottofascicoli, corretta archiviazione dei documenti al loro interno), secondo i criteri indicati nell'*Allegato 7 – Titolare di classificazione* e nell'*Allegato 6 – Piano di fascicolazione*. Ogni Direzione/Struttura deve gestire il proprio archivio corrente per la conservazione della documentazione riguardante i procedimenti in corso.

I fascicoli cartacei dell'archivio corrente sono conservati a cura dei responsabili dei procedimenti amministrativi negli uffici di competenza.

7.2 Archivio di deposito

L'archivio di deposito è l'archivio nel quale vengono conservati i fascicoli chiusi relativi a procedimenti definiti.

Le singole Direzioni/Strutture collaborano con il Responsabile dell'Archivio Generale nella selezione dello scarto, nel versamento all'archivio storico e nella redazione dei relativi elenchi.

7.3 Archivio storico

I documenti cartacei che costituiscono l'archivio storico del Comune di Genova (quelli relativi ad affari esauriti da oltre quarant'anni, giudicati degni di conservazione permanente) sono conservati nell'Archivio Storico del Comune.

Il Responsabile dell'archivio generale provvede al versamento dei documenti dell'archivio di deposito all'archivio storico, previa compilazione e sottoscrizione di un elenco recante l'indicazione di titolo, classe e sottoclasse, numero e tipologia delle unità archivistiche (faldoni, fascicoli, registri, ecc.), estremi cronologici e descrizione della documentazione.

8. CONSERVAZIONE A NORMA

Il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione tutti i documenti protocollati dall'Ente, nonché i documenti informatici inseriti nei registri particolari e ulteriori documenti su specifica richiesta dell'AOO.

L'Amministrazione ha deciso di affidare la gestione del servizio di conservazione a un fornitore esterno, selezionandolo da un elenco degli enti abilitati.

8.1 Regole per il versamento in conservazione

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- documenti informatici con i metadati a essi associati;
- aggregazioni documentali con i metadati ad esse associati, contenenti i riferimenti che identificano univocamente i singoli oggetti documentali che costituiscono le aggregazioni stesse.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Informazioni puntuali saranno oggetto di apposito Manuale di conservazione in fase di elaborazione.

8.2 Processi di gestione

L'invio degli oggetti da conservare prevede la creazione da parte del produttore, ossia l'AOO, di pacchetti di versamento generati nelle modalità e con il formato previsti dall'*Allegato 2 – Manuale del servizio di conservazione*.

In caso di eccezioni e anomalie segnalate dal servizio di conservazione, resta a carico del RGD la risoluzione delle problematiche emerse, per esempio file corrotti.

8.3 Metadati

I metadati minimi da allegare agli oggetti da inviare in conservazione sono definiti all'interno delle vigenti Linee Guida AgID.

9. SCARTO

Il Responsabile dell'Archivio Generale, in collaborazione con le singole Direzioni/Strutture, effettua periodicamente le operazioni di selezione e scarto del materiale documentario.

La selezione è effettuata sulla base del massimario di selezione adottato dall'Ente (*Allegato 7 – Massimario di scarto*).

I documenti selezionati per lo scarto devono essere descritti in un elenco redatto dal RGD, in collaborazione con le singole Direzioni/Strutture.

Tale elenco deve contenere i riferimenti a titolo, classe e sottoclasse, numero e tipologia delle unità archivistiche (faldoni, fascicoli, registri ecc.), estremi cronologici, descrizione della documentazione, motivi dello scarto e indicazione sommaria del peso, in caso di documenti cartacei.

L'elenco, sotto forma di proposta di scarto, deve essere recepito in una determinazione dirigenziale della Direzione responsabile degli archivi, predisposta di concerto con la Direzione/Struttura i cui documenti dovranno essere inviati allo scarto. La determinazione dirigenziale dovrà essere trasmessa alla Soprintendenza Archivistica per la Liguria per ottenere la necessaria autorizzazione. Ottenuta l'autorizzazione, il materiale può essere scartato.

10. ACCESSO AGLI ATTI

L'accesso agli atti è distinto in tre tipologie:

- accesso documentale (Legge 07/08/1990, n. 241) = diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi;
- accesso civico cosiddetto semplice (Decreto legislativo 14/03/2013, n. 33) = diritto di chiunque di chiedere la pubblicazione di documenti, informazioni o dati che le Pubbliche Amministrazioni abbiano omesso di pubblicare nella sezione del sito istituzionale "Amministrazione Trasparente";
- accesso civico cosiddetto generalizzato (Decreto legislativo 25/05/2016, n. 97) = diritto di chiunque ad accedere a documenti, informazioni o dati detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria
- accesso agli atti dei Consiglieri Comunali e Provinciali di cui all'art. 43 co. 2 TUEL.

Il sistema di protocollo informatico dell'AOO consente di distinguere in sede di classificazione tra queste tre tipologie. In caso di richiesta, occorrerà procedere alla corretta classificazione in sede di registrazione della stessa.

Per ulteriori informazioni si rimanda all'*Allegato 8 – Accesso agli atti*

10.1 Trasparenza

L'Ente garantisce l'accessibilità totale delle informazioni che riguardano l'organizzazione e le proprie attività, allo scopo di favorire forme diffuse di controllo democratico sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse di pubblicazione dei dati sul sito istituzionale.

A tale scopo, è possibile accedere a tali informazioni consultando la sezione "Amministrazione trasparente" all'interno del sito istituzionale.

11. INFRASTRUTTURA INFORMATICA DELL'ENTE

11.1 Strumenti

Oltre al sistema informatico di protocollo, al fine di svolgere una corretta gestione documentale, l'Ente ha a disposizione degli strumenti di produzione e di firma di documenti informatici.

Le funzionalità complete del Sistema di Protocollo e degli altri strumenti informatici a disposizione sono descritte nei manuali operativi pubblicati nella sezione dedicata della intranet istituzionale, consultabile al seguente link <https://smart.comune.genova.it/contenuti/manuale-di-gestione-del-protocollo-informatico>.

11.2 Posta elettronica

L'AOO si dota di una casella di posta elettronica certificata (PEC) istituzionale per la corrispondenza, sia in ingresso che in uscita: tale casella costituisce l'indirizzo virtuale dell'AOO. La responsabilità di tale casella istituzionale è affidata all'Ufficio Archivio e Protocollo Generale. Quest'ultimo procede, con frequenza quotidiana, alla lettura della corrispondenza ivi pervenuta, alla relativa protocollazione ed assegnazione alle Direzioni/Strutture competenti.

Le Direzioni possono essere dotate di PEC specifica per le materie di loro competenza. In questo caso, la gestione della casella viene demandata alla struttura titolare della PEC.

Inoltre, secondo quanto previsto dalla Direttiva del Ministro per l'Innovazione e le Tecnologie 18/11/2005 sull'impiego della posta elettronica nelle Pubbliche Amministrazioni, l'Amministrazione fornisce a tutti i propri dipendenti una casella di posta elettronica ordinaria (PEO).

11.3 Sicurezza

Per quanto concerne le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali, si rimanda al piano di sicurezza generale dell'Ente.

12. PRODUZIONE E AGGIORNAMENTO DEL MANUALE

12.1 Modalità creazione, gestione e adozione

L'Amministrazione adotta, su proposta del RGD, e con i necessari provvedimenti, il presente Manuale. Il presente Manuale dovrà essere aggiornato, e sottoposto a nuova approvazione a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativa in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti.

Inoltre, si precisa che il presente Manuale e/o i relativi allegati potrà essere aggiornato e modificato con determinazioni dirigenziali, assunte di concerto tra la Direzione responsabile degli archivi e la Direzione dei sistemi informativi, in tutti i casi di aggiornamenti e modifiche non sostanziali.

Con l'entrata in vigore del presente Manuale è annullato il Manuale di Gestione Documentale adottato con Deliberazione della Giunta Comunale 11/08/2005, n. 816.

12.2 Pubblicità del presente Manuale

Il presente Manuale è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.

Inoltre, copia del presente Manuale è:

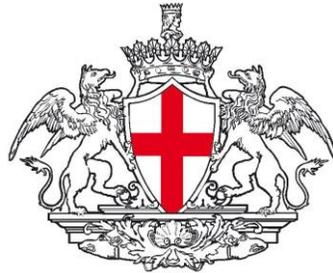
- fornita a tutto il personale del Comune di Genova mediante la rete intranet;
- pubblicato sul sito istituzionale dell'Amministrazione.

13. ALLEGATI

Di seguito la lista degli allegati:

- Allegato 1 - Glossario
- Allegato 2 - Manuale del servizio di conservazione
- Allegato 3 - Formati
- Allegato 4 - Registro di emergenza
- Allegato 5 - Titolario di classificazione
- Allegato 6 - Piano di fascicolazione
- Allegato 7 – Massimario di scarto
- Allegato 8 – Accesso agli atti.

Comune di Genova



Allegato 1 – Glossario

Termine	Definizione
Accesso	Operazione che consente di prendere visione dei documenti informatici.
Affidabilità	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
Aggregazione documentale informatica	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
Archivio	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
Archivio informatico	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.
Area Organizzativa Omogenea - AOO	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 co. 4 del TUDA - DPR 445/2000. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
Autenticità	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
Certificazione	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
Classificazione	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
Cloud della PA	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
Conservatore	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.

Termine	Definizione
Conservazione	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
Convenzioni di denominazione del file	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
Coordinatore della Gestione Documentale	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'art. 50 co. 4 del TUDA - DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
Destinatario	Soggetto o sistema al quale il documento informatico è indirizzato.
Documento informatico amministrativo	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
Documento elettronico	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Duplicato informatico	Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario. CAD art. 1, co. 1, lett. i-quinquies.
Estratto di documento informatico	Parte del documento tratto dal documento originale
Estratto per riassunto informatico	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.
Estrazione statica dei dati	Estrazione di informazioni utili da grandi quantità di dati attraverso metodi automatici o semi-automatici
Evidenza informatica	Sequenza finita di bit che può essere elaborata da una procedura informatica.
Fascicolo informatico	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
File	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.

Termine	Definizione
Filesystem	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare
Firma elettronica avanzata	Una firma elettronica avanzata soddisfa i seguenti requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche
Formato contenitore	Formato di file progettato per consentire l'inclusione (imbustamento o wrapping), in uno stesso file, di una o più evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
Formato del documento informatico	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
Formato deprecato	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
Funzioni aggiuntive del protocollo informatico	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
Funzioni minime del protocollo informatico	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'art. 56 del TUDA – DPR 445/2000.
Funzione di hash crittografica	Funzione matematica che genera, a partire da una evidenza informatica, un'impronta crittografica o digest in modo tale che risulti computazionalmente difficile a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
Gestione Documentale	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
Hash	Termine inglese usato, impropriamente, come sinonimo d'uso di impronta crittografica o digest .

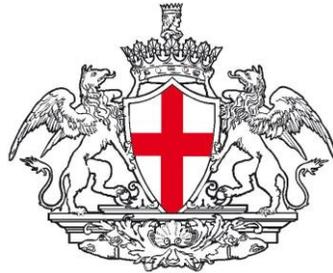
Termine	Definizione
Identificativo univoco	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
Impronta crittografica	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di hash crittografica a un'evidenza informatica.
Integrità	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
Interoperabilità	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
Leggibilità	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
Manuale di conservazione	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
Manuale di gestione	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
Metadati	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
Oggetto di conservazione	Oggetto digitale versato in un sistema di conservazione.
Oggetto digitale	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.
Pacchetto di archiviazione	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
Pacchetto di file (file package)	Insieme finito di più file che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.

Termine	Definizione
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
Pacchetto informativo	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
Piano della sicurezza del sistema di gestione Informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
Piano di classificazione (Titolario)	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.
Piano di conservazione	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'art. 68 del TUDA – DPR 445/2000.
Piano di fascicolazione	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
Piano generale della sicurezza	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
Processo	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
Produttore dei PdV	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.

Termine	Definizione
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.
Registro di protocollo	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
Registro particolare	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare.
Regolamento eIDAS	electronic IDentification Authentication and Signature, Regolamento (UE) No 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Repertorio	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
Responsabile della conservazione	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
Responsabile della gestione documentale	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del TUDA – DPR 445/2000.
Responsabile della protezione dei dati	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'art. 39 del Regolamento (UE) 2016/679.
Responsabile della sicurezza dei sistemi di conservazione	Soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
Riferimento temporale	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
Riversamento	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
Scarto	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.

Termine	Definizione
Serie	Raggruppamento di documenti con caratteristiche omogenee (vedi anche Aggregazione documentale informatica).
Sigillo elettronico	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
Sistema di conservazione	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, co. 1, del CAD.
Sistema di gestione informatica dei documenti	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito della pubblica amministrazione è il sistema di cui all'art. 52 del TUDA – DPR 445/2000.
Timeline	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di timeline un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
Titolare dell'oggetto di conservazione	Soggetto produttore degli oggetti di conservazione.
Trasferimento	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
Ufficio	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
Utente abilitato	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
Versamento	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato, operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

Comune di Genova



Allegato 2 – Manuale del servizio di conservazione



Engineering Ingegneria Informatica S.p.a. dispone di due differenti servizi di Conservazione Digitale, uno denominato DigiDoc e l'altro denominato DigiBox (sistema ereditato dall'incorporazione di Infogroup).

Di seguito i due manuali.

Manuale di Conservazione DigiDoc di Engineering Ingegneria Informatica

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	08/05/2018	Martinucci Valentina	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
	08/05/2018	Mancini Barbara	Responsabile funzione archivistica di conservazione
Verifica	09/05/2018	Nigro Cosimo	Responsabile servizio di conservazione
	09/05/2018	Cafiso Giuseppe	Responsabile Sicurezza dei sistemi per la conservazione
Approvazione	09/05/2018	Pizzonia Mario Carmelo	Responsabile ECM Competence Center

REGISTRO DELLE VERSIONI

N°Ver/Rev/ Bozza	Data emissione	Modifiche apportate	Osservazioni
1.0	09/06/2015	Prima versione	
1.1	03/07/2015	Modificato paragrafo 5.2 : inserita delega Marten Canavesio	
1.2	22/09/2015	Modifiche e integrazioni richieste da AgID in fase di accreditamento.	
1.3	8/01/2016	Eliminato il cap. 4 “Certification e time stamping authority” e adeguato al nuovo schema AgID	
1.4	19/05/2017	§ 5 modificate figure 2 e 3 relative alla strutture organizzative § 6.2 Modificati canali comunicazione	Non inviate in AGID in quanto prima dell’invio sono state rilevate delle osservazioni da parte di DNV

1.5	28/06/2017	§3.2 aggiornata standard di riferimento §§ 5.4, 8.3, 9.1 Adeguamenti per modifiche Organizzative precisando la distinzione tra le attività di responsabilità di Engineering Ingegneria Informatica S.p.A. e quelle in carico al fornitore Engineering.MO S.p.A. §8.3 aggiornata normativa di riferimento componenti fisiche	
1.6	19/07/2017	Recepita la indicazione di AgID in merito alla sostituzione del termine “Lotto” e “Volume di conservazione”	
1.7	21/08/2017	Recepita la variazione della denominazione Sociale di Engineering.mo SpA in Engineering D.HUB SpA	
1.8	08/05/2018	§1 Recepita l’incorporazione di Infogroup in Engineering Ingegneria Informatica Corretti i riferimenti alla norma 14721:2012	

INDICE DEL DOCUMENTO

1.	SCOPO E AMBITO DEL DOCUMENTO	6
2.	TERMINOLOGIA (GLOSSARIO E ACRONIMI).....	7
2.1	Acronimi	7
2.2	Glossario.....	8
3.	NORMATIVA E STANDARD DI RIFERIMENTO	18
3.1	Normativa di riferimento	18
3.2	Standard di riferimento	19
4.	RUOLI E RESPONSABILITA'	20
4.1	Il Responsabile del servizio di conservazione	22
4.1.1	<i>Dati anagrafici del Responsabile del servizio di Conservazione.....</i>	<i>24</i>
4.2	Formazione.....	24
4.3	Delegati del Responsabile del servizio di Conservazione	25
4.4	Coinvolgimento di altri pubblici ufficiali.....	25
5.	STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE.....	27
5.1	Organigramma.....	27
5.2	Strutture organizzative.....	28
5.3	Focus sul Centro di Competenza ECM (Enterprise Content Management)	29
5.4	Focus sui servizi erogati da Engineering D.HUB	30
6.	OGGETTI SOTTOPOSTI A CONSERVAZIONE	31
6.1	Oggetti conservati	31
6.2	Pacchetto di versamento.....	31
6.3	Pacchetto di archiviazione.....	33
6.4	Pacchetto di Distribuzione	33
6.5	Formati	34
6.6	Metadati conservati	34
6.7	Tempi di conservazione.....	35
6.8	Peculiarità e gestione delle eccezioni.....	35
7.	IL PROCESSO DI CONSERVAZIONE.....	37
7.1	Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico	37
7.2	Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti	39
7.2.1	<i>Controllo impronta del pacchetto di versamento.....</i>	<i>39</i>
7.2.2	<i>Controllo dell'identità del soggetto produttore del pacchetto.....</i>	<i>39</i>
7.2.3	<i>Controllo delle Firme Digitali.....</i>	<i>40</i>
7.2.4	<i>Controllo dei Formati digitali</i>	<i>41</i>
7.2.5	<i>Controllo della Presenza di Macro e Codice Eseguitibile</i>	<i>43</i>

7.2.6	Controllo dei Metadati	44
7.2.7	Controllo Impronta.....	45
7.3	Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico ..	45
7.3.1	Rinnovo marche temporali in scadenza	45
7.4	Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie.....	46
7.5	Preparazione e gestione del pacchetto di archiviazione	46
7.5.1	Creazione Indice di Conservazione	47
7.6	Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione.....	48
7.6.1	Funzionalità di ricerca	48
7.6.2	Funzionalità di esibizione	50
7.7	Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti	53
7.8	Scarto dei pacchetti di archiviazione	54
7.9	Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori	55
7.10	Riversamento diretto e sostitutivo.....	55
7.10.1	Riversamento diretto	55
7.10.2	Riversamento sostitutivo.....	55
8.	IL SISTEMA DI CONSERVAZIONE	57
8.1	Componenti Logiche.....	57
8.2	Componenti Tecnologiche.....	57
8.2.1	Software di base.....	57
8.2.2	Framework di sviluppo utilizzati.....	58
8.2.3	Scalabilità.....	58
8.3	Componenti Fisiche	60
8.4	Procedure di gestione e di evoluzione	62
9.	MONITORAGGIO E CONTROLLI.....	71
9.1	Procedure di monitoraggio.....	71
9.2	Verifica di integrità degli archivi	72
9.3	Soluzioni adottate in caso di anomalie.....	73

INDICE DELLE FIGURE

Figura 1 – Strutture Organizzative	27
Figura 2 – Strutture Organizzative Servizio di Conservazione	28
Figura 3 – Relazioni tra Responsabile della conservazione e strutture Organizzative	28
Figura 4 – Versamento del documento nel sistema di conservazione	38
Figura 5 - Visualizzazione documento	50
Figura 6 - Configurazione del sistema con un 1° livello di scalabilità	59
Figura 7 - Configurazione del sistema con un 2° livello di scalabilità	59
Figura 8 - Configurazione ambienti di collaudo e produzione.....	60
Figura 9: Organizzazione dell'Operation Center	72

1. SCOPO E AMBITO DEL DOCUMENTO

Engineering Ingegneria Informatica dispone di due differenti servizi di Conservazione Digitale, uno denominato DigiDoc e l'altro denominato DigiBox (sistema ereditato dall'incorporazione di Infogroup); il presente documento costituisce il manuale di conservazione di DigiDoc adottato da Engineering Ingegneria Informatica S.p.A., nel seguito indicato come Eng, per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento.

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

Si precisa che alcuni argomenti che riguardano aspetti delle specifiche forniture del servizio di conservazione non saranno inseriti nel presente manuale, ma saranno sviluppati nel documento "Specificità del contratto" / "Proposta tecnica" in coerenza e/o facendo riferimento alla documentazione contrattuale prevista dal contratto di servizio stipulato da Eng con la propria clientela.

[Torna al sommario](#)

2. TERMINOLOGIA (GLOSSARIO E ACRONIMI)

2.1 Acronimi

Acronimo	Definizione
ACL	Access Control List
AIP	Archival Information Package (ex OAIS), ovvero il pacchetto di archiviazione ex DPCM 3 Dicembre 2013
AgID	Agenzia per l'Italia Digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
CAD	Codice dell'Amministrazione Digitale, ovvero D.lgs 7 marzo 2005, n.82 e successive modificazioni e integrazioni
CAdES	CMS (Cryptographic Message Syntax) Advanced Electronic Signatures
CNS	Carta Nazionale dei Servizi provvista almeno del certificato di autenticazione (recante il codice fiscale del titolare)
DB	Database
DIP	Dissemination Information Package (ex OAIS), ovvero il pacchetto di distribuzione DPCM 3 Dicembre 2013
DPCM	Decreto del Presidente del Consiglio dei Ministri
DigiDoc	È il sistema utilizzato da Eng per erogare il servizio di Conservazione
GUI	Graphical User Interface
FTP server	programma che permette di accettare connessioni in entrata e di comunicare con un Client attraverso il protocollo FTP
HSM	Hardware Security Module
ORM	Object-relation Mapping
OAIS	Open Archival Information System, standard ISO 14721:2012
PAdES	PDF Advanced Electronic Signatures
PEC	Posta Elettronica Certificata
PdV	Pacchetto di Versamento
RdV	Rapporto di Versamento
PdA	Pacchetto di Archiviazione
IdC	Indice di Conservazione

Responsabile della conservazione	E' il soggetto responsabile dell'insieme delle attività elencate dall'art. 7 comma 1 delle Regole tecniche. Viene designato dal Titolare all'interno della propria struttura organizzativa nelle pubbliche amministrazioni deve essere ricoperto obbligatoriamente da un dirigente o funzionario formalmente designato (art. 7 comma 3 delle Regole tecniche).
Responsabile del servizio di conservazione	E' la persona designata da Eng a gestire il sistema di conservazione affidato in outsourcing alla società dal Titolare dei documenti informatici. L'attività del responsabile consiste nel gestire ed erogare il servizio di conservazione come definito nell'accordo di servizio e nel presente Manuale di Conservazione utilizzando strumenti e metodi aggiornati tecnicamente e conformi alla normativa vigente.
SdI	Sistema di Interscambio (per le fatture elettroniche destinate alle pubbliche amministrazioni)
SIP	Submission Information Package (ex OAIS), ovvero il pacchetto di versamento DPCM 3 Dicembre 2013
Soggetto Produttore	Il titolare dei documenti. E' il soggetto o l'ente che produce i documenti che vengono affidati al soggetto al quale è affidato il processo di Conservazione
SSO	Single Sign On
TSA	TimeStamping Authority
UI	User Interface
UO	Unità organizzativa (cfr glossario)
URI	Uniform Resource Identifier
XAdES	XML Advanced Electronic Signatures

[Torna al sommario](#)

2.2 Glossario

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

Termine	Definizione
Accesso	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia Digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di

Termine	Definizione
	conservazione
Affidabilità	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
Archivio	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell'attività
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Area organizzativa omogenea	Un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del Testo Unico
Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
Autenticità	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico
Base di dati	Collezione di dati registrati e correlati tra loro
CAD	Decreto legislativo 7 Marzo 2005, n. 82 e successive modificazioni e integrazioni
CADES	CMS Advanced Electronic Signatures – Formato di firma che può essere apposto su qualsiasi tipo di file. Genera una busta genera una busta crittografica contenente il file originale. Si presenta come un file la cui estensione è p7m

Termine	Definizione
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto dall'AgID il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Certificato di firma	Certificato destinato alla generazione delle firme apposte ai documenti digitali.
Certificato di marcatura temporale	Certificato destinato alla generazione di marche temporali.
Classificazione	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Conservatore accreditato	Soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'AgID, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
Conservazione	Insieme delle attività finalizzate a definire ad attuare le politiche complessive del sistema di conservazione e a governare la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della gestione documentale	Responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50, comma 4 del Testo Unico nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
Copia analogica del documento informatico	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle Regole tecniche per il sistema di conservazione
Destinatario	Identifica il soggetto/sistema al quale il documento informatico è indirizzato
DOI	Digital Object Identifier
Duplicazione dei documenti informatici	Produzione di duplicati informatici
Esibizione	Operazione che consente di visualizzare un

Termine	Definizione
	documento conservato e di ottenerne copia
Estratto per riassunto	Documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
Evidenza informatica	Sequenza di simboli binari, ossia di bit, che può essere elaborata da una procedura informatica
Fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'art. 41 del CAD
Firme multiple	Firme digitali apposte da diversi sottoscrittori allo stesso documento.
Firme parallele	Firme apposte da differenti soggetti al medesimo documento digitale utilizzando una sola busta crittografica.
Firme verticali	Firme apposte da differenti soggetti, l'una ad un documento firmato in precedenza da un altro soggetto, creando delle buste crittografiche innestate l'una dentro l'altra.
Formato	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file
Funzione di hash	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
Immodificabilità	Caratteristica che rende il contenuto del

Termine	Definizione
	documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
Impronta	Sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione ad una sequenza informatica d'origine di un'opportuna funzione di hash
Indice di conservazione	Evidenza informatica che elenca in forma strutturata – xml - le impronte, gli identificativi e le informazioni descrittive dei documenti digitali sottoposti insieme a processo di conservazione a norma. Tale file è conforme al <i>UNI 11386:2010 Standard SInCRO</i> ed è firmato digitalmente dal responsabile del servizio di conservazione e marcato temporalmente.
Insieme minimo di metadati del documento informatico	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 delle Regole tecniche, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta
Integrità	Insieme delle caratteristiche di un documento informatico che ne dichiarano le qualità di essere completo ed inalterato
Interoperabilità	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
ISBN	International Standard Book Number
Leggibilità	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
Log di sistema	Registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
Manuale di conservazione	Strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'art. 9 delle Regole tecniche del sistema di

Termine	Definizione
	conservazione
Manuale di gestione	Strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico DPCM 31 ottobre 2000 e successive modificazioni e integrazioni
Marca temporale	Evidenza informatica che consente di rendere opponibile a terzi un riferimento temporale. La marca temporale può essere solamente rilasciata da una <i>Time Stamping Authority</i>
Memorizzazione	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 delle Regole Tecniche del sistema di conservazione
Pacchetto di archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento
Pacchetto di distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
Pacchetto di versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
Pacchetto informativo	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche solo i metadati riferiti agli oggetti da conservare
PAdES	PDF Advanced Electronic Signatures– Formato di firma che può essere apposto esclusivamente sul tipo di file pdf.
Piano della sicurezza del sistema di conservazione	Documento che, nel contesto del piano generale

Termine	Definizione
	di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano della sicurezza del sistema di gestione informatica dei documenti	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
Piano di conservazione	Strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'art. 68 del Testo Unico
Piano generale della sicurezza	Documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
Posta elettronica certificata	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici
Presenza in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'art. 10 delle Regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica, di norma diversa dal soggetto che ha firmato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

Termine	Definizione
Registrazione informatica	Insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
Registro particolare	Registro informatico di particolari tipologie di atti o documenti nell'ambito della pubblica amministrazione previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
Registro di protocollo	Registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
Repertorio informatico	Registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
Responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61 del Testo Unico, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione
Responsabile del servizio di conservazione	Soggetto a cui sono affidati, dal responsabile della conservazione, l'insieme delle attività elencate nell'art. 7 delle Regole tecniche del sistema di conservazione
Responsabile del trattamento dei dati	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali
Responsabile della sicurezza	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
Riferimento temporale	Informazione contenente la data e l'ora con

Termine	Definizione
	riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
Scarto	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
Scheda documento	Aggregato logico costituito da uno o più documenti digitali e/o analogici che sono considerati come un tutto unico e come tali costituiscono l'oggetto di una singola descrizione: nel caso in cui sia formata da più documenti uno di essi si configura come "primario" e gli altri sono gli "allegati" che trovano il loro significato compiuto solo in relazione al primario. E' l'unità minima, concettualmente non divisibile, di cui è composto l'archivio.
Sistema di classificazione	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
Sistema di conservazione	Sistema di conservazione dei documenti informatici di cui all'art. 44 del CAD
Sistema di gestione informatica dei documenti	Nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del Testo Unico; per i privati è il sistema che consente la tenuta di un documento informatico
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione
Tag	Marcatori (etichette) per assegnare una semantica al testo nei file xml
Testo Unico	Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 e successive modificazioni
Transazione informatica	Particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche alla base dati

Termine	Definizione
Unità di aggregazione	Aggregato logico di schede documento collegate tra loro che si forma nell'archivio corrente e che può costituire un'unità di versamento in conservazione. Il fascicolo che scaturisce da un procedimento amministrativo è il caso più comune di unità di aggregazione, altri esempi sono costituiti dalle serie tipologiche (delibere, contratti ecc).
Unità organizzativa	Qualsiasi articolazione di un'Area Organizzativa Omogenea, ovvero un nodo della struttura gerarchica – mappa organizzativa - in cui si organizza un'Amministrazione
URI	Uniform Resource Identifier
Utente	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
Versamento agli Archivi di Stato	Operazione con cui il Responsabile del servizio di conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

[Torna al sommario](#)

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

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

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

[Torna al sommario](#)

3.2 Standard di riferimento

Di seguito sono riportati gli standard ai quali si fa riferimento per il Manuale di Conservazione:

- 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 15836-1:2017 Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.
- Moreq - Model Requirements for Electronic Records Management
- Pronom - registro internazionale sui formati idonei alla conservazione a lungo termine

[Torna al sommario](#)

4. RUOLI E RESPONSABILITA'

Il sistema di conservazione DigiDoc, gestito dal Responsabile del Servizio di Conservazione di Engineering, è basato su un modello organizzativo di riferimento definito formalmente nei ruoli e nelle responsabilità dei vari attori coinvolti nel processo di conservazione dei documenti informatici, come riportato nella tabella successiva, in conformità ai ruoli e alle attività ad essi associati indicati nel documento “Profili professionali” pubblicato da AgID sul proprio sito istituzionale.

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
Responsabile del servizio di conservazione	Nigro Cosimo	Definizione e attuazione delle politiche complessive del sistema di conservazione, nonché del governo della gestione del sistema di conservazione; definizione delle caratteristiche e dei requisiti del sistema di conservazione in conformità alla normativa vigente; corretta erogazione del servizio di conservazione all'ente produttore; gestione delle convenzioni, definizione degli aspetti tecnico-operativi e validazione dei disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.	Giugno 2015
Responsabile Sicurezza dei sistemi per la conservazione	Cafiso Giuseppe	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.	gennaio 2015
Responsabile funzione archivistica di conservazione	Mancini Barbara	Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni	Giugno 2015

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		<p>documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;</p> <p>definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;</p> <p>monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;</p> <p>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.</p>	
Responsabile trattamento dati personali	Nigro Cosimo	<p>Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali;</p> <p>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</p>	Gennaio 2010
Responsabile sistemi informativi per la conservazione	Carrozzo Massimo	<p>Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione;</p> <p>monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore;</p> <p>segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive;</p> <p>pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione;</p> <p>controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del</p>	Giugno 2015

Ruoli	Nominativo	Attività di competenza	Periodo nel ruolo
		servizio di conservazione.	
Responsabile dello sviluppo e della manutenzione del sistema di conservazione	Martinucci Valentina	- Coordinamento dello sviluppo e manutenzione delle componenti hardware e software del sistema di conservazione; pianificazione e monitoraggio dei progetti di sviluppo del sistema di conservazione; monitoraggio degli SLA relativi alla manutenzione del sistema di conservazione; interfaccia con l'ente produttore relativamente alle modalità di trasferimento dei documenti e fascicoli informatici in merito ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software, alle eventuali migrazioni verso nuove piattaforme tecnologiche; gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.	Giugno 2015

[Torna al sommario](#)

4.1 Il Responsabile del servizio di conservazione

Nel presente paragrafo sono dettagliate le competenze del Responsabile del servizio di conservazione secondo quanto previsto dal decreto [8].

- Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove

- necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
 - adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 decreto [8];
 - assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
 - assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
 - provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
 - predispose il manuale di conservazione di cui all'art. 8 del decreto [8] e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
 - Definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
 - Archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
 1. descrizione del contenuto dell'insieme dei documenti;
 2. estremi identificativi del responsabile del servizio di conservazione;
 3. estremi identificativi delle persone eventualmente delegate dal responsabile del servizio di conservazione, con l'indicazione dei compiti alle stesse assegnati;
 4. indicazione delle copie di sicurezza;
 - Mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
 - Verifica la corretta funzionalità del sistema e dei programmi in gestione;
 - Adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione e delle copie di sicurezza dei supporti di memorizzazione;
 - Richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
 - Definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
 - Verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

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

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

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

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

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

[Torna al sommario](#)

4.1.1 Dati anagrafici del Responsabile del servizio di Conservazione

Nel presente paragrafo sono riportati i dati anagrafici, del responsabile del servizio di conservazione attualmente in carica; sono altresì riportati i dati "storici" di tutti i responsabili della conservazione che si sono avvicendati nel tempo.

Con decorrenza dal 03 giugno 2015

il responsabile del servizio di conservazione attualmente in carica, come da apposita nomina, è

cognome NIGRO nome COSIMO

nato a SAN VITO DEI NORMANNI Prov. (BR) il 25/10/1965

cod. fiscale NGRCSM65R25I396M

[Torna al sommario](#)

4.2 Formazione

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

[Torna al sommario](#)

4.3 Delegati del Responsabile del servizio di Conservazione

I delegati del responsabile del servizio di conservazione sono nominati a cura del responsabile stesso e la loro nomina decade automaticamente con la revoca o decadenza del responsabile che li ha nominati.

La nomina dei delegati avviene attraverso un documento sottoscritto dal responsabile del servizio di conservazione, e, per accettazione, dal/i delegati nominati; tale documento viene conservato all'interno dello stesso sistema di conservazione.

La delega può essere:

- di tutte le funzioni del responsabile (fatta comunque salva la facoltà di delegare altri) o solo di alcune, da dettagliare;
- a tempo determinato oppure indeterminato

tutti questi elementi devono essere esplicitamente riportati nel documento di delega pena la non validità della delega stessa.

L'elenco dei delegati sono riportati nell'allegato 5 del presente manuale.

La delega come responsabile del servizio di conservazione può in qualsiasi momento essere revocata dal responsabile del servizio di conservazione formalizzando la revoca nelle stesse forme e modalità della delega (salvo che ovviamente la revoca non deve essere sottoscritta dal/i delegati ma solo dal responsabile del servizio di conservazione); parimenti un delegato ha facoltà di dimettersi/rinunciare alla delega e le dimissioni risultano esecutive a decorrere da 30 giorni dalla presentazione formale – a protocollo generale o alla casella PEC dedicata al sistema di conservazione - del documento di dimissioni/rinuncia (in formato analogico o digitale) sottoscritto dal delegato dimissionario/rinunciatario.

Sia in caso di revoca che di dimissioni/rinuncia è a cura del responsabile del servizio di conservazione mettere in conservazione il documento di revoca/dimissioni/rinuncia, ed aggiornare l'allegato inserendo il termine della delega, il motivo del termine, e gli estremi - id. nel sistema di conservazione ed impronta - del documento che formalizza la fine della delega.

[Torna al sommario](#)

4.4 Coinvolgimento di altri pubblici ufficiali

Qualora il coinvolgimento di pubblici ufficiali che non siano quelli che ricoprono i ruoli di cui ai § 4.1 e 4.3 dovesse rendersi necessario esso andrà formalizzato a cura del responsabile del servizio di conservazione o suo delegato (dotato di opportuna delega), con modalità del tutto analoghe alla nomina dei delegati del responsabile del servizio di conservazione, ed in particolare con l'obbligo di indicare nel documento di formalizzazione dell'incarico al/i pubblici ufficiali le motivazioni e l'ambito di pertinenza dell'intervento richiesto.

L'incarico del pubblico ufficiale, anche se a tempo indeterminato, decade automaticamente con la revoca o decadenza del responsabile del servizio di conservazione o suo delegato che ha formalizzato l'incarico (attraverso sottoscrizione digitale del relativo documento).

Il presente paragrafo riporta gli estremi degli eventuali incarichi a pubblici ufficiali che non siano quelli che ricoprono i ruoli di cui ai § 4.1 e 4.3, ovvero almeno:

- i dati anagrafici necessari ad identificare il pubblico ufficiale (cognome e nome, codice fiscale, luogo e data di nascita);

- il ruolo del pubblico ufficiale e gli estremi dell'amministrazione pubblica in cui ricopre tale ruolo;
- il periodo di validità dell'incarico (senza estremo superiore se l'incarico è ancora in essere ed è a tempo indeterminato);
- le motivazioni e l'ambito di pertinenza dell'incarico al pubblico ufficiale;

[Torna al sommario](#)

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. nel suo complesso:



Figura 1 – Strutture Organizzative

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. coinvolte nel processo di conservazione:

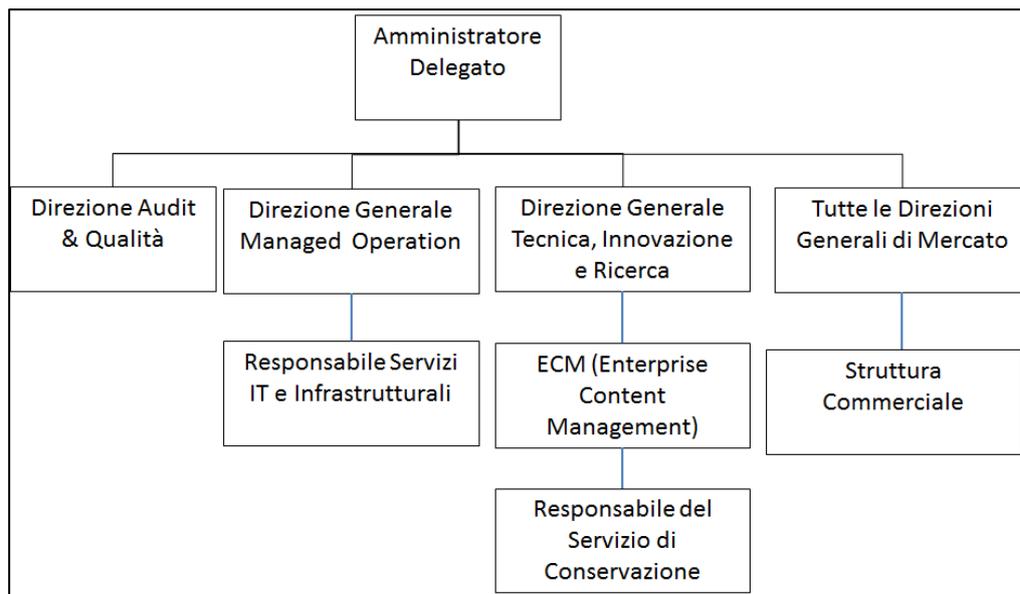


Figura 2 – Strutture Organizzative Servizio di Conservazione

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. ed Engineering D.HUB, che si relazionano con il responsabile del servizio di conservazione:

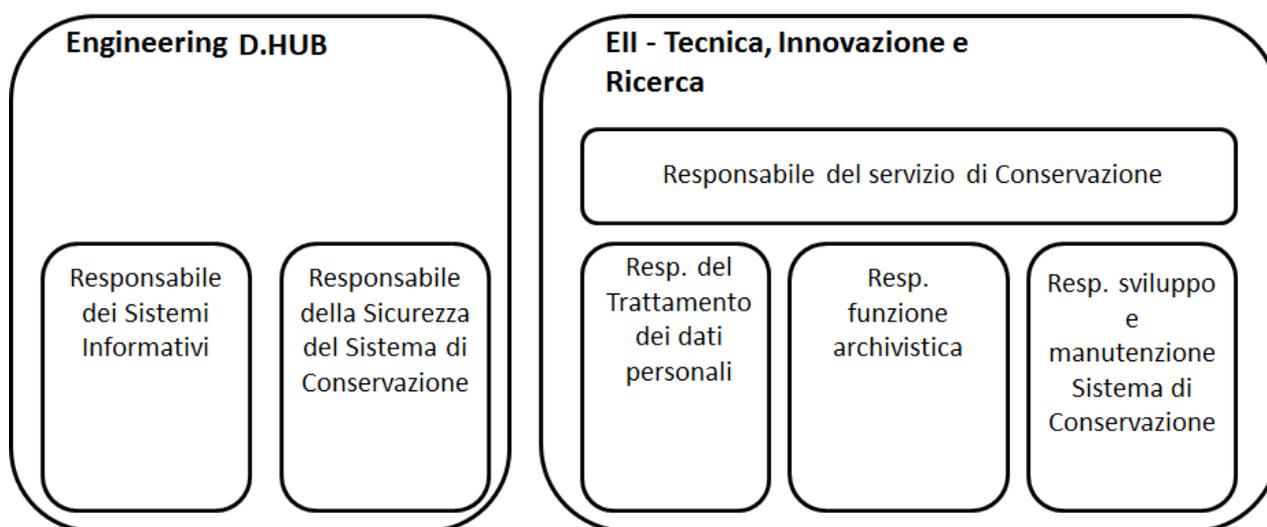


Figura 3 – Relazioni tra Responsabile della conservazione e strutture Organizzative

[Torna al sommario](#)

5.2 Strutture organizzative

Compiti delle strutture organizzative individuate nel capitolo precedente ad esclusione delle strutture che fungono da:

- Amministratore Delegato, nomina il responsabile del servizio di conservazione e le altre figure professionali indicate nel capitolo 5;

- Direzione Audit & Qualità, gestisce il sistema di gestione della qualità e sicurezza redatto secondo le normative ISO 9001 e ISO 27001. La funzione si occupa inoltre di verificare periodicamente la conformità a normativa e standard di riferimento;
- Team del Responsabile del servizio di conservazione, è il team che comprende tutti i ruoli già indicati al capitolo 5 e loro eventuali delegati e si occupa di attivare il servizio di conservazione, censire il Titolare nel sistema di conservazione, concordare col Titolare o con il suo Responsabile della Conservazione, documenti, metadati, tempistiche, regole di validazione, tempistiche e parametri di conservazione, fornire supporto ai Titolari che ne facciano richiesta anche sui loro sistemi per verificare e configurare le applicazioni di trasferimento dei documenti da conservare nel rispetto dei permessi ottenuti dai Titolari medesimi, configurare i metadati e le regole di validazione, le tempistiche e i parametri di conservazione nel sistema di conservazione; definire col Titolare e censire nel sistema di conservazione l'elenco degli utenti autorizzati ad accedere al sistema ed i loro limiti di accesso e utilizzo, erogare il servizio di assistenza ai Titolari del servizio di conservazione, monitorare il sistema di conservazione relativamente all'acquisizione e all'elaborazione dei documenti;
- Responsabile dei servizi IT e infrastrutturali, si occupa della gestione delle componenti hardware e software del sistema di conservazione;
- Struttura commerciale, si occupa di definire i parametri contrattuali e raccogliere la firma dei Titolari sulla richiesta di attivazione del servizio di conservazione;
- Direzione Tecnica, Innovazione e Ricerca, si occupa di gestire lo sviluppo, la correzione di eventuali anomalie, il change management, il rilascio ed il monitoraggio del software del sistema di conservazione, acquisire, verificare e gestire i PdV ricevuti, predisporre il rapporto di versamento per i PdV presi in carico, predisporre il rapporto di rifiuto per i PdV rifiutati; preparare e gestire i PdA tramite applicazioni automatizzate, preparare e gestire i PdD ai fini dell'esibizione e della produzione di duplicati informatici e copie informatiche su richiesta tramite applicazioni automatizzate, verificare integrità e leggibilità dei documenti del sistema di conservazione tramite applicazioni automatizzate.

[Torna al sommario](#)

5.3 Focus sul Centro di Competenza ECM (Enterprise Content Management)

La mission del Centro di competenza ECM di Engineering è fornire soluzioni e servizi per trasformare le informazioni in patrimonio aziendale, supportando i clienti nella selezione degli strumenti migliori per soddisfare i requisiti individuati nei progetti.

Tale centro di competenza fornisce soluzioni e servizi per trasformare contenuti analogici e digitali di un'organizzazione in un patrimonio informativo pienamente fruibile con strumenti di groupware, content, document, workflow e knowledge management. Dispone di competenze sull'intero ciclo di vita documentale, dalla creazione del documento fino alla sua archiviazione, sia dal punto di vista di gestione del processo organizzativo che della normativa; nel centro operano professionisti certificati sulle principali tecnologie di riferimento di mercato e/o open source (pacchetti e piattaforme quali EMC Documentum, IBM FileNet, Alfresco, DRUPAL, OpenCMS, ecc.). All'interno di tale centro di competenza è presente una struttura dedicata alla Dematerializzazione e Conservazione che fornisce conoscenze di alto livello non solo sulla "conservazione a norma", ma anche sui temi organizzativi, normativi e di responsabilità giuridica. Sono presenti risorse esperte con competenze sul modello OAIIS (Open Archival Information System).

[Torna al sommario](#)

5.4 Focus sui servizi erogati da Engineering D.HUB

L'azienda Engineering D.HUB, dispone di soluzioni verticali ed eroga servizi utilizzando la propria rete di Data Center..

I principali servizi offerti da Engineering D.HUB sono:

- gestione centralizzata e distribuita di piattaforme tecnologiche eterogenee
- strutture organizzative di Enterprise Monitoring Center e di Server, Storage & Network Management;
- hosting e housing;
- gestione dei posti di lavoro e degli utenti con servizi di “fleet management”, “service desk” e “help desk”;
- soluzioni e servizi per la gestione di progetti complessi di aggiornamento tecnologico, ottimizzazione di risorse elaborative, implementazione di soluzioni specifiche, come re-hosting di ambienti mainframe, server consolidation & virtualization, disaster recovery;
- application management, business process outsourcing, facility management;
- servizi professionali di consulenza tecnologica, progettuale e metodologica.

[Torna al sommario](#)

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

6.1 Oggetti conservati

Il servizio offerto da Eng permette potenzialmente il trattamento e la conservazione di qualunque tipologia di documento. Il cliente che intende usufruirne, deciderà per quali tipologie documentali attivare il servizio di conservazione e, una volta comunicatele a Eng, collaborerà col il team DigiDoc nelle operazioni di definizione del relativo trattamento.

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

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

Il dettaglio delle informazioni sopra indicate, concordate con il soggetto Produttore, sono descritte nello specifico accordo di servizio.

[Torna al sommario](#)

6.2 Pacchetto di versamento

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

Fra i diversi aspetti da concordare, i principali sono:

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

Il responsabile del servizio di conservazione coordina l'intero processo e si accerta del rispetto delle regole fissate negli specifici accordi di servizio. Viene verificata la presenza dei metadati minimi che il soggetto produttore deve associare alle tipologie documentali informatiche che si accinge a versare nel sistema. Sono conservati i seguenti oggetti: Documenti informatici, documenti amministrativi informatici e fascicoli informatici e per ciascuno di queste tipologie di oggetti sono previsti determinati requisiti minimi.

Per il documento informatico sono previsti i seguenti metadati minimi:

- identificativo univoco e persistente
- data di chiusura
- oggetto (sintesi del contenuto di un documento)

- soggetto che ha formato il documento
- impronta

Per il documento amministrativo informatico, specifico per le pubbliche amministrazioni sono previsti i seguenti metadati minimi:

- codice identificativo dell'amministrazione (codice IPA)
- codice identificativo dell'area organizzativa omogenea (codice IPA)
- codice identificativo del registro
- data di protocollo
- progressivo di protocollo
- impronta.

Per il fascicolo amministrativo sono previsti i seguenti metadati minimi:

- identificativo
- oggetto
- responsabile del procedimento
- elenco dei documenti contenuti nel fascicolo

Il pacchetto di versamento è corredato dal un file xml - SIPManifest.xml, il cui schema è fornito nell'allegato Allegato1 - SIPManifest (Indice di Versamento).pdf - che contiene sia le descrizioni della documentazione che i puntatori e le impronte dei file che compongono la documentazione digitale da inviare in conservazione. In caso di documentazione già inviata in conservazione e di cui si devono solo aggiornare dati e/o file, per le unità di descrizione - schede documento, unità di aggregazione di documenti ecc - e i documenti digitali da aggiornare basta specificare i tag relativi ai dati e/o file da aggiornare. Occorre considerare che la valorizzazione dei tag all'interno delle CustomInfo sostituisce i valori precedentemente specificati per lo stesso item.

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

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

- tutta la documentazione venga inviata in conservazione correttamente "tipizzata" nel pacchetto di versamento secondo quanto specificato nell'accordo di servizio, cosicché dalla tipologia specificata il sistema di conservazione sia in grado di impostare correttamente sia il termine entro cui obbligatoriamente deve essere effettuato il processo di conservazione che il termine fino cui decorre l'obbligo di conservazione della documentazione;
- tutta la documentazione sia inviata al sistema di conservazione in tempo utile affinché la conservazione possa avvenire nel rispetto delle tempistiche imposte dalla normativa vigente e secondo quanto concordato negli accordi di servizio;
- la documentazione venga inviata in conservazione corredata almeno dei metadati obbligatori previsti dal profilo specifico della tipologia documentale specificata.

Per quanto concerne gli allegati delle fatture

- nel caso delle fatture attive in base alle nuove regole tecniche della fatturazione elettronica gli eventuali allegati, recanti ad esempio il dettaglio di ciò che viene fatturato, sono inglobati all'interno della fatturaPA (embedded in base 64 nell'xml della fattura stessa), e dato che la fattura è firmata digitalmente sono inviati in conservazione come parte integrante del documento xml

principale della fattura (esattamente come ricevuti dal SdI); tuttavia per garantire una maggior leggibilità vengono anche versati in conservazione come documenti distinti (allegati) della scheda documento della fattura, “estraendoli” dall’xml firmato in cui sono inglobati;

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

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

[Torna al sommario](#)

6.3 Pacchetto di archiviazione

L’elaborazione del pacchetto di versamento verifica dati e file dei documenti versati al fine di stabilire quali dei documenti del pacchetto possano esser presi in carico da DiGiDoc e quali vadano rifiutati (vi può essere anche una presa in carico parziale). Al termine di questa elaborazione i risultati e i dettagli dei controlli effettuati su tutti i documenti del pacchetto, sia quelli accettati che quelli rifiutati, sono riportati nel rapporto di versamento (SIPResult.xml, il cui schema è fornito nell’allegato Allegato2 - SIPResult (Rapporto di Versamento).pdf) che viene restituito al versatore e al tempo stesso diviene esso stesso oggetto di conservazione in DiGiDoc.

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

- I documenti conservati nel formato utilizzato all’atto del versamento;
- Il file indice IPdA firmato e marcato temporalmente: esso è un file XML formato secondo le regole tecniche definite nella norma UNI 11386:2010 Standard SInCRO - Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali; nella sezione MoreInfo prevista dallo standard contiene per ciascun documento del PdA:
 - il corrispondente tag *Item* del SIPManifest.xml con cui il documento è stato versato in conservazione (per dettagli si rimanda all’allegato *Allegato1 - SIPManifest (Indice di Versamento).pdf*);
 - il corrispondente tag del *Item* del SIPResult.xml, ovvero il rapporto di versamento, contenente l’esito dei controlli effettuati sul documento (per dettagli si rimanda all’allegato *Allegato2 - SIPResult (Rapporto di Versamento).pdf*).

[Torna al sommario](#)

6.4 Pacchetto di Distribuzione

Il Pacchetto di distribuzione (PdD) o Dissemination Information Package (DIP) secondo la terminologia OAIS, consente di rispettare l’obbligo di esibizione dei documenti conservati; esso viene generato dal Sistema a partire dai Pacchetti di archiviazione conservati ed è finalizzato a mettere a disposizione degli Utenti, in una forma idonea alle specifiche esigenze di utilizzo, gli oggetti sottoposti a conservazione. Un pacchetto di distribuzione può coincidere con un pacchetto di archiviazione, ma è possibile gestire la

produzione di pacchetti di distribuzione specifici in relazione a particolari esigenze. In relazione alle sue caratteristiche e agli utilizzi a cui è destinato, il Pacchetto di distribuzione può essere generato al momento della richiesta da parte di un Utente e non conservato nel Sistema.

[Torna al sommario](#)

6.5 Formati

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

Qui di seguito l'elenco dei principali formati ammessi:

	FORMATO	ESTENSIONE	MIMETYPE
Bmp	File bitmap	bmp	image/bmp
Doc	Microsoft Word	doc	application/msword
docx	Microsoft Word 2007	docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Gif	Graphics Interchange Format (GIF)	gif	image/gif
Jpeg	Joint Photographic Experts Group	jpg	image/jpeg
jpeg2000	Joint Photographic Experts Group	jp2	image/jp2
Odg	OpenDocument Drawing	odg	application/vnd.oasis.opendocument.graphics
Odp	OpenDocument Presentation	odp	application/vnd.oasis.opendocument.presentation
Ods	OpenDocument Spreadsheet	ods	application/vnd.oasis.opendocument.spreadsheet
Odt	OpenDocument Text Document	odt	application/vnd.oasis.opendocument.text
Ots	OpenDocument Spreadsheet Template	ots	application/vnd.oasis.opendocument.spreadsheet-template
Ott	OpenDocument Text Template	ott	application/vnd.oasis.opendocument.text-template
Pdf	Portable Document Format	pdf	application/pdf
Plaintext		txt	text/plain
Png	Portable Network Graphics	png	image/png
Ppt	Microsoft Power Point	ppt	application/powerpoint
pptx	Microsoft Power Point 2007	pptx	application/vnd.openxmlformats-officedocument.presentationml.presentation
Project	Microsoft Project	mpp	application/vnd.ms-project
Ps	postscript	ps	application/postscript
Rtf	Rich Text Format	rtf	text/richtext
Tar	Tape archive (TAR)	tar	application/x-tar
Tiff	Tagged Image File	tiff	image/tiff
Wav	Audio file	wav	audio/wav
xls	Microsoft Excel	xls	application/excel
xlsx	Microsoft Excel 2007	xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Xml	eXtensible Markup Language	xml	application/xml
Zip	Archivio compresso (zip, gzip, gz, tgz)	zip	application/x-compressed
eml	email	eml	message/rfc822

[Torna al sommario](#)

6.6 Metadati conservati

Il sistema di conservazione consente di gestire tutti i metadati obbligatori previsti dalla normativa vigente ai quali vanno aggiunti quelli presenti negli accordi specifici. Per quanto riguarda le fatture, ad oggi, tenuto conto della normativa vigente, i dati obbligatori da fornire in sede di versamento in conservazione delle fatture e degli altri documenti afferenti ai cicli di fatturazione attivo e passivo (acconti, note di credito, note di debito ecc) sono i seguenti:

- indicazione se documento relativo al ciclo attivo o passivo;
- tipologia del documento, dalla quale vengono ricavati il termine entro cui il documento deve essere messo in conservazione e il termine fino a cui deve essere conservato;
- cognome e nome o denominazione dell'emittente e cognome e nome o denominazione del destinatario;
- codice fiscale e/o eventuale altro identificativo fiscale (es. partita IVA) del emittente/destinatario del documento (a seconda se documento del ciclo passivo o attivo);
- data di emissione della fattura;

- periodo fiscale, numero della fattura e sezionale (vale a dire il registro di numerazione, gestito come dato separato dal n.ro solo nel caso delle fatture attive)

Sia i dati obbligatori di cui sopra che i seguenti dati opzionali:

- importo della fattura
- valuta della fattura

sono stati configurati nel Sistema di Conservazione nel profilo specializzato per i documenti dei cicli di fatturazione attivo e passivo e pertanto vanno/possono essere specificati nel pacchetto di versamento dei documenti afferenti a ciclo attivo e passivo di fatturazione (una volta indicata la tipologia documentale), nei tag AttributoCustom del tag relativo al documento principale della scheda documento.

Essendo specificati nei dati di descrizione del pacchetto di versamento questi dati sono altresì fruibili come chiavi di ricerca delle fatture conservate.

[Torna al sommario](#)

6.7 Tempi di conservazione

Il sistema di conservazione consente di gestire i tempi entro cui è necessario mettere in conservazione e quelli per cui è necessario conservare i documenti. Tali informazioni sono fornite dal produttore all'atto del versamento oppure sono indicati negli accordi di servizio ed associati alle specifiche tipologie documentali.

Tali informazioni relativamente ai documenti dei cicli di fatturazione attivo e passivo sono configurati nel sistema di conservazione su tutte le tipologie documentali interessate. Pertanto nei pacchetti di versamento contenenti i documenti dei cicli di fatturazione attivo e passivo i sistemi produttori non specificano il termine di conservazione né il termine entro cui il documento deve essere sottoposto a conservazione : dalla tipologia dei documenti, in particolare dal fatto che afferiscano al ciclo passivo o a quello attivo di fatturazione, il sistema determina in automatico il tempo di conservazione e il termine entro cui è indispensabile che il processo di conservazione del documento sia perfezionato (con la firma e marca temporale dell'Indice di Conservazione contenente l'impronta e i dati del documento). Ciò detto è responsabilità fondamentale del produttore indicare correttamente la tipologia documentale: in caso di mancata o errata attribuzione della tipologia il sistema di conservazione non potrà procedere all'avvio e mantenimento della conservazione secondo le corrette tempistiche.

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

[Torna al sommario](#)

6.8 Peculiarità e gestione delle eccezioni

Nel caso di fatture attive, i documenti afferenti ad un certo registro (o sezionale) e periodo fiscale devono essere sottoposti a conservazione senza soluzione di continuità, ovvero non devono esserci "buchi" nella numerazione progressiva in quel registro e quell'anno fiscale. Qualora vi siano dei "buchi" la conservazione può essere "forzata" ma i "buchi di numerazione" vanno opportunamente motivati e documentati a cura dei responsabili dei processi di produzione e di conservazione delle fatture.

Per soddisfare questo requisito il Sistema di Conservazione prevede meccanismi di controllo ad hoc in fase di creazione degli Indici di Conservazione, mentre il versamento in conservazione può avvenire anche senza rispettare la non soluzione di continuità nelle numerazioni dei registri delle fatture attive. Quando il sistema procede alla chiusura, automaticamente o su richiesta, dei pacchetti di conservazione e

alla creazione automatica dei relativi Indici di Conservazione verifica se nel pacchetto vi sono documenti del ciclo attivo di fatturazione, nel qual caso controlla che:

1. per ogni registro (o sezionale) e anno delle fatture attive presenti nel pacchetto, tutti i numeri precedenti al minore presente nel pacchetto siano già in conservazione (ovvero in un Indice di Conservazione già firmato e marcato temporalmente);
2. per ogni registro e anno delle fatture attive presenti nel pacchetto, vi siano tutte le fatture con numeri compresi tra il minore e il maggiore di quelli presenti per il dato registro e anno

Se questi controlli non vengono superati il file Indice non viene creato e il pacchetto non viene chiuso; viene invece corredato in automatico di un messaggio che dettaglia il motivo per cui la chiusura del pacchetto non è stata possibile: il messaggio appare in evidenza al RdSC quando procede all'attività ordinaria di verifica dei pacchetti da firmare. Il RdSC deve allora verificare se le fatture mancanti, al fine di garantire la non soluzione di continuità della numerazione, sono in altri pacchetti aperti o sono ancora "da consolidare" (ovvero accettate dal sistema di conservazione ma non ancora inserite in un pacchetto) e nel caso la/le trovi procede a spostarle nel pacchetto di cui è fallita la chiusura, dopodiché procede ad una normale chiusura. Diversamente il RdSC è tenuto a verificare insieme al produttore – vale a dire la persona che ha la responsabilità del sistema/applicativo che ha versato le fatture, e qualora questi non sia designato, il coordinatore della gestione documentale e il/i responsabili del cliente cui fanno capo le fatture - il motivo per cui le fatture mancanti non risultino ancora versate in conservazione:

- a) qualora il versamento della/e fatture mancanti non possa essere effettuato per motivate ragioni, che in ultima analisi possono essere solo l'errore umano o applicativo/di infrastruttura informatica che abbia prodotto la mancanza o perdita della fattura anche nel sistema produttore, ciò andrà debitamente documentato dal RdSC, in base alle indicazioni fornite dal produttore; inserite queste motivazioni in apposito form il RdSC può forzare la chiusura del pacchetto nel cui Indice di Conservazione, poi firmato dal RdSC, verranno automaticamente riportate sia le ragioni che impedivano la chiusura che le motivazioni della forzata chiusura compilate a cura del RdSC
- b) qualora le fatture mancanti siano rintracciate all'interno del sistema produttore che non ha ancora proceduto a versarle in conservazione o le ha versate ma senza riuscire a farle prendere in carico al Sistema di Conservazione a causa di errori commessi nella formazione del pacchetto di versamento e mai sanati, è responsabilità del produttore effettuare il versamento in modalità corretta e responsabilità del RdSC fornire al produttore tutto il supporto necessario e verificare che il versamento avvenga tempestivamente e vada a buon fine.

[Torna al sommario](#)

7. IL PROCESSO DI CONSERVAZIONE

DigiDoc adotta lo standard ISO 14721:2012, comunemente noto come OAIS (Open Archival Information System), che costituisce lo standard di riferimento per qualsiasi sistema si occupi di digital preservation.

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

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

Le funzionalità gestite dal sistema permettono di garantire:

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

[Torna al sommario](#)

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

Il processo di invio in conservazione inizia con l'invocazione da parte di un sistema/applicativo del Soggetto Produttore del web service di SendSIP esposto da DigiDoc.

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

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

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

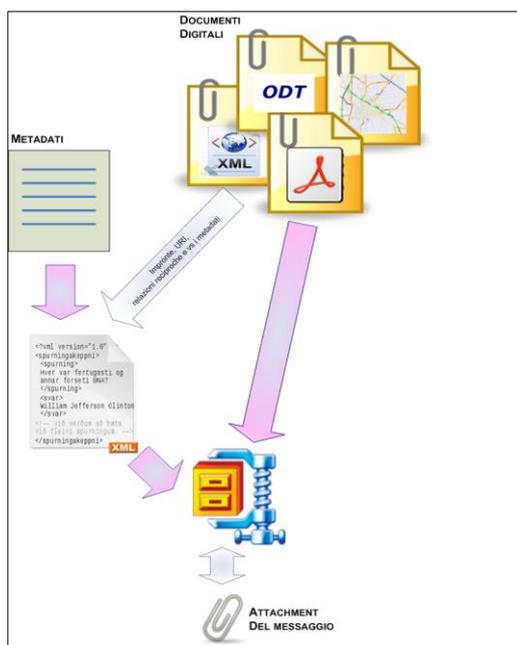


Figura 4 – Versamento del documento nel sistema di conservazione

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

In automatico viene anche prodotto giornalmente e avviato alla conservazione il file PDF/A del registro di tutti i SIP ricevuti (comprensivo delle impronte dei *SIPManifest.xml*): essendo un registro tenuto secondo i crismi di un registro di protocollo esso provvede l'apposizione di un riferimento temporale certo sul SIP.

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

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

[Torna al sommario](#)

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

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

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

[Torna al sommario](#)

7.2.1 Controllo impronta del pacchetto di versamento

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

[Torna al sommario](#)

7.2.2 Controllo dell'identità del soggetto produttore del pacchetto

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

[Torna al sommario](#)

7.2.3 Controllo delle Firme Digitali

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

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

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

Dunque ad oggi è in grado di verificare:

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

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

Il sistema traccia tutti i controlli effettuati e i relativi esiti (corredandoli del timestamp in cui li ha effettuati). In particolare dato che il servizio di verifica firma restituisce tutti i dati ottenuti dall'analisi

della busta crittografica - superamento o meno dei vari gradi di validità; estremi degli intestatari dei certificati di firma e delle CA che li hanno emessi; timestamp delle eventuali marche temporali associate; tipo di busta crittografica ecc – tutti questi dati vengono memorizzati nel pacchetto di archiviazione del documento.

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

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

[Torna al sommario](#)

7.2.4 Controllo dei Formati digitali

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

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

- PDF e PDF/A;
- tutti i formati della suite MS Office (inclusi Power Point, Visio e Project);
- tutti i formati della suite Open Office;
- RTF;
- formati immagine tiff, bmp, jpeg e jpeg2000, png, gif, pdf immagine;
- xml, ascii (txt, csv, ecc);
- formati audio e video quali wave, aiff;
- gli archivi compressi zip

- mail in formato eml

Il formato eml di fatto è un formato archivio/busta che a loro volta contengono delle parti con dei loro formati. Quindi quando vengono verificati, come nel caso delle buste crittografiche, il servizio di verifica formato va a verificare anche i contenuti del file archivio e delle parti della busta eml (attachment e body): se questi sono riconosciuti e ammessi il file archivio o eml è ammissibile in conservazione, altrimenti no. E' anche gestita la verifica ricorsiva dei formati dei file contenuti se nel file archivio/eml vi sono dei file/attachment che sono a loro volta file archivio o e-mail. Il fatto che il servizio di verifica formato sia in grado di riconoscere e verificare il contenuto di questi formati "contenitore", anche nel caso di annidamenti di buste, mette il Sistema di Conservazione nella condizione di poter accettare in conservazione:

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

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

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

- aperti
- ben documentati
- standard, possibilmente de-jure
- non proprietari
- largamente diffusi
- indipendenti dalla piattaforma
- che permettono di includere nei file l'insieme di metadati - self-documentation - che ne descrivono il contenuto e il processo di produzione, fornendo anche i dettagli tecnici per la loro rappresentazione negli ambienti tecnologici del futuro
- che non possano contenere macroistruzioni o per i quali siano disponibili strumenti efficaci per rilevare con sufficiente sicurezza la presenza di macroistruzioni
- che non prevedano meccanismi tecnici di protezione e di limitazione sull'utilizzo
- accessibili e robusti
- caratterizzati da un'elevata stabilità (backward e forward compatibility)

E' buona norma considerare che i formati per cui siano disponibili viewer o reader solo per una o poche piattaforme, anche se non vietati e quindi inseribili nel set dei formati ammessi, andranno comunque

evitati quanto più possibile, perché utilizzarli corrisponderebbe a creare una limitazione forte sulla capacità dei sistemi e client fruitori di riprodurre i documenti, e di conseguenza sulla capacità del sistema di conservarli.

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

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

Nel dettaglio del formato sono inoltre presenti:

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

[Torna al sommario](#)

7.2.4.1 Funzionalità di configurazione

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

- nome ed eventuale versione del formato: è questa la coppia che lo identifica univocamente tra tutti gli altri formati censiti;
- estensione principale dei file del dato formato: tale estensione sarà quella che verrà aggiunta in automatico ai nomi dei file accettati in conservazione qualora i nomi originali specificati nel tracciato di versamento/trasferimento non abbiano estensione o ne abbiano una ma non congruente con quella/e previste per il formato effettivo dei file;
- lista dei viewer/reader che sono utilizzabili per il rendering dei file del dato formato.

[Torna al sommario](#)

7.2.5 Controllo della Presenza di Macro e Codice Eseguitabile

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

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

[Torna al sommario](#)

7.2.6 Controllo dei Metadati

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

- di obbligatorietà: verifica la presenza di taluni metadati (o loro combinazioni) in assenza dei quali l'item non può essere accettato in conservazione;
- di correttezza sintattica: effettua controlli formali – di tipo e formato, di appartenenza ad un certo range/set predefinito di valori ecc – su tutti i metadati;
- di coerenza interna: verifica che non vi siano incongruenze tra i metadati all'interno dello stesso SIPManifest (ad esempio: verifica che le date dei documenti di un certo fascicolo non vadano oltre la data di chiusura specificata per il fascicolo);
- di coerenza con il contesto archivistico e organizzativo dell'ente: può essere configurato per verificare che i metadati che riconducono la documentazione versata al contesto amministrativo, organizzativo e archivistico dell'ente – classificazione, tipologia documentale, ufficio/struttura che ha prodotto il dato fascicolo, tipo del procedimento da cui è scaturito il fascicolo ecc – siano coerenti con il contesto stesso, così come è stato definito a sistema (se è stato definito); può verificare altresì che il sistema del Soggetto Produttore utilizzi solo quelle parti degli strumenti archivistici - voci del piano di classificazione, tipologie documentarie ecc. – che gli sono consentite (qualora siano definite delle limitazioni in tal senso)
- di unicità: il SIP Manager è anche in grado di verificare, sulla base di alcuni dati del SIPManifest che fanno parte delle informazioni di identificazione di OAIS, se un certo documento o unità di aggregazione di documenti è già stato inviato in conservazione o risulta descritto più volte nello stesso SIPManifest (nel qual caso può dar luogo ad un errore bloccante o solo ad un avvertimento)

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

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

- è obbligatorio specificare un identificativo (univoco per il sistema che invia) per ogni documento o aggregato di documenti
- è obbligatorio specificare un'etichetta/segnetura per ogni documento o aggregato di documenti (nel caso di documento protocollato potrebbero essere gli estremi di protocollo, nel caso di un fascicolo archivistico la sua segnetura basata sulla classifica e l'anno di apertura)
- è obbligatorio specificare un'intitolazione ovvero una descrizione/oggetto per ogni aggregato di documenti o singolo documento
- è obbligatorio specificare almeno un riferimento cronologico (data di acquisizione/produzione/registrazione a protocollo; data/anno di apertura o chiusura del fascicolo ecc) per ogni documento o aggregato di documenti
- è obbligatorio specificare una tra tipologia, classifica o procedimento amministrativo che ha dato luogo alla documentazione, ovvero specificare il tempo o termine di conservazione se non

desumibile da nessuno degli elementi precedenti. Se il tempo è specificato sul documento o aggregato inviato, non può essere inferiore ma solo superiore a quello stabilito da eventuali regole del massimario di selezione e scarto applicabili a quel documento o aggregato.

Inoltre ai dati del nucleo minimo richiesto, nel caso di documentazione tributaria o fiscalmente rilevante come le fatture si aggiungono i dati già indicati al § 6.6.

[Torna al sommario](#)

7.2.7 Controllo Impronta

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

[Torna al sommario](#)

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

Gli audit dei controlli effettuati, con dettaglio di esiti ed eventuali risultati (ad esempio nel caso della verifica della validità delle firme, tra i risultati vi sono i dati dei certificati di firma) vengono memorizzati per tutti gli item del SIP, sia quelli accettabili che quelli rifiutati, andando a costituire il “rapporto di versamento” SIPResult.xml, il cui schema è fornito nell'allegato Allegato2 - SIPResult (Rapporto di Versamento).pdf. Il rapporto viene esso stesso archiviato e avviato alla conservazione per tempo illimitato. Come detto in precedenza anche il SIPManifest.xml viene archiviato e avviato alla conservazione, il tutto al fine di attestare nel tempo il flusso di tutto ciò che è arrivato in conservazione e come tale flusso è stato trattato. Più precisamente il rapporto di versamento SIPResult.xml viene archiviato collegandolo al relativo pacchetto di versamento attraverso l'inserimento della sua impronta, data e ora di generazione e URI nella stessa tabella di archiviazione dei dati dei SIP. Analogamente al SIP anche il rapporto di versamento, non appena generato, viene sottoposto a registrazione in apposito registro dei rapporti di versamento che quotidianamente viene prodotto in formato PDF/A e avviato alla conservazione.

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

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

[Torna al sommario](#)

7.3.1 Rinnovo marche temporali in scadenza

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

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

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

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

[Torna al sommario](#)

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

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

- Verifica impronta del pacchetto;
- Apertura della busta crittografica dei file firmati;
- Conformità del formato della busta crittografica dei file firmati alla normativa italiana;
- Formati dei documenti digitali.

Viene prodotto un report dello scarto in cui viene riportato il timestamping in cui è avvenuto il controllo ed un dettaglio dei controlli effettuati ed il loro esito. Tale report viene inviato al referente tecnico indicato dal produttore.

[Torna al sommario](#)

7.5 Preparazione e gestione del pacchetto di archiviazione

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

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

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

I documenti digitali accettati vengono consolidati attraverso l'aggregazione dei documenti stessi in insiemi logici chiamati pacchetti in consolidamento (ovvero pacchetti non ancora chiusi, vedi § successivo). Già al momento dell'accettazione in conservazione per ogni scheda documento e ogni unità di aggregazione sia tutti i dati presenti nel SIPManifest.xml che quelli frutto dei controlli vengono “impacchettati” in xml, a formare i pacchetti di archiviazione, e in questa forma archiviati sullo storage del sistema di conservazione. Sul database relazionale vengono memorizzati i puntatori ai pacchetti di archiviazione conservati su storage. Al tempo stesso i dati di descrizione di ciascun item versato e accettato vengono inseriti nella banca dati relazionale del Sistema di Conservazione.

E' possibile configurare:

- sia i trigger di innesco automatico della creazione degli Indici di Conservazione, quali i seguenti:

- quando si raggiunge la soglia minima di giorni dallo scadere del termine entro cui la documentazione deve essere messa in conservazione perché scadono i certificati delle firme digitali apposte;
- per rispettare dei termini stabiliti dalla norma (ad esempio nel caso di documentazione fiscalmente rilevante quali le fatture e i libri contabili che va messa in conservazione entro un certo lasso di tempo a partire dalla data di emissione/produzione);
- quando sono stati accumulati un determinato numero o una determinata dimensione di documenti;
- con una certa cadenza temporale, ad esempio settimanale o mensile;
- sia i vincoli da rispettare nella creazione dei pacchetti quali
 - se fare pacchetti omogenei per certe tipologie o formati digitali di documenti;
 - se creare pacchetti che contengono documentazione i cui termini di conservazione devono restare entro un certo range (in modo tale che tutta la documentazione del pacchetto diventi scartabile in un intervallo temporale relativamente ristretto).

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

[Torna al sommario](#)

7.5.1 Creazione Indice di Conservazione

L'attività di chiusura dei pacchetto in consolidamento, ovvero di creazione dei relativi Indici di Conservazione conformi al UNI 11386:2010 Standard SInCRO, è svolta per lo più in modo automatico, ma se necessario, in rari casi, può essere forzata manualmente dal RdSC o suo delegato. La chiusura manuale dei pacchetti si rende necessaria ad esempio se essi contengono documentazione fiscalmente rilevante con numerazione progressiva interrotta.

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

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

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

- gli URI che puntano allo stream dei componenti digitali di ciascun documento sullo storage del sistema: l'URI permette il reperimento certo dei file ma non è un path assoluto, cosicché qualora i

file dovessero essere riversati (riversamento diretto) su altro storage l'URI può non cambiare, il che costringerebbe a riformare e certificare nuovamente i PdA contenenti quei documenti;

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

[Torna al sommario](#)

7.5.2 Certificazione PdA (firma e apposizione riferimento temporale)

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

Le attività di certificazione dei PdA consistono pertanto in questi passaggi:

- individuazione da parte del Sistema di Conservazione dei PdA chiusi che devono essere firmati
- segnalazione della lista al Responsabile del servizio di conservazione. Questa operazione può avvenire tramite notifica al Responsabile via posta elettronica.

Una volta che il Responsabile del servizio di conservazione o suo delegato ha firmato il PdA, se il PdA che in base alla normativa vigente prevede una seconda firma dell'Indice di Conservazione (da parte di un notaio o di un pubblico ufficiale), il Sistema di Conservazione gestisce anche questa casistica e inserisce il PdA che manca della seconda firma in un apposito elenco di PdA in attesa della seconda firma.

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

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

[Torna al sommario](#)

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

7.6.1 Funzionalità di ricerca

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

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

- sicuro
- semplice
- guidato

- adeguato alle esigenze

La sicurezza dell'accesso è garantita attraverso:

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

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

La semplicità dell'accesso è principalmente ottenuta attraverso l'adozione del motore di indicizzazione con cui vengono indicizzati sia il testo dei documenti digitali (eventualmente anche quelli cartacei, previa loro digitalizzazione e sottomissione a processo di OCR) che i metadati (almeno quelli più significativi): in questo modo in una modalità semplice e intuitiva – per così dire google like – è possibile effettuare una ricerca per parole che agisce sia sui metadati che sul contenuto dei documenti (ricerca full-text). Al tempo stesso DIGIDOC permette di adeguare la modalità di accesso alle esigenze di chi ricerca: infatti consente di impostare filtri di ricerca “strutturati” – con operatori di uguaglianza, somiglianza, maggiore, minore, compreso tra, valorizzato e non valorizzato - su tutti i principali metadati della documentazione conservata, inclusi quelli specifici di certe tipologie documentali.

Permette altresì di ricercare la documentazione navigando le diverse strutture gerarchiche – piano di classificazione, articolazione dell'archivio in serie, sottoserie ecc, indici tematici, organigramma dell'Ente produttore – secondo cui la documentazione è organizzata o alle quali si raccorda.

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

- il/i file che compongono il documento
- i metadati trasmessi dal versatore
- i metadati calcolati dal sistema in fase di versamento
- l'esito dei singoli controlli eseguiti
- le informazioni del PdA di appartenenza del documento (stato del PdA, descrizione, data creazione, etc)

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

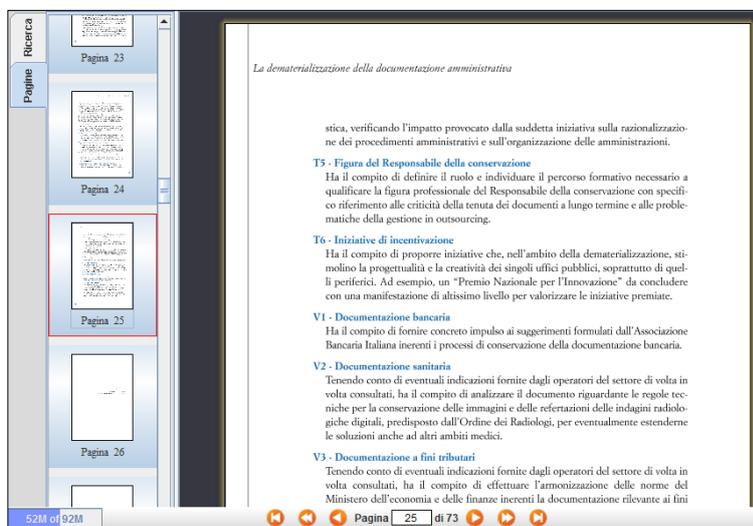


Figura 5 - Visualizzazione documento

[Torna al sommario](#)

7.6.2 Funzionalità di esibizione

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

- in cooperazione applicativa, dei web service che in modo completamente automatizzato consentono di recuperare uno o più documenti conservati da parte del sistema/applicativo che li ha versati in conservazione o altri applicativi con opportuni diritti di accesso, unitamente, se richiesti, alle prove di conservazione (Indice di Conservazione firmato e marcato) e/o all'attestato di conformità all'originale conservato e/o ai viewer/reader necessari alla lettura dei componenti digitali dei documenti;
- attraverso le web GUI con cui RdSC e suoi delegati nonché personale abilitato dei soggetti produttori possono visionare la documentazione conservata.

[Torna al sommario](#)

7.6.2.1 Esibizione in cooperazione applicativa

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

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

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

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

- indicazione se deve essere inserito nel DIP anche il viewer o reader relativo al formato del documento (per un dato sistema operativo specificato)
- indicazione se è richiesto anche l'Indice di Conservazione attestante che il documento è conservato secondo norma
- indicazione se è richiesta anche la ricevuta di conformità all'originale conservato

Qualora siano stati richiesti il viewer/reader e/o l'Indice di conservazione e/o la ricevuta di conformità anch'essi vengono inseriti nell'archivio compresso che implementa il DIP.

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

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

al fine di ottenere che il DIP restituito contenga metadati e componenti digitali di tutti i documenti della lista, ovvero di tutti i documenti appartenenti alla/e aggregazioni di documenti specificate.

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

- sincrona, quando il richiedente resta in attesa della risposta contenente il DIP. Consente l'esibizione di un solo documento alla volta, ed è ammessa solo per documenti di dimensione inferiore ad una soglia prestabilita; qualora la dimensione del documento richiesto superi il valore soglia la richiesta viene respinta.
- asincrona, quando a fronte dell'invocazione del servizio il richiedente ottiene solo un ticket di richiesta con il quale, in un momento successivo, va a richiedere lo stato della sua richiesta e l'eventuale risultato – il DIP – qualora la richiesta sia stata evasa.

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

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

[Torna al sommario](#)

7.6.2.2 Esibizione on-line

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

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

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

- per il client non vi sia un viewer/reader in grado di restituirgli il documento nel formato originale;
- l'utente che chiede la visualizzazione non voglia o non possa installare sul proprio client il viewer o reader necessario alla restituzione del documento digitale nel formato originale in cui è conservato

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

[Torna al sommario](#)

7.6.2.3 Esibizione tramite download da web GUI

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

7.6.2.4 Esibizione di singolo documento

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

- link attraverso cui scaricare anche il viewer o reader corrispondente al formato del documento: se per il dato formato DigiDoc dispone di più viewer o reader per diverse piattaforme e sistemi operativi, vengono forniti altrettanti link, indicando per ognuno la piattaforma a cui si riferisce. Da notare che in caso di documenti che siano buste crittografiche p7m, tsd o m7m, il sistema propone lo scarico del/i viewer o reader relativi al formato del file contenuto nella busta crittografica
- in caso di documento firmato digitalmente che sia una busta crittografica p7m, tsd o m7m, vengono forniti due link, uno per scaricare la busta e uno per scaricarne il contenuto depurato delle firme (il file “sbustato”)
- nel caso di documenti con firme e/o marche temporali *detached* o comunque formati da più componenti digitali (i.e. più file) il sistema dà un'opzione per scegliere se effettuare lo scarico di tutti i componenti digitali come un unico file archivio (zip o tar, a scelta)
- scelta se scaricare o meno anche il file xml “Indice di Conservazione”, firmato dal Responsabile del servizio di conservazione (o suo delegato) e marcato temporalmente, attestante la conservazione a norma del documento
- per alcuni formati viene data la possibilità, esattamente come nella visualizzazione on-line, di ottenere il documento digitale convertito in formato PDF o PDF/A - che non è quello di conservazione - e di scaricare quest'ultimo: in questo caso l'utente viene avvertito che si tratta di una versione in formato diverso da quello di conservazione
- il sistema consente di scaricare la ricevuta di “conformità all'originale conservato” del documento, ovvero un PDF/A che contiene: i riferimenti dell'Ente produttore; gli estremi e i principali dati descrittivi del documento; un timbro digitale – codice a barre bidimensionale - contenente le impronte del/dei componenti digitali del documento

[Torna al sommario](#)

7.6.2.5 Esibizione tramite Stampa

Anche questa modalità di esibizione è messa a disposizione dalle GUI web di DigiDoc: laddove sono rese disponibili l'esibizione online e il download del/dei file del documento (esibizione tramite download) è data anche una funzione per effettuarne la stampa: selezionandola il sistema attiva la stampa dei file sul client – purché questo sia già dotato dei programmi necessari ad aprire e mandare in stampa quei file – ed eventualmente, se richiesto, la fa seguire dalla stampa della ricevuta di conformità.

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

[Torna al sommario](#)

7.6.2.6 Esibizione telematica

DigiDoc prevede anche l'esibizione telematica dei documenti attraverso canale e-mail, PEC o ordinaria.

La richiesta di esibizione telematica si effettua dalla stessa interfaccia web dalla quale si richiamano le modalità di esibizione on-line e tramite download e tramite stampa.

Per chi effettua la richiesta deve essere noto un indirizzo e-mail a cui indirizzare l'esibizione, o altrimenti il richiedente deve fornirlo al volo nel momento in cui sottometta la richiesta di esibizione.

L'esibizione via e-mail avviene attraverso caselle e-mail, ordinarie o di PEC, che sono state messe a disposizione di DigiDoc. L'esibizione via e-mail è disponibile solo per i documenti la cui dimensione è inferiore ad una soglia prestabilita (una dimensione ragionevole per l'allegato di una e-mail). Infatti l'e-mail di esibizione contiene come allegati:

- i file che compongono il documento;
- la ricevuta di conformità, se richiesta;
- un Manifest.xml con i metadati del documento, se richiesto.

Il corpo della mail spiega il significato di ciascun allegato, mentre il suo oggetto riporta gli estremi identificativi del documento e la data e ora in cui ne è stata richiesta l'esibizione.

[Torna al sommario](#)

7.6.2.7 Esibizione di copia conforme all'originale conservato a norma

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

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

La firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.4. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

[Torna al sommario](#)

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

Dalle web GUI che DiGiDoc mette a disposizione è possibile selezionare uno o più documenti e aggregati di documenti al fine di richiedere un pacchetto di distribuzione contenente tutta la documentazione selezionata. Una volta acquisita la richiesta DiGiDoc attiva in modo asincrono l'elaborazione del DIP richiesto e quando questo è pronto rende scaricabile il DIP da apposita GUI in cui il richiedente consulta lo stato delle richieste di esibizione effettuate. Il DIP è un archivio compresso che oltre ai documenti richiesti contiene un file indice conforme allo schema documentato in *Allegato4 - ResponseEsibizione.pdf*

Nei casi previsti dalla normativa, la firma sarà apposta da un pubblico ufficiale le cui modalità di coinvolgimento sono descritte nel paragrafo 4.4. Per ogni cliente, nel contratto di affidamento, viene regolamentata l'attività del pubblico ufficiale.

[Torna al sommario](#)

7.8 Scarto dei pacchetti di archiviazione

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

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

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

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

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

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

A partire dalla proposta predisposta in automatico l'archivista redige la proposta di scarto definitiva e la sottomette alla Sovrintendenza per autorizzazione. La Sovrintendenza verifica la documentazione contenuta nella proposta e seleziona quella di cui autorizzare lo scarto.

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

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

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

[Torna al sommario](#)

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

Il sistema DiGiDoc rispetta lo standard OAIS; pertanto è in grado di esportare secondo lo schema documentato in *Allegato4 - ResponseEsibizione.pdf* i pacchetti di archiviazione conservati in pacchetti seguendo le regole che permettono la loro importazione in un altro sistema aderente allo standard OAIS.

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

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

[Torna al sommario](#)

7.10 Riversamento diretto e sostitutivo

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

[Torna al sommario](#)

7.10.1 Riversamento diretto

DiGiDoc prevede le funzioni che consentono al Responsabile del servizio di conservazione, su propria iniziativa o su richiesta di un soggetto produttore, di schedare il riversamento diretto di tutti i documenti che risiedono su un certo storage / dispositivo di memorizzazione piuttosto che di una particolare selezione di documenti: dovrà naturalmente indicare quale/i sono i nuovi supporti fisici di memorizzazione. Tali funzioni consentono anche, dove i supporti di memorizzazione di provenienza lo consentano, di specificare se il riversamento deve spostare i documenti al nuovo supporto di memorizzazione o piuttosto farne una copia mantenendo quella sul vecchio supporto.

Tutte le informazioni relative ai riversamenti diretti che un documento ha subito durante la sua conservazione in DIGIDOC vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento.

[Torna al sommario](#)

7.10.2 Riversamento sostitutivo

Secondo quanto specificato dalle normative, il riversamento sostitutivo è il "processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica" (Delibera CNIPA 11/2004 art. 1 comma 1).

Nel momento in cui un formato diventa obsoleto, ovvero quando è prossimo a non essere più leggibile, vengono messe a disposizione del Responsabile del servizio di conservazione delle funzioni di riversamento sostitutivo atte a migrare ad altro formato i documenti già conservati a norma che hanno il formato obsoleto.

Tutte le informazioni relative ai riversamenti sostitutivi, come già quelle relative ai riversamenti diretti, che un documento ha subito durante la sua conservazione in DIGIDOC vengono man mano ad arricchire il set di metadati contenuti nell'AIP del documento (oltre che essere memorizzate negli audit trail generali del sistema): in particolare di ogni riversamento sostitutivo vengono memorizzati nell'AIP i

formati originale e di destinazione e gli eventuali dettagli sul formato originale (versione, rischi connessi ecc).

[Torna al sommario](#)

8. IL SISTEMA DI CONSERVAZIONE

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

8.1 Componenti Logiche

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

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

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

[Torna al sommario](#)

8.2 Componenti Tecnologiche

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

8.2.1 Software di base

Ambiente
Java Runtime
SQL
JDK e JRE Compatibility level

[Torna al sommario](#)

8.2.2 Framework di sviluppo utilizzati

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

[Torna al sommario](#)

8.2.3 Scalabilità

Adottando una politica di scalabilità orizzontale sulla configurazione base il sistema viene configurato in più nodi applicativi bilanciati da un load Balancer, in modo da distribuire il carico su più nodi e fornire meccanismi di fault avoidance, oltre che rendere il sistema più affidabile e ridurre il down-time dello stesso.

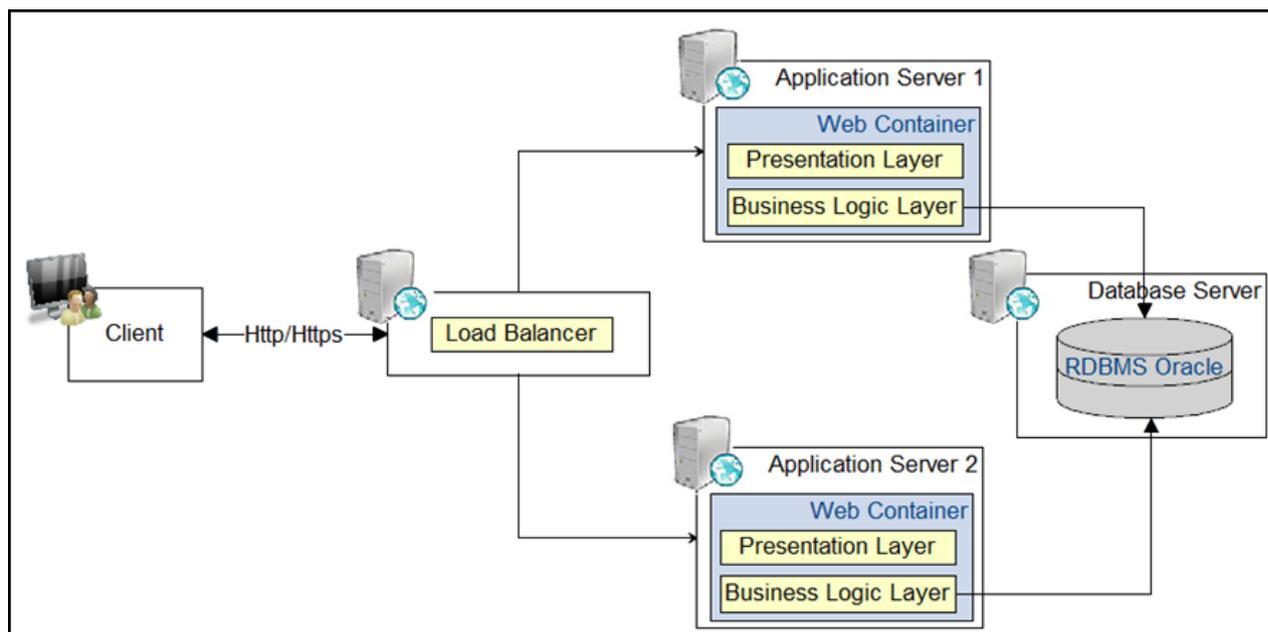


Figura 6 - Configurazione del sistema con un 1° livello di scalabilità

Tale suddivisione non comporta nessuna modifica all'applicativo, ma occorre solamente configurare il load balancer in modo che punti ai vari nodi application server. Sui nodi application server sono installati sia il presentation layer che il business logic layer di tutti i componenti del sistema.

Passando ad un livello ulteriore di scalabilità orizzontale si passa ad una configurazione come quella illustrata nella figura successiva: anche in questo caso il sistema viene scalato senza dover modificare alcuna parte dell'applicativo, ma solamente modificandone le configurazioni.

In questa configurazione oltre al load balancer e alla divisione dell'applicativo su più nodi vengono suddivisi in nodi distinti il presentation layer dal business logic layer.

La comunicazione tra i due layer avviene tramite web service, principalmente in modalità RESTful, secondariamente anche SOAP.

In questa configurazione le chiamate ai web service del sistema da parte di altre applicazioni o altri moduli esterni creano carico di lavoro solo sugli application server contrassegnati dalla lettera b; viceversa delle chiamate alle web UI dei vari componenti del sistema (in particolare le UI di ricerca ed esibizione della documentazione conservata) vanno a creare carico di lavoro sia sugli application server contrassegnati dalla lettera a che su quelli contrassegnati dalla lettera b.

La configurazione potrebbe essere ulteriormente scalata separando su application server distinti i diversi moduli del sistema (naturalmente quelli che hanno dipendenze da altri verranno installati comprensivi delle librerie jar dei moduli da cui dipendono).

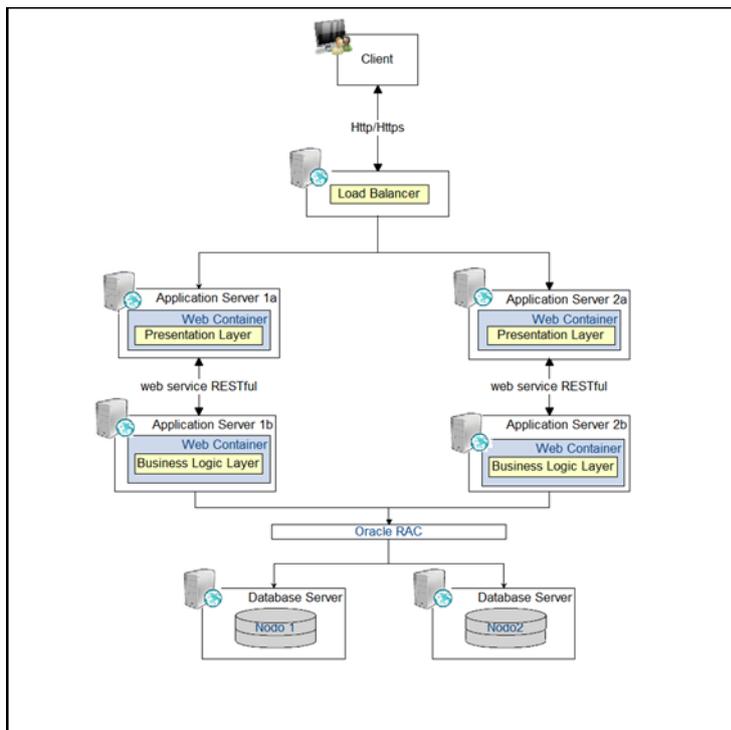


Figura 7 - Configurazione del sistema con un 2° livello di scalabilità

In figura viene anche illustrato come il sistema supporti una soluzione scalata orizzontalmente anche per ciò che riguarda il data layer, ovvero il database: infatti supporta la configurazione Real Cluster Application (RAC), in modo da aumentare la capacità transazionale del database, rendere il sistema più affidabile e ridurre il down-time.

Parimenti anche per lo storage dei file conservati l'architettura applicativa consente di distribuire lo storage su più container fisici (Oracle WCC o altri tipi di storage, anche non veloci ma solo ad alta affidabilità).

[Torna al sommario](#)

8.3 Componenti Fisiche

L'infrastruttura tecnologica necessaria per erogare le attività di conservazione è ospitata nei seguenti data center di Engineering D.HUB:

- Vicenza, Via Vecchia Ferriera 5: Data Center Primario ove risiedono i sistemi di conservazione, strutturato in modo da garantire la sicurezza logica e fisica, nonché i servizi di backup e monitoraggio.
- Pont Saint-Martin (AO), Viale C. Viola 76: Data Center secondario avente le stesse caratteristiche di sicurezza di quello primario ed utilizzato per erogare il servizio di Disaster Recovery (DR).

Il dettaglio degli asset come previsto dalla norma ISO/IEC:27001/2013 è descritto nel sistema ECMDB di Engineering D.HUB.

Gli schemi relativi all'ambiente di produzione e all'ambiente di collaudo sono di seguito riportati.

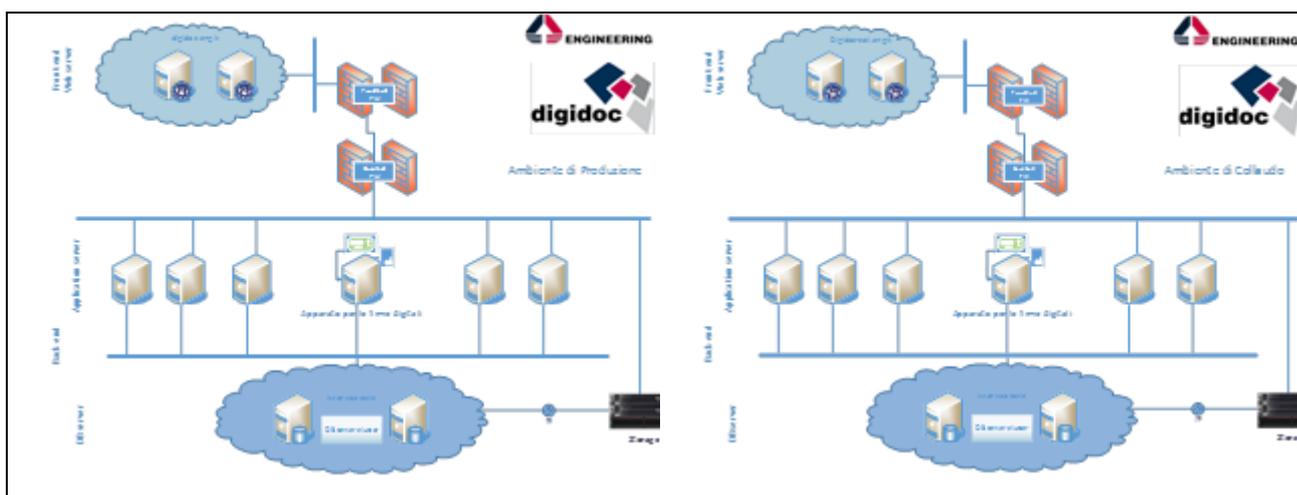


Figura 8 - Configurazione ambienti di collaudo e produzione

Le attività di gestione degli impianti presenti nei Data Center in cui viene erogato il servizio di conservazione, nonché le attività di gestione degli allarmi originati dalle piattaforme di monitoraggio impiantistica sono descritte nella procedura presente nel SGQ “RS08PR05 Procedura Gestione Impianti Data Center”. Tali attività hanno l'obiettivo di assicurare che:

- Gli impianti siano sempre in piena efficienza grazie ad una corretta manutenzione preventiva malfunzionamenti o “fault” siano immediatamente segnalati alle funzioni preposte, al fine di consentire un tempestivo avvio delle azioni di ripristino
- siano evidenziate eventuali situazioni critiche, che attestino degrado degli impianti o potenziali incidenti futuri.

In particolare, sono oggetto delle attività di gestione i seguenti impianti:

- Impianti elettrici (GE, UPS, trasformatore, quadri di sala);
- Impianti meccanici (condizionamento, pompaggio acqua, trattamento dell'aria, etc.)

- Impianti antincendio;
- Impianti di sicurezza (anti-intrusione, sorveglianza)

L'architettura degli impianti presenti nei DC delle aziende del Gruppo Engineering che ospitano l'archiviazione, è formalizzata in appositi schemi aggiornati e archiviati (in formato cartaceo e/o elettronico), a cura del Site Manager dello specifico DC.

Dal punto di vista organizzativo, le attività di controllo e gestione degli impianti del DC sono svolte da personale della funzione Infrastrutture DC di D.HUB (Site Manager ed eventuali collaboratori), mentre la parte "operativa" della manutenzione ordinaria/straordinaria è oggetto di apposito appalto a ditte specializzate.)

Gli accordi contrattuali che regolano le attività di manutenzione affidate a ditte esterne sono definiti e gestiti in armonia alla procedura aziendale PGA02 Gestione Ciclo Passivo.

Nei Data Center di Engineering D.HUB che ospitano gli ambienti per la conservazione, sono presenti le seguenti tipologie di infrastruttura:

- Infrastrutture elettriche
- Infrastrutture "meccaniche" (raffreddamento)
- Infrastrutture antincendio
- Infrastrutture di sicurezza

Il "perimetro" degli impianti è delimitato a monte dall'eventuale provider di servizi e a valle dal singolo apparato presente nei DC.

Appartengono alla categoria Infrastrutture Elettriche i seguenti impianti:

- tutte le linee elettriche, sia in bassa tensione (BT) che in media tensione (MT),
- tutti i quadri elettrici (generali e di distribuzione con i relativi rifasatori), sia in asservimento agli apparati come server, dischi, ecc. sia in asservimento ad altre tipologie di impianti sia "servono" al data center (es. impianto elettrico dei condizionatori),
- i sistemi di continuità assoluta (UPS statici e dinamici),
- i gruppi elettrogeni (compreso motore e cisterna carburante),
- le centraline che sovrintendono gli automatismi degli interruttori di potenza elettromeccanici,
- le "celle" di arrivo e partenza,
- i trasformatori MT/BT.

Appartengono alla categoria Infrastrutture Meccaniche tutti quegli impianti che permettono il raffreddamento delle sale tecnologiche:

- i condizionatori ad espansione diretta,
- i gruppi frigo ad acqua (comprese le unità di ventilazione interne alle sale),
- le torri evaporative,
- le pompe e i circuiti idraulici,
- il sistema di trattamento dell'acqua per le torri evaporative,
- le unità di trattamento dell'aria (UTA),
- valvole, termostati, filtri ecc., facenti parte integrante della macchina e relativi al corretto funzionamento degli apparati refrigeranti.

Fanno parte delle Infrastrutture Antincendio, tutti gli impianti di rivelazione e spegnimento:

- gli estintori manuali,
- le bombole di Azoto o Argon,
- i sensori di rivelazione fumi,
- le centraline che sovrintendono il funzionamento sensori di rivelazione fumo,
- l'impianto di estinzione automatica.

Fanno parte delle Infrastrutture di Sicurezza tutti gli impianti che assicurano la sicurezza perimetrale, quali l'impianto di sorveglianza TVCC e gli impianti anti-intrusione (porte allarmate).

Il servizio di manutenzione svolge le attività avvalendosi di figure professionali competenti, in armonia alle normative di Legge vigenti (ad es. DM 37/08, D.Lgs. 81/2008).

Le prestazioni vengono svolte nelle ore e nei giorni compatibili con le operazioni da compiere, senza comunque ostacolare le normali attività di erogazione dei servizi in corso. In caso di necessità di intervento di manutenzione, il DC Site Manager concorda con il personale di manutenzione orari e modalità per intervenire. Nel caso di interventi la cui interferenza con le attività di erogazione dei servizi non può essere evitata, il DC Site Manager concorda orari diversi da quelli di lavoro oppure orari notturni, in modo da minimizzare gli impatti.

E' cura del personale di manutenzione tenere aggiornata tutta la documentazione tecnica relativa alle apparecchiature in manutenzione.

Il Servizio di Manutenzione ha la responsabilità di organizzare il lavoro del proprio personale in garanzia del raggiungimento degli scopi prefissati (formalizzati nei documenti contrattuali che regolano il rapporto con i fornitori del servizio) e il rispetto dei tempi previsti, compresi eventuali turni di reperibilità, soprattutto per garantire un tempestivo intervento in caso di problemi su impianti/dispositivi i cui guasti potrebbero causare disservizi rilevanti, se non riparati prontamente.

Le operazioni di manutenzione da eseguire alle scadenze specificate sono registrate in un apposito calendario annuale riassuntivo (Cronoprogramma), nel quale si riportata la settimana nella quale è previsto l'intervento di manutenzione, l'apparato oggetto della manutenzione e il codice della scheda di manutenzione contenente la lista delle operazioni da effettuare.

Il Cronoprogramma deve essere verificato ed aggiornato ogni qualvolta varia l'architettura degli impianti (e quindi anche la lista degli impianti in manutenzione) e comunque almeno con cadenza annuale.

- Gestione piattaforme di monitoraggio, in termini di riesame delle utenze; I risultati di tali riesami periodici devono essere formalizzati, nella misura in cui vi siano indicazioni per il periodo successivo o qualora costituiscano input all'esecuzione di altri processi aziendali (es. RS02 Processo Gestione Approvvigionamento, MS01 Processo Gestione Misurazioni Analisi Miglioramento).

[Torna al sommario](#)

8.4 Procedure di gestione e di evoluzione

Qui di seguito l'elenco delle procedure riguardanti la sicurezza del sistema di conservazione. Tali procedure fanno parte del Sistema di Gestione per la Qualità di Engineering, sono rese disponibili al personale coinvolto nelle attività sulla intranet aziendale, in considerazione del livello di riservatezza attribuito a ciascun documento.

Ambito	Descrizione sintetica	Nome della procedura
Sistema di Gestione per la Qualità	Manuale della Qualità di Engineering D.HUB e Manuale della Qualità di Engineering Ingegneria Informatica	D.HUB QM01 Manuale Qualità EII QM01 Manuale Qualità
Sistema di Gestione per la Qualità	Visione complessiva ed unitaria dei Processi Aziendali costituenti il Sistema di Gestione per la Qualità	QS01 Processo Gestione Sistema Qualità
Sistema di Gestione per la Qualità	Descrive la struttura documentale della Information Security Policy e le modalità con cui i documenti aziendali sono resi disponibili al personale coinvolto nelle attività, anche in considerazione del livello di riservatezza attribuito a ciascun documento. Alla base dei criteri di accessibilità degli elementi documentali vi è il principio del " <i>need to know, need to use</i> ": in base a tale principio, le informazioni devono essere disponibili esclusivamente per il personale che ha bisogno di conoscerle e di utilizzarle per motivi di lavoro.	QS01P01 Procedura Gestione documentale
Sistema di Gestione per la Qualità	La procedura descrive il flusso di creazione, modifica, rimozione delle utenze di tipo applicativo sulla piattaforma DigiDoc (nei vari ambienti a disposizione), di gestione delle password per garantire tali accessi, nonché indicazioni sugli oggetti e le modalità di gestione dei log applicativi	RS09P01 Procedura Gestione Utenze Applicative DigiDoc
Sistema di Gestione per la Qualità	La procedura descrive le modalità con cui si gestiscono gli interventi correttivi e/o evolutivi sulla piattaforma DigiDoc, in garanzia dell'efficacia dell'intervento stesso, e in modo da assicurarne la tracciatura.	RS09P02 Procedura di Manutenzione Correttiva / Evolutiva DigiDoc
Impostazione, implementazione e gestione della Sicurezza delle Informazioni	Politica per la Sicurezza delle Informazioni: documenti di riferimento per la descrizione generale delle modalità adottate da Engineering ed Engineering D.HUB per la gestione della Sicurezza delle Informazioni. il primo documento è applicabile al	RS08A02 Information Security Policy RS09A01 Information Security Policy – Conservazione Digitale

	<p>perimetro dei servizi erogati da Engineering D.HUB (outsourcing infrastrutturale), mentre il secondo documento si applica al perimetro relativo all'erogazione del servizio di Conservazione dei Documenti Informatici, incluse le attività di manutenzione della Piattaforma DigiDoc.</p> <p>Quanto descritto nel documento è mandatorio sia per i processi che vengono gestiti ed eseguiti interamente all'interno del contesto aziendale, sia per quei processi che prevedono il coinvolgimento di terze parti (es. che coinvolgono Clienti, Partner, Fornitori).</p> <p>I documenti citati forniscono le linee guida e i rimandi a procedure aziendali di dettaglio per la assicurare la Sicurezza delle Informazioni all'interno dei due perimetri di riferimento (Outsourcing Infrastrutturale ed erogazione del Servizio di Conservazione Documenti Digitali). Essi danno evidenza, inoltre, del rispetto delle misure minime previste dal D.Lgs.196/2003.</p>	
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>censimento dei controlli e obiettivi di controllo adottati da Engineering D.HUB (per il perimetro relativo all'Outsourcing Infrastrutturale) e da Engineering Ingegneria Informatica (per il perimetro relativo all'erogazione del Servizio di Conservazione dei Documenti Informatici), per garantire la Sicurezza delle Informazioni, inclusa la motivazione di eventuali esclusioni.</p>	<p>RS08A07 Dichiarazione di Applicabilità</p> <p>RS09A02 Dichiarazione di Applicabilità – Conservazione dei Documenti Informatici</p>
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Definizione di modalità di comunicazione tra Engineering D.HUB e il Cliente Engineering – DigiDoc durante l'erogazione dei servizi. Garantisce che le informazioni a perimetro siano adeguatamente protette secondo appropriati livelli di riservatezza, la disponibilità delle adeguate istruzioni di lavoro al personale</p>	<p>RS0802P01 Procedura Service Transition</p>

	sulla base del principio "need to know"	
Aspetti Organizzativi	<p>Descrive le Modalità con cui Engineering D.HUB ed Engineering (per il perimetro relativo al Servizio di Conservazione dei Documenti Informatici) interagisce con le Pubbliche Autorità nel caso di circostanze configurabili come reato informatico. Si garantisce che i contatti con le Autorità competenti, in caso di circostanze rilevanti per la Sicurezza delle Informazioni aventi impatto legale, siano gestiti in modo uniforme da una interfaccia ufficialmente incaricata dall'Azienda.</p>	<p>RS0803P02 Procedura Contatti con Autorità</p> <p>RS09A01 Information Security Policy – Conservazione Digitale</p>
Aspetti Organizzativi	<p>Descrive le attività di gestione del personale nel ciclo di vita del rapporto lavorativo per garantire che il personale che sarà coinvolto nella erogazione dei Servizi abbia i requisiti (anche di affidabilità) adeguati per gestire le attività, nel rispetto della Sicurezza delle Informazioni. Il personale deve essere reso consapevole delle proprie responsabilità in termini di sicurezza delle informazioni.</p> <p>È necessario evitare che, al momento della fuoriuscita del personale, siano trattenuti indebitamente asset e informazioni aziendali.</p>	PGP09 Gestione Risorse Umane
Security awareness e professionalità del personale	<p>Descrive le modalità con cui viene garantita la formazione e l'awareness sulla Sicurezza delle Informazioni e su specifici aspetti legati alle procedure aziendali, per il personale coinvolto nei Servizi</p>	PGP02 Procedura Gestione Esigenze Formative
Aspetti Organizzativi	<p>Garantisce che vengano presi adeguati provvedimenti nei confronti di chi commette infrazioni alla sicurezza delle informazioni</p>	CCNL Metalmeccanici
Aspetti Organizzativi	<p>Descrizione delle modalità con cui sono assegnati, modificati e rimossi i privilegi di accesso fisico/logico per locali/sistemi/apparati/applicazioni a perimetro.</p>	RS0803P03 Procedura Gestione Privilegi di Accesso
Aspetti Organizzativi	<p>Assunzione di responsabilità per la sicurezza delle informazioni da parte del</p>	RS08D02 Non Disclosure Agreement

	<p>personale esterno coinvolto nella erogazione di Servizi</p> <p>Il personale deve essere reso consapevole delle proprie responsabilità in termini di sicurezza delle informazioni</p>	
Aspetti Organizzativi	<p>Descrive le modalità di accesso a ciascun DC per garantire che l'accesso ai locali indicati (sale macchine/CED) avvenga solo da parte del personale autorizzato sulla base del principio "need to use", nonché il controllo degli accessi fisici alle aree ove si trattano informazioni riservate.</p> <p>Garantisce inoltre che, in occasione di carico-scarico merci, non vi siano intrusioni di personale non autorizzato nei locali del perimetro.</p>	RS08A05 Accessi Fisici a Data Center
Gestione controllata accessi fisici e logici	<p>Politiche di tracciatura e conservazione dei log di accesso fisico e logico alle informazioni a perimetro per consentire l'analisi di dati in occasione di eventi critici (manomissioni, accessi non autorizzati, etc.) su asset/locali del perimetro.</p> <p>Definisce i controlli degli accessi fisici alle aree ove si trattano informazioni riservate.</p> <p>Descrive le modalità in cui sono preservati i dati di accesso fisico/logico da modifica, cancellazione, non tracciatura per superamento capienza sul sistema nativo.</p>	RS08A03 Log Management Policy
Gestione controllata accessi fisici e logici	<p>Definisce le regole di utilizzo della dotazione hw/sw in uso al personale e le regole da seguire per lo scambio di informazioni. Definisce l'utilizzo della modalità di connessione wireless in modo che avvenga in modalità sicura solo da parte delle persone autorizzate e in garanzia della RID</p>	<p>RS08A06 Utilizzo servizi informatici e trasmissione informazioni</p> <p>RGP01 Regolamento Uso Risorse Aziendali</p>
Gestione controllata accessi fisici e logici	<p>Elenco delle tecnologie e gli strumenti autorizzati (e quelli espressamente vietati) dal Management a supporto della erogazione dei Servizi erogati da Engineering D.HUB</p>	RS08A04 Tecnologie e Strumenti Autorizzati
Sicurezza dei	<p>Fornisce le indicazioni per identificare,</p>	RS0805P01 Procedura Incident

sistemi e degli asset	classificare, gestire e risolvere le situazioni direttamente individuabili come incidenti di Information Security oppure che, degenerando o aggravandosi, potrebbero diventare tali.	Management
Impostazione, implementazione e gestione della Sicurezza delle Informazioni	<p>Descrive il processo di Change Management per la gestione dei cambiamenti a servizi o a componenti di servizio. L'obiettivo primario di questo processo è quello di gestire i cambiamenti ai servizi ICT o alle componenti di servizio, in maniera sistematica, organica e controllata con la finalità di ridurre, per quanto possibile, i rischi ed eventuali disservizi correlati all'implementazione del cambiamento. Deve essere garantito un adeguato livello di controllo e autorizzazione in occasione di modifiche a servizi o componenti di servizi, aventi impatto anche sulla sicurezza delle informazioni.</p> <p>Il primo documento citato si applica ai servizi di Outsourcing infrastrutturale erogati da Engineering D.HUB, mentre il secondo si applica alle modifiche apportate alla piattaforma Digidoc, nell'ambito dell'erogazione del servizio di Conservazione dei Documenti Informatici.</p>	<p>RS0807 Processo Change Management</p> <p>RS09P02 Procedura di Manutenzione Correttiva / Evolutiva DigiDoc</p>
Sicurezza dei sistemi e degli asset	Modalità con cui si effettua la valutazione, analisi e gestione dei Rischi pertinenti la Sicurezza delle Informazioni	RS0803P01 Procedura Analisi e Gestione Rischi
Sicurezza dei sistemi e degli asset	Individuazione e analisi delle vulnerabilità tecniche di Information Security	RS0803P04 Procedura Vulnerability Assessment e Penetration Test
Sicurezza dei sistemi e degli asset	Descrive il modello logico dell'infrastruttura IT e dei Servizi ICT erogati da Engineering D.HUB che consenta la gestione controllata e sistematica dei configuration item e delle relazioni tra gli stessi, per tutto il loro ciclo di vita. Lo scopo principale è quello di fornire accurate ed aggiornate informazioni di configurazione agli altri processi implementati, in particolare per la gestione	RS0809P01 Procedura Configuration Management

	<p>degli incidenti, dei problemi e dei cambiamenti.</p> <p>Per memorizzare e gestire adeguatamente tutte le informazioni relative agli elementi della configurazione è stato implementato il repository aziendale Engineering Configuration Management Data Base.</p> <p>È così possibile effettuare il censimento degli asset e assegnare gli ownership</p>	
Sicurezza dei sistemi e degli asset	<p>Il processo garantisce che l'accesso fisico e la movimentazione degli asset infrastrutturali avvengano in garanzia della protezione dell'asset stesso e delle informazioni in esso contenute</p>	RS08PR02 Procedura Asset Disposal e Logistica
Sicurezza dei sistemi e degli asset	<p>Definizione di regole per la gestione dei supporti magnetici/elettronici/cartacei ove risiedono informazioni, compresa la loro distruzione quando non più necessari</p>	RS08PR03 Procedura Gestione dei supporti di memorizzazione
Sicurezza dei sistemi e degli asset	<p>La procedura descrive criteri e modalità attraverso i quali viene erogato, da parte della direzione Operation DTM Nord di D.HUB, il servizio di Software Control & Distribution (SC&D).</p> <p>Il servizio, finalizzato alla distribuzione controllata del sw alle sole Postazioni di Lavoro (PdL), si suddivide nei seguenti sottoservizi:</p> <ol style="list-style-type: none"> 1. Software Distribution 2. Patch Management 3. Image Management 4. Antivirus Management 	RS08PR01 Procedura gestione PDL aziendali
Sicurezza dei sistemi e degli asset	<p>Definisce le modalità di gestione dei sistemi in garanzia della sicurezza delle informazioni</p>	RS08PR11 Procedura Gestione Sistemi
Sicurezza dei sistemi e degli asset	<p>descrive il servizio di gestione reti e connettività</p>	RS08PR07 Procedura Network Management
Sicurezza dei sistemi e degli asset	<p>Lo scopo della gestione degli eventi di monitoraggio è conoscere lo stato delle infrastrutture IT e dei servizi erogati rilevando qualsiasi scostamento dal funzionamento normale o atteso. La</p>	RS08PR02 Procedura Monitoring

	<p>procedura descrivere le attività svolte per gestire gli eventi originati dai tool di monitoraggio dell'infrastruttura IT in tutto il loro ciclo di vita. Le attività descritte hanno l'obiettivo di assicurare che eventuali malfunzionamenti o guastidegli apparati IT (ad esempio server, sistemi storage, apparati di rete, reti, backup) siano analizzati tempestivamente al fine di attivare le appropriate procedure di escalation e ripristino del servizio.</p>	
Sicurezza dei sistemi e degli asset	<p>L'adozione di adeguate misure di sicurezza è un prerequisito imprescindibile per la gestione delle infrastrutture IT e l'erogazione dei servizi ai Clienti. Il Patch Mangement è il processo mediante il quale le patch, incluse quelle di sicurezza, sono collezionate, analizzate, verificate ed implementate nell'ambiente IT. La procedura, che rientra nel più vasto ambito di gestione di sistemi, descrive criteri, regole e modalità di esecuzione delle attività finalizzate alla gestione delle patch sui server, costituenti l'infrastruttura IT attraverso la quale vengono erogati servizi ai Clienti sia interni che esterni. Vengono trattati esclusivamente aspetti tecnici ed operativi; sono esclusi temi inerenti le implicazioni legali, le valutazioni di impatto sul business e le strategie di sicurezza (audit, vulnerabilità assessment,...).</p>	RS08PR04 Procedura Patch Management
Sicurezza dei sistemi e degli asset	<p>La procedura descrive i criteri e le modalità di gestione del "servizio schedulazione dei lavori batch</p>	RS08PR12 Procedura Schedulazione Lavori
Sicurezza dei sistemi e degli asset	<p>Descrive le modalità di gestione della manutenzione impianti presenti nei DC</p>	RS08PR05 Procedura Gestione Impianti di Data Center
Sicurezza dei sistemi e degli asset	<p>Definisce le modalità con cui sono effettuati, conservati e utilizzati i dati di backup relativi a Servizi D.HUB</p>	RS08PR08 Procedura Gestione Backup
Gestione della business continuity	<p>L'obiettivo della procedura è di assicurare che le risorse tecniche e i servizi ICT possano essere ripristinati, a fronte di una interruzione totale del servizio, in tempi</p>	RS0814P01 Procedura Service Continuity

	<p>ritenuti accettabili.</p> <p>La procedura di IT Service Continuity Management riguarda gli aspetti di ripristino del servizio nel caso di eventi che comportano fermi di grande rilevanza. In altre parole, l'obiettivo del processo è garantire la continuità del servizi a fronte di eventi qualificabili come "disastri".</p>	
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Il processo di Capacity Management ha lo scopo di assicurare che esistano le capacità adeguate a soddisfare le esigenze di business attuali e future, in relazione ai servizi che l'Azienda intende erogare nel tempo ai propri Clienti.</p> <p>È necessario garantire un costante monitoraggio dell'utilizzo delle risorse, anche in ottica di pianificazione delle necessità future</p>	<p>RS0811 Processo Capacity Management</p>
<p>Gestione delle terze parti</p>	<p>Descrive la gestione dei fornitori per garantire il rispetto dei requisiti di sicurezza del perimetro nei casi di servizio o porzione di esso affidata a terze parti, gestendo, inoltre, le eventuali modifiche alla fornitura, sempre in garanzia dei requisiti di sicurezza delle informazioni. Rendere le terze parti coinvolte nel perimetro consapevoli dei requisiti dell'org.ne relativamente alla sicurezza delle informazioni</p>	<p>RS02 Processo Gestione Approvvigionamento</p> <p>Condizioni Generali Contratti Acquisizione Prestazioni, art.19</p>
<p>Impostazione, implementazione e gestione della Sicurezza delle Informazioni</p>	<p>Descrive le modalità con cui sono effettuati gli audit interni, anche relativi alla Sicurezza delle Informazioni che devono verificare l'adozione di procedure volte a garantire la gestione controllata delle attività tecniche, in garanzia della sicurezza delle informazioni</p>	<p>MS01P01 Procedura Gestione Audit Interni</p>

[Torna al sommario](#)

9. MONITORAGGIO E CONTROLLI

9.1 Procedure di monitoraggio

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

- Implementazione dei sistemi di monitoraggio e relativo aggiornamento
- Rilevazione degli eventi di allarme
- Tracciamento su Sistema di Ticketing
- Applicazione dell'opportuna procedura di fixing o innesco della Procedura di Escalation Operativa / Informativa
- Follow-up del problema in caso di escalation

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

Il servizio di Monitoraggio viene erogato centralmente dall'Operation Centre (OC): esso opera in modalità H24 ed è presidiato da operatori che tengono sotto controllo lo stato dei sistemi; l'obiettivo è il Monitoring Proattivo per rilevare condizioni di criticità e porvi rimedio prima che l'insorgenza del problema generi un disservizio percepibile all'utente.

La Control Room dove risiedono gli operatori è dotata di appositi wall-screen che permettono di rappresentare visivamente lo stato del monitoraggio dell'infrastruttura tecnologica dei clienti

La procedura nelle operazioni di Monitoring prevede che all'insorgere di un allarme gli operatori, dopo aver verificato che l'evento sia stato tracciato sul sistema di Ticketing (la creazione del Ticket avviene in automatico da parte del sistema di Event Management), verificano sulla "Knowledge Base" la corretta procedura da intraprendere e mettono in atto le azioni previste (esecuzione di procedure di recovery, dispatching ad enti interni o esterni codificati, ecc.).

Nel caso l'anomalia non sia risolta a questo livello, o non esista ancora una procedura codificata, l'operatore che ha in carico il problema ne passa le competenze a una struttura di secondo livello interna all'OC che si preoccupa di effettuare una analisi più approfondita (trouble-shooting).

Questo II° livello interno all'OC opera con un presidio 7.00-19.00 e garantisce la copertura h24 in regime di reperibilità. In caso di risoluzione al II° livello il ticket viene chiuso e dopo aver dato riscontro al Cliente la procedura di recovery utilizzata viene inserita/aggiornata sul sistema di Knowledge Management.

Nel caso in cui il problema non possa ancora essere risolto all'interno dell'OC il ticket viene scalato ai competence center specifici (interni ad Engineering, del Cliente o Fornitori terze parti) secondo la natura del problema e in base alle procedure concordate ed il ticket viene inoltrato al gruppo competente.

Nel caso di dispatching a Competence Center (interni, o esterni) il problema rimarrà comunque in carico all'operatore che, ricevuta la notifica di chiusura da parte della struttura tecnica incaricata, verificherà il ripristino delle condizioni di funzionalità e provvederà alla chiusura del ticket (follow-up).

L'organizzazione dell'Operation Center può essere schematizzata come segue:



Figura 9: Organizzazione dell'Operation Center

Per apparati router di proprietà del carrier è richiesto almeno la disponibilità del monitoraggio con il protocollo SNMP.

Per il monitoraggio degli apparati di rete Engineering D.HUB utilizza la suite dei prodotti di Solarwinds.

In aggiunta alla suite Solarwinds vengono utilizzati opzionalmente altri tools quali il Netflow, utilizzato per analizzare il traffico. Mentre Orion NPM indica la percentuale di utilizzo di un link, tramite il protocollo Netflow è possibile identificare informazioni su protocolli o hosts che stanno utilizzando il link o generando traffico e verso quale destinazione, in modo da avere rapidamente una chiara situazione dell'utilizzo di banda. Queste informazioni possono essere utilizzate per definire e gestire (ove previste) le classi di servizio (Class of Services, CoS) della Quality of Service (QoS) riuscendo così a rendere prioritario il traffico ritenuto business.

[Torna al sommario](#)

9.2 Verifica di integrità degli archivi

Il sistema DigiDoc garantisce la conservazione a lungo termine dei documenti mediante funzionalità che verificano periodicamente l'integrità degli archivi. Le verifiche sono relative a:

- Integrità del documento;
- Validità della firma e della marca temporale del Responsabile del Servizio di conservazione;
- Integrità e consistenza dell'archivio;
- Leggibilità dei documenti conservati.

In fase di caricamento di un documento nell'archivio viene verificata la sua integrità confrontando la sua impronta con quella dichiarata nel SipManifest.xml. Tale verifica viene effettuata periodicamente con cadenza almeno annuale confrontando l'impronta memorizzata con quella calcolata per ogni documento. Viene altresì verificata la validità della firma digitale del responsabile del servizio di conservazione e la marca temporale.

Ogni controllo genera un report in formato xml che può essere consultato da parte del Responsabile del servizio di conservazione per attestare l'attività di verifica e per definire le eventuali azioni correttive.

Per garantire la leggibilità dei documenti, il Responsabile della Conservazione almeno una volta ogni cinque anni, sceglie un campione documentale composto da almeno un documento per ciascuna tipologia di documenti ed effettua la verifica tramite il viewer ad esso associato.

Se dalle verifiche dovessero emergere dei problemi, il Responsabile del servizio di conservazione avvierà le procedure atte a garantire il ripristino dei documenti conservati attraverso il riversamento dei documenti secondo quanto indicato nel paragrafo 7.10.

[Torna al sommario](#)

9.3 Soluzioni adottate in caso di anomalie

Con la finalità di raccogliere dati oggettivi per monitorare le attività di gestione degli impianti e delle infrastrutture dei Data Center, il Responsabile Infrastrutture DC, su base trimestrale, raccoglie, dai diversi DC Site Manager, informazioni relative a:

- Anomalie su impianti/infrastrutture verificatesi nel periodo di riferimento: tali informazioni possono essere veicolate attraverso i moduli RS08D12 Registro Anomalie Impianti DC che ciascun Site Manager compila per il proprio DC di riferimento, con il censimento di quanto accaduto nel periodo, in termini di anomalie da manutenzione ordinaria, straordinaria, prove di continuità; tali informazioni consentono di effettuare analisi di tipo statistico, ad esempio trend delle anomalie ricorrenti, o sulle performance dei fornitori del Servizio di Manutenzione nella gestione degli interventi di risoluzione anomalie.

[Torna al sommario](#)

Manuale di Conservazione DigiBox di Engineering Ingegneria Informatica

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	11/5/2018	Stefano Mannori	Responsabile dello sviluppo e della manutenzione del sistema di conservazione
	11/5/2018	Francesca Pranzo Zaccaria	Responsabile funzione archivistica di conservazione
Verifica	15/5/2018	Andrea Pugi	Responsabile servizio di conservazione
	15/5/2018	Stefano Ciuffi	Responsabile Sicurezza dei sistemi per la conservazione
Approvazione	15/5/2018	Pizzonia Mario Carmelo	Responsabile ECM Competence Center

REGISTRO DELLE VERSIONI

N°Ver/ Rev/	Data emissione	Modifiche apportate	Osservazioni
beta	30/07/2014	Stesura iniziale	Distribuzione interna
v-1	25/09/2014	Seconda Stesura	Distribuzione interna
v-1	5/12/2014	Rilascio documento	Distribuzione interna
v1.1	27/1/2015	Modifiche per integrazione informazioni sicurezza e monitoraggio (manuale AgID ver.2)	
V2	4/3/2015	Integrazione con descrizione struttura PDD nel cap.4	
V4	15/1/2016	Redazione aderente allo schema v.2 pubblicato da AgID	
V5	10/2/2016	Correzioni a seguito di richiesta "accessibilità"	
V6	10/4/2017	Integrazioni per evolutive funzionali rilevanti nel processo di conservazione; aggiornamento contratto Resp. Tratt. Dati personali	
V8	20/6/2017	Versione interna workingprogress per aggiornamento al nuovo SW	Distribuzione interna
V9	2/8/2017	Integrazioni con nuove funzionalità per evoluzione prodotto sw di Conservazione	

V10	15/1/2018	Modifiche per cambio Proprietà Azienda (cambio logo)	
v11	15/5/2018	Modifiche per cambio societario: recepita l'incorporazione di Infogroup in Engineering; modificata organizzazione ed altri dettagli legati alla denominazione Aziendale	Cambio nome del documento

INDICE

	REGISTRO DELLE VERSIONI	2
1	Scopo e Ambito del Documento	6
2	Terminologia (glossario/acronimi)	7
	2.1 Glossario	7
	2.2 Acronimi	13
3	Normativa e Standard di Riferimento	14
	3.1 Normativa di riferimento	14
	3.2 Standard di riferimento	15
4	Ruoli e Responsabilità	16
	4.1 <i>Produttore</i>	16
	4.2 <i>Utente</i>	16
	4.3 <i>Responsabile del Servizio di conservazione</i>	17
	4.4 <i>Il Responsabile della Funzione archivistica</i>	18
	4.5 <i>Responsabile Applicativo</i>	18
	4.6 <i>Responsabile dei Sistemi Informativi</i>	18
	4.7 <i>Responsabile della Sicurezza</i>	19
	4.8 <i>Responsabile del trattamento dati personali</i>	19
5	Struttura Organizzativa	20
	5.1 <i>Organigramma</i>	20
	5.2 <i>Strutture Organizzative</i>	22
	5.2.1 <i>Supporto operativo</i>	22
	5.2.2 <i>Servizio di Supporto Applicativo</i>	23
	5.2.3 <i>Servizio Sistemistico</i>	24
6	Oggetti sottoposti a Conservazione	26
	6.1 <i>Oggetti sottoposti a conservazione</i>	26
	6.2 <i>Formati e metadati</i>	26
	6.3 <i>Pacchetto di Versamento (PdV)</i>	27
	6.4 <i>Pacchetto di Archiviazione</i>	28
	6.4.1 <i>Contenuti dell'indice del PdA (SinCRO)</i>	29
	6.5 <i>Pacchetto di Distribuzione</i>	30
7	Processo di Conservazione	31
	7.1 <i>Descrizione del servizio</i>	31
	7.2 <i>Attivazione e chiusura del Servizio</i>	32

7.3	<i>Controlli sulla ricezione dei PdV</i>	33
7.4	<i>Verifica del Pacchetto di Versamento</i>	33
7.5	<i>Accettazione o Rifiuto del PdV</i>	34
7.6	<i>Rapporto di Versamento (RdV)</i>	35
7.7	<i>Costruzione e conservazione del Pacchetto di Archiviazione</i>	36
7.8	<i>Processo di Esibizione tramite Pacchetto di Distribuzione</i>	38
7.9	<i>Veicolazione dei PdD e Gestione dei supporti rimovibili</i>	38
7.10	<i>Interoperabilità: cessione o acquisizione documenti da altro conservatore</i>	39
7.11	<i>Scarto del pacchetto di Archiviazione</i>	40
7.12	<i>Conservazione documenti Pregressi</i>	40
8	Il Sistema di Conservazione	41
8.1	<i>Applicativo di Conservazione</i>	41
8.2	<i>Componenti Logiche</i>	42
8.3	<i>Componenti Tecnologiche</i>	44
8.4	<i>Componenti Fisiche</i>	45
8.5	<i>Procedure di Gestione e di Evoluzione</i>	48
9	MONITORAGGIO E CONTROLLI	49
9.1	<i>Tracciabilità delle operazioni</i>	49
9.2	<i>Monitoraggio dell'applicazione</i>	49
9.3	<i>Controlli periodici di integrità</i>	50
9.4	<i>Soluzioni adottate in caso di Anomalie</i>	51
9.5	<i>Procedure di Continuità Operativa e Disaster Recovery</i>	51

1 Scopo e Ambito del Documento

Engineering Ingegneria Informatica dispone di due differenti servizi di Conservazione Digitale, uno denominato DigiDoc e l'altro denominato DigiBox (sistema ereditato dall'incorporazione di Infogroup); il presente documento costituisce il manuale di conservazione di DigiBox, (ex-Infogroup) adottato da Engineering Ingegneria Informatica S.p.A., nel seguito indicato come Eng, per il processo di conservazione della documentazione digitale ai sensi della vigente normativa in materia elencata nell'apposito capitolo del presente documento

Il presente manuale ha lo scopo di descrivere:

- il modello organizzativo adottato da Eng per l'erogazione del Servizio, in cui sono evidenziati i ruoli e le responsabilità attribuite ad attori interni o affidate a soggetti esterni;
- i processi di erogazione del servizio, facendo riferimento anche a documentazione operativa esterna per la descrizione di attività di dettaglio;
- le attività di controllo sul processo e sugli archivi in modo da verificare la corretta gestione dei processi di erogazione del servizio;
- l'infrastruttura tecnologica a supporto del servizio;
- le misure di sicurezza logiche e fisiche;

Il documento rappresenta il riferimento principale relativo a qualsiasi aspetto che regola il corretto funzionamento del Servizio.

In particolare, il presente documento, rappresenta la linea guida per la gestione della comunicazione tra Engineering e il Cliente, è verificato dal Responsabile del Servizio di Conservazione ed è approvato dal Responsabile del Competence Center ECM.

Le responsabilità assegnate nell'erogazione del servizio di conservazione vengono riportate nel capitolo specifico di questo manuale.

Si riportano, sempre all'interno del presente documento, i dettagli degli oggetti che vengono conservati, le modalità con cui vengono mantenuti nel tempo, le infrastrutture su cui tali servizi si poggiano ed i sistemi di monitoraggio che controllano l'erogazione.

Eventuali modifiche e aggiornamenti a questo documento potranno essere effettuate dal Responsabile del servizio di Conservazione, previa condivisione con il Responsabile del trattamento dei dati personali, il Responsabile della Sicurezza e con il Responsabile dei Sistemi Informativi.

Qualora si concordi con uno specifico cliente o per uno specifico servizio di conservazione, di operare in modo differente rispetto a quanto riportato nel presente manuale, le particolarità definite saranno riportate in uno specifico allegato, riferito allo specifico contratto o servizio, denominato "specificità contrattuali".

[torna al sommario](#)

2 Terminologia (glossario/acronimi)

In questo paragrafo sono riportate in ordine alfabetico le principali definizioni, termini, e concetti direttamente riferiti o collegati al processo di conservazione a norma

2.1 Glossario

TERMINE	DEFINIZIONE
accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
accreditamento	riconoscimento, da parte dell’Agenzia per l’Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
affidabilità	caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico
aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all’oggetto e alla materia o in relazione alle funzioni dell’ente
archivio	complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell’attività
archivio informatico	archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
area organizzativa omogenea	un insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell’articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445
attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico	dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico
autenticità	caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L’autenticità può essere valutata analizzando l’identità del sottoscrittore e l’integrità del documento informatico
base di dati	collezione di dati registrati e correlati tra loro
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall’ Agenzia per l’Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza

TERMINE	DEFINIZIONE
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
codice eseguibile	insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici
conservatore accreditato	soggetto, pubblico o privato, che svolge attività di conservazione al quale sia stato riconosciuto, dall'Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, dall'Agenzia per l'Italia digitale
conservazione	insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
Coordinatore della Gestione Documentale	responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più Aree Organizzative Omogenee
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
duplicazione dei documenti informatici	produzione di duplicati informatici
esibizione	operazione che consente di visualizzare un documento conservato e di ottenerne copia
estratto per riassunto	documento nel quale si attestano in maniera sintetica ma esaustiva fatti, stati o qualità desunti da dati o documenti in possesso di soggetti pubblici
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica
fascicolo informatico	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
formato	modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file

TERMINE	DEFINIZIONE
funzionalità aggiuntive	le ulteriori componenti del sistema di protocollo informatico necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni
funzionalità interoperative	le componenti del sistema di protocollo informatico finalizzate a rispondere almeno ai requisiti di interconnessione di cui all'articolo 60 del D.P.R. 28 dicembre 2000, n. 445
funzionalità minima	la componente del sistema di protocollo informatico che rispetta i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445
funzione di hash	una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti
generazione automatica di documento informatico	formazione di documenti informatici effettuata direttamente dal sistema informatico al verificarsi di determinate condizioni
identificativo univoco	sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione
immodificabilità	caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso
impronta	la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash
insieme minimo di metadati del documento informatico	complesso dei metadati, la cui struttura è descritta nell'allegato 5 del presente decreto, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta integrità insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato
interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
leggibilità	insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti
log di sistema	registrazione cronologica delle operazioni eseguite su di un sistema informatico per finalità di controllo e verifica degli accessi, oppure di registro e tracciatura dei cambiamenti che le transazioni introducono in una base di dati
manuale di conservazione	strumento che descrive il sistema di conservazione dei documenti informatici ai sensi dell'articolo 9 delle regole tecniche del sistema di conservazione
manuale di gestione	strumento che descrive il sistema di gestione informatica dei documenti di cui all'articolo 5 delle regole tecniche del protocollo informatico ai sensi delle regole tecniche per il protocollo informatico D.P.C.M. 31 ottobre 2000 e successive modificazioni e integrazioni
memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici

TERMINE	DEFINIZIONE
metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del decreto "regole tecniche in materia di Conservazione"
pacchetto di archiviazione	pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione
pacchetto di distribuzione	pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta
pacchetto di versamento	pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione
pacchetto informativo	contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare
piano della sicurezza del sistema di conservazione	documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano della sicurezza del sistema di gestione informatica dei documenti	documento, che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi nell'ambito dell'organizzazione di appartenenza
piano di conservazione	strumento, integrato con il sistema di classificazione per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445
piano generale della sicurezza	documento per la pianificazione delle attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza
presa in carico	accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione
processo di conservazione	insieme delle attività finalizzate alla conservazione dei documenti informatici di cui all'articolo 10 delle regole tecniche del sistema di conservazione
produttore	persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.
rapporto di versamento	documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore

TERMINE	DEFINIZIONE
registrazione informatica	insieme delle informazioni risultanti da transazioni informatiche o dalla presentazione in via telematica di dati attraverso moduli o formulari resi disponibili in vario modo all'utente
registro particolare	registro informatico di particolari tipologie di atti o documenti; nell'ambito della pubblica amministrazione è previsto ai sensi dell'articolo 53, comma 5 del D.P.R. 28 dicembre 2000, n. 445
registro di protocollo	registro informatico di atti e documenti in ingresso e in uscita che permette la registrazione e l'identificazione univoca del documento informatico all'atto della sua immissione cronologica nel sistema di gestione informatica dei documenti
repertorio informatico	registro informatico che raccoglie i dati registrati direttamente dalle procedure informatiche con cui si formano altri atti e documenti o indici di atti e documenti secondo un criterio che garantisce l'identificazione univoca del dato all'atto della sua immissione cronologica
responsabile della gestione documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi	dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
responsabile della conservazione	soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 delle regole tecniche del sistema di conservazione
responsabile del trattamento dei dati	la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali
responsabile della sicurezza	soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza
riferimento temporale	informazione contenente la data e l'ora con riferimento al Tempo Universale Coordinato (UTC), della cui apposizione è responsabile il soggetto che forma il documento
scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
sistema di classificazione	strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata
sistema di conservazione	sistema di conservazione dei documenti informatici di cui all'articolo 44 del Codice
sistema di gestione informatica dei documenti	nell'ambito della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico
staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione

TERMINE	DEFINIZIONE
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, integrità e persistenza delle modifiche della base di dati
integrità e persistenza delle modifiche della base di dati	Testo unico decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni
ufficio utente	riferito ad un area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico
utente	persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse
versamento agli archivi di stato	operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali

[torna al sommario](#)

2.2 Acronimi

AgID	Agenzia per l'Italia Digitale
ASP	Application Service Providing
CA	Certification Authority (indica l'Autorità di certificazione di un dispositivo di firma digitale)
CAD	Codice Amministrazione Digitale
CAGE	Spazio Tecnico presente all'interno di un DC ad uso esclusivo dell'affittuario.
CD	Compact Disk
DL	Decreto Legge
D.Lgs	Decreto Legislativo
DM	Decreto ministeriale
DMEF	Decreto del Ministero dell'Economia e delle Finanze
DMS	Document Management System
DPCM	Decreto Presidente del Consiglio dei Ministri
DPR	Decreto Presidente della Repubblica
DVD	Digital Versatile Disk
FTP	File Transfer Protocol
GC	Gestore della Conservazione
GU	Gazzetta Ufficiale
HTTP	Hyper Text Transfer Protocol (identificativo convenzionale per un sito)
HTTPS	Secure Hyper Text Transmission Protocol. Protocollo sviluppato allo scopo di cifrare e decifrare le pagine Web che vengono inviate dal server ai client.
IPDA	Indice del Pacchetto di Archiviazione
HW	Hardware
L	Legge
NTP	Network Time Protocol
PdA	Pacchetto di Archiviazione
PdD	Pacchetto di Distribuzione
PDF	Portable Document Format
PdV	Pacchetto di Versamento
PEC	posta elettronica certificata
PKI	Public Key Infrastructure (infrastruttura necessaria per creare, gestire, conservare e revocare i certificati delle firme elettroniche basati su crittografia a chiave pubblica)
RDC	Responsabile della Conservazione
RdV	Rapporto di Versamento
SLA	Service Level Agreement
SSL	Secure Socket Layer. Protocollo che consente, grazie a tecniche di crittografia, il trasferimento di dati tramite la rete Internet in modo sicuro.
STORAGE	Infrastruttura tecnologica composta da più Dischi Ottici ad alta capacità di immagazzinamento dati.
SW	Software
TSA	Time Stamping Authority
TU	Testo Unico
URL	Uniform Resource Locator (indica la modalità per individuare univocamente un sito Internet)
UTC	Universal Time Coordinated (Misura del tempo così come stabilito dall'International Radio Consultative Committee – CCIR)

[torna al sommario](#)

3 Normativa e Standard di Riferimento

3.1 Normativa di riferimento

La Conservazione a Norma di documenti informatici (e delle loro impronte), avviene attraverso la memorizzazione in supporti idonei e si completa con l'apposizione del riferimento temporale (marca temporale) e della firma digitale da parte del Responsabile del servizio di Conservazione (o del RdC se espressamente richiesto dal Cliente) che ne attesta il corretto svolgimento del processo.

Il documento conservato deve essere reso leggibile, in qualunque momento, presso il sistema di Conservazione ed esibito per via telematica.

Il servizio di Conservazione a norma recepisce le seguenti normative di riferimento:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

[torna al sommario](#)

3.2 Standard di riferimento

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

[torna al sommario](#)

4 Ruoli e Responsabilità

Il Servizio di Conservazione a Norma Digibox, che Eng eroga ai propri clienti, prevede la seguente struttura Organizzativa:

- Produttore;
- Utente;
- Responsabile del Servizio di Conservazione;
- Responsabile dell'erogazione del Servizio;
- Responsabile Applicativo;
- Responsabile dei Sistemi Informativi;
- Responsabile della Sicurezza;
- Responsabile della Privacy;

[torna al sommario](#)

4.1 Produttore

E' il responsabile della creazione del pacchetto di versamento e del suo invio verso il sistema di Conservazione. Verifica l'esito della presa in carico da parte del Servizio di conservazione tramite opportuni sistemi di rendicontazione (on line o batch) che il sistema restituisce al mittente, ed eventualmente con il controllo del Rapporto di Versamento (RdV).

[torna al sommario](#)

4.2 Utente

Persona, ente o sistema in grado di richiedere al Sistema di Conservazione a Norma l'esibizione del pacchetto di distribuzione ovvero fruire delle informazioni di interesse.

I ruoli **interni all'organizzazione per l'erogazione del servizio** sono stati così assegnati:

PROFILO	Nominativo	Periodo nel Ruolo	Contratto
Responsabile del Servizio di Conservazione	Andrea Pugi	2009	Tempo indeterminato
Responsabile della funzione archivistica di conservazione	Francesca Pranzo Zaccaria	2010	Tempo indeterminato
Responsabile della sicurezza dei sistemi per la conservazione	Stefano Ciuffi	2008	Tempo indeterminato
Responsabile del trattamento dei dati personali	Cosimo Nigro	2018	Tempo Indeterminato

PROFILO	Nominativo	Periodo nel Ruolo	Contratto
Responsabile dei sistemi informativi per la conservazione	Enzo Cati	2011	Tempo indeterminato
Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Resp. Applicativo)	Stefano Mannori	2009	Tempo indeterminato

I 6 profili richiesti per l'accreditamento dall'Agenzia sono stati mappati su figure professionali i cui compiti sono dettagliati nei paragrafi seguenti.

[torna al sommario](#)

4.3 Responsabile del Servizio di conservazione

Opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi oltre che con il responsabile della gestione documentale e:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;
- se richiesto dal cliente genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013 (nuove regole tecniche in materia di sistema di conservazione);
- predispone il manuale di conservazione di cui all'art. 8 del DPCM 3 dicembre 2013 (nuove regole tecniche in materia di sistema di conservazione) e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Avvalendosi della struttura organizzativa specifica (descritta nei paragrafi seguenti) assicura che tutte le componenti erogate dal servizio vengano evase secondo gli SLA concordati e i requirement specifici dei documenti mandati in conservazione.

All'interno di supporto applicativo è stato incarico un referente per le seguenti funzioni operative:

1. gestisce il processo di conservazione

2. genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
3. effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

[torna al sommario](#)

4.4 Il Responsabile della Funzione archivistica

Definisce, in accordo con l'ente produttore, le modalità di trasferimento dei documenti informatici verso il sistema di conservazione.

Si occupa di stabilire:

- Modalità di acquisizione
- Modalità di aggregazione (se necessari)
- Set di metadati associati ai flussi documentali

Svolge le attività specifica per assicurare la:

- definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferite, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato;
- definizione del set di metadati di conservazione dei documenti e dei fascicoli informatici;
- monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione;
- collaborazione con l'ente produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

[torna al sommario](#)

4.5 Responsabile Applicativo

E' la persona di riferimento la quale assicura che tutte le nuove richieste di evoluzione funzionale e/o di integrazione con altre applicazioni vengano ricevute, valutate e applicate al sistema di conservazione secondo i tempi e i requisiti concordati con il cliente e in accordo con le indicazioni del Responsabile del Servizio di Conservazione. Ha in carico la manutenzione dell'applicazione a supporto del servizio di Conservazione a Norma.

E' colui che adegua il servizio alle evoluzioni richieste dai clienti e imposte dai cambiamenti normativi adottando le soluzioni appositamente predisposte sul sistema di conservazione. Inoltre è responsabile della pronta segnalazione al Responsabile del Servizio di Conservazione degli incidenti con livello di gravità massimo.

[torna al sommario](#)

4.6 Responsabile dei Sistemi Informativi

E' la persona che gestisce l'esercizio delle componenti hardware e software del sistema di conservazione, garantendone l'adeguatezza nel tempo. Si occupa del monitoraggio dei livelli

di servizio dell'infrastruttura e segnala eventuali difformità degli SLA al Responsabile del Servizio, pianificando eventuali azioni correttive.

[torna al sommario](#)

4.7 Responsabile della Sicurezza

E' la persona che stabilisce e mantiene le policy di sicurezza relative al sistema di conservazione, le condivide con il Responsabile del Servizio di Conservazione e ne verifica l'applicazione nel tempo. Individua eventuali difformità, le comunica al Responsabile del servizio e pianifica le azioni correttive individuate.

[torna al sommario](#)

4.8 Responsabile del trattamento dati personali

Garantisce il rispetto della normativa vigente in materia del trattamento dei dati personali e del rispetto delle istruzioni impartite dal Titolare del trattamento.

[torna al sommario](#)

5 Struttura Organizzativa

5.1 Organigramma

Si riporta di seguito l'organigramma di Engineering Ingegneria Informatica S.p.A.

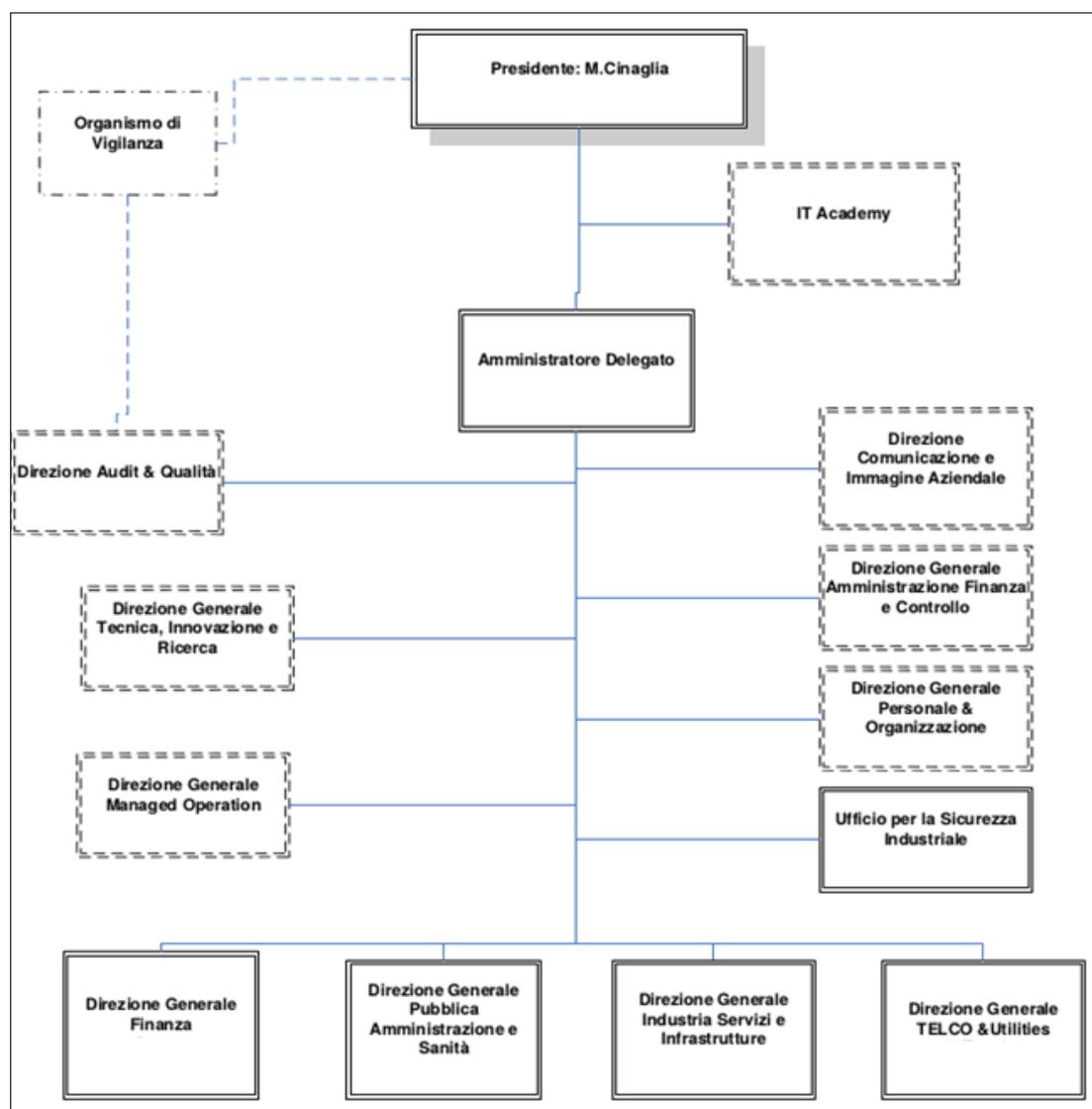


Figura 1 – Organigramma Engineering Ingegneria Informatica

Nella figura che segue sono riportate le strutture organizzative di Engineering Ingegneria Informatica S.p.A. coinvolte nel processo di conservazione

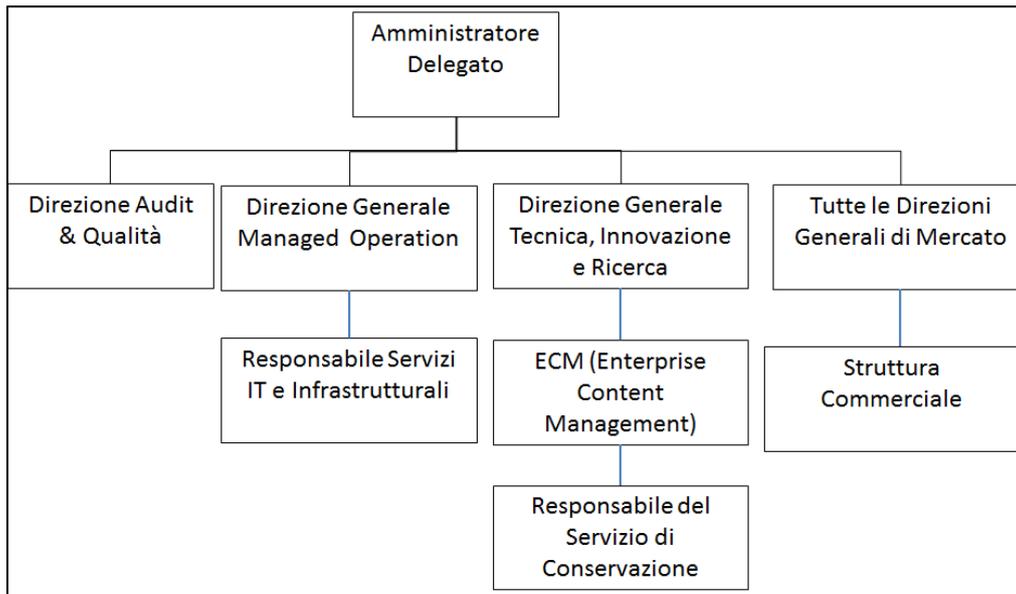


Figura 2 – strutture coinvolte nell'erogazione del servizio

Per l'erogazione del servizio di Conservazione a norma sono state definite specifiche figure interne all'organizzazione dell'Azienda in grado di garantire la corretta erogazione e adeguati supporti nei confronti del Produttore e dell'Utente.

Queste figure sono coordinate dal Responsabile di Erogazione del Servizio.



Figura 3 – Organizzazione specifica del servizio

[torna al sommario](#)

5.2 Strutture Organizzative

5.2.1 Supporto operativo

Il Supporto operativo rappresenta il principale punto di contatto Single Point of Contact relativo alle segnalazioni provenienti dai clienti (Produttore e Utente) e strutture interne che possono accedere al servizio di Supporto operativo attraverso l'invio di una e-mail all'indirizzo Servizio_CN@Eng.it .

Il Supporto operativo, prende in carico la segnalazione tracciando opportunamente la richiesta nel Sistema di Trouble Ticketing Eng, catalogando la segnalazione per tipologia e livello di gravità.

Sotto vengono riportate le tipologie selezionabili e i livelli di gravità gestiti:

Tipologie di Segnalazione:

- Incident;
- Change Request;
- Service Request.

Per la tipologia Incident vengono riportati sotto i livelli di Gravità, in ordine decrescente:

- Livello 4;
- Livello 3;
- Livello 2;
- Livello 1.

I livelli di Gravità sono definiti in base all'impatto dell'incidente:

Descrizione	criticità	Caratteristiche per la classificazione
Incidente	4	Evento che provoca (o può provocare) una interruzione di attività, un guasto, una perdita o una riduzione del servizio. L'evento è gestito.
Malfunzionamento	3	Evento che compromette l'asset ma in modo discontinuo
Incidente non bloccante	2	Evento dannoso che non ha impatti significativi rispetto al sistema di produzione, che continua, quindi a funzionare correttamente e completamente
Anomalia	1	Evento sporadico che non compromette gli asset e l'operatività dei processi.

Sulla base dei contenuti della segnalazione, il Supporto operativo prende in carico la richiesta ed esegue quanto necessario per chiuderla autonomamente oppure la indirizza verso il livello specialistico competente per la sua risoluzione:

- Supporto Applicativo;
- Supporto Sistemistico.

In ogni caso è il Supporto operativo che comunica all'entità interessata la chiusura del ticket.

Le tipologie di **Change Request** scalabili al Supporto operativo sono:

- richiesta configurazione nuovi Clienti;
- richiesta configurazione nuove famiglie documentali;
- richiesta creazione nuovi report di servizio;
- modifica configurazione Clienti/famiglie documentali esistenti;

- modifica alla reportistica già esistente.

Le tipologie di **Service Request** scalabili al Supporto operativo sono:

- chiarimenti funzionali relativi all'utilizzo dell'interfaccia Web del sistema di conservazione;
- verifiche relative alla configurazione del servizio;
- richiesta produzione supporti.

Inoltre nel caso in cui il sistema di Conservazione a Norma rilevi situazioni anomale dovute alla presenza di dati errati forniti dal Produttore (metadati non coerenti, problemi sui flussi, sequenze di numerazione non rispettate, ecc.), il Supporto operativo prende in carico l'anomalia, e può contattare il Produttore tramite i canali e le modalità concordate per la notifica e per eventuali azioni da intraprendere per la chiusura del ticket.

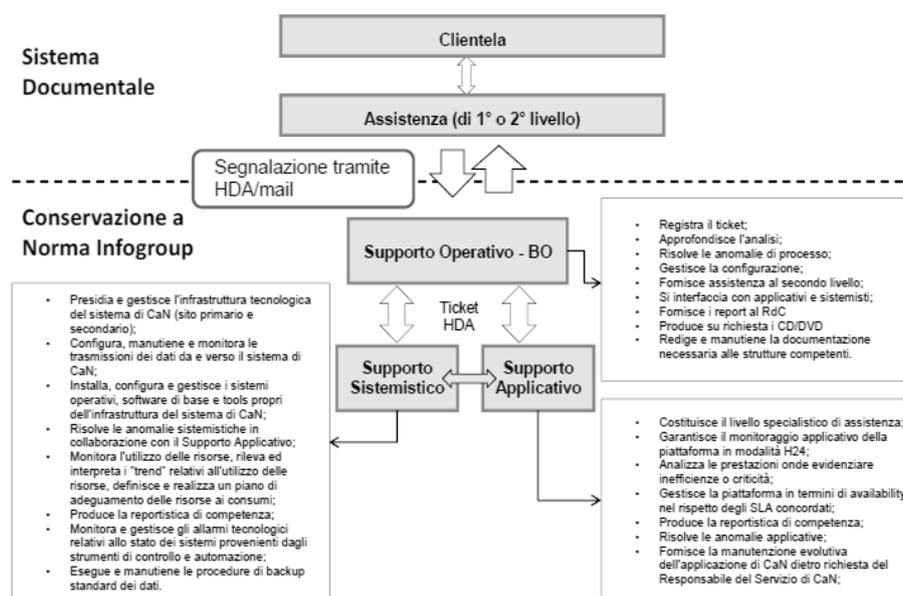


Figura 4 - workflow di lavorazione delle segnalazioni

[torna al sommario](#)

5.2.2 Servizio di Supporto Applicativo

Il servizio è gestito dal Responsabile Applicativo e ha lo scopo di assicurare il corretto funzionamento dell'applicativo di Conservazione a Norma e opera di concerto con il Supporto Operativo per la gestione delle eventuali segnalazioni di malfunzionamento.

Il servizio di Supporto Applicativo, dietro indicazione del Responsabile del Servizio di Conservazione, mantiene aggiornata l'applicazione secondo le esigenze dei Clienti e secondo le evoluzioni della normativa vigente che regola la Conservazione a Norma.

Il Supporto Applicativo ha i seguenti compiti:

- monitoraggio applicativo in modalità H24;
- supporto specialistico di Assistenza Applicativa;
- produzione della reportistica di competenza;
- Presa in carico delle Change Request provenienti dal Supporto Operativo;
- gestione delle Service Request provenienti dal Supporto Operativo.

Le principali tipologie di segnalazione gestite dal Supporto Applicativo sono:

- segnalazioni di malfunzionamenti generati dalla piattaforma di Conservazione;
- segnalazioni di malfunzionamenti dovuti ad un'errata formattazione dei PdV/documenti ricevuti del Produttore;
- Problematiche relative ad aspetti funzionali sul processo che alimenta la piattaforma di Conservazione a Norma.

[torna al sommario](#)

5.2.3 Servizio Sistemistico

Il servizio è gestito dal Responsabile dei Sistemi Informativi e ha lo scopo di assicurare il corretto funzionamento dell'infrastruttura tecnologica del servizio di Conservazione a Norma e opera di concerto con il Supporto Operativo e il Supporto Applicativo per la gestione delle eventuali segnalazioni di malfunzionamento.

Di seguito sono elencate in sintesi le principali attività svolte dal Servizio Sistemistico:

- Presidia e gestisce l'infrastruttura tecnologica del sistema di Conservazione a Norma (sito primario e secondario);
- Configura, manutene e monitora le trasmissioni dei dati da e verso il sistema di Conservazione a Norma;
- Installa, configura e gestisce i sistemi operativi, software di base e tools propri dell'infrastruttura del sistema di Conservazione a Norma;
- Risolve le anomalie sistemistiche in collaborazione con il Supporto Applicativo;
- Monitora l'utilizzo delle risorse, rileva ed interpreta i "trend" relativi all'utilizzo delle risorse, definisce e realizza un piano di adeguamento delle risorse ai consumi;
- Produce la reportistica di competenza;
- Monitora e gestisce gli allarmi tecnologici relativi allo stato dei sistemi provenienti dagli strumenti di controllo e automazione;
- Esegue e manutene le procedure di backup standard dei dati.

Per maggiori dettagli delle attività svolte si rimanda all'allegato specifico (descrizione infrastruttura)

Matrice	Responsabile del Servizio di Conservazione	Responsabile della funzione archivistica di conservazione	Responsabile della sicurezza dei sistemi per la conservazione	Responsabile del trattamento dei dati personali	Responsabile dei sistemi informativi per la conservazione	Responsabile dello sviluppo e della manutenzione del sistema di conservazione (Resp. Applicativo)
attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	R	C	C	I		A
acquisizione, verifica e gestione dei pacchetti di versamento presi in carico e generazione del rapporto di versamento	R	A			C	
preparazione e gestione del pacchetto di archiviazione	R	C				A
preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	R	C		I	C	A
scarto dei pacchetti di archiviazione		R		I	C	A
chiusura del servizio di conservazione (al termine di un contratto)	R	I		I	C	C
conduzione e manutenzione del sistema di conservazione				C	C	R
monitoraggio del sistema di conservazione	I	I			R	A
change management				C	C	R
verifica periodica di conformità a normativa e standard di riferimento	R	C				

- **R**: Responsabile
- **A**: Agisce
- **C**: Collabora
- **I**: Informato

[torna al sommario](#)

6 Oggetti sottoposti a Conservazione

6.1 Oggetti sottoposti a conservazione

Sono oggetti del sistema di conservazione:

- a) i **documenti informatici** e i **documenti amministrativi informatici** prodotti dal Cliente e acquisiti da Eng, con i metadati ad essi associati di cui all'allegato 5 delle Regole Tecniche;
- b) i **fascicoli informatici** ovvero le aggregazioni documentali informatiche con i metadati ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.

Segue un esempio di tabella dei formati gestiti. **Tabella aggiornata.**

visualizzatore	Produttore	formato del file	versione del formato	sistema operativo
Acrobat	ISP – sportello	Pdf, p7m	1.4 (Acrobat 5)	WinXP/7/8
Acrobat	ISP – Contratti	Pdf, p7m	Vari formati	WinXP/7/8
Acrobat	ISP – Easy Fattura	Xml, Pdf, p7m, tsd	Vari formati	WinXP/7/8
Acrobat	ISP – Terzo valore	Pdf, p7m	Vari formati	WinXP/7/8
Acrobat	ISP – Applicazione Data certa	Pdf, tsr	Vari formati	WinXP/7/8
Immagini	ISP – Applicazione Data certa	Tiff, tsr	Vari formati	WinXP/7/8

Integrazioni alla presente tabella possono essere presenti nell'allegato "specificità del contratto".

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi come descritto nel presente documento e conformemente all'art. 4 delle Regole Tecniche:

- Pacchetti di Versamento
- Pacchetti di Archiviazione
- Pacchetti di Distribuzione

[torna al sommario](#)

6.2 Formati e metadati

Le tipologie documentali afferenti agli oggetti descritti nel precedente paragrafo sono individuate dal Responsabile del servizio di Conservazione d'intesa con il la funzione archivistica ed applicativa, in fase di attivazione del servizio e conformemente a quanto stipulato in sede contrattuale, tenendo conto delle:

- a) peculiarità delle classi documentali;
- b) dei formati dei file accettabili in conservazione.

Ai sensi della normativa vigente sono conservati solo i formati di file idonei ad essere correttamente conservati, individuati dall'allegato 2 alle Regole Tecniche, a cui integralmente si rinvia, rispettando i requisiti ivi previsti di "standard aperti", in modo da garantire a chiunque in futuro la possibilità tecnica di avere accesso ai dati conservati, corredati da una struttura di dati per la memorizzazione nel sistema di conservazione in grado di assicurare l'interoperabilità tra sistemi.

Tutti i documenti versati sul sistema di conservazione Eng sono contraddistinti da un set di metadati obbligatori per il sistema, che li identificano univocamente, e che sono descritti nel capitolo relativo al PdV.

[torna al sommario](#)

6.3 Pacchetto di Versamento (PdV)

Il servizio di Conservazione riceve i documenti inviati dal Produttore attraverso canali di comunicazione sicuri concordati col Cliente in sede di attivazione del servizio.

I documenti da sottoporre a conservazione devono essere predisposti secondo quanto previsto contrattualmente per quanto attiene la presenza della firma digitale, dei metadati e la correttezza del formato.

I documenti contenuti nel PdV confluiscono, nelle modalità di seguito descritte, in uno o più PDA.

Il prodotto offre una completa personalizzazione riguardo alla configurazione dei metadati ed alla loro obbligatorietà, consentendo totale piena libertà rispetto alla scelta di quali includere, e di conseguenza la piena adesione allo standard Dublin Core Metadata ISO 15836:2009.

A livello di documento è possibile definire un set di metadati minimi che il documento deve possedere per poter essere versato nel sistema di conservazione (il set di metadati minimi è condiviso con il Cliente/produttore e viene dettagliato nel documento Specificità di Contratto)

Di default il set di metadati minimo è il seguente:

- Id documento
- Soggetto produttore (codifica definita con il cliente; es. nome, cognome, piva, cod fiscale,....)
- Data documento
- Tipo documento/oggetto

A livello di PdV si sono definiti dei parametri (collocati nella testata del flusso) che identificano univocamente il produttore del PdV stesso.

A livello di documento si sono definiti i seguenti metadati (es. di uno specifico servizio):

Nome metadato	Note
CHIAVE/NUMERO	Obbligatorio. Questo dato deve essere sempre presente all'interno
ANNO	Concorre a formare l'univocità della chiave
REGISTRO	Concorre a formare l'univocità della chiave

Non tutti i seguenti sono obbligatori:

Nome metadato	Note
COD_SOC	Indica la società o ente produttore
COD_UO	Unità Organizzativa
COD_SPORTELLO	Sportello operante (dettaglio applicazione/sezione della UO)
WORKSTATION	ID della workstation dell'operatore
OPERATORE	Matricola dell'operatore (del produttore)
COD_RAPPORTO	Rapporto del Cliente (per documento Clientela)
NDG	NDG del Cliente
NOME	Nome del Cliente
COGNOME	Cognome del Cliente
IMPORTO	Importo dell'operazione
COD_ADESIONE	Specifico per Fascicolo
FG_ANNULLO	flag
EMAIL_CLIENTE	e-mail del Cliente
TRANSAZIONE	Tipo di transazione (es. BONIF)
DATA_CONTABILE	Se operazioni contabile
DATA_CREAZIONE	Obbligatoria
DATA_FIRMA	Se documento firmato
VERSIONE	Dettaglio del viewer/applicativo generatore

Le strutture dati di colloquio tra Cliente e Conservatore sono dettagliate nell'allegato Specificità del Contratto e concordate con il cliente.

[torna al sommario](#)

6.4 Pacchetto di Archiviazione

Il PdA contiene un numero variabile di documenti ed un indice.

L'indice del PDA è un file in formato XML che riporta, per ognuno dei file inclusi nel blocco, alcune informazioni tra cui un "urn" (unified resource name) e un "hash".

L'urn è una stringa univoca che identifica l'oggetto digitale, mentre l'hash è un'impronta del documento, ovvero una sequenza di bit che può essere ricavata dal file in modo ripetibile e standardizzato e che garantisce una corrispondenza esatta col contenuto originale.

La modalità di conservazione mediante indice permette di **verificare l'integrità** di ogni singolo file, a prescindere da tutti gli altri file conservati nello stesso blocco. Infatti sarà sufficiente essere in possesso di un file "candidato" e conoscere il suo urn identificativo per poter eseguire la funzione di hash e confrontare l'impronta ricalcolata con la stringa riportata nell'indice.

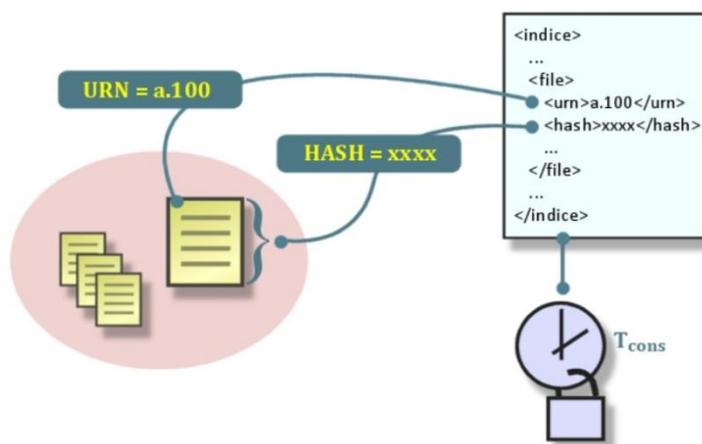


Figura 5 struttura dell'indice del PdA

Il Pacchetto di Archiviazione viene composto a partire da uno o più PDV ed è un'entità logica nella quale sono contenuti uno o più documenti, in base a criteri che possono essere definiti con il Produttore/Committente o Responsabile della Conservazione.

[torna al sommario](#)

6.4.1 Contenuti dell'indice del PdA (SinCRO)

La soluzione Digibox adottata da Eng è compliant con lo standard UNI 11386 [UNI 11386:2010 - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali (SinCRO)].

All'interno della sottocommissione DIAM/SC11 (Gestione dei documenti archivistici) dell'Ente nazionale italiano di unificazione (UNI), un apposito gruppo di lavoro denominato SInCRO, ha definito la struttura dell'insieme dei dati a supporto del processo di conservazione individuando gli elementi informativi necessari alla creazione di un Indice di Conservazione.

L'implementazione di tale indice, del quale SInCRO ha descritto sia la semantica sia l'articolazione, permette di utilizzare una struttura-dati condivisa e raggiungere un soddisfacente grado d'interoperabilità nei processi di migrazione, mediante l'adozione di uno Schema XML appositamente elaborato. Di seguito lo schema SinCRO implementato.

In aggiunta a quanto previsto dalla normativa, il software prevede alcuni metadati aggiuntivi (non obbligatori) sfruttando il tag MoreInfo.

A livello generale:

- CRL al momento dell'avvenuto versamento
- CRL al momento della chiusura del RdV relativo al documento specifico (come specificato al par. "Costruzione e conservazione del Pacchetto di Archiviazione")
- Certificati-Trusted: vengono inseriti i nomi dei certificati Trusted relativi alle firme presenti nei documenti contenuti nel PdA

A livello di singolo file:

- Informazioni sulle verifiche di firma effettuate (Forza Accettazione / Forza Conservazione)

- Nome e cognome del firmatario (se le verifiche sono attivate e la firma è presente)
- Esiti di verifica firma. Informazioni sulla validità della firma, verifica crittografica, controllo certificato stato della revoca, con riferimento alle CRL reperite nella sezione “Generale”, sopra menzionata

Si allega un Indice di esempio:



SInCRO-2472_ITOD
24721510906201131

Si descrive nel capitolo successivo il processo di generazione e la struttura definitiva del PDA .

[torna al sommario](#)

6.5 Pacchetto di Distribuzione

Il sistema permette all’utente la ricerca e la visualizzazione degli oggetti conservati.

La visualizzazione avviene tramite un sistema di autenticazione e autorizzazione anche da remoto. L’oggetto che il sistema genera per la consultazione è il Pacchetto di Distribuzione che viene confezionato dal Servizio di Conservazione secondo quanto previsto dalla normativa vigente.

L’accesso ai documenti avviene tramite una serie di servizi webservice esposti dall’applicazione (in modalità sicura) che restituiscono:

- il documento conservato all’interno dell’archivio a norma;
- le prove di conservazione (idPdA);

in particolare il pacchetto di distribuzione relativo ad uno o più documenti è composto da:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marca temporale)
- RdV del (o dei) PdV relativi ai documenti presenti nel PdD
- dati e metadati (collocati su file XML)
- documento o documenti richiesti

Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PDD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti dal Responsabile del Servizio di Conservazione.

[torna al sommario](#)

7 Processo di Conservazione

7.1 Descrizione del servizio

Nel seguito una breve descrizione delle caratteristiche principali del servizio di Conservazione a Norma erogato da Eng:

- **Conservazione a Norma dei documenti:** memorizzazione dei documenti informatici inviati dal Cliente su un supporto di cui sia garantita l'integrità e la leggibilità nel tempo secondo le prescrizioni stabilite dalla normativa vigente in materia, con le modalità, nei tempi e limiti definiti contrattualmente. Il servizio comprende la verifica periodica dell'integrità dei documenti, l'eventuale riversamento diretto e le attività necessarie per le ottemperanze fiscali, ove richiesto.
- **Consultazione dei documenti conservati a Norma:** ricerca e visualizzazione dei documenti inviati in conservazione. Tale servizio ed il relativo software di visualizzazione è garantito per il tempo definito contrattualmente per la conservazione a Norma dei documenti.
- **Produzione di supporti dei documenti conservati a Norma:** il servizio consiste nella generazione e invio di supporti fisici a Norma contenenti i Pacchetti di Distribuzione, a seguito di una specifica richiesta del Cliente.
- **Riversamento dei documenti,** su richiesta esplicita del Cliente, secondo quanto stabilito contrattualmente e definito successivamente.

Eng eroga il servizio di Conservazione a Norma (Digibox) utilizzando infrastrutture tecnologiche che soddisfano i requisiti di alta affidabilità richiesti dalla normativa. Il servizio è erogato su due siti per garantirne la continuità:

Primario: Settimo Torinese (TO) presso il Data Center sito in
Viale della Costituzione, 3 – 10036 Settimo Torinese (TO)

Secondario: Firenze presso il Data Center sito in
Via della Toscana, 31 – 50127 Firenze (FI)

Si descrive di seguito il processo di Conservazione. Il processo è in linea con quanto richiesto dalla normativa:

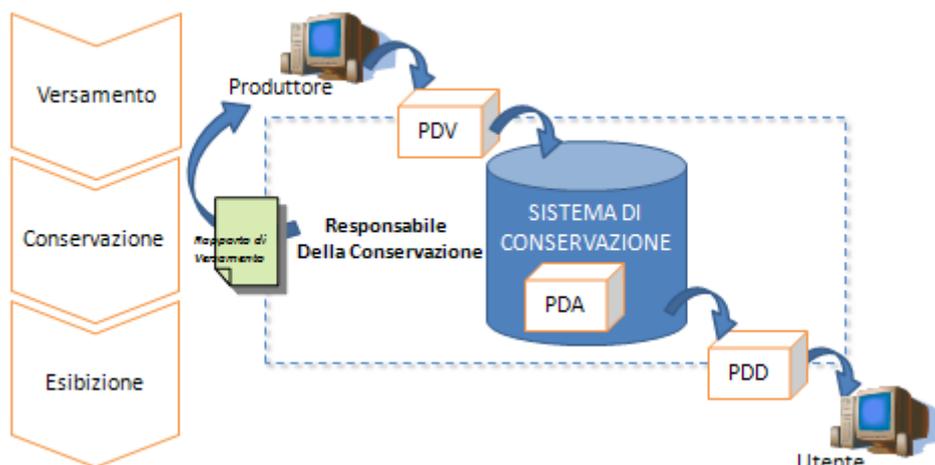


Figura 6 - Processo di Conservazione

[torna al sommario](#)

7.2 Attivazione e chiusura del Servizio

Il servizio di Conservazione dei documenti Informatici per ogni Cliente/Famiglia Documentale viene attivato al termine di un processo di configurazione che segue questi fasi fondamentali:

- a) condivisione informazioni tecniche di richiesta configurazione PDV: questa fase comprende la definizione di dettaglio dei PDV che il produttore (o Cliente) andrà a produrre ed i controlli che verranno attivati sul sistema di conservazione.
- b) consolidamento delle informazioni tecniche propedeutiche all'attivazione del servizio (famiglia documentale, metadati);
- c) validazione delle configurazioni da parte del Responsabile del Servizio di Conservazione e del Responsabile sicurezza del Servizio di Conservazione;
- d) configurazione ambiente di test;
- e) ricezione ed elaborazione Pacchetti di Versamento da conservare in ambiente di Test;
- f) configurazione ambiente di produzione e start-up del servizio;
- g) canali di comunicazione per la ricezione dei Pacchetti di Versamento e ricezione reportistica periodica.

Ognuna delle fasi sopra indicate viene eseguita per ogni tipologia di configurazione e tipologia documentale richiesta.

Nella fase di attivazione del servizio vengono definiti canali utilizzati per lo scambio informativo tra Produttore e Conservatore. Tali canali avranno caratteristiche di sicurezza ed identificazione del mittente:

- SFTP
- https
- Certificato lato Client
- Etc etc

Il canale utilizzato e relativi livelli di servizio andranno definiti nell'allegato Specificità del Contratto

Il processo di **cessazione** del servizio di Conservazione per ogni Cliente/Famiglia Documentale segue queste fasi principali:

- a) condivisione informazioni tecniche di richiesta cessazione;
- b) consolidamento delle informazioni tecniche propedeutiche alla cessazione del servizio, definizione della data formale di Cessazione;
- c) notifica della chiusura e delle sue modalità al Responsabile del Servizio di Conservazione;
- d) cessazione tecnica;
- e) attivazione di un piano di riversamento su richiesta del cliente.

Le modalità di riversamento previste, sono riportate a chiusura del presente capitolo del Manuale.

[torna al sommario](#)

7.3 Controlli sulla ricezione dei PdV

La corretta ricezione dei PdV, proveniente dal Produttore/Cliente, è monitorata dal Servizio Sistemistico tramite presidio del canale di comunicazione concordato.

In caso di anomalie il Supporto Operativo prende in carico la segnalazione proveniente dal Servizio Sistemistico, identificando la soluzione ed eventualmente contattando i riferimenti tecnici del cliente.

[torna al sommario](#)

7.4 Verifica del Pacchetto di Versamento

Il processo di conservazione dei documenti prevede il mantenimento nel tempo di un insieme di evidenze informatiche (documenti e metadati) contenute nel pacchetto di versamento oltre a quelle generate dal sistema di conservazione (prove di conservazione).

Queste evidenze comprovano l'integrità dei dati e l'autenticità dei documenti firmati digitalmente dal Produttore.

All'atto della ricezione dei documenti contenuti all'interno del PdV, il sistema esegue le seguenti operazioni :

- Controlli pregiudiziali:
 - o Verifica presenza dei metadati minimi e di quelli concordati
 - o Verifica della correttezza dell'impronta hash del documento ricevuto
 - o Verifica che il formato dichiarato dal Produttore sia corrispondente a quanto concordato
 - o Verifica della firma digitale su ogni documento.
- Altri controlli:
 - o specifici relativi alla tipologia di documento da inviare in conservazione.
 - o possibilità di definire ulteriori controlli che sono concordati con il Cliente in sede contrattuale e definiti nella fase di attivazione del servizio.

Nel caso che uno di questi controlli abbia un esito negativo si genera un'eccezione che può essere gestita come:

- warning: si segnala che c'è una difformità rispetto a quanto atteso ma il processo prosegue nella conservazione.
- error: l'esito ha generato uno blocco del processo per lo specifico pacchetto/documento e necessità di un intervento da parte del Supporto Operativo (p.e. il controllo dell'hash è bloccante).

Eseguiti i controlli pregiudiziali ha inizio la fase di versamento.

Le operazioni di versamento, come tutte le operazioni di rilievo normativo, vengono tracciate in specifici log applicativi, su tabelle del database ovvero su file system, a seconda della tipologia delle informazioni ivi contenute.

I log memorizzati su database vengono mantenuti online per tutta la durata del periodo di conservazione, mentre quelli su file system vengono opportunamente suddivisi per mese / anno per una maggior facilità di consultazione (come descritto nel piano di sicurezza).

Esempio di log delle operazioni riguardanti le interazioni con l'esterno (con documenti esito negativo per doppia chiave primaria):

ID	Data	Operazione	User	Ruolo	ID oggetto	Cliente	Chiave logica	Esito
713308	13/07/2017 22:16	CENSIMENTO	usr_vers	Versatore	450451	Cliente 1	CONS201707120151000	OK
768392	13/07/2017 23:11	VERSAMENTO	usr_vers	Versatore	238737049	Cliente 2	3960620170712CAMVA111145330	OK
1107672	30/06/2017 17:18	RECUPERO	usr_recupero	Versatore				KO
1107660	30/06/2017 11:46	RECUPERO	usr_recupero	Recuperatore	231196691	Cliente 3	15_2016_File79	OK

[torna al sommario](#)

7.5 Accettazione o Rifiuto del PdV

Qualora i controlli precedentemente descritti sui documenti ricevuti abbiano dato **esito positivo**, il sistema:

- memorizza i documenti nella propria base dati di lavoro e sono disponibili per essere inseriti in un PdA.
- predispone i dati per produzione degli esiti di avvenuta presa in carico del PDV e dei singoli documento (Rapporto di Versamento).
- procede alla costruzione del PdA conformemente alle regole specifiche per la tipologia di documento e Cliente.

Nel caso in cui venga rilevato un **esito negativo** di uno dei controlli sui documenti ricevuti, il sistema può procedere un tre differenti modalità:

1. Accettazione parziale del PdV: se "esito negativo" ha gravità "ERRORE" si rifiuta il documento e si segnala nel RdV l'impossibilità di conservare il documento e se ne tiene traccia nel RdV.
2. Accettazione dell'intero PdV: se "esito negativo" ha gravità "WARNING" si accetta l'intero contenuto del PdV e si tiene traccia del warning nei log Applicativi.

3. Rifiuto del PdV: se tutti i records contenuti nel PdV generano errore, oppure il PdV non risulta elaborabile (p.e. problemi di integrità) si rifiuta l'intero PdV e si genera un esito di ricezione con stato KO.

Nel terzo caso il mittente/cliente concorda con il Responsabile del Servizio di Conservazione una modalità per sanare l'errore. Le verifiche e controlli eseguiti vengono tracciati nel log applicativi che per loro natura conservano un riferimento temporale.

[torna al sommario](#)

7.6 Rapporto di Versamento (RdV)

E' un file XML generato in modo automatico alla chiusura della fase di controllo ed è relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC) e l'impronta relativa al PdV (o ai PdV) oltre alle chiavi univoche dei documenti eventualmente rifiutati.

Su tale XML si appone firma e marca temporale che avviene contestualmente alla sua creazione ed attesta il contenuto del PdV e l'istante in cui vengono terminate le attività di verifica.

Esempio di rapporto di versamento

```
<RDV id="351">
  <DataGenerazione>06072017</DataGenerazione>
  <PacchettiDiVersamento>
    <PDV>
      <NomePacchetto>CONS201706222xxxx.zip</NomePacchetto>
      <DataVersamento>06072017</DataVersamento>
      <Canale>FLUSSO</Canale>
      <DocumentiVersati>887</DocumentiVersati>
      <ElementiPDV>
        <ElementoPDV id="8276158" tipo="IDX_STD">
          <URN>AziendaCliente:Paperless:2500:448530:INDICE.xml</URN>
          <Hash algoritmo="SHA-256" codifica="B64">kS09eBJW5HMuYzqJCLQbVO/v5PMBfUW/yYcVA2s61dl=</Hash>
          <Path>
            S3://000001/2500/001/PDV/CONS201706222500000-INDICE.xml
          </Path>
        </ElementoPDV>
        <ElementoPDV id="8276160" tipo="IDX_CLI">
          <URN>
            AziendaCliente:Paperless:2500:448530:INDICE-CLIENTE.xml
          </URN>
          <Hash algoritmo="SHA-256" codifica="B64">RwglkIZ3FItYAyhxyCQBIAwji0nEnlBfa2oykX29Pbkg=</Hash>
          <Path>
            S3://000001/2500/001/PDV/CONS201706222500000-INDICE-CLIENTE.xml
          </Path>
        </ElementoPDV>
      </ElementiPDV>
      <Motivazione/>
    </PDV>
  </PacchettiDiVersamento>
</RDV>
```

Il Rapporto di Versamento viene conservato, memorizzato su DB e legato ai documenti che sono oggetto dei PDV a cui si riferisce. Sarà possibile risalire al RdV dal singolo documento ricercato.

Il sistema provvede ad un primo reperimento delle CRL di tutti i certificati TRUSTED corrispondenti ai certificati di firma al momento dei controlli che vengono eseguiti sul

pacchetto di versamento. Avremo quindi tante CRL quanti sono le autorità di certificazione riconducibili alle firme presenti sui documenti.

Le seconde CRL vengono invece reperite per consolidare la fase di costruzione del Rapporto di Versamento con l'assoluta certezza della validità dei certificati delle firme dei documenti ricevuti.

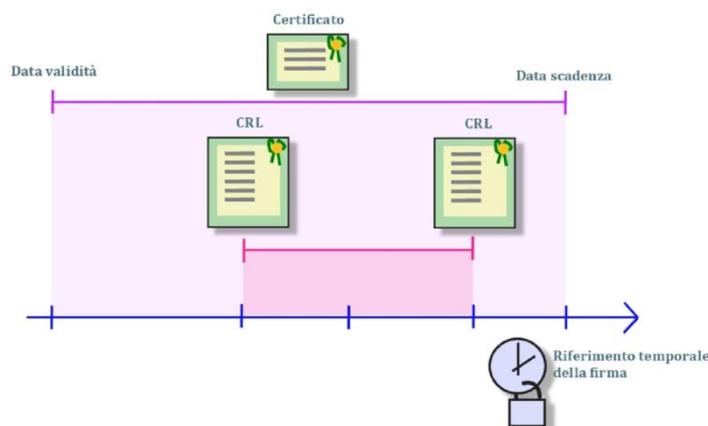


Figura 7 - Controllo CRL

[torna al sommario](#)

7.7 Costruzione e conservazione del Pacchetto di Archiviazione

Superate le fasi di controllo sui PDV e generazione del RdV il sistema abilita l'esecuzione di una serie di regole che permettono la formazione del PDA; tali regole sono completamente configurabili e riguardano ad esempio:

- Dimensione del semilavorato (che formerà il pacchetto)
- Anzianità del documento (dal tempo di ingresso nel sistema)
- Firmato o non firmato (o certificato di firma in scadenza)
- Regole basate su specifici metadati (codice fiscale, mittente,... altro)
- PdA coincidenti con un PdV ricevuto

Opportuni allarmi segnalano la presenza di documenti che sono in attesa di conservazione e non vengono inclusi in nessuna regola di costruzione PdA.

Definendo, eventualmente nuove regole di costruzione del PdA viene attivato un nuovo processo di costruzione del PDA, per eventuali documenti che precedentemente non sono stati inclusi in nessun range di regole, L'inserimento di nuove regole è tracciato nei file di log del sistema.

I documenti così lavorati e che hanno superato le fasi precedenti, concorrono a formare il Pacchetto di Archiviazione, che è assemblato dal sistema nei tempi e con i criteri di raggruppamento scelti e concordati in fase di attivazione del servizio di conservazione.

Il Pacchetto di Archiviazione si forma contestualmente alla creazione del suo indice; il processo è descritto nei punti seguenti:

- a) Creazione di dell'indice xml (in formato Sincro) relativo al blocco di documenti da inviare in conservazione.
- b) Reperimento delle prove di conservazione (certificati trusted delle firme dei documenti, CRL dei certificati scaricate per costruzione RdV) per la totalità dei documenti firmati presenti nel Pacchetto, che verranno inserite nel “more info” dell'indice.
- c) Sottoscrizione dell'indice xml (in formato Sincro) con firma digitale del Responsabile del servizio di Conservazione e successiva apposizione di una marca temporale per fornire data certa al Pacchetto di Archiviazione.

Al termine di queste fasi è formato il PdA che è costituito da un insieme di file comprovanti la autenticità dei documenti in conservazione (vedi schema riportato nel paragrafo specifico).

L'indice del PDA è strutturato secondo lo standard e contiene:

- Info varie previste dallo standard Sincro
- Per ogni documento:
 - o Hash
 - o Urn
 - o Nel campo “more info”: le CRL relative al documento e l'esito dei controlli effettuati.
 - o Riferimento al RdV

La conservazione dei documenti digitali vera e propria ha inizio con la formazione del PdA e la costruzione dell'indice.

Una volta terminata la raccolta delle prove, queste vengono associate ai documenti conservati. A questo punto il sistema provvede a creare l'indice Sincro, sottoscriverlo ed apporre il timestamp definitivo di conservazione

Parte integrante di questo processo è la sottoscrizione digitale dell'Indice (Sincro) da parte del Responsabile del servizio di Conservazione. In questa fase è inclusa anche l'apposizione di un “time-stamp”, ovvero un riferimento temporale certificato che costituisce evidenza dell'esistenza e dell'esatta composizione del file collegato all'istante indicato.

Apponendo un time stamp all'indice lo si “sigilla” e contemporaneamente si fissa il riferimento temporale.

Con questo procedimento, dunque, si viene a costituire un riferimento temporale certificato per ognuno dei file inclusi nel PdA.

In conclusione di tale processo abbiamo il PDA così costituito:

- idPdA.xml.p7m (firmato dal RdC)
- idPdA.xml.tsr (marca temporale)
- dati e metadati
- documento o documenti di cui l'indice idPdA

[torna al sommario](#)

7.8 Processo di Esibizione tramite Pacchetto di Distribuzione

L'esibizione dei documenti avviene tramite autenticazione.

L'utente può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge. Tali informazioni vengono fornite ai soggetti autorizzati tramite l'accesso diretto, anche da remoto, al documento informatico conservato, attraverso la produzione di un pacchetto di distribuzione selettivo tramite specifica ricerca nel sistema di Conservazione a Norma.

Per quanto riguarda 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 è consentito dal servizio webservice esposto dall'applicazione e sottoposto ad autenticazione ed autorizzazione. Il Cliente, autenticato ed autorizzato, tramite l'interfaccia messa a disposizione, può pertanto richiedere la visualizzazione di tutti i documenti conservati al fine di :

- Visionare e scaricare il documento conservato all'interno dell'archivio a norma;
- Verificare ed eventualmente scaricare le prove di conservazione (idPdA);

Il sistema di Conservazione a Norma può essere anche integrato con il sistema Documentale o altra applicazione del cliente per facilitare la fruizione del servizio di consultazione.

Se il Cliente lo richiede può essere effettuata una ricerca massiva con produzione di specifico PDD veicolato al cliente o sotto forma di supporto o tramite canali precedentemente definiti.

Il Pacchetto di distribuzione relativo ad un PdA risulta quindi composto da:

- idPdA.xml.p7m (formato dal RdC)
- idPdA.xml.tsr (marca temporale)
- dati e metadati (collocati su file di testo)
- documento o documenti di cui l'indice idPdA (in sequenza)
- RdV (relativo ai documenti contenuti nel PdA)

Il sistema di conservazione documentale è soggetto a meccanismi di protezione dei dati che transitano in rete, in modo da impedire accessi fraudolenti o non autorizzati. Tale protezione è realizzata mediante apparati di sicurezza che analizzano il traffico e su base di specifiche regole di abilitazione viene consentito il flusso di dati strettamente necessario al funzionamento dell'applicazione.

[torna al sommario](#)

7.9 Veicolazione dei PdD e Gestione dei supporti rimovibili

Il servizio di conservazione è organizzato per conservare i blocchi o PDA completi su repository informatici on-line disponibili nel centro dati di Eng. L'applicazione Digibox consente la produzione di PDD che possono essere forniti al Cliente tramite opportuni canali sicuri.

Può essere anche definita una modalità sicura di scambio di supporti rimovibili a partire da uno o più PDD e le modalità vengono concordate con il cliente e riportate negli allegati contrattuali; il supporto viene generato su richiesta del cliente e sotto la supervisione del Responsabile del servizio di Conservazione.

Se necessario, può essere applicato un meccanismo di crittografia per mettere in sicurezza la delivery del supporto removibile.

In ogni supporto vengono riversati dei pacchetti di distribuzione (PdD), uno per ogni PDA e contenenti sia gli oggetti che l'insieme delle evidenze di conservazione.

[torna al sommario](#)

7.10 Interoperabilità: cessione o acquisizione documenti da altro conservatore

Per interoperabilità si intende la capacità di cedere o acquisire copie o duplicati dei documenti conservati, da un supporto ad un altro senza che ciò comporti una alterazione del contenuto digitale dei medesimi e del valore degli stessi.

Tale procedimento verrà eseguito sotto la responsabilità del responsabile del servizio e verrà concordato con il Responsabile della Conservazione (del Cliente) dei documenti oggetto di "travaso".

Viene eseguita normalmente su richiesta del Cliente e si effettua mediante generazione dell'ISO oppure altro metodo da definire con il Cliente (ed eventualmente con l'altro Conservatore).

Se nel processo di acquisizione risultasse necessario una "trasformazione" dei documenti o dei PdA forniti, sarà necessario effettuare una copia dei documenti conservati da un supporto ad un altro con una alterazione del contenuto digitale dei medesimi. Questa è una attività ammessa dalla normativa, nel caso in cui si voglia ad esempio aggiornare tecnologicamente l'archivio sostitutivo per garantire la possibilità di esibizione della documentazione a fronte di innovazioni tecnologiche. In questo caso potrebbe essere necessaria l'apposizione di una ulteriore firma digitale, o l'attestazione di conformità all'archivio esistente da parte di Pubblico Ufficiale che viene coinvolto dal Responsabile della Conservazione (del Cliente) o del Servizio di Conservazione.

Il coinvolgimento di un Pubblico Ufficiale esperto in processi di conservazione può essere richiesto al fine di:

- a) validare il piano di acquisizione o cessione
- b) verificare che il processo di trasformazione del formato dei documenti non alteri il contenuto e la forma dei documenti stessi;
- c) validare il processo di apposizione delle firme digitali sui documenti acquisiti in conformità con le normative vigenti;

Per procedere all'acquisizione di documenti che risiedono presso altro conservatore, tramite un "travaso massivo" sia di copie che di duplicati informatici sarà necessario definire una mappatura dei dati o metadati forniti dal conservatore cedente ed acquisiti dal nuovo conservatore.

La procedura di import prevede:

- la costruzione di nuovi PdA a partire dai PdD forniti dal cedente
- il popolamento della base dati dei metadati a partire dal db export dati del cedente.

La procedura prevede una fase di quadratura pre e post migrazione, sotto la supervisione del Responsabile del servizio.

[torna al sommario](#)

7.11 Scarto del pacchetto di Archiviazione

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

Per dare la possibilità di poter prolungare i termini di conservazione prima dello scarto, verrà data informativa al produttore con congruo anticipo (almeno 6 mesi) al fine di confermare la cancellazione ovvero mantenere in conservazione i PdA per un ulteriore anno.

Il Responsabile delle Conservazione del produttore ha la possibilità di richiedere lo scarto di tutti o alcuni i PdA segnalati dal sistema, tramite approvazione con propria firma digitale.

La cancellazione avverrà soltanto dopo che sono state eseguite le fasi di approvazione esplicita da parte del RdC.

[torna al sommario](#)

7.12 Conservazione documenti Progressi

Il sistema permette la gestione di archivi di documenti conservati secondo la normativa precedente al DPCM del 3 Dicembre 2013.

In questo caso sarà possibile eseguire su tutti questi documenti le analoghe funzioni sopra descritte con l'eccezione del fatto che l'indice del PdA (indice del blocco) non avrà un formato Sincro ma conterrà comunque le evidenze di conservazione previste dalla normativa pre 2013.

[torna al sommario](#)

8 Il Sistema di Conservazione

8.1 Applicativo di Conservazione

Il sistema software utilizzato per la gestione del processo di conservazione legale dei documenti digitali è costituito da un prodotto SW (Digibox) di Eng, interamente (ed internamente) realizzato e mantenuto.

E' un sistema integrato e completo per la conservazione a norma dei documenti informatici ed è realizzato per "lavorare" su un sistema di storage ad oggetti, una tecnologia appositamente introdotta per questa tipologia di servizio.

Il pacchetto software esegue la conservazione nel tempo dei documenti informatici e presenta le seguenti caratteristiche generali:

- Completezza - presenza di qualsiasi documento emesso
- Robustezza - garanzia di consistenza dei dati inseriti
- Sicurezza - protezione dalla manipolazione non autorizzata dei dati
- Affidabilità - indipendenza dai guasti dell'hardware
- Chiarezza - facilità di consultazione secondo diversi criteri di ricerca

garantendo:

- la completezza e l'inalterabilità dei documenti inviati in conservazione
- la possibilità di verifica dell'integrità dei documenti conservati
- i riferimenti temporali certi.

Inoltre è in grado di gestire diverse tipologie di documenti, relativi a diversi ambiti applicativi, e diversi formati, per esempio:

- Documenti di sportello bancario
- Contratti ed allegati
- Fatture attive e Fatture passive
- Libri e registri sociali
- Libri e registri contabili
- Libri e registri assicurativi
- Assegni
- Mandati di pagamento e Reversali d'incasso
- Ricevute e quietanze di pagamento
- Delibere, determine, atti e provvedimenti
- Altro..

Ognuna di queste tipologie è caratterizzata da specifici metadati e apposite regole, definibili in modo parametrico, che consentono di gestire insieme di documenti omogenei.

Il sistema è progettato per partizionare in maniera opportuna i dati gestiti al fine di garantire la separazione per contesto organizzativo o utente.

Il partizionamento opera tra i dati di Aziende diverse o di diversi dipartimenti o uffici afferenti ad una stessa Azienda I fascicoli e documenti, provenienti anche da flussi diversi di conservazione, identificati univocamente tramite una chiave primaria, fin dal loro ingresso in conservazione.

Il sistema di partizionamento è direttamente collegato al sistema di controllo degli accessi e tracciatura, viene quindi garantita la riservatezza dei dati presenti in archivio.

Tutti i documenti sono disponibili on-line, congiuntamente alle rispettive prove di conservazione, per le funzioni di ricerca ed esibizione, così come previsto dalla normativa vigente. La struttura architettonica del prodotto consente di definire diversi livelli operativi e garantisce che ciascuna Azienda/Ente, Area Organizzativa, Agenzia, Ufficio, Dipartimento, ecc. possa accedere solo ed esclusivamente ai suoi documenti, in base alle credenziali e alle politiche di accesso attivate.

Il pacchetto software prevede la conservazione singola e/o cumulativa, dei documenti elettronici firmati ed implementa un formato di composizione delle marche tale da permettere l'esibizione probatoria di un singolo documento.

Ogni singolo file può essere esibito insieme ai suoi metadati, registrati nel data base, e alle sue prove di conservazione in maniera assolutamente INDIPENDENTE dagli altri documenti. Infatti, nei file contenenti le prove di conservazione l'unico riferimento ai file originali è l'hash del documento stesso, che non ha quindi nessun vincolo di riservatezza.

[torna al sommario](#)

8.2 Componenti Logiche

L'applicazione è logicamente divisibile in 3 principali gruppi:

- Versamento
- Conservazione
- Verifiche e allarmi
- Esibizione
- Console di Gestione

Versamento

La parte di versamento è in grado di ricevere i documenti tramite 2 principali modalità :

- Versamento massivo tramite flussi di documenti
- Versamento singolo, tramite Webservice

Si occupa di effettuare le verifiche iniziali e la creazione del RdV (verifica del formato, firma etc) e di recupero da internet delle CRL.

Conservazione

E' la parte che si occupa di tutti i processi di conservazione, in particolare

- Verifica dei documenti ai fini della conservazione: ricalcolo e confronto hash, verifiche di firma, etc.
- Reperimento e verifica delle prove di conservazione: controllo catena trusted, CRL, etc.
- Creazione PdA
- Firma del RdC
- Apposizione marche temporali

Verifiche e allarmi

Tramite questa componente si rende possibile l'assoluta coerenza del sistema e di tutti i suoi processi. Un sistema di allarmi provvede infatti ad informare tempestivamente il personale

addetto al presidio dell'eventuale presenza di un problema, o più semplicemente di un ritardo nelle fasi elaborative. Gli allarmi sono configurabili in base a diversi parametri e per ciascuna fase elaborativa. Gli allarmi arrivano per e-mail e contengono:

- Nel Subject: una breve descrizione del problema e della sua gravità
- Nel body: possono contenere il dettaglio del problema rilevato

Alcuni esempi di allarmi

- Presenza di documenti non conservati ad una certa ora. Questo allarme scatta nel caso in cui, ad una certa ora, almeno un documento non abbia raggiunto lo stato di "conservato". Nel subject della mail è presente una sintesi del problema (ad esempio: presenza di 2 documenti non conservati). Nel body della mail troviamo l'elenco di tutti i documenti, per un veloce riscontro
- Documenti di un determinato Cliente non pervenuti. Ad esempio, nel caso in cui un Cliente spedisca i suoi documenti sempre ad una determinata ora oppure entro un cut-off, questo allarme è utile ad individuare un eventuale problema nella spedizione dei documenti e induce il personale di presidio a verificare eventuali problemi di connettività o di file transfer

Esibizione

La parte di esibizione di occupa di garantire il reperimento dei documenti conservati e delle prove della loro conservazione nel tempo. L'esibizione può essere richiesta in 3 diverse modalità:

- WebService; tipicamente tramite un applicativo, che fa richiesta del documento e/o delle sue prove di conservazione
- Interfaccia WEB. L'utente può direttamente ricercare e scaricare file e prove di conservazione
- Supporti. Su richiesta del Cliente, è possibile la creazione di supporti digitali contenenti una selezione di documenti con le relative prove di conservazione

Console di Gestione

La console di gestione è l'applicativo web che consente di supervisionare tutte le funzionalità dell'applicazione ed è suddivisa in due grandi filoni

- Gestione applicativo
- Interrogazione contenuti

Gestione applicativo

La gestione dell'applicativo consente la configurazione e la gestione dei task, ovvero:

- Censimento e manutenzione delle tipologie documentali, metadati etc.
- Configurazione utenti, Clienti e loro abilitazioni e personalizzazioni
- Configurazione parametri generali dell'applicazione
- Gestione dei task, monitoraggio del sistema, stop / start dei servizi e dei singoli task

Interrogazione contenuti

La parte di interrogazione contenuti consente una piena navigabilità, con parametri di ricerca predefiniti e rende possibile la ricerca di documenti e files conservati, l'interrogazione ed il download dei documenti e delle loro prove di conservazione.

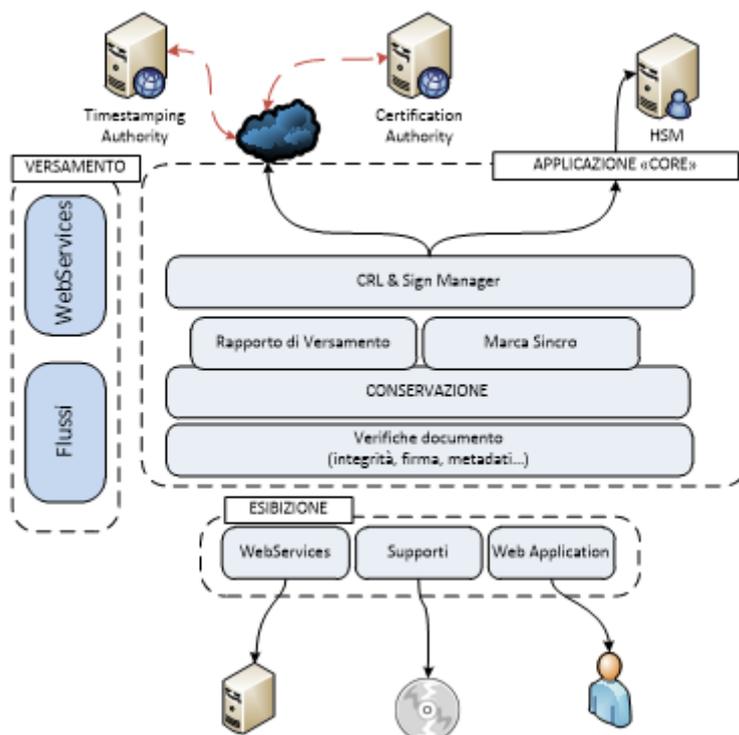


Figura 8: schema logico applicazione

[torna al sommario](#)

8.3 Componenti Tecnologiche

L'applicazione di conservazione è una applicazione Web a tre livelli (desktop, application e database) e utilizzabile da posti di lavoro dotati di sistema operativo Windows (XP, Vista o 7) o Linux, per mezzo di browser standard quali ad esempio Internet Explorer vers. 7 o superiore, Mozilla Firefox 3.6 o superiore, Google Chrome 11.0.696.7 o superiore, Apple Safari 5.0.5 o superiore. Per le postazioni che dovranno operare sulle funzionalità di firma è necessario che localmente siano attivi i driver del dispositivo di firma (lettore, smart card o token USB di firma, tablet per la firma grafometrica, ecc.), oppure che sia utilizzato un dispositivo HSM (Hardware Security Module) raggiungibile via rete.

Tutte le componenti applicative del sistema poggiano su una piattaforma architeturale uniforme:

- Java J2EE
- Framework ORM Hibernate
- Architettura SOA
- RDBMS

- Application server Wildfly 10+
- HCP (Hitachi Content Platform)

La base dati utilizzato è un data base relazionale interfacciato attraverso Hibernate e supporta Oracle RAC 11g Enterprise Edition.

Il bilanciamento applicativo è effettuato tramite Message Queue JMS (Active MQ).

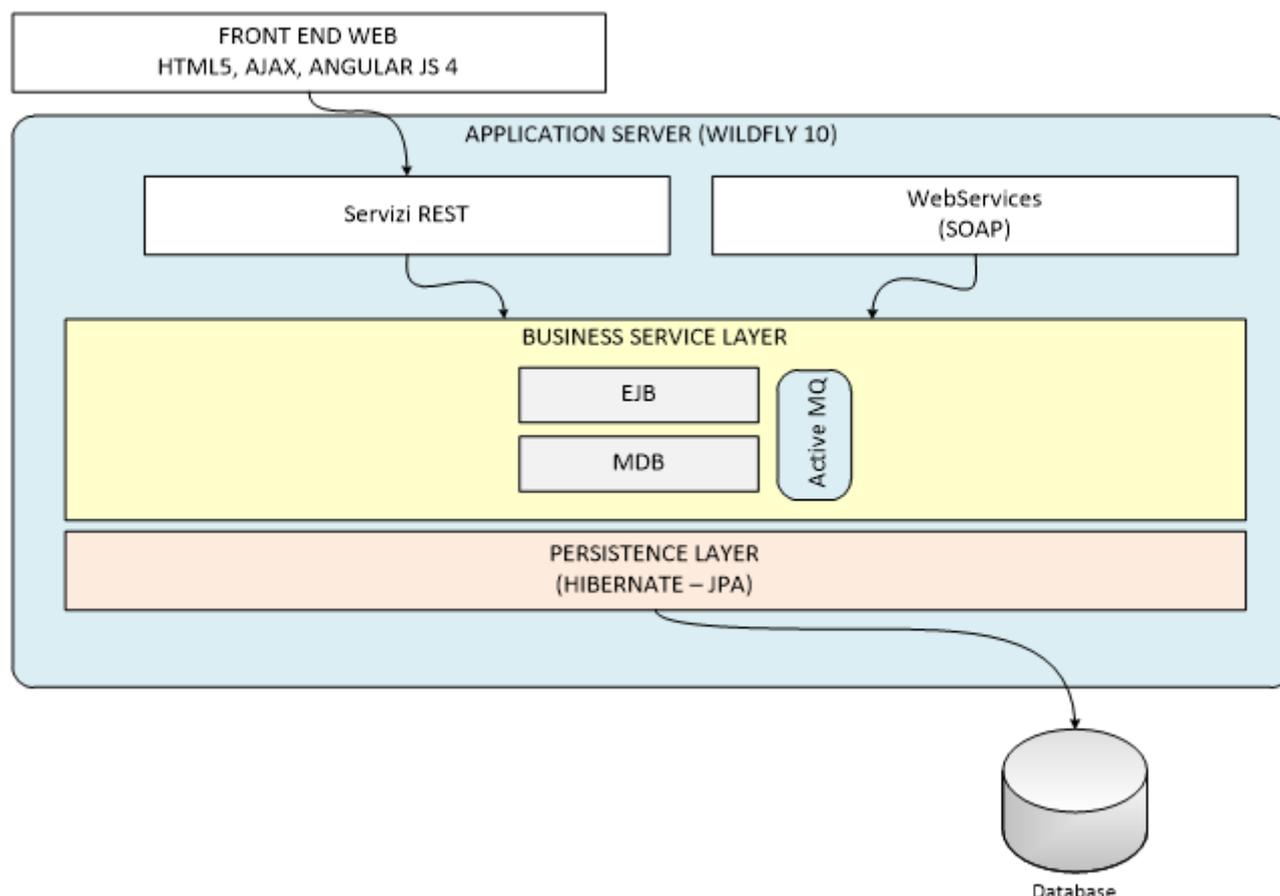


Figura 9: framework applicativo

[torna al sommario](#)

8.4 Componenti Fisiche

Eng eroga i servizi all'interno dei propri Data Center primario e secondario, attraverso i quali è in grado di offrire un servizio di alta qualità in termini di continuità ed affidabilità. Tale qualità è ottenuta grazie alle caratteristiche progettuali che hanno contraddistinto la realizzazione dei Data Center, con criteri focalizzati sempre sull'obiettivo di fornire ad ogni livello le massime garanzie di sicurezza e continuità, sia per quanto riguarda l'erogazione di energia elettrica, sia attraverso un opportuno condizionamento climatico, sia attraverso un adeguato meccanismo di sicurezza fisica (impianto antincendio e sorveglianza con allarmi 24x7), sia attraverso la ridondanza architettonica dei sistemi, delle infrastrutture di rete e delle connessioni verso l'esterno.

I criteri progettuali e realizzativi dei Datacenter Eng rispondono ai requisiti imposti ai datacenter di livello T4, livello massimo previsto dallo standard Uptime Institute Tier Standard.

Di seguito si riportano le principali caratteristiche dei Data Center Eng:

- Ambiente protetto con accesso garantito solo al personale autorizzato;
- Linee elettriche doppie provenienti da rami diversi (doppia cabina elettrica, doppio G.E., doppi UPS);
- Sistema di raffreddamento ridondato;
- UPS ridondati e monitorati;
- Sistema per la rilevazione fumi e lo spegnimento incendi automatico;
- Pavimento flottante e canalizzazioni separate per l'impianto elettrico e cablaggio dati;

Le principali caratteristiche delle architetture deputate alla erogazione dei servizi sono riportate, invece, qui sotto:

- Architettura di switching layer 3 completamente ridondata con connessioni a 1Gbit/s o superiori;
- Sistemi Firewall ridondati, in diverse tecnologie;
- Storage Area Network centralizzata e ridondata con doppio fabric;
- Storage di classe Enterprise;
- Sistemi di RDBMS ridondati (principali fornitori di mercato);
- Backup Centralizzato attraverso LAN dedicata ad 1Gbit/s e via SAN;
- Sistema di Monitoring dello stato della rete, dei sistemi e dei servizi;
- Connessioni ad Internet tramite linee di differenti Carrier;
- Completa remotizzazione dei sistemi di amministrazione.

CONSERVAZIONE Ambiente di produzione

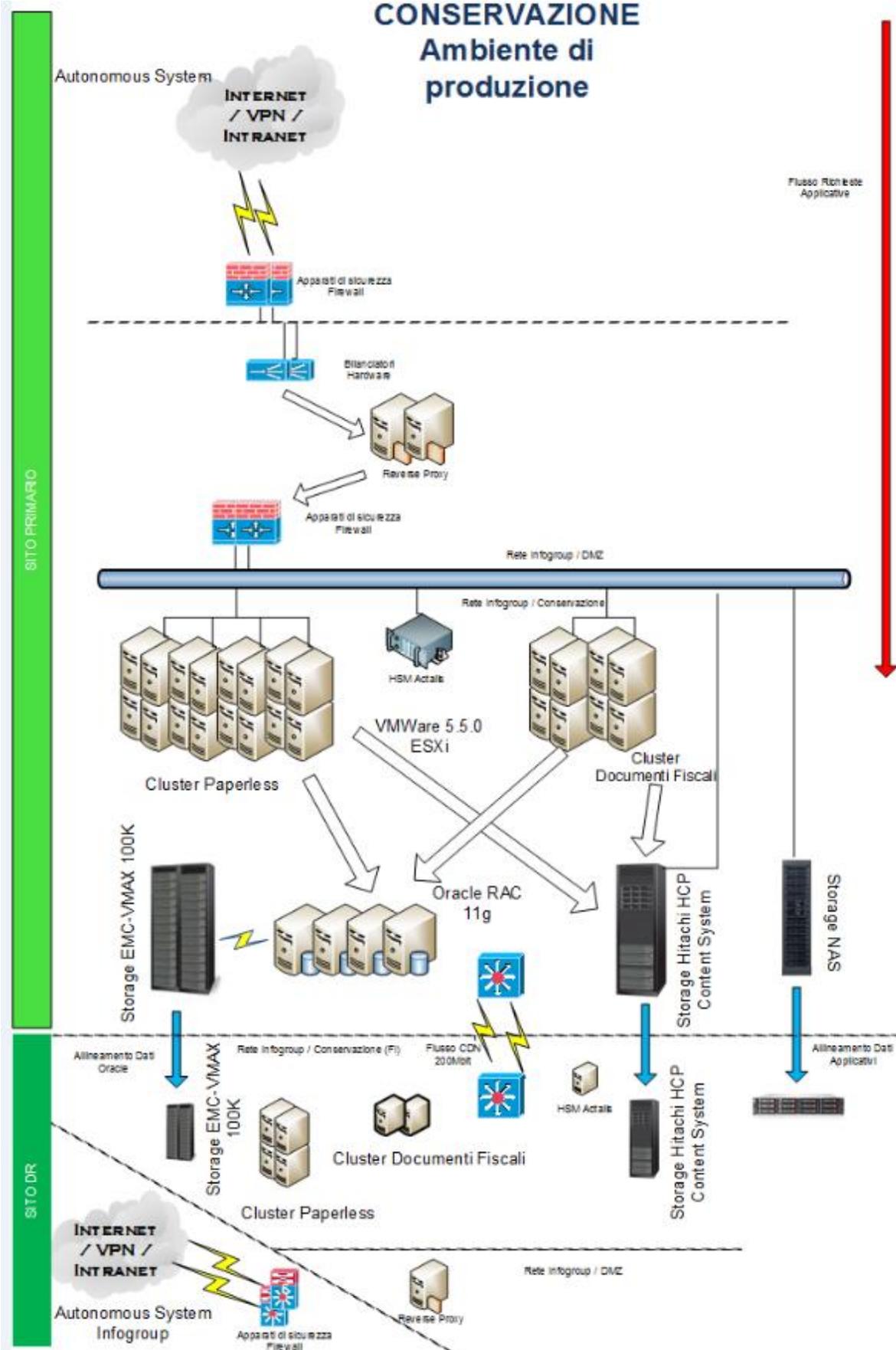


Figura 10 Schema infrastruttura

[torna al sommario](#)

8.5 Procedure di Gestione e di Evoluzione

L'erogazione del servizio è regolata dalle procedure di "ciclo di vita di una infrastruttura" e "ciclo di vita del SW".

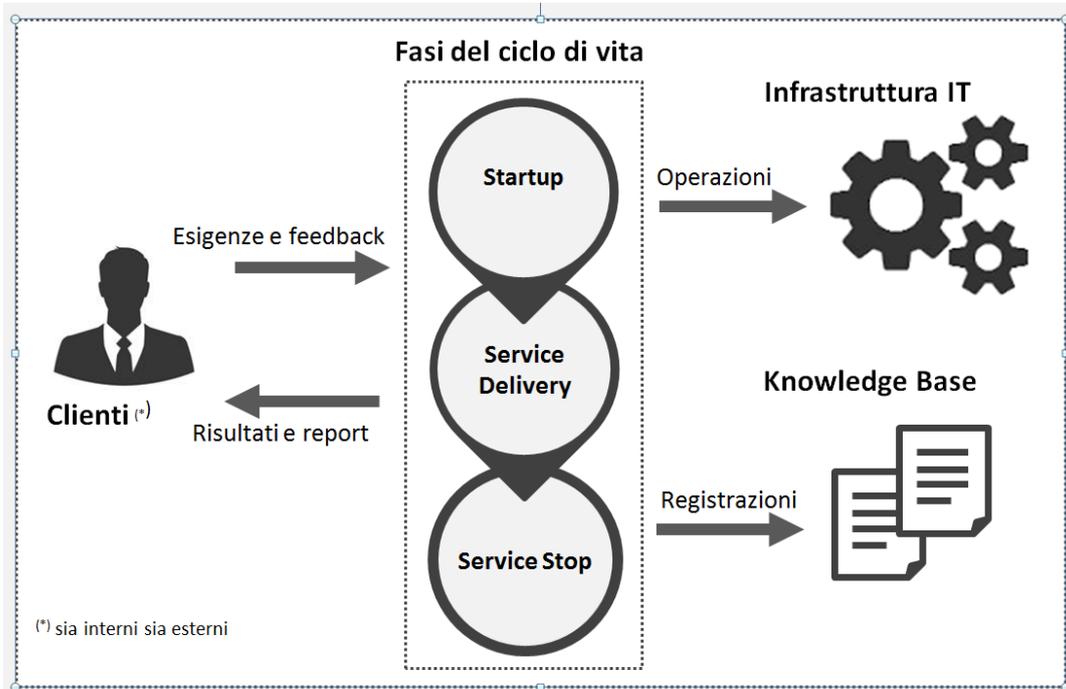


Figura 11 - ciclo di vita del Servizio

Le procedure che regolano la gestione e l'evoluzione sono legate alla fase di Service delivery.

Nella fase Service Delivery:

- è assicurato il funzionamento del software, seguendo quanto dettato nei processi Incident Management, Change Management e Request Management,
- il software è allineato alle variazioni delle esigenze dei Clienti, seguendo quanto dettato nei processi Customer Relation Management e Change Management,
- sono individuate e messe in atto le azioni preventive e migliorative pertinenti il software, seguendo quanto dettato dai processi Review Management e Change Management.

La procedura centrale del processo di gestione è quella di Change management; queste richieste di change possono scaturire:

- da nuove esigenze dei Clienti,
- da una azione, migliorativa o preventiva, decisa in sede di review del software,
- per un workaround o per eliminarne le cause di un difetto del software.

Le richieste di change possono essere attivate dal Service Manager. Maggiori dettagli si trovano nelle procedure aziendali.

[torna al sommario](#)

9 MONITORAGGIO E CONTROLLI

La normativa che disciplina il processo di conservazione dei documenti informatici prevede un alto livello di sicurezza per quanto riguarda le policy di archiviazione e accessibilità dei documenti conservati. I Dettagli sono riportati nel Piano di Sicurezza.

[torna al sommario](#)

9.1 *Tracciabilità delle operazioni*

Un apposito servizio centralizza i files di log di tutte le componenti HW e applicative; La sincronizzazione di tutti i sistemi sul tempo campione proveniente dalla fonte esterna prevista dalla legge consente la ricostruzione della corretta sequenzialità di accadimento delle operazioni registrate nei file di log.

Eng implementa un SIEM (Security Information and Event Management) basato su tecnologia McAfee per la gestione dei log provenienti da sistemi, apparati di rete e Firewall. Il sistema si compone di numero tre elementi: Event Receiver Collector, LogManager, Enterprise Security Manager.

I tre moduli svolgono compiti distinti, in particolare:

- Event Receiver Collector (ERC): McAfee Event Receiver raccoglie eventi e log di terze parti più velocemente e con maggiore affidabilità di ogni altra soluzione, utilizzando un sistema integrato di raccolta dei flussi di rete.
- LogManager (ELM): McAfee Enterprise Log Manager consente la gestione automatizzata e l'analisi di log di tutti i tipi, come i log degli eventi di Windows, dei database, delle applicazioni e di sistema. I log sono firmati e convalidati per garantire autenticità e integrità: un requisito per la conformità alla normativa e di valore legale. I set predefiniti di regole per la conformità e la reportistica semplificano la dimostrazione del rispetto della conformità e dell'esecuzione delle policy da parte dell'azienda.
- Enterprise Security Manager (ESM) : McAfee Enterprise Security Manager fornisce i contesti in modo veloce e approfondito per identificare le minacce critiche, agire rapidamente e rispondere in modo semplice ai requisiti di conformità. L'aggiornamento continuo sulle minacce globali e sui rischi aziendali consente una gestione dei rischi adattiva e autonoma, rendendo disponibili le risposte alle minacce e la reportistica per le questioni di conformità nell'ordine di minuti anziché di ore.

L'azione sinergica delle tre componenti permette di procedere alla raccolta dei log, la loro correlazione e analisi nonché la storicizzazione e la retention nel rispetto delle normative attuali.

Questo servizio permette anche l'identificazione di condizioni di allarme in corrispondenza delle quali si attivano specifiche azioni fra cui anche l'apertura di trouble ticket gestiti dalla piattaforma o tramite mail verso l'ufficio sicurezza Eng e l'ufficio Sistemi Eng.

[torna al sommario](#)

9.2 *Monitoraggio dell'applicazione*

Tutte le componenti hardware, i sistemi operativi e le applicazioni sono sottoposte a continuo monitoraggio da parte del personale sistemistico Eng. Questo monitoraggio permette di rilevare componenti non funzionanti, degradate o sature.

Il monitoraggio di queste due ultime condizioni (degradazione e saturazione delle risorse) consente di prevenire fenomeni bloccanti e limitare i disservizi derivanti. Inoltre monitorare queste condizioni consente di pianificare eventuali upgrade o modifiche dell'architettura.

La struttura di monitoraggio ha due tipologie di controlli:

- Sistemistici (utilizzo risorse, controllo accessi,)
- Applicativi (sonde su servizi dummy, quadrature, monitoraggio picchi elaborativi,)

I livelli di servizio sono regolati da SLA definite con il cliente i cui KPI sono monitorati e verificati periodicamente.

[torna al sommario](#)

9.3 Controlli periodici di integrità

I controlli periodici di integrità dei documenti conservati sono pianificati dal Responsabile del servizio di Conservazione, tenendo conto dello stato e dell'importanza dei processi e delle aree oggetto di verifica, nonché dei risultati delle precedenti verifiche. La frequenza con la quale vengono disposti i controlli di integrità è almeno biennale. Periodicamente viene predisposto il relativo report di verifica.

La scelta del personale verificatore viene fatta in modo da garantire obiettività ed imparzialità nel processo di verifica.

Di seguito le tipologie di verifiche attuate nel processo di controllo di integrità:

- verifiche periodiche sullo stato di conservazione dei supporti di memorizzazione, tendenti a verificare con l'ausilio di software appropriati, lo stato di conservazione dei supporti di memorizzazione e a ricercare eventuali difetti, provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.
- verifiche periodiche sui documenti conservati, tendenti a verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva integrità dei documenti stessi, provvedendo, se necessario, al loro riversamento. La procedura che gestisce il processo di conservazione presenta delle funzionalità di controllo massivo dei dati conservati: questi controlli consistono nell'impostare a livello informatico la periodicità dei controlli da effettuare; attualmente, il sistema è configurato per verificare giornalmente un milione di documenti, eseguendo ogni giorno i controlli a rotazione su documenti diversi. L'applicazione che gestisce il processo di conservazione, effettua un check automatico registrando per ogni PdA/documento conservato, la data e ora in cui è stata eseguita l'ultima verifica di integrità. Nel caso siano verificate delle anomalie viene aperto un incident al fine di recuperare il dato dalle copie di sicurezza.

verifiche di leggibilità dei documenti in conservazione da parte di operatori (human readability) possono essere eseguite a richiesta del Committente, tramite apertura di un campione pseudocasuale statistico dei documenti. I dati rilevati, relativamente al numero di documenti verificati ed agli eventuali risultati negativi, saranno inseriti in apposito report inviato al committente. La cadenza dei controlli e le dimensioni del campione da considerare sono da definire a livello contrattuale

[torna al sommario](#)

9.4 Soluzioni adottate in caso di Anomalie

Il presentarsi di un evento anomalo viene gestito con la creazione di un ticket verso la struttura preposta a mantenere il servizio. E' prevista, in caso di anomalia l'apertura di un incident.

Si distinguono due tipi di incident del software: l'incident normale e l'incident grave. Gli incident gravi sono quelli che causano un impatto sul Cliente. È prerogativa del Service Manager decidere che un incident è grave perché è il soggetto designato a valutare i danni ai Clienti.

In generale l'incident viene sempre generato se l'anomalia causa un non rispetto delle SLA contrattualizzate con un qualsiasi Cliente.

Una volta che l'anomalia viene rilevata, verrà:

- analizzata
- si procederà alle azioni di ripristino del servizio
- e di determineranno e documenteranno le azioni di correzione.

Per ripristinare, tempestivamente, il corretto funzionamento il Team deve individuare ed eseguire, anche con la collaborazione degli utenti e dei Clienti, le operazioni per lo workaround di ogni incident, documentando le operazioni eseguite come workaround dell'incident, quando dette operazioni sono state eseguite ed i risultati ottenuti con l'esecuzione di dette operazioni.

Se lo workaround di un incident ha ripristinato il corretto funzionamento del software, il Team deve documentare quando il software ha ripreso a funzionare correttamente.

Se invece lo workaround di un incident non ha sortito effetti: il Service Manager (o responsabile del servizio) deve attivare un change in emergenza per ripristinare, tempestivamente, il corretto funzionamento del servizio.

Maggiori dettagli sono descritti nelle procedure Aziendali di gestione incident.

[torna al sommario](#)

9.5 Procedure di Continuità Operativa e Disaster Recovery

Qualora si verifichi un evento che comporti l'indisponibilità del sistema di conservazione Primario, viene proposta l'attivazione delle misure di Continuità Operativa in funzione dell'effettiva gravità ed estensione dell'emergenza.

La soluzione di Continuità Operativa definita per gestire questa tipologia di emergenza prevede che **le risorse critiche che supportano il servizio di Conservazione (Team di Emergenza) si trasferiscano presso uno o più siti alternativi** per la prosecuzione delle proprie attività. Il trasferimento riguarda risorse preventivamente identificate in numero sufficiente a garantire

la **sopravvivenza delle sole attività critiche** per il tempo necessario all'organizzazione di contromisure durature nel tempo.

L'architettura del Disaster Recovery a supporto della Continuità Operativa prevede il Sito Primario presso l'infrastruttura tecnologica di Settimo Torinese (TO), mentre il sito

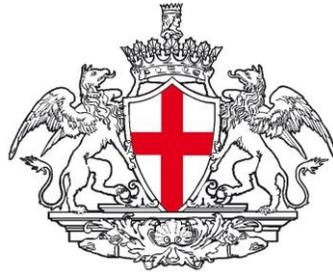
Secondario è implementato presso il Data Center di Firenze, distante oltre 300 Km dal sito primario.

Il sito secondario permette di usufruire dei servizi in Produzione in caso di indisponibilità del Data Center Primario, nel rispetto dei requisiti (RTO e RPO) riportati negli SLA definiti contrattualmente ed in sede di attivazione del servizio.

[torna al sommario](#)

----- *fine documento* -----

Comune di Genova



Allegato 3 - Formati

Ai fini della ricezione, gestione, produzione, trasmissione e conservazione a norma dei documenti informatici, l'Amministrazione garantisce la produzione dei documenti informatici in formati coerenti con le regole tecniche previste dalle LLGG, Allegato 2.

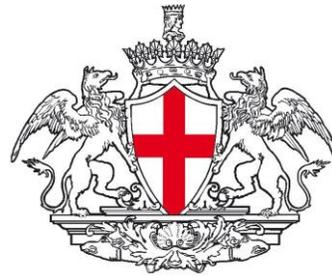
Nello specifico:

- Documenti impaginati — PDF, Microsoft® OOXML (.docx) e Word (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® InDesign® Markup Language (.idml)
- Ipertesti — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md)
- Dati strutturati — SQL, CSV, Microsoft® OOXML (.accdb) e Access (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT4
- Posta elettronica — .eml, .mbox
- Fogli di calcolo — Microsoft® OOXML (.xlsx) e Excel (.xls), OpenDocument Spreadsheet (.ods)
- Presentazioni multimediali — Microsoft® OOXML (.pptx) e PowerPoint (.ppt), OpenDocument Presentation (.odp)
- Immagini raster — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® Photoshop® (.psd), DPX, ARRIRAW (.ari)
- Immagini vettoriali e modellazione digitale — SVG, Adobe® Illustrator® (.ai), Encapsulated PostScript™ (.eps)
- Modelli digitali — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™
- Caratteri tipografici — OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2)
- Suono — Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici codec audio
- Video — formati video delle famiglie MPEG2 e MPEG4; molteplici codec video
- Sottotitoli — TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL
- Contenitori multimediali — MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM
- Pacchetti multimediali — pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM
- Archivi compressi — TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, ...), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg)
- Documenti amministrativi — fattura elettronica, fascicolo sanitario elettronico, response SAML SPID, segnatura di protocollo
- Applicazioni e codice sorgente — eseguibili Microsoft® (.exe, .com), applet Java (.jar); pacchetti applicativi Windows® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .?sh, .bat, .cmd, .py, .perl, .js, .go, .r, ...); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, ...)
- Applicazioni crittografiche — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, ...); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CAAdES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

In ogni caso i documenti digitali dovranno essere privi di elementi attivi, tra cui macro e campi variabili. Formati differenti da quelli indicati nel precedente elenco sono ammessi in relazione a specifici flussi documentali solo se previsti da atti normativi e formali.

I formati indicati sono tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi in base alla normativa vigente riguardante specifiche tipologie documentali.

Comune di Genova



Allegato 4 – Registro di emergenza

DIREZIONE

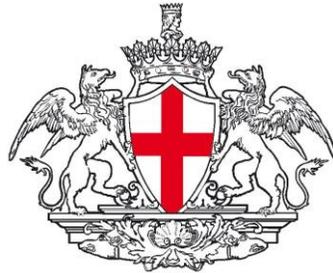
PROTOCOLLO - REGISTRO DI EMERGENZA

COD. -----

Interruzione delle procedure informatiche di registrazione dalle ore ... del giorno dovuta alle procedure di avvio del nuovo sistema del Registro di protocollo.

Protocollo – Registro di emergenza

Comune di Genova



Allegato 5 – Titolario di classificazione

Indice (Ordinamento)	Indice	"Descrizione"	"
00001	1	Amministrazione Generale	
00001.00001	1.1	Legislazione e circolari esplicative	
00001.00001.00001	1.1.1	Legislazione e circolari esplicative	
00001.00002	1.2	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica	
00001.00002.00001	1.2.1	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica	
00001.00003	1.3	Statuto	
00001.00003.00001	1.3.1	Statuto	
00001.00004	1.4	Regolamenti	
00001.00004.00001	1.4.1	Regolamenti	
00001.00005	1.5	Stemma, gonfalone, sigillo	
00001.00005.00001	1.5.1	Stemma, gonfalone, sigillo	
00001.00006	1.6	Archivio generale	
00001.00006.00001	1.6.1	Archivio generale	
00001.00007	1.7	Sistema informativo	
00001.00007.00001	1.7.1	Sistema informativo	
00001.00007.00002	1.7.2	Statistiche del personale	
00001.00007.00003	1.7.3	Banche dati del personale	
00001.00007.00004	1.7.4	Telefonia Fissa	
00001.00007.00005	1.7.5	Telefonia Mobile	
00001.00007.00006	1.7.6	Sistemi Informativi Territoriali	
00001.00007.00007	1.7.7	Sviluppo hardware, software, infrastrutture	
00001.00007.00008	1.7.8	Statistiche Economiche	
00001.00007.00009	1.7.9	Statistiche Socio-Demografiche	
00001.00008	1.8	Informazioni e relazioni con il pubblico	
00001.00008.00001	1.8.1	Informazioni e relazioni con il pubblico	
00001.00009	1.9	Politica del personale, ordinamento degli uffici e dei servizi	
00001.00009.00001	1.9.1	Politica del personale, ordinamento degli uffici e dei servizi	
00001.00009.00002	1.9.2	Organizzazione	
00001.00009.00003	1.9.3	Analisi processi	
00001.00009.00004	1.9.4	Valutazione posizioni/prestazioni/potenziale	

00001.00009.00005	1.9.5	Gruppi di miglioramento
00001.00009.00006	1.9.6	Pari opportunità
00001.00010	1.10	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
00001.00010.00001	1.10.1	Relazioni con le organizzazioni sindacali e di rappresentanza del personale
00001.00010.00002	1.10.2	Relazioni con OOSS
00001.00010.00003	1.10.3	Permessi. Distacchi/aspettative sindacali
00001.00011	1.11	Controlli esterni
00001.00011.00001	1.11.1	Controlli esterni
00001.00012	1.12	Editoria e attività informativo-promozionale interna ed esterna
00001.00012.00001	1.12.1	Editoria e attività informativo-promozionale interna ed esterna
00001.00013	1.13	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
00001.00013.00001	1.13.1	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti
00001.00013.00002	1.13.2	Promozione della città'
00001.00014	1.14	Interventi di carattere politico e umanitario; rapporti istituzionali
00001.00014.00001	1.14.1	Interventi di carattere politico e umanitario; rapporti istituzionali
00001.00015	1.15	Forme associative per l'esercizio di funzioni e servizi
00001.00015.00001	1.15.1	Forme associative per l'esercizio di funzioni e servizi
00001.00016	1.16	Area e città metropolitana
00001.00016.00001	1.16.1	Area e città metropolitana
00001.00017	1.17	Associazionismo e partecipazione
00001.00017.00001	1.17.1	Associazionismo e partecipazione
00001.00018	1.18	Accesso agli atti
00001.00018.00001	1.18.1	Documentale
00001.00018.00002	1.18.2	Civico
00001.00018.00003	1.18.3	Generalizzato

00002 2 ORGANI DI GOVERNO, GESTIONE, CONTROLLO, CONSULENZA E GARANZIA

00002.00001	2.1	Sindaco
00002.00001.00001	2.1.1	Sindaco
00002.00001.00002	2.1.2	Conferenza dei Sindaci
00002.00002	2.2	Vice-Sindaco
00002.00002.00001	2.2.1	Vice-Sindaco
00002.00003	2.3	Consiglio

00002.00003.00001	2.3.1	Consiglio
00002.00004	2.4	Presidente del Consiglio
00002.00004.00001	2.4.1	Presidente del Consiglio
00002.00005	2.5	Conferenza dei capigruppo e Commissioni del Consiglio
00002.00005.00001	2.5.1	Conferenza dei capigruppo e Commissioni del Consiglio
00002.00006	2.6	Gruppi consiliari
00002.00006.00001	2.6.1	Gruppi consiliari
00002.00007	2.7	Giunta
00002.00007.00001	2.7.1	Giunta
00002.00008	2.8	Commissario prefettizio e straordinario
00002.00008.00001	2.8.1	Commissario prefettizio e straordinario
00002.00009	2.9	Segretario e Vice-segretario
00002.00009.00001	2.9.1	Segretario e Vice-segretario
00002.00010	2.10	Direttore generale e Dirigenza
00002.00010.00001	2.10.1	Direttore generale e Dirigenza
00002.00011	2.11	Revisore dei conti
00002.00011.00001	2.11.1	Revisore dei conti
00002.00012	2.12	Difensore civico
00002.00012.00001	2.12.1	Difensore civico
00002.00013	2.13	Commissario ad acta
00002.00013.00001	2.13.1	Commissario ad acta
00002.00014	2.14	Organi di controllo interni
00002.00014.00001	2.14.1	Organi di controllo interni
00002.00014.00002	2.14.2	Controllo di Gestione
00002.00015	2.15	Organi consultivi
00002.00015.00001	2.15.1	Organi consultivi
00002.00016	2.16	Consigli circoscrizionali
00002.00016.00001	2.16.1	Consigli circoscrizionali
00002.00017	2.17	Presidente dei Consigli circoscrizionali
00002.00017.00001	2.17.1	Presidente dei Consigli circoscrizionali
00002.00018	2.18	Organi esecutivi circoscrizionali
00002.00018.00001	2.18.1	Organi esecutivi circoscrizionali

00002.00019	2.19	Commissioni dei Consigli circoscrizionali
00002.00019.00001	2.19.1	Commissioni dei Consigli circoscrizionali
00002.00020	2.20	Segretari delle circoscrizioni
00002.00020.00001	2.20.1	Segretari delle circoscrizioni
00002.00021	2.21	Commissario ad acta delle circoscrizioni
00002.00021.00001	2.21.1	Commissario ad acta delle circoscrizioni
00002.00022	2.22	Conferenza dei Presidenti di quartiere
00002.00022.00001	2.22.1	Conferenza dei Presidenti di quartiere
00003	3	RISORSE UMANE
00003.00001	3.1	Concorsi, selezioni, colloqui
00003.00001.00001	3.1.1	Concorsi, selezioni, colloqui
00003.00001.00002	3.1.2	Concorsi a tempo indeterminato
00003.00001.00003	3.1.3	Selezioni tempo determinato
00003.00002	3.2	Assunzioni e cessazioni
00003.00002.00001	3.2.1	Assunzioni e cessazioni
00003.00002.00002	3.2.2	Domande cessazione
00003.00002.00003	3.2.3	Domande assunzione (generiche)
00003.00002.00004	3.2.4	Matricola/fascicolo
00003.00003	3.3	Comandi e distacchi; mobilità
00003.00003.00001	3.3.1	Comandi e distacchi; mobilità
00003.00003.00002	3.3.2	Comandi
00003.00003.00003	3.3.3	Distacchi
00003.00003.00004	3.3.4	Mobilità interna
00003.00003.00005	3.3.5	Mobilità esterna
00003.00004	3.4	Attribuzione di funzioni, ordini di servizio e missioni
00003.00004.00001	3.4.1	Attribuzione di funzioni, ordini di servizio e missioni
00003.00004.00002	3.4.2	Ordini di servizio
00003.00004.00003	3.4.3	Incarichi (dirigenti - posizioni organizzative ecc.)
00003.00004.00004	3.4.4	Mansioni
00003.00004.00005	3.4.5	Trasferte
00003.00005	3.5	Inquadramenti e applicazione contratti collettivi di lavoro
00003.00005.00001	3.5.1	Inquadramenti e applicazione contratti collettivi di lavoro

00003.00005.00002	3.5.2	Applicazioni contrattuali
00003.00005.00003	3.5.3	Problematiche giuridiche
00003.00005.00004	3.5.4	Legge privacy
00003.00006	3.6	Retribuzioni e compensi
00003.00006.00001	3.6.1	Retribuzioni e compensi
00003.00006.00002	3.6.2	Retribuzioni
00003.00006.00003	3.6.3	Straordinario
00003.00006.00004	3.6.4	Indennità
00003.00006.00005	3.6.5	Recupero crediti
00003.00006.00006	3.6.6	Anagrafe delle prestazioni
00003.00007	3.7	Adempimenti fiscali, contributivi e assicurativi
00003.00007.00001	3.7.1	Adempimenti fiscali, contributivi e assicurativi
00003.00007.00002	3.7.2	730
00003.00007.00003	3.7.3	770
00003.00007.00004	3.7.4	INAIL
00003.00007.00005	3.7.5	INPS
00003.00007.00006	3.7.6	Contributi previdenziali ed assistenziali
00003.00008	3.8	Tutela della salute e sicurezza sul luogo di lavoro
00003.00008.00001	3.8.1	Tutela della salute e sicurezza sul luogo di lavoro
00003.00008.00002	3.8.2	Sorveglianza sanitaria
00003.00008.00003	3.8.3	Prevenzione e protezione
00003.00009	3.9	Dichiarazioni di infermità ed equo indennizzo
00003.00009.00001	3.9.1	Dichiarazioni di infermità ed equo indennizzo
00003.00009.00002	3.9.2	Equo indennizzo
00003.00009.00003	3.9.3	Infortuni
00003.00010	3.10	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
00003.00010.00001	3.10.1	Indennità premio di servizio e trattamento di fine rapporto, quiescenza
00003.00010.00002	3.10.2	Indennità di fine rapporto
00003.00010.00003	3.10.3	Pensioni integrative
00003.00011	3.11	Servizi al personale su richiesta
00003.00011.00001	3.11.1	Servizi al personale su richiesta
00003.00011.00002	3.11.2	Ritenute extralegali (cessione V - assegni familiari ecc.)

00003.00011.00003	3.11.3	Attività secondarie
00003.00011.00004	3.11.4	Uffici Giudiziari
00003.00011.00005	3.11.5	Attività connesse all'assistenza sociale ai dipendenti
00003.00011.00006	3.11.6	Benefici L. 104
00003.00011.00007	3.11.7	Patrocinio gratuito
00003.00012	3.12	Orario di lavoro, presenze e assenze
00003.00012.00001	3.12.1	Orario di lavoro, presenze e assenze
00003.00012.00002	3.12.2	Orario di lavoro
00003.00012.00003	3.12.3	Assenze
00003.00012.00004	3.12.4	Aspettative
00003.00012.00005	3.12.5	Part time
00003.00013	3.13	Giudizi, responsabilità e provvedimenti disciplinari
00003.00013.00001	3.13.1	Giudizi, responsabilità e provvedimenti disciplinari
00003.00013.00002	3.13.2	Provvedimenti disciplinari
00003.00013.00003	3.13.3	Funzioni ispettive
00003.00013.00004	3.13.4	Contenzioso
00003.00014	3.14	Formazione e aggiornamento professionale
00003.00014.00001	3.14.1	Formazione e aggiornamento professionale
00003.00014.00002	3.14.2	Scuola Themis
00003.00014.00003	3.14.3	Formazione interna
00003.00014.00004	3.14.4	Convenzioni per tirocini
00003.00014.00005	3.14.5	Formazione informatica
00003.00015	3.15	Collaboratori esterni
00003.00015.00001	3.15.1	Collaboratori esterni
00003.00015.00002	3.15.2	Collaborazioni coordinate continuative
00003.00015.00003	3.15.3	Consulenze
00003.00015.00004	3.15.4	Contratti prestazioni professionali

00004 4 RISORSE FINANZIARIE E PATRIMONIO

00004.00001	4.1	Entrate
00004.00001.00001	4.1.1	Entrate
00004.00001.00002	4.1.2	Entrate derivanti da fondi fuori bilancio
00004.00001.00003	4.1.3	Recupero danni

00004.00002	4.2	Uscite
00004.00002.00001	4.2.1	Uscite
00004.00002.00002	4.2.2	Albo fornitori
00004.00003	4.3	Partecipazioni finanziarie
00004.00003.00001	4.3.1	Partecipazioni finanziarie
00004.00004	4.4	Bilancio preventivo, variazioni di bilancio, verifiche contabili
00004.00004.00001	4.4.1	Bilancio preventivo, variazioni di bilancio, verifiche contabili
00004.00005	4.5	Piano esecutivo di gestione (PEG)
00004.00005.00001	4.5.1	Piano esecutivo di gestione (PEG)
00004.00006	4.6	Rendiconto della gestione
00004.00006.00001	4.6.1	Rendiconto della gestione
00004.00006.00002	4.6.2	Residui attivi e passivi
00004.00007	4.7	Adempimenti fiscali
00004.00007.00001	4.7.1	Adempimenti fiscali
00004.00007.00002	4.7.2	I.V.A.
00004.00007.00003	4.7.3	Imposte Dirette
00004.00007.00004	4.7.4	Fiscale Contratti
00004.00008	4.8	Inventari e consegnatari dei beni
00004.00008.00001	4.8.1	Inventari e consegnatari dei beni
00004.00009	4.9	Beni immobili
00004.00009.00001	4.9.1	Beni immobili
00004.00009.00002	4.9.2	Concessioni Demaniali
00004.00010	4.10	Beni mobili
00004.00010.00001	4.10.1	Beni mobili
00004.00011	4.11	Economato
00004.00011.00001	4.11.1	Economato
00004.00011.00002	4.11.2	Forniture e Servizi
00004.00012	4.12	Oggetti smarriti e recuperati
00004.00012.00001	4.12.1	Oggetti smarriti e recuperati
00004.00013	4.13	Tesoreria
00004.00013.00001	4.13.1	Tesoreria
00004.00013.00002	4.13.2	Cassa Economale

00004.00013.00003	4.13.3	Cassa Gare e Contratti
00004.00014	4.14	Concessionari ed altri incaricati della riscossione delle entrate
00004.00014.00001	4.14.1	Concessionari ed altri incaricati della riscossione delle entrate
00004.00015	4.15	Pubblicità e pubbliche affissioni
00004.00015.00001	4.15.1	Pubblicità e pubbliche affissioni
00005	5	AFFARI LEGALI
00005.00001	5.1	Contenzioso
00005.00001.00001	5.1.1	Contenzioso
00005.00002	5.2	Responsabilità civile e patrimoniale verso terzi; assicurazioni
00005.00002.00001	5.2.1	Responsabilità civile e patrimoniale verso terzi; assicurazioni
00005.00003	5.3	Pareri e consulenze
00005.00003.00001	5.3.1	Pareri e consulenze
00006	6	PIANIFICAZIONE E GESTIONE DEL TERRITORIO
00006.00001	6.1	Urbanistica: piano regolatore generale e varianti
00006.00001.00001	6.1.1	Aggiornamento e revisione PRG (PUC)
00006.00001.00002	6.1.2	Varianti
00006.00001.00003	6.1.3	Piani di settore
00006.00002	6.2	Urbanistica: strumenti di attuazione del Piano regolatore generale
00006.00002.00001	6.2.1	Urbanistica
00006.00002.00002	6.2.2	Centri storici
00006.00002.00003	6.2.3	Estetica urbana
00006.00002.00004	6.2.4	Assetto del verde
00006.00002.00005	6.2.5	Conferenza dei servizi
00006.00002.00006	6.2.6	Intese Stato-Regione
00006.00002.00007	6.2.7	Programmi e progetti complessi
00006.00002.00008	6.2.8	Programmi e progetti comunitari
00006.00003	6.3	Edilizia privata
00006.00003.00001	6.3.1	Pratiche edilizie
00006.00003.00002	6.3.2	Abusi edilizi
00006.00003.00003	6.3.3	Edilizia per le attività produttive
00006.00003.00004	6.3.4	Condomo edilizio
00006.00004	6.4	Edilizia pubblica

00006.00004.00001	6.4.1	Edilizia pubblica
00006.00004.00002	6.4.2	Procedure di Esproprio
00006.00004.00003	6.4.3	Programmi di Edilizia Agevolata e Sovvenzionata
00006.00004.00004	6.4.4	Programmi e Convenzioni ERP
00006.00004.00005	6.4.5	Strutture Sociali
00006.00004.00006	6.4.6	Strutture educative 0/6
00006.00004.00007	6.4.7	Strutture scuola dell'obbligo
00006.00005	6.5	Opere pubbliche
00006.00005.00001	6.5.1	Edilizia pubblica
00006.00005.00002	6.5.2	Impianti
00006.00005.00003	6.5.3	Strade e piazze
00006.00005.00004	6.5.4	Verde
00006.00005.00005	6.5.5	Programmazione, progettazione ed esecuzione OO.PP.
00006.00005.00006	6.5.6	Rapporti con Società partecipate
00006.00005.00007	6.5.7	Appalti Lavori
00006.00005.00008	6.5.8	Contratti di Acquisizione e Cessione
00006.00006	6.6	Catasto
00006.00006.00001	6.6.1	Catasto
00006.00007	6.7	Viabilità
00006.00007.00001	6.7.1	Viabilità
00006.00007.00002	6.7.2	Parcheggi
00006.00007.00003	6.7.3	Segnaletica
00006.00007.00004	6.7.4	Piani del traffico e della mobilità
00006.00007.00005	6.7.5	Rottura Suolo, Concessioni per occupazione suolo e sottosuolo
00006.00008	6.8	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
00006.00008.00001	6.8.1	Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi
00006.00008.00002	6.8.2	Attivazione utenze e liquidazione fatturazioni
00006.00008.00003	6.8.3	Conduzione e manutenzione Impianti Termici
00006.00008.00004	6.8.4	Servizi per la vivibilità della Città
00006.00009	6.9	Ambiente: autorizzazioni, monitoraggio e controllo
00006.00009.00001	6.9.1	Difesa del territorio

00006.00009.00002	6.9.2	Ambiente
00006.00009.00003	6.9.3	Bonifiche
00006.00009.00004	6.9.4	Rifiuti
00006.00009.00005	6.9.5	Idrico
00006.00009.00006	6.9.6	Atmosferico
00006.00009.00007	6.9.7	Igiene industriale
00006.00009.00008	6.9.8	Igiene urbana
00006.00009.00009	6.9.9	Impianti
00006.00009.00010	6.9.10	Educazione ambientale
00006.00009.00011	6.9.11	Rumore
00006.00009.00012	6.9.12	Energia
00006.00009.00013	6.9.13	Sicurezza impianti
00006.00009.00014	6.9.14	Risparmio Energetico
00006.00009.00015	6.9.15	Problematiche amianto negli edifici di competenza comunale
00006.00010	6.10	Protezione civile ed emergenze
00006.00010.00001	6.10.1	Protezione civile ed emergenze

00007 7 SERVIZI ALLA PERSONA

00007.00001	7.1	Diritto allo studio e servizi
00007.00001.00001	7.1.1	Diritto allo studio e servizi
00007.00001.00002	7.1.2	Sostegno all'handicap
00007.00001.00003	7.1.3	Patto scuola
00007.00001.00004	7.1.4	Ristorazione scolastica
00007.00002	7.2	Asili nido e scuola materna
00007.00002.00001	7.2.1	Asili nido e scuola materna
00007.00002.00002	7.2.2	Asili nido - area gestionale
00007.00002.00003	7.2.3	Asili nido - area tecnica
00007.00002.00004	7.2.4	Scuola infanzia - area gestionale
00007.00002.00005	7.2.5	Scuola infanzia - area tecnica
00007.00002.00006	7.2.6	Servizi integrativi 0/6 (attività e relazioni con Settore)
00007.00002.00007	7.2.7	Laboratorio interculturale
00007.00003	7.3	Promozione e sostegno delle istituzioni di istruzione e delle loro attività
00007.00003.00001	7.3.1	Promozione e sostegno delle istituzioni di istruzione e delle loro attività

00007.00003.00002	7.3.2	Laboratori Educativi Territoriali
00007.00003.00003	7.3.3	Istituti Civici Superiori
00007.00003.00007	7.3.7	*****
00007.00004	7.4	Orientamento professionale; educazione degli adulti; mediazione culturale
00007.00004.00001	7.4.1	Orientamento professionale; educazione degli adulti; mediazione culturale
00007.00005	7.5	Istituti Culturali(Musei,Biblioteche,Teatri,Scuola Comunale di musica,etc.)
00007.00005.00001	7.5.1	Istituti Culturali
00007.00005.00002	7.5.2	Musei
00007.00005.00003	7.5.3	Biblioteche
00007.00005.00004	7.5.4	Palazzo Ducale
00007.00005.00005	7.5.5	Teatri
00007.00006	7.6	Attività ed eventi culturali
00007.00006.00001	7.6.1	Attività ed eventi culturali
00007.00006.00002	7.6.2	Attività ed eventi Musei
00007.00006.00003	7.6.3	Attività ed eventi Biblioteche
00007.00006.00004	7.6.4	Promozione turistica e delle tradizioni locali - Violini storici
00007.00006.00005	7.6.5	Progetti Europei
00007.00006.00006	7.6.6	Violini storici
00007.00007	7.7	Attività ed eventi sportivi
00007.00007.00001	7.7.1	Attività ed eventi sportivi
00007.00008	7.8	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
00007.00008.00001	7.8.1	Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale
00007.00008.00002	7.8.2	Piano Regolatore Sociale
00007.00008.00003	7.8.3	Legge 328/2000 - Segreterie Tecniche
00007.00008.00004	7.8.4	Servizio Civile Volontario
00007.00009	7.9	Prevenzione,recupero e reintegrazione dei soggetti a rischio
00007.00009.00001	7.9.1	Prevenzione,recupero e reintegrazione dei soggetti a rischio
00007.00009.00002	7.9.2	Politiche attive del lavoro
00007.00009.00003	7.9.3	Inserimenti lavorativi fasce deboli
00007.00010	7.10	Informazione, consulenza ed educazione civica

00007.00010.00001	7.10.1	Informazione, consulenza ed educazione civica
00007.00011	7.11	Tutela e curatela di incapaci
00007.00011.00001	7.11.1	Tutela e curatela di incapaci
00007.00011.00002	7.11.2	Affido familiare
00007.00011.00003	7.11.3	Adozioni
00007.00012	7.12	Assistenza diretta e indiretta, benefici economici
00007.00012.00001	7.12.1	Assistenza diretta e indiretta, benefici economici
00007.00012.00002	7.12.2	Assistenza residenziale e semiresidenziale minori
00007.00012.00003	7.12.3	Assistenza residenziale e semiresidenziale anziani
00007.00012.00004	7.12.4	Assistenza residenziale e semiresidenziale disabili
00007.00012.00005	7.12.5	Contributi economici
00007.00012.00006	7.12.6	Sostegno alla maternita'
00007.00012.00007	7.12.7	Stranieri non residenti
00007.00012.00008	7.12.8	Nomadi
00007.00012.00009	7.12.9	Cittadini senza territorio
00007.00013	7.13	Attività ricreativa e di socializzazione
00007.00013.00001	7.13.1	Attività ricreativa e di socializzazione
00007.00013.00002	7.13.2	Spettacoli e concerti
00007.00014	7.14	Politiche per la casa
00007.00014.00001	7.14.1	Politiche per la casa ed ERP
00007.00014.00002	7.14.2	Gestione contributi abitativi
00007.00014.00003	7.14.3	Contributi IPAB

00008 8 ATTIVITA' ECONOMICHE

00008.00001	8.1	Agricoltura e Pesca
00008.00001.00001	8.1.1	Agricoltura e Pesca
00008.00002	8.2	Artigianato
00008.00002.00001	8.2.1	Artigianato
00008.00002.00002	8.2.2	Estetisti
00008.00002.00003	8.2.3	Parrucchieri
00008.00003	8.3	Industria
00008.00003.00001	8.3.1	Industria
00008.00003.00002	8.3.2	Promozione d'impresa

00008.00004	8.4	Commercio
00008.00004.00001	8.4.1	Attività produttive
00008.00004.00002	8.4.2	Commercio in sede fissa
00008.00004.00003	8.4.3	Occupazione suolo pubblico
00008.00004.00004	8.4.4	Pubblici esercizi
00008.00004.00005	8.4.5	Edicole
00008.00004.00006	8.4.6	Distributori di carburanti
00008.00004.00007	8.4.7	Agenzie d'affari
00008.00005	8.5	Fiere e Mercati
00008.00005.00001	8.5.1	Mercati all'ingrosso
00008.00005.00002	8.5.2	Mercati rionali
00008.00005.00003	8.5.3	Mercati merci varie
00008.00005.00004	8.5.4	Fiere
00008.00006	8.6	Esercizi Turistici e Strutture Ricettive
00008.00006.00001	8.6.1	Alberghi
00008.00006.00002	8.6.2	Campeggi
00008.00006.00003	8.6.3	Stabilimenti balneari
00008.00006.00004	8.6.4	Agriturismo
00008.00006.00005	8.6.5	Bed & Breakfast, Case per ferie, Affittacamere
00008.00007	8.7	Promozione e Servizi
00008.00007.00001	8.7.1	Promozione e Servizi
00009	9	POLIZIA LOCALE E SICUREZZA PUBBLICA
00009.00001	9.1	Prevenzione ed educazione stradale
00009.00001.00001	9.1.1	Prevenzione ed educazione stradale
00009.00002	9.2	Polizia Stradale
00009.00002.00001	9.2.1	Polizia Stradale
00009.00002.00002	9.2.2	Trasporti eccezionali
00009.00003	9.3	Informative
00009.00003.00001	9.3.1	Informative
00009.00004	9.4	Sicurezza ed Ordine Pubblico
00009.00004.00001	9.4.1	Sicurezza ed Ordine Pubblico
00009.00004.00002	9.4.2	Licenze e autorizzazioni

00010 10 TUTELA DELLA SALUTE

00010.00001	10.1	Salute e igiene pubblica
00010.00001.00001	10.1.1	Igiene
00010.00001.00002	10.1.2	Annonario
00010.00001.00003	10.1.3	Presidio sanitario - socio sanitario - sociale
00010.00001.00004	10.1.4	Asili nido e servizi integrativi
00010.00001.00005	10.1.5	Vigilanza sanitaria
00010.00001.00006	10.1.6	Igiene edilizia
00010.00001.00007	10.1.7	Palestre
00010.00002	10.2	Trattamento Sanitario Obbligatorio
00010.00002.00001	10.2.1	Trattamento Sanitario Obbligatorio
00010.00003	10.3	Farmacie
00010.00003.00001	10.3.1	Farmacie
00010.00004	10.4	Zooprofilassi veterinaria
00010.00004.00001	10.4.1	Zooprofilassi veterinaria
00010.00005	10.5	Randagismo animale e ricoveri
00010.00005.00001	10.5.1	Tutela animali

00011 11 SERVIZI DEMOGRAFICI

00011.00001	11.1	Stato Civile
00011.00001.00001	11.1.1	Stato Civile
00011.00001.00002	11.1.2	Nascite
00011.00001.00003	11.1.3	Cittadinanze
00011.00001.00004	11.1.4	Decessi
00011.00001.00005	11.1.5	Matrimoni
00011.00001.00006	11.1.6	Archivio
00011.00002	11.2	Anagrafe e Certificazioni
00011.00002.00001	11.2.1	Anagrafe e Certificazioni
00011.00002.00002	11.2.2	Schedario
00011.00002.00003	11.2.3	Immigrazioni
00011.00002.00004	11.2.4	Emigrazioni
00011.00002.00005	11.2.5	Anagrafe Italiani Residenti all'Estero
00011.00002.00006	11.2.6	Variazioni Anagrafiche

00011.00002.00007	11.2.7	Anagrafe Stranieri
00011.00002.00008	11.2.8	Anagrafe Comunitari
00011.00002.00009	11.2.9	XXXXXX
00011.00003	11.3	Censimenti
00011.00003.00001	11.3.1	Censimenti
00011.00004	11.4	Polizia Mortuaria e Cimiteri
00011.00004.00001	11.4.1	Polizia Mortuaria e Cimiteri
00011.00004.00002	11.4.2	Servizi Cimiteriali
00011.00004.00003	11.4.3	Tariffe Cimiteriali
00011.00004.00004	11.4.4	Concessioni, retrocessioni, rimborsi, ecc...
00011.00004.00005	11.4.5	Gestione amministrativa ed operativa dell'attività cimiteriale
00011.00004.00006	11.4.6	Aree Cimiteriali
00011.00004.00007	11.4.7	Attività tecniche aree cimiteriali
00011.00004.00008	11.4.8	Coordinamento Trasporti Funebri

00012 12 ELEZIONI ED INIZIATIVE POPOLARI

00012.00001	12.1	Albi elettorali
00012.00001.00001	12.1.1	Albi elettorali
00012.00001.00002	12.1.2	Scrutatori
00012.00001.00003	12.1.3	Presidenti
00012.00001.00004	12.1.4	Giudici Popolari
00012.00002	12.2	Liste Elettorali
00012.00002.00001	12.2.1	Liste Elettorali
00012.00003	12.3	Elezioni
00012.00003.00001	12.3.1	Elezioni
00012.00003.00002	12.3.2	Amministrative
00012.00003.00003	12.3.3	Politiche
00012.00003.00004	12.3.4	Regionali
00012.00003.00005	12.3.5	Parlamento Europeo
00012.00004	12.4	Referendum
00012.00004.00001	12.4.1	Referendum
00012.00005	12.5	Istanze, Petizioni ed Iniziative Popolari
00012.00005.00001	12.5.1	Istanze, Petizioni ed Iniziative Popolari

00012.00005.00002 12.5.2 Cittadini

00012.00005.00003 12.5.3 Organi Politici

00012.00005.00004 12.5.4 Altri Enti

00013 13 LEVA MILITARE

00013.00001 13.1 Leva

00013.00001.00001 13.1.1 Leva

00013.00002 13.2 Ruoli matricolari

00013.00002.00001 13.2.1 Ruoli matricolari

00013.00003 13.3 Caserme, alloggi e servitù militari

00013.00003.00001 13.3.1 Caserme, alloggi e servitù militari

00013.00004 13.4 Requisizioni per utilità militari

00013.00004.00001 13.4.1 Requisizioni per utilità militari

00014 14 OGGETTI DIVERSI

00014.00001 14.1 Oggetti Diversi

00014.00001.00001 14.1.1 Oggetti Diversi

00014.00001.00002 14.1.2 Qualita' e certificazione

Comune di Genova



Allegato 6 – Piano di fascicolazione

Indice

Premessa	3
Fascicoli	3
Fascicolo per affare	4
Fascicolo per persona fisica o giuridica	4
Fascicolo per attività	5
Fascicolo per procedimento	5
Serie	5
Repertorio	5
Linee guida per la formazione e organizzazione dei fascicoli	7

Premessa

L'aggregazione e organizzazione dei documenti, oltre a essere una buona prassi archivistica, è un'operazione prescritta dal Decreto del Presidente della Repubblica 28/12/2000, n. 445, art. 65: «*Il sistema per la gestione dei flussi documentali deve: a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato*». Fascicoli e serie sono due modalità di organizzazione e aggregazione dei documenti secondo criteri logici predefiniti, citati esplicitamente dal Decreto del Presidente della Repubblica 28/12/2000, n. 445, art. 67.

Il Comune di Genova, al fine di supportare i propri utenti nella realizzazione corretta dei fascicoli e delle serie, ha predisposto questo allegato, prendendo spunto dalle Linee guida per la formazione e organizzazione dei fascicoli redatte dal Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni. Questo strumento fornisce suggerimenti pratici su come organizzare fascicoli e serie che vengono man mano prodotti nella cornice e con riferimento al piano di classificazione.

In questo documento si ripercorre la struttura del titolario, indicando quali tipologie di fascicoli si possono aprire e con quali criteri si possono costituire le serie. Il titolario, in quanto basato sulle funzioni del Comune, è astratto e prevede quello che può verificarsi, mentre l'attività concreta e quotidiana dell'Ente si stratifica in documenti che devono essere organizzati in aggregazioni e sono espressione di quanto si è effettivamente verificato. Si ricorda che i fascicoli devono essere aperti all'ultimo livello della struttura gerarchica del titolario.

Infine, si specifica che gli esempi di fascicoli e serie indicate nelle successive linee guida, in quanto tali, non devono essere riportati nella loro totalità: infatti, si rimanda per competenza alle singole Direzioni la possibilità di escludere alcuni di essi, in quanto oggetto di tematiche/procedimenti obsoleti o non più in uso.

Fascicoli

Come già definito nel Manuale di Gestione Documentale, il fascicolo è l'aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico affare/procedimento.

Si precisa che procedimento e fascicolo non sempre coincidono, in quanto talvolta un procedimento può dar luogo a più fascicoli. È il caso, ad esempio, della costruzione di alloggi popolari: il PEEP (Piano Edilizia Economica Popolare) va classificato 6.2; la costruzione va in 6.4; l'assegnazione va in 7.14.

I fascicoli sono organizzati per:

- affare = conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta
- persona fisica o giuridica = comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona fisica o giuridica. Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte
- attività = comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale
- procedimento amministrativo = conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Fascicolo per affare

Il fascicolo per affare deve essere aperto all'ultimo livello della struttura gerarchica del titolare e comprende i documenti prodotti da un ufficio per la trattazione di un affare specifico e concreto, recanti tutti la medesima classificazione. Qualche esempio di fascicoli per affare: la costruzione di un nuovo edificio comunale (titolo 6, classe 5); la realizzazione di un evento culturale (titolo 7, classe 6); l'effettuazione di un concorso o di un bando di selezione del personale (titolo 3, classe 1).

Il fascicolo per affare si individua con:

- anno di apertura
- titolo e classe
- numero del fascicolo, progressivo all'interno dell'ultimo livello della struttura gerarchica del titolare di classificazione
- oggetto (stringa di testo che descrive compiutamente l'affare o il procedimento amministrativo).

Si ricorda che il fascicolo, oltre ai dati citati in precedenza, è corredato da ulteriori metadati, richiesti obbligatoriamente dalle Linee guida vigenti.

Un esempio: 2022-7.6/13 «Alba di Ferragosto nel parco di Villa Durazzo Pallavicini», dove:

- 2022 è l'anno di apertura
- 7 è il titolo (Servizi alla persona)
- 6 è la classe (Eventi e attività culturali)
- 13 è il numero progressivo attribuito al fascicolo su base cronologica durante l'anno 2022 all'interno del titolo 7 e della classe 6.

Il fascicolo per affare ha una data di apertura, una durata circoscritta, che può non coincidere perfettamente con l'anno solare, e una data di chiusura: può comunque essere gestito su base annuale e "trasportato a nuovo anno" se non viene chiuso nell'anno di apertura.

Fascicolo per persona fisica o giuridica

Il fascicolo per persona fisica o giuridica comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona.

Il fascicolo si configura così come aggregazione di documenti diversamente classificati e si apre indipendentemente dalle classi. Si può aprire a livello di titolo (ad esempio, per i dipendenti nel Titolo 3 oppure per le ditte nel Titolo 8) o a livello di classe (ad esempio, gli assistiti del servizio sociale nelle classi 9-14 del Titolo 7 o le associazioni alla classe 17 del Titolo 1).

Ai fini dell'individuazione e della denominazione del fascicolo si considera, in genere, per i dipendenti il numero attribuito alla persona all'interno dell'organizzazione (numero di matricola), ma talvolta anche il cognome e nome: questi dati costituiscono l'elemento unificante dei documenti recanti classifiche differenti, che comunque si possono organizzare all'interno del fascicolo in sottofascicoli.

Un esempio per persona fisica: 2005-3.0.6749 «Mario Rossi». Questo fascicolo si individua quindi con:

- 2005 è l'anno di apertura
- 3 è il titolo (Risorse umane)
- 0 è la classe
- 6749 è il numero di matricola.

Un esempio per persona giuridica: 2005-8.0.86334519757 «Ipse Dixit Srl». Questo fascicolo si individua quindi con:

- 2005 è l'anno di apertura
- 8 è il titolo (Attività economiche)
- 0 è la classe
- 86334519757 è la partita IVA.

Fascicolo per attività

Il fascicolo per attività è costituito per comprendere i documenti prodotti nello svolgimento di un'attività amministrativa semplice, non discrezionale e ripetitiva, che si esaurisce in riposte obbligate o meri adempimenti. A titolo di esempio, le richieste di informazioni bibliografiche e relative risposte (titolo 7, classe 6, sottoclasse 3). Il fascicolo per attività comprende documenti con destinatari e oggetti diversi, ma con identica classificazione: di durata annuale, può articolarsi in sottofascicoli con diverse cadenze temporali (ad esempio, mensili).

Fascicolo per procedimento

Il fascicolo per procedimento è costituito per comprendere una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo. A titolo di esempio, la richiesta del permesso di costruire per edilizia privata (titolo 6, classe 3, sottoclasse 1). Il fascicolo per procedimento comprende documenti con destinatari diversi, ma con identica classificazione: di durata annuale, può articolarsi in sottofascicoli con diverse cadenze temporali (ad esempio, mensili).

Serie

Non sempre i documenti prodotti dal Comune vengono aggregati in base solo all'oggetto e quindi utilizzando il titolario di classificazione; talvolta essi costituiscono serie, in base alla tipologia documentaria (ad esempio, i decreti, le ordinanze, le deliberazioni) o di provenienza (nel senso che sono prodotti dal medesimo ufficio od organo: ad esempio, il Sindaco oppure il Consiglio).

Con il termine serie sono indicati quindi tutti i raggruppamenti, costituiti dal produttore, di documenti o di fascicoli con caratteristiche omogenee in relazione:

- alla natura e alla forma dei documenti
- all'oggetto e alla materia
- alle funzioni del produttore.

Oltre alle serie di documenti, esistono anche le serie di fascicoli: per esempio, i fascicoli personali dei dipendenti, omogenei tra di loro per contenuto e materia. La serie di fascicoli può essere costituita a livello di titolo (per esempio, la serie dei fascicoli personali dei dipendenti che si incardina nel Titolo 3 Risorse umane) oppure a livello di classe (ad esempio, la serie dei fascicoli dei soggetti a TSO nel Titolo 10 Classe 2).

Il Decreto del Presidente della Repubblica 28/12/2000, n. 445, non accenna ai criteri di costituzione e organizzazione delle serie, proprio perché si tratta di questioni legate alla natura di ciascun ente produttore, alle sue funzioni e, quindi, al piano di classificazione di cui si dota.

Repertorio

In ambiente cartaceo i repertori sono quei registri su cui si trascrivono e nei quali si inseriscono in sequenza determinata (in genere cronologica) documenti uguali per forma e/o provenienza, ma differenti per contenuto e che sono corredati da uno strumento (il repertorio, appunto), atto al reperimento del singolo documento ricercato.

I documenti repertoriati, secondo la procedura di registrazione particolare prevista dal Decreto del Presidente della Repubblica 28/12/2000, n. 445, art. 53, com. 5, che, quando elenca i documenti soggetti a registrazione obbligatoria effettuata tramite il registro di protocollo generale, unico per

l'intera AOO, annovera tra quelli esclusi «tutti i documenti già soggetti a registrazione particolare dall'amministrazione», possono e, nel caso siano su supporto informatico, devono essere registrati nel protocollo generale. Il singolo documento repertoriato viene pertanto identificato e citato tramite due numeri: quello di repertorio (ad esempio, n. 1729/2005 del repertorio delle ordinanze) e quello di protocollo generale (ad esempio, 93.812/2005). Inoltre, il singolo documento registrato in un repertorio, quando non contiene oggetti multipli (come nel caso, ad esempio, dei verbali delle riunioni di un organo collegiale), viene classificato in base alla materia che tratta. Invece il repertorio, accogliendo una prassi consolidata nei Comuni, configurandosi come una serie di documenti, non viene classificato, ma viene comunque gestito dal sistema informatico, tramite apposita funzione prevista dal software.

Questi repertori, costituiti da documenti con oggetti multipli, sono indicati in coda al titolo I, in quanto essi si riferiscono all'amministrazione generale del Comune.

Il repertorio dei fascicoli, invece, è lo strumento sul quale vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni più basse del titolario (per il Comune di Genova, il terzo livello o sottoclasse). Il repertorio dei fascicoli svolge una funzione analoga al registro di protocollo, il quale registra, all'interno dell'archivio, la presenza di un certo documento; il repertorio dei fascicoli registra, sempre all'interno dell'archivio, la presenza di un determinato fascicolo.

Linee guida per la formazione e organizzazione dei fascicoli

1. AMMINISTRAZIONE GENERALE

1.1 Legislazione e circolari esplicative

Fascicolo annuale dei pareri chiesti dal Comune su leggi specifiche (uno per ciascun parere), eventualmente articolato in sottofascicoli

Repertorio annuale, servito da indici, delle circolari pervenute al Comune

Repertorio annuale, servito da indici, delle circolari emanate dal Comune

Fascicolo della denominazione del Comune

1.2 Denominazione, territorio e confini, circostrizioni di decentramento, toponomastica

Fascicolo dell'attribuzione del titolo di città

Fascicolo dei confini del Comune

Un fascicolo per ciascuna costituzione delle circoscrizioni

Repertorio annuale dei verbali e delle deliberazioni della Commissione comunale per la toponomastica

1.3 Statuto

Fascicolo delle redazioni, modifiche e interpretazioni dello statuto

1.4 Regolamenti

Repertorio annuale dei regolamenti emessi dal Comune

Un fascicolo per ciascuna redazione dei regolamenti

1.5 Stemma, gonfalone, sigillo

Fascicolo annuale delle definizioni, modifiche, e riconoscimento dello stemma

Fascicolo annuale delle definizioni, modifiche e riconoscimento del gonfalone

Fascicolo annuale delle definizioni, modifiche e riconoscimento del sigillo

Fascicolo annuale per attività di concessione del patrocinio gratuito e del connesso uso dello stemma del Comune

1.6 Archivio generale

- Registro di protocollo
 - Repertorio dei fascicoli
 - Fascicolo annuale per l'organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolare e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati)
 - Interventi straordinari (ad esempio, traslochi, restauri, gestione servizi esterni, scelta del software di gestione): un fasc. per ciascun affare
 - Richieste di informazioni archivistiche e richieste per motivi di studio: fasc. annuale per attività, eventualmente articolato in sottofascicoli mensili
 - Schedoni (su supporto cartaceo o informatico) degli studiosi: uno per persona (in ordine alfabetico), da rinnovare ogni anno
 - Richieste di pubblicazione all'albo pretorio: fasc. annuale per attività, eventualmente articolato in sottofascicoli mensili, con allegati
 - Registro dell'Albo pretorio
 - Richieste di notifica presso la casa comunale: fasc. annuale per attività, eventualmente articolato in sottofascicoli mensili, con allegati
 - Registro delle notifiche
 - Registri delle spedizioni e delle spese postali
 - Ordinanze emanate dal Sindaco: repertorio annuale
 - Decreti del Sindaco: repertorio annuale
 - Ordinanze emanate dai dirigenti: repertorio annuale
 - Determinazioni dei dirigenti: un repertorio annuale per ciascuna UOR
 - Deliberazioni del Consiglio comunale: repertorio annuale
 - Deliberazioni della Giunta comunale: repertorio annuale
 - Verbali delle adunanze del Consiglio comunale: repertorio annuale (facoltativo)
 - Verbali delle adunanze della Giunta comunale: repertorio annuale (facoltativo)
 - Verbali degli altri organi collegiali del Comune: repertorio annuale
 - Contratti e convenzioni: un repertorio annuale per ciascuna UOR
 - Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa): repertorio
 - Deliberazioni dei Consigli circoscrizionali: un repertorio annuale per ciascun quartiere
 - Deliberazioni degli Esecutivi circoscrizionali: un repertorio annuale per ciascun quartiere
 - Verbali delle adunanze dei Consigli circoscrizionali: un repertorio annuale per ciascun quartiere
 - Verbali delle adunanze degli Esecutivi circoscrizionali: un repertorio annuale per ciascun quartiere
 - Verbali degli organi collegiali delle circoscrizioni: un repertorio annuale per ciascun quartiere
 - Registro dell'Albo della circoscrizione: un repertorio annuale per ciascun quartiere
 - Contratti e convenzioni delle circoscrizioni: un repertorio annuale per ciascun quartiere
 - Atti rogati dai segretari delle circoscrizioni (contratti e atti unilaterali in forma pubblica amministrativa): repertorio
-

1.7 Sistema informativo	<p>Fascicolo annuale per organizzazione del sistema, con eventuali sottofascicoli mensili</p> <hr/> <p>Un fascicolo per statistica</p>
1.8 Informazioni e relazioni con il pubblico	<p>Un fascicolo per ciascuna iniziativa dell'URP</p> <hr/> <p>Repertorio annuale dei reclami dei cittadini (comunque presentati: URP, UOR, Difensore civico)</p> <hr/> <p>Fascicolo annuale degli atti del Difensore civico, con eventuali sottofascicoli mensili</p> <hr/> <p>Repertoio annuale dei bandi e degli avvisi a stampa</p> <hr/> <p>Gestione del sito Web:</p> <ul style="list-style-type: none"> - fascicolo annuale dei materiali preparatori inviati dalle UOR per la pubblicazione sul sito, con eventuali sottofascicoli mensili - copie periodiche della pagina, effettuate dall'URP
1.9 Politica del personale; ordinamento degli uffici e dei servizi	<p>Fascicolo annuale delle attribuzioni di competenze agli uffici, con eventuali sottofascicoli mensili</p> <hr/> <p>Un fascicolo per ciascuna definizione dell'organigramma</p> <hr/> <p>Un fascicolo per ciascuna organizzazione degli uffici</p> <hr/> <p>Fascicolo annuale degli orari di apertura degli uffici comunali e degli altri uffici insistenti sul territorio comunale, con eventuali sottofascicoli mensili</p> <hr/> <p>Un fascicolo del materiale preparatorio per le deliberazioni in materia di politica del personale</p>
1.10 Relazioni con le organizzazioni sindacali e di rappresentanza del personale	<p>Un fascicolo per ciascun rapporto di carattere generale</p> <hr/> <p>Un fascicolo per ciascuna costituzione delle rappresentanze del personale</p> <hr/> <p>Repertorio annuale dei verbali della Delegazione trattante per la contrattazione integrativa decentrata</p>
1.11 Controlli esterni	<p>Un fascicolo per ciascun controllo</p>

	Raccolta bibliografica delle pubblicazioni istituzionali del Comune (libri, riviste, inserzioni o altro)
1.12 Editoria e attività informativo-promozionale interna ed esterna	<p>Pubblicazioni istituzionali del Comune (materiali preparatori): un fascicolo per ciascun numero</p> <p>Comunicati stampa: un fascicolo per ciascun periodo</p>
	Un fascicolo per ciascuna iniziativa specifica
1.13 Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti	<p>Onorificenze (concesse e ricevute): un fascicolo per ciascun evento</p> <p>Fascicolo annuale delle concessioni dell'uso del sigillo</p>
	Un fascicolo per ciascuna iniziativa specifica, per esempio gemellaggi, adesione a movimenti di opinione
1.14 Interventi di carattere politico e umanitario; rapporti istituzionali	<p>Un fascicolo per ciascun gemellaggio</p> <p>Promozione di comitati: un fascicolo per ciascuna iniziativa</p>
	Costituzione di enti controllati dal Comune (comprensivo della nomina dei rappresentanti e dei verbali inviati per approvazione): un fascicolo per ciascun ente
1.15 Forme associative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti): un fascicolo per ciascun ente
1.16 Area e città metropolitana	Costituzione e rapporti istituzionali: un fascicolo per ciascun anno

Un fascicolo per ciascuna politica di incoraggiamento e appoggio alle associazioni

1.17 Associazionismo e partecipazioni

Albo dell'associazionismo: elenco delle associazioni accreditate

Un fascicolo per ciascuna associazione che chiede l'iscrizione all'albo

1.18 Accesso agli atti

Fascicolo annuale delle richieste di accesso per fini amministrativi, con eventuali sottofascicoli mensili

**2. ORGANI DI
GOVERNO,
GESTIONE,
CONTROLLO,
CONSULENZA
E GARANZIA**

2.1 Sindaco

Fascicolo personale, da chiudere al termine del mandato

2.2 Vice-Sindaco

Fascicolo personale, da chiudere al termine del mandato

2.3 Consiglio

Un fascicolo per ciascun consigliere, da chiudere al termine del mandato

Fascicolo annuale delle convocazioni del Consiglio e OdG, eventualmente articolato in sottofascicoli mensili

Un fascicolo per ciascuna interrogazione e mozione consiliare (materiale preparatorio e connesso)

Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive

2.4 Presidente del Consiglio

Fascicolo personale, da chiudere al termine del mandato

2.5 Conferenza dei capigruppo e Commissioni del Consiglio

Repertorio annuale dei verbali della Conferenza dei capigruppo

Repertorio annuale dei verbali delle Commissioni, uno per ciascuna Commissione

2.6 Gruppi consiliari

Un fascicolo per ciascun Gruppo accreditato presso il Comune, da chiudere al termine del mandato

2.7 Giunta

Nomine, revoche e dimissioni degli assessori: un fascicolo per ogni assessore, da chiudere al termine del mandato

Fascicolo annuale delle convocazioni della Giunta e OdG, eventualmente articolato in sottofascicoli mensili

**2.8 Commissario
prefettizio e
straordinario**

Fascicolo personale, da chiudere al termine del mandato

**2.9 Segretario e
Vice-segretario**

Fascicolo personale, da chiudere al termine dell'incarico

**2.10 Direttore generale
e dirigenza**

Fascicolo personale, da chiudere al termine del mandato

2.11 Revisori dei conti

Fascicoli personali, da chiudere al termine del mandato

Repertorio annuale delle relazioni

2.12 Difensore civico

Fascicolo personale, da chiudere al termine del mandato

**2.13 Commissario
ad acta**

Fascicolo personale, da chiudere al termine del mandato

**2.14 Organi di controllo
interni**

Un fascicolo relativo al funzionamento di ciascun organo

Repertorio annuale delle relazioni degli organi di controllo

Un fascicolo relativo al funzionamento di ciascun organo

2.15 Organi consultivi

Repertorio annuale delle relazioni degli organi consultivi

2.16 Consigli circoscrizionali	<p>Un fascicolo per ciascun consigliere, da chiudere al termine del mandato</p> <hr/> <p>Fascicolo annuale delle convocazioni del Consiglio e OdG, con eventuali sottofascicoli mensili</p> <hr/> <p>Un fascicolo per ciascuna interrogazione e mozione consiliare (materiale preparatorio e connesso)</p> <hr/> <p>Repertorio dei bollettini della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive</p>
<hr/>	
2.17 Presidenti dei Consigli circoscrizionali	<p>Fascicoli personali, da chiudere al termine del mandato</p>
<hr/>	
2.18 Organi esecutivi circoscrizionali	<p>Nomine e dimissioni degli assessori: un fascicolo per ogni assessore, da chiudere al termine del mandato</p> <hr/> <p>Fascicolo annuale delle convocazioni della Giunta e OdG</p>
<hr/>	
2.19 Commissioni dei Consigli circoscrizionali	<p>Repertorio annuale dei verbali delle Commissioni, uno per ciascuna Commissione</p>
<hr/>	
2.20 Segretari delle circoscrizioni	<p>Fascicoli personali, da chiudere al termine dell'incarico</p>
<hr/>	
2.21 Commissario ad acta delle circoscrizioni	<p>Fascicolo personale, da chiudere al termine del mandato</p>
<hr/>	
2.22 Conferenza dei Presidenti di quartiere	<p>Repertorio annuale dei verbali della Conferenza dei Presidenti di quartiere</p>

3. RISORSE UMANE

Un fascicolo per ogni dipendente o assimilato, inclusi collaboratori a contratto o a progetto.

Si rimanda al paragrafo "Fascicolo per persona fisica o giuridica" per le possibili modalità di individuazione del fascicolo

3.1 Concorsi, selezioni, colloqui

Criteri generali e normativa per il reclutamento del personale: un fascicolo con eventuali sottofascicoli

Un fascicolo per ciascun procedimento di reclutamento personale, con sottofascicoli: bando e manifesto, domande, allegati, verbali, prove d'esame scritte, copie bando restituite al Comune

Serie dei curricula inviati per richieste di assunzione

Serie delle domande di assunzione pervenute senza indizione di concorso o selezione

3.2 Assunzioni e cessazioni

Criteri generali e normativa per le assunzioni e cessazioni: un fascicolo con eventuali sottofascicoli

Determinazioni di assunzione e cessazione (nomine, licenziamenti, dimissioni, promessa solenne, giuramento, nomina in prova), da inserire nei rispettivi fascicoli personali

3.3 Comandi e distacchi; mobilità

Criteri generali e normativa per comandi, distacchi, mobilità: un fascicolo con eventuali sottofascicoli

Determinazioni individuali di comandi, distacchi e mobilità, da inserire nei rispettivi fascicoli personali

3.4 Attribuzione di funzioni, ordini di servizio e missioni

Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni: un fascicolo con eventuali sottofascicoli

Determinazioni, da inserire nei rispettivi fascicoli personali

Repertorio annuale degli ordini di servizio collettivi

Autorizzazioni allo svolgimento di attività esterne, da inserire nei fascicoli personali

3.5 Inquadramenti e applicazione contratti collettivi di lavoro

Criteri generali e normativa per gli inquadramenti e le applicazioni dei contratti collettivi di lavoro: un fascicolo con eventuali sottofascicoli

Determinazione dei ruoli e contratti: un fascicolo per ciascun procedimento

Determinazioni, da inserire nei rispettivi fascicoli personali

3.6 Retribuzioni e compensi	<p>Criteria generali e normativa per le retribuzioni e compensi: un fascicolo con eventuali sottofascicoli</p> <hr/> <p>Database dell'anagrafe delle prestazioni</p> <hr/> <p>Database e tabulati dei ruoli degli stipendi</p> <hr/> <p>Determinazioni relative ai singoli per la definizione delle voci accessorie dello stipendio, da inserire nei rispettivi fascicoli personali</p> <hr/> <p>Provvedimenti giudiziari di requisizione dello stipendio</p>
3.7 Adempimenti fiscali, contributivi e assicurativi	<p>Criteria generali e normativa per il trattamento fiscale, contributivo e assicurativo: un fascicolo con eventuali sottofascicoli</p> <hr/> <p>Determinazioni specifiche e provvedimenti circa il trattamento fiscale, contributivo e assicurativo, da inserire nei rispettivi fascicoli personali</p> <hr/> <p>Assicurazioni obbligatorie, da inserire nei rispettivi fascicoli personali</p>
3.8 Tutela della salute e sicurezza sul luogo di lavoro	<p>Fascicolo dei criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro</p> <hr/> <p>Rilevazione dei rischi, ai sensi della 626/94: un fascicolo per ciascuna sede</p> <hr/> <p>Prevenzione infortuni: un fascicolo per ciascun procedimento</p> <hr/> <p>Repertorio dei registri infortuni</p> <hr/> <p>Repertorio dei verbali delle rappresentanze dei lavoratori per la sicurezza</p> <hr/> <p>Denuncia di infortunio e relativa pratica, da inserire nei rispettivi fascicoli personali</p> <hr/> <p>Fascicoli relativi alle visite mediche ordinarie: un fascicolo per ciascuna campagna di visite</p>
3.9 Dichiarazioni di infermità ed equo indennizzo	<p>Criteria generali e normativa per le dichiarazioni di infermità: un fascicolo con eventuali sottofascicoli</p> <hr/> <p>Dichiarazioni di infermità e calcolo dell'indennizzo: un fascicolo per ciascun procedimento, da inserire nel relativo fascicolo personale</p>
3.10 Indennità premio di servizio e trattamento di fine rapporto, quiescenza	<p>Criteria generali e normativa per il trattamento di fine rapporto: un fascicolo con eventuali sottofascicoli</p> <hr/> <p>Trattamento pensionistico e di fine rapporto: un fascicolo per ciascun affare, da inserire nel relativo fascicolo personale</p>

3.11 Servizi al personale su richiesta	Criteri generali e normativa per i servizi su richiesta: un fascicolo con eventuali sottofascicoli
	Domande di servizi su richiesta: un fascicolo per periodo
3.12 Orario di lavoro, presenze e assenze	Criteri generali e normativa per le assenze: un fascicolo con eventuali sottofascicoli
	Domande e dichiarazioni dei dipendenti sull'orario e sulle assenze, da inserire nel fascicolo personale
	Referti delle visite di controllo, da inserire nei fascicoli personali
	Fascicolo annuale dei fogli firma, cartellini marcatempo e tabulati elettronici di rilevazione presenze, con eventuali sottofascicoli mensili
	Rilevazioni delle assenze per sciopero: un fascicolo per ciascuno sciopero
3.13 Giudizi, responsabilità e provvedimenti disciplinari	Criteri generali e normativa per i provvedimenti disciplinari: un fascicolo con eventuali sottofascicoli
	Un fascicolo per ciascun provvedimento disciplinare, da inserire nel relativo fascicolo personale
3.14 Formazione e aggiornamento professionale	Criteri generali e normativa per la formazione e l'aggiornamento professionale: un fascicolo con eventuali sottofascicoli
	Organizzazione di corsi di formazione e aggiornamento: un fascicolo per ciascun corso
	Partecipazione dei dipendenti a corsi: inserire le singole domande nel relativo fascicolo personale
3.15 Collaboratori esterni	Criteri generali e normativa per il trattamento dei collaboratori esterni: un fascicolo con eventuali sottofascicoli
	Repertorio degli elenchi degli incarichi conferiti

**4 RISORSE
FINANZIARIE E
PATRIMONIO**

4.1 Entrate

Un fascicolo per ciascun contribuente comunale in rapporto a ciascun tipo di imposte, con eventuali sottofascicoli (variazioni, ricorsi, ecc.)

Database dei seguenti ruoli: ICI, imposta comunale sulla pubblicità, diritti sulle pubbliche affissioni, TARSU, COSAP

Contratti di mutuo: un fascicolo per ciascun mutuo

Proventi da affitti e locazioni: un fascicolo annuale per ciascun immobile locato

Diritti di segreteria: registri annuali o pagamenti virtuali

Registri annuali delle matrici dei bollettari delle entrate

Ricevute dei versamenti alla tesoreria delle somme riscosse nelle differenti UOR per diritti di segreteria

Repertorio annuale delle fatture emesse

Repertorio annuale delle reversali

Repertori annuali dei bollettari vari

Fascicolo annuale per ricevute di pagamenti vari, eventualmente articolato in sottofascicoli mensili

4.2 Uscite

Repertorio annuale degli impegni di spesa (determinazioni dei dirigenti delle UOR) inviate dalle UOR alla Ragioneria

Repertorio annuale delle fatture ricevute

Repertorio annuale degli atti di liquidazione con allegati trasmessi da ciascuna UOR, se sono distinti dai mandati, oppure allegati ai mandati stessi

Repertorio annuale dei mandati di pagamento con allegati emessi dalla Ragioneria e inviati alla Tesoreria

4.3 Partecipazioni finanziarie

Gestione delle partecipazioni finanziarie: un fascicolo per ciascuna partecipazione

4.4 Bilancio preventivo, variazioni di bilancio, verifiche contabili

Bilancio preventivo e allegati (organizzati in fascicoli): un fascicolo per ciascuna risorsa o ciascun intervento, tra cui Relazione previsionale e programmatica

Gestione: un fascicolo per ciascuna variazione

4.5 Piano esecutivo di gestione (PEG)

PEG, articolato in fascicoli: un fascicolo per ciascun obiettivo. I fascicoli possono essere organizzati in serie in riferimento ai responsabili dei servizi

Gestione: un fascicolo per ciascuna variazione

4.6 Rendiconto della gestione

Rendiconto della gestione, articolato in Conto del bilancio, Conto del patrimonio e Conto economico

4.7 Adempimenti fiscali

Mod. 770: un fascicolo per ogni anno

Ricevute dei versamenti (IVA, IRPEF, ecc.): un fascicolo per ciascuna tipologia di imposta per ciascun periodo

Pagamento dei premi dei contratti assicurativi

4.8 Inventari e consegnatari dei beni

Registro o database perenne dell'inventario dei beni immobili

4.9 Beni immobili

Un fascicolo per ciascun bene immobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: acquisizione, gestione, uso, alienazione e dismissione

Repertorio delle concessioni di occupazione di spazi e aree pubbliche

Repertorio delle concessioni di beni del demanio statale

Repertorio delle concessioni cimiteriali

Un fascicolo per ciascun concessionario

Inventari dei beni mobili: uno per consegnatario

4.10 Beni mobili

Un fascicolo per ciascun bene mobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: acquisizione, manutenzione, concessione in uso, alienazione e altre forme di dismissione. In alternativa, si possono prevedere fascicoli annuali per attività

4.11 Economato	Un fascicolo per ciascuna acquisizione di beni e servizi, eventualmente organizzati in serie connesse ai Centri di spesa

	Repertorio dell'elenco dei fornitori

	Repertorio annuale dei verbali di rinvenimento

4.12 Oggetti smarriti e recuperati	Repertorio annuale delle ricevute di riconsegna ai proprietari

	Vendita o devoluzione: fascicolo periodico

4.13 Tesoreria	Repertorio annuale dei giornali di cassa

	Mandati quietanzati, che vengono inviati in Ragioneria: repertorio periodico (mese/anno)

4.14 Concessionari ed altri incaricati della riscossione delle entrate	Un fascicolo per ciascun concessionario

	Repertorio annuale delle autorizzazioni alla pubblicità stabile

4.15 Pubblicità e pubbliche affissioni	Repertorio annuale delle autorizzazioni alla pubblicità circoscritta

	Un fascicolo per ciascuna richiesta di affissione (con allegati da affiggere)

**5. AFFARI
LEGALI****5.1 Contenzioso**

Un fascicolo per ciascuna causa. A seconda delle esigenze, la serie dei fascicoli di causa può essere suddivisa in sottoserie (cause civili, cause amministrative, cause penali, cause tributarie). Ciascun fascicolo può articolarsi in sottofascicoli (fasi della causa, ecc.)

**5.2 Responsabilità
civile e patrimoniale
verso terzi;
assicurazioni**

Un fascicolo per ciascun contratto assicurativo

Un fascicolo per ciascuna richiesta e pratica di risarcimento

5.3 Pareri e consulenze

Un fascicolo per ciascun parere/consulenza

**6.
PIANIFICAZIONE
E GESTIONE DEL
TERRITORIO**

Fascicolo annuale del PRG

**6.1 Urbanistica: piano
regolatore generale e
varianti**

Fascicolo annuale dei pareri su piani
sovracomunali

Fascicolo annuale dei certificati di
destinazione urbanistica

Un fascicolo per ciascuna variante al PRG

**6.2 Urbanistica:
strumenti di attuazione
del piano regolatore
generale**

Un fascicolo per ciascun piano:
particolareggiati, di lottizzazione, PEEP, PI,
PAT, PATI, PRRUST, PPIS, PIP

Un fascicolo per ciascun programma:
PIRU, PIRUEA, di riqualificazione urbana e di
sviluppo sostenibile del territorio

6.3 Edilizia privata

Repertorio annuale delle autorizzazioni
edilizie

Un fascicolo per ciascun richiedente di
autorizzazione

Un fascicolo per abusi accertati e repressi

Repertorio annuale delle denunce e relazioni
finali delle opere in cemento armato

6.4 Edilizia pubblica

Un fascicolo per ciascuna costruzione di edilizia popolare

Un fascicolo per ciascuna opera pubblica realizzata

6.5 Opere pubbliche

Un fascicolo annuale per ciascuna attività di manutenzione ordinaria. In alternativa, un fascicolo per ciascun edificio

Un fascicolo per ciascun intervento di manutenzione straordinaria

6.6 Catasto

Catasto terreni: mappe, registri, indice alfabetico dei possessori, estratti catastali, denunce di variazione

Catasto fabbricati: mappe, registri, indice alfabetico dei possessori, estratti catastali, denunce di variazione

6.7 Viabilità

Un fascicolo per ciascun Piano Urbano del Traffico

Un fascicolo per ciascun Piano Urbano della Mobilità

Repertorio annuale delle autorizzazioni in deroga

6.8 Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi

Un fascicolo annuale per organizzazione e funzionamento di approvvigionamento idrico o produzione di energia elettrica o altre fonti energetiche, con eventuali sottofascicoli mensili

Un fascicolo per ciascun utente titolare di contratto di distribuzione dell'acqua, di energia elettrica o altre fonti energetiche

Un fascicolo annuale per gestione trasporti pubblici, con eventuali sottofascicoli mensili

Un fascicolo annuale per vigilanza sui gestori dei servizi, con eventuali sottofascicoli mensili: in caso di anomalie, un fascicolo per ciascuna anomalia

Un fascicolo annuale per ciascuna iniziativa di sensibilizzazione degli utenti per consumi razionali

Repertorio annuale delle dichiarazioni di conformità degli impianti

6.9 Ambiente: autorizzazioni, monitoraggio e controllo

Un fascicolo per ciascuna iniziativa a favore dell'ambiente

Un fascicolo per ciascuna valutazione e parere di impatto ambientale

Fascicolo annuale per monitoraggi di qualità (acque, aria, etere, ecc.), con eventuali sottofascicoli mensili: in caso di irregolarità, un fascicolo per ciascuna irregolarità

Fascicolo annuale per controlli a campione sugli impianti termici dei privati, con eventuali sottofascicoli mensili: in caso di irregolarità, un fascicolo per ciascuna irregolarità

6.10 Protezione civile ed emergenze

Fascicolo annuale delle segnalazioni preventive di condizioni metereologiche avverse

Fascicolo annuale degli addestramenti ed esercitazioni per la protezione civile

Interventi per emergenze: un fascicolo per ciascuna emergenza

7. SERVIZI ALLA PERSONA

Un fascicolo per ciascuna persona assistita.

Si rimanda al paragrafo "Fascicolo per persona fisica o giuridica" per le possibili modalità di individuazione del fascicolo

7.1 Diritto allo studio e servizi

Un fascicolo per ciascun bando per concessione di borse di studio, articolato in sottofascicoli per bando, domande, graduatorie e assegnazioni

Distribuzione buoni libro: un fascicolo per ciascuna scuola

Gestione buoni pasto degli iscritti alle scuole: un fascicolo per ciascun periodo

Repertorio dei verbali del comitato genitori per la mensa

Un fascicolo per ciascuna azione di promozione e sostegno del diritto allo studio

Un fascicolo per ciascuna mensa scolastica e per ciascun periodo di gestione delle mense scolastiche

Un fascicolo per ciascuna integrazione di neo-immigrati e nomadi

Gestione trasporto scolastico: un fascicolo per ciascun periodo e per ciascuna tratta

7.2 Asili nido e scuola materna

Domande di ammissione agli asili nido e alle scuole materne: un fascicolo per ciascun asilo/scuola

Graduatorie di ammissione: un fascicolo per ciascun asilo/scuola

Funzionamento degli asili e delle scuole materne: un fascicolo per ciascuna struttura

7.3 Promozione e sostegno delle istituzioni di istruzione e della loro attività

Un fascicolo per ciascuna iniziativa specifica

Repertorio dei registri scolastici (del professore e della classe) prodotti dalle scuole civiche

7.4 Orientamento professionale; educazione degli adulti; mediazione culturale

Un fascicolo per ciascuna iniziativa specifica

7.5 Istituti culturali (Musei, biblioteche, teatri, Scuola comunale di musica, ecc.)	Funzionamento delle istituzioni culturali: un fascicolo per ciascun istituto
	Repertorio dei verbali degli organi di gestione degli istituti culturali
7.6 Attività ed eventi culturali	Fascicolo annuale per ciascuna attività ordinaria
	Un fascicolo per ciascun evento culturale
	Un fascicolo per ciascuna festa civile e/o religiosa
	Un fascicolo per ciascuna iniziativa culturale
	Un fascicolo per ciascun prestito di beni culturali
7.7 Attività ed eventi sportivi	Un fascicolo per ciascun evento/attività sportiva
7.8 Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale	Fascicolo annuale dei piani sociali, con eventuali sottofascicoli
	Programmazione per settori: un fascicolo per settore
	Accordi con i differenti soggetti: un fascicolo per ciascun soggetto
7.9 Prevenzione, recupero e reintegrazione dei soggetti a rischio	Un fascicolo per ciascuna campagna di prevenzione
	Un fascicolo per ciascun intervento di recupero e reintegrazione dei soggetti a rischio
	Un fascicolo per ciascuna ricognizione dei rischi

**7.10 Informazione,
consulenza ed
educazione civica**

Funzionamento e attività delle strutture (consultori, informagiovani, ecc.): un fascicolo annuale per ciascuna struttura, con eventuali sottofascicoli

Un fascicolo per ciascuna iniziativa di vario tipo

**7.11 Tutela e curatela
di incapaci**

Un fascicolo per ciascun intervento per le persone sottoposte a tutela e curatela

**7.12 Assistenza
diretta e indiretta,
benefici economici**

Funzionamento e attività delle strutture (cucine economiche, dormitori, servizio domiciliare, telesoccorso, ecc.): un fascicolo annuale per ciascuna struttura

Un fascicolo per ciascuna iniziativa specifica

**7.13 Attività
ricreativa e di
socializzazione**

Funzionamento e attività delle strutture (colonie, centri ricreativi, ecc.): un fascicolo annuale per ciascuna struttura

Un fascicolo per ciascuna iniziativa specifica

**7.14 Politiche per la
casa**

Un fascicolo per ciascun bando di assegnazione degli alloggi, organizzato in sottofascicoli per bando, domande, graduatoria e assegnazione

Un fascicolo per ciascun assegnatario

8. ATTIVITA' ECONOMICHE

Un fascicolo per ciascun esercente di attività economica.

Si rimanda al paragrafo "Fascicolo per persona fisica o giuridica" per le possibili modalità di individuazione del fascicolo

8.1 Agricoltura e pesca

Un fascicolo per ciascuna iniziativa specifica

Comunicazioni di vendita dei prodotti ricavati dalla propria terra: un fascicolo per ciascun periodo

8.2 Artigianato

Un fascicolo per ciascuna iniziativa specifica

Repertorio delle autorizzazioni artigiane

8.3 Industria

Un fascicolo per ciascuna iniziativa specifica

Un fascicolo per ciascun accertamento dell'impatto ambientale degli insediamenti industriali

8.4 Commercio

Un fascicolo per ciascuna iniziativa specifica

Comunicazioni dovute (ferie, saldi, ecc.): un fascicolo per ciascun periodo (mese o anno)

Repertorio delle autorizzazioni commerciali

8.5 Fiere e mercati

Un fascicolo per ciascuna iniziativa specifica

8.6 Esercizi turistici e strutture ricettive

Un fascicolo per ciascuna iniziativa specifica del Comune in materia

Repertorio delle autorizzazioni turistiche

8.7 Promozione e servizi

Un fascicolo per ciascuna iniziativa specifica

**9. POLIZIA
LOCALE E
SICUREZZA
PUBBLICA**

**9.1 Prevenzione ed
educazione
stradale**

Un fascicolo per ciascuna iniziativa specifica di prevenzione

Un fascicolo per ciascun corso di educazione stradale nelle scuole

9.2 Polizia stradale

Un fascicolo di direttive e disposizioni, con eventuali sottofascicoli

Un fascicolo annuale per l'organizzazione del servizio di pattugliamento, con eventuali sottofascicoli mensili

Repertorio annuale dei verbali di accertamento di violazioni al Codice della strada

Un fascicolo per ciascun accertamento di violazioni al Codice della strada e conseguente erogazione di sanzioni (pecuniarie, amministrative, penali)

Repertorio annuale dei verbali di rilevazione incidenti

Un fascicolo annuale delle statistiche delle violazioni e degli incidenti, con eventuali sottofascicoli mensili

Un fascicolo per ciascun veicolo rimosso

9.3 Informative

Un fascicolo per ciascuna persona residente nel Comune

**9.4 Sicurezza e
ordine pubblico**

Un fascicolo annuale di direttive e disposizioni generali

Un fascicolo annuale per servizio ordinario di pubblica sicurezza

Un fascicolo per ciascun servizio straordinario di pubblica sicurezza, in caso di eventi particolari (manifestazioni, concerti, etc.)

Repertorio annuale delle autorizzazioni di pubblica sicurezza, con eventuali sottoserie per ciascuna categoria obbligata alla richiesta di autorizzazione

Un fascicolo per ciascun richiedente l'autorizzazione di pubblica sicurezza

Repertorio annuale dei verbali degli accertamenti nei diversi settori, uno per ciascun settore di accertamento

**10. TUTELA
DELLA SALUTE****10.1 Salute e igiene
pubblica**

Un fascicolo per ciascuna emergenza sanitaria

Un fascicolo per ciascuna misura di igiene pubblica

Un fascicolo per ciascun intervento di derattizzazione,
dezanarizzazione, ecc.

Un fascicolo per ciascun trattamento fitosanitario e di
disinfestazione

Un repertorio annuale delle autorizzazioni sanitarie

Un fascicolo per ciascuna persona o ditta richiedente
autorizzazioni sanitarie

Un repertorio annuale delle concessioni di agibilità

Un fascicolo per ciascun richiedente l'agibilità

**10.2 Trattamento
Sanitario Obbligatorio**

Un fascicolo per ciascun procedimento TSO

Un fascicolo per ciascun procedimento ASO

Un fascicolo personale per ciascuno dei soggetti a
trattamento

10.3 Farmacie

Un fascicolo per ciascuna farmacia istituita

Un fascicolo per ciascun periodo (mese o anno) di
funzionamento delle farmacie

**10.4 Zooprofilassi
veterinaria**

Un fascicolo per ciascun evento di epizoozia (epidemia
animale)

**10.5 Randagismo
animale e ricoveri**

Un fascicolo per ciascun procedimento di gestione dei
ricoveri e degli eventi connessi

**11. SERVIZI
DEMOGRAFICI****11.1 Stato civile**

Un repertorio annuale per ciascuno dei seguenti registri:
- Nati
- Morti
- Matrimoni
- Cittadinanza

Comunicazioni dei nati all'Agenzia per le entrate: un fascicolo per ciascun periodo

Atti per registrazioni: un fascicolo per ciascun procedimento

Atti per annotazioni sui registri di stato civile: un fascicolo per ciascun periodo

**11.2 Anagrafe e
certificazioni**

APR 4: iscrizioni anagrafiche: un fascicolo per ciascuna persona

AIRE: un fascicolo per ciascuna persona

Richieste certificati: un fascicolo per ciascun periodo (mese o anno)

Corrispondenza con altre amministrazioni per rilascio e trasmissione documenti: un fascicolo per ciascun periodo

Cartellini per carte d'identità: uno per ciascuna persona

Carte d'identità scadute e riconsegnate: un fascicolo per ciascuna persona

Cambi di abitazione e residenza: un fascicolo per ciascuna persona

Cancellazioni: un fascicolo per ciascuna persona

Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fascicolo per ciascun periodo

Database dei registri della popolazione

11.3 Censimenti

Schedoni statistici del censimento

Atti preparatori e organizzativi

**11.4 Polizia
mortuaria e
cimiteri**

Un repertorio per ciascuno dei seguenti registri:

- Seppellimento
- Tumulazione
- Esumazione
- Estumulazione
- Cremazione
- Distribuzione topografica delle tombe con annesse schede onomastiche

Un fascicolo per ciascun trasferimento di salma

12. ELEZIONI E INIZIATIVE POPOLARI	12.1 Albi elettorali	Albo dei presidenti di seggio: un elenco per ciascuna elezione
		Albo degli scrutatori: un elenco per ciascuna elezione
		Liste generali e sezionali
	12.2 Liste elettorali	Repertorio dei verbali della commissione elettorale comunale
		Copia dei verbali della Commissione elettorale mandamentale in ordine alle operazioni e deliberazioni adottate dalla Commissione elettorale comunale
		Schede dello schedario generale e degli schedari sezionali
		Un fascicolo personale per ciascun elettore
		Elenchi recanti le proposte di variazione delle liste elettorali
		Carteggio concernente la tenuta e la revisione delle liste elettorali
		Convocazione dei comizi elettorali: un fascicolo per ciascuna elezione
	12.3 Elezioni	Manifesto di presentazione delle liste
		Presentazione delle liste: un fascicolo per ciascuna elezione, eventualmente articolato in sottofascicoli (uno per lista) oppure, un fascicolo per ciascuna lista
		Atti relativi alla costituzione e arredamento dei seggi
		Repertorio dei verbali dei presidenti di seggio
		Schede
Atti preparatori		
12.4 Referendum	Atti relativi alla costituzione e arredamento dei seggi	
	Repertorio dei verbali dei presidenti di seggio	
	Schede	
12.5 Istanze, petizioni e iniziative popolari	Un fascicolo per ciascuna raccolta di firme per referendum previsti dallo statuto	

**13. LEVA
MILITARE**

Una lista di leva per anno in doppio originale, uno trattenuto dal Comune, uno inviato al Distretto militare

13.1 Leva

Una lista degli eliminati/esentati per anno in doppio originale, uno trattenuto dal Comune, uno inviato al Distretto militare

13.2 Ruoli matricolari

Un fascicolo annuale in doppio originale, uno trattenuto dal Comune, uno inviato al Distretto militare

**13.3 Caserme, alloggi e
servitù militari**

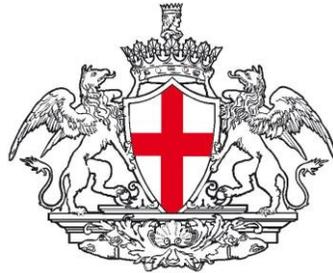
Un fascicolo per ciascun procedimento specifico

**13.4 Requisizioni per
utilità militari**

Un fascicolo per ciascun procedimento specifico

14. OGGETTI DIVERSI**14.1. Oggetti diversi**

Comune di Genova



Allegato 7 – Massimario di scarto

Premessa

Il presente massimario rappresenta lo strumento archivistico deputato all'identificazione dei documenti ritenuti rilevanti e come tali destinati alla conservazione illimitata e/o dei documenti da avviare allo scarto. È redatto allo scopo di uniformare e snellire le operazioni necessarie all'eliminazione definitiva di una parte della documentazione prodotta o ricevuta dall'Ente che non si ritiene opportuno conservare e consente di individuare la documentazione che dovrà essere conservata illimitatamente in un contesto storico omogeneo e consultabile, in quanto testimonianza storica dell'attività amministrativa dell'Ente.

Esso infatti si compone di due parti: la prima indica la documentazione fondamentale che deve essere conservato senza limiti di tempo; la seconda, invece, la documentazione che può essere proposta per lo scarto dopo il periodo minimo di conservazione espressamente indicato per le varie tipologie. Tuttavia anche in tale seconda parte viene prevista la conservazione illimitata per atti o documenti che rappresentano la riepilogazione e la sintesi delle notizie contenute nel materiale proponibile per lo scarto, assicurando così la conservazione delle informazioni essenziali.

Si rileva che il massimario, per la grande varietà di tipologie documentarie presenti nell'archivio comunale, accentuatasi specialmente negli ultimi decenni, non ha la pretesa di essere completamente esaustivo, di comprendere cioè ogni sorta di atto o documento che possa essere prodotto nel corso della quotidiana attività amministrativa.

Parte prima:

DISPOSIZIONI GENERALI

1. Documento: demanio pubblico e bene culturale.

Gli artt. 822 e 824 del Codice Civile stabiliscono che gli archivi e i documenti degli enti pubblici sono soggetti al regime del demanio pubblico e pertanto sono inalienabili; inoltre, il citato "Codice dei beni culturali" - D.Lgs. n. 42/2004 - stabilisce che tutti i documenti e archivi degli enti pubblici appartengono al Patrimonio culturale nazionale (artt. 2 e 10). Secondo tali norme, gli archivi e i documenti pubblici sono sempre da considerarsi beni culturali, indipendentemente dalla loro età, tipologia o contenuto; dunque, tutti i documenti prodotti, ricevuti o conservati a qualsiasi titolo da una pubblica amministrazione possiedono fin dall'origine la duplice natura di atti pubblici e di beni culturali. È necessario segnalare, pertanto, che ogni attività attinente alla gestione degli archivi è un'attività pratica, operativa, e, nel contempo, subordinata a dettami scientifici e metodologici rigorosi in quanto gli atti, portatori e testimoni di diritti e interessi pubblici e privati, vanno preservati da ogni alterazione, falsificazione e sottrazione, evitando ogni forma di uso improprio.

2. Archivio.

Ogni documento prodotto o acquisito dall'Ente è parte di un insieme organico e strutturato di documenti e di informazioni che rispecchiano la concreta attività amministrativa. Le relazioni che si stabiliscono tra i documenti in corso dell'attività istituzionali sono stabilite e sono il risultato del modo concreto in cui l'ente esercita i propri compiti. L'archivio è, quindi, il sistema all'interno del quale i documenti sono organizzati e reciprocamente collegati. Di conseguenza è necessario che i documenti vengano organizzati e fascicolati, già nell'archivio corrente, secondo regole certe e funzionali, sulla base del Titolare di classificazione, allo scopo di svolgere i compiti che gli sono stati affidati. L'archiviazione dei documenti, sia digitali/informatici che cartacei, ha l'obiettivo, infatti, di fornire supporto all'Ente nell'esercizio dell'attività amministrativa, di consentire la conservazione nel tempo dei documenti garantendone l'autenticità e l'integrità, l'accessibilità nel tempo, nel rispetto delle disposizioni in materia di tutela dei dati personali.

3. Scarto documentale.

Lo scarto d'archivio è l'operazione mediante la quale si provvede all'eliminazione dei documenti che hanno esaurito la loro validità giuridico-amministrativa e che, nello stesso tempo, si ritengono privi di interesse quali fonti storiche. La periodica eliminazione di tali documenti è funzionale ad una ordinata gestione dell'archivio e permette di garantire la conservazione ottimale di quanto si ritiene investito di valore permanente. Lo scarto costituisce, inoltre, il risultato di un'operazione di notevole rilevanza culturale, ovvero la selezione di quelle fonti documentarie che la nostra epoca ritiene di tramandare alle generazioni future per consentire una migliore conoscenza di sé. Lo scarto documentale è subordinato ad autorizzazione delle Soprintendenze archivistica e bibliografiche competenti territorialmente (art. 21, c. 1 lett. d), D. Lgs 42/2004). È considerata una forma di scarto anche la cancellazione di documenti informatici. Il criterio fondamentale della selezione è quello di tutelare, per scopi giuridico-amministrativi e per finalità storiche, la testimonianza essenziale delle funzioni istituzionali svolte. L'operazione di scarto si realizza con l'eliminazione definitiva di una parte della documentazione che l'amministrazione ha prodotto o ricevuto nello svolgimento della sua attività. Pertanto, presupposto dello scarto, è l'attività di valutazione della documentazione attraverso la quale si attribuisce alle carte un valore amministrativo, legale e di testimonianza storica.

4. La procedura di autorizzazione allo scarto.

L'autorizzazione allo scarto o all'eliminazione di documenti di archivi pubblici o degli archivi privati per i quali sia intervenuta la dichiarazione di interesse culturale l'autorizzazione allo scarto è un procedimento amministrativo ad istanza di parte di competenza della soprintendenza archivistiche e bibliografiche secondo quanto disposto dall'art. 21, c. 1, lett. d), del d.lgs. 22 gennaio 2004, n. 42 ("Codice dei beni culturali e del paesaggio"). L'istanza è corredata da determina dirigenziale, con allegata tabella che dettagli la documentazione da scartare, e motivi la decisione allo scarto. La tabella contiene i seguenti campi:

- 1) descrizione degli atti che si intende scartare, con indicazione, ove possibile, dell'indice di classificazione relativo;
- 2) estremi cronologici;
- 3) numero pezzi (faldoni, buste, pacchi, fogli...);
- 4) peso in kg.;
- 5) motivazione dell'eliminazione

La soprintendenza, valutato il materiale oggetto della istanza, ai sensi dell'allegato I del D.P.C.M. 22 dicembre 2010 n. 271, ha l'obbligo di concludere il procedimento, entro 60 giorni dalla ricezione della richiesta, fatta salva la richiesta di maggiori informazioni, che interrompe il termine citato. A valutazione esperita la Soprintendenza può rilasciare un'autorizzazione totale o parziale motivando, in quest'ultimo caso, le ragioni alla base dell'esclusione dallo scarto dei documenti indicati.

Parte seconda:

DOCUMENTAZIONE DA CONSERVARE SENZA LIMITI DI TEMPO

- (1) Deliberazioni destinate a formare la raccolta ufficiale del Consiglio e della Giunta (sono equiparate alle deliberazioni degli organi collegiali le determinazioni dirigenziali);
- (2) Protocolli della corrispondenza;
- (3) Inventari, schedari, rubriche e repertori dell'archivio, libretti o schede di trasmissione di carte tra i vari uffici, anche non più in uso;
- (4) Inventari dei beni mobili e immobili del Comune;
- (5) Regolamenti e capitolati d'oneri;
- (6) Fascicoli del personale in servizio e in quiescenza, di ruolo e non di ruolo;
- (7) Ruoli riassuntivi del personale e Libri matricola;
- (8) Libri infortuni o documentazione equivalente;
- (9) Posizioni previdenziali, stipendiali, tributarie dei dipendenti quando non integralmente conservate nei fascicoli personali;
- (10) Fascicoli degli amministratori e dei membri delle commissioni;
- (11) Ordinanze e circolari del Comune;
- (12) Registri dei verbali e protocolli delle commissioni comunali;
- (13) Bilanci e consuntivi originali (o nell'unica copia esistente);
- (14) Libri mastri, libri giornale, verbali di chiusura dell'esercizio finanziario;
- (15) Libri contabili obbligatori in base alle leggi fiscali;
- (16) Documentazione generale per la richiesta di mutui, anche estinti;
- (17) Contratti;
- (18) Rilevazioni di carattere statistico non pubblicate;
- (19) Corrispondenza, salvo quanto indicato nella seconda parte;
- (20) Originali dei verbali delle commissioni di concorso;
- (21) Atti relativi ai lavori pubblici, eseguiti e non eseguiti, limitatamente a: originali dei progetti e dei loro allegati, perizie di spesa, libri delle misure;
- (22) Verbali delle procedure di gara;
- (23) Atti e documenti del contenzioso legale;
- (24) Elenchi dei poveri;
- (25) Ruoli delle imposte comunali;
- (26) Corrispondenza generale del servizio esattoria e tesoreria;
- (27) Tariffe delle imposte di consumo e delle altre tasse riscosse a tariffa;
- (28) Verbali delle commissioni elettorali;
- (29) Liste di leva e dei renitenti;
- (30) Ruoli matricolari;

- (31) Piani regolatori generali e particolareggiati; piani delle lottizzazioni; regolamenti edilizi; licenze, concessioni e autorizzazioni edilizie;
- (32) Piani commerciali; licenze e autorizzazioni amministrative all'esercizio del commercio fisso;
- (33) Piani economici dei beni silvo-pastorali;
- (34) Programmi pluriennali di attuazione e piani di suddivisione in lotti delle aree suscettibili di attività estrattiva;
- (35) Relazioni annuali dell'Ufficiale sanitario;
- (36) Registro delle popolazioni comprensivo dei fogli di famiglia eliminati, registri e specchi riassuntivi del movimento della popolazione;
- (37) Verbali di sezione per l'elezione dei consigli comunali e dei consigli circoscrizionali;
- (38) Atti delle Commissioni elettorali mandamentali concernenti la presentazione delle candidature (eventualmente salvo la parte più analitica);
- (39) Schede personali delle vaccinazioni;
- (40) Schedario dell'ONMI;
- (41) Qualunque atto o documento per il quale la legge speciale imponga la conservazione illimitata.

PARTE TERZA

DOCUMENTAZIONE PER LA QUALE PUO' ESSERE PROPOSTO LO SCARTO

A) Documentazione eliminabile dopo cinque anni

CATEGORIA I: AMMINISTRAZIONE

- (1) Rubriche interne per il calcolo dei congedi e delle aspettative;
- (2) Atti rimessi da altri Enti per l'affissione all'albo;
- (3) Atti rimessi da altri Enti per notifiche;
- (4) Copie di atti notori;
- (5) Carteggi per la richiesta di atti notori e di certificati diversi con eventuale copia degli stessi;
- (6) Bollettari di prelevamento oggetti dall'Economato;
- (7) Conto dell'Economato (conservando eventuali prospetti generali),
- (8) Registro di carico e scarico dei bollettari;
- (9) Registri e bollettari di spese postali;

- (10) Prospetti dei lavori eseguiti dai cantonieri;
- (11) Brogliacci di viaggio degli automezzi comunali;
- (12) Circolari per l'orario degli uffici e per il funzionamento degli uffici;
- (13) Prospetti di carattere pubblicitario, richiesti e non richiesti, preventivi di massima non utilizzati;
- (14) Lettere di rifiuto di partecipazione alle aste, offerte di ditte non prescelte;

CATEGORIA II: OPERE PIE E BENEFICIENZA

- (1) Copie di deliberazioni per contributi assistenziali diversi (conservando le richieste o le proposte);
- (2) Copie di deliberazioni per contributi ad enti e associazioni diverse (conservando le richieste);
- (3) Domande di partecipazione alla Befana e ad altre elargizioni;

CATEGORIA III: POLIZIA URBANA E RURALE

- (1) Domande per pubbliche affissioni (conservando le pratiche che danno luogo a contenzioso);
- (2) Domande di occupazione temporanea di spazi ed aree pubbliche per fiere, mostre, comizi, feste (conservando quelle relative a concessioni permanenti – es. passi carrabili – per quarant'anni ed eventuali registri indefinitamente);
- (3) Copie di attestati di servizio;
- (4) Elenchi dei turni di servizio delle guardie municipali (conservando i regolamenti);
- (5) Informazioni varie per buona condotta, stato professionale, ecc.;

CATEGORIA IV: SANITA' E IGIENE

- (1) Atti relativi all'orario degli ambulatori;
- (2) Tessere sanitarie restituite al Comune;
- (3) Stampati e circolari per campagne nazionali di lotta contro le malattie;
- (4) Copia delle delibere della Farmacia comunale inviate per notizia (conservando quelle inviate per l'approvazione e la raccolta ufficiale);
- (5) Copia di lettere di trasmissione di denunce di malattie infettive;

CATEGORIA V: FINANZE

- (1) Bollettari di ricevute dell'esattoria;
- (2) Carteggio interlocutorio per la concessione in uso di locali e oggetti di proprietà comunale;
- (3) Solleciti di pagamento di fatture pervenuti al Comune;
- (4) Documenti di carico e scarico dei bollettari delle imposte;
- (5) Copia di delibere di approvazione del ruolo per l'acquedotto comunale;
- (6) Copia di delibere per il pagamento di gettoni di presenza ai partecipanti delle commissioni;

CATEGORIA VI: GOVERNO

- (1) Corrispondenza interlocutoria per commemorazioni e solennità civili (conservando carteggi generali per l'organizzazione delle manifestazioni, una copia degli inviti, degli stampati e dei manifesti, gli atti dei comitati, eventuali rendiconti particolari ed eventuali fatture per dieci anni);
- (2) Telegrammi della Prefettura per l'esposizione della bandiera nazionale (conservando le ordinanze e gli avvisi del sindaco);
- (3) Copia di deliberazioni per liquidazione indennità alla Commissione elettorale mandamentale e ad altre commissioni non comunali;
- (4) Fascicoli non rilegati del Bollettino della Prefettura;

Materiale elettorale: atti generali

- (5) Atti relativi alla costituzione e all'arredamento dei seggi (conservando il prospetto delle sezioni e della loro ubicazione);
- (6) Matrici dei certificati elettorali in bianco e non consegnati;
- (7) Scadenziari dell'Ufficio elettorale per la compilazione delle liste;
- (8) Liste sezionali se esistono le liste generali;
- (9) Fascicoli e schede personali di cittadini cancellati dalle liste per morte o emigrazione;
- (10) Atti relativi alla regolamentazione della propaganda (conservando la documentazione riassuntiva);
- (11) Copie di istruzioni a stampa (conservandone una per ciascuna elezione);
- (12) Tabelle provvisorie delle preferenze non costituenti verbale;
- (13) Verbali di consegna di materiale elettorale; verbali di controllo dei verbali sezionali per l'accertamento che non vi siano fogli in bianco;
- (14) Copie delle comunicazioni delle sezioni relative ai dati parziali sul numero dei votanti (conservando eventualmente la copia dei fonogrammi trasmessi per l'insieme delle sezioni);

Materiale elettorale: atti per singoli tipi di elezioni

Referendum istituzionale

- (15) Verbali sezionali con allegati;
- (16) Verbali degli uffici centrali circoscrizionali concernenti il completamento delle operazioni;

Elezioni dei deputati alla costituente

- (17) Verbali sezionali con allegati;
- (18) Verbali degli uffici centrali di circoscrizione concernenti il completamento delle operazioni;

Elezioni della Camera e del Senato

- (19) Verbali sezionali, privi di allegati;
- (20) Verbali degli uffici centrali di circoscrizione per il completamento delle operazioni;
- (21) Carteggio relativo alla designazione dei rappresentanti di lista presso gli uffici di sezione, dal 1976;

Referendum abrogativi

- (22) Carteggio relativo alla designazione dei rappresentanti dei partiti e dei gruppi politici e comitati promotori presso le sezioni (conservando eventualmente la documentazione contenente dati generali);
- (23) Verbali sezionali privi di allegati;
- (24) Verbali di completamento dello spoglio delle schede eseguito da parte dell'Ufficio provinciale per il Referendum;
- (25) Estratti del verbale dell'Ufficio provinciale per il referendum relativo al riesame dei voti contestati e provvisoriamente non assegnati, per ogni sezione;

Parlamento Europeo

- (26) Verbali sezionali privi di allegati (non prima della decisione di eventuali ricorsi previsti dagli artt. 42 e 43 della L. 24 gennaio 1979, n.18);
- (27) Estratti del verbale dell'Ufficio elettorale provinciale per il riesame delle schede di voti contestati (non prima della decisione c.s.);
- (28) Verbali dell'Ufficio elettorale provinciale per il riesame delle schede dei voti contestati (non prima della decisione c.s.);
- (29) Verbali dell'Ufficio provinciale relativi al completamento di operazioni;
- (30) Carteggi relativi alle designazioni dei rappresentanti di lista presso gli uffici di sezione (conservando eventualmente la documentazione contenente dati più generali);

Consiglio regionale e provinciale

- (31) Verbali sezionali privi di allegati (comunque non prima della decisione di eventuali ricorsi);
- (32) Verbali dell'Ufficio centrale circoscrizionale relativi al completamento delle operazioni elettorali;
- (33) Estratti dei verbali dell'Ufficio centrale circoscrizionale relativi al riesame dei voti contestati;

CATEGORIA VII: GRAZIA GIUSTIZIA E CULTO

- (1) Liste dei giudici popolari;
- (2) Fascicoli e schede personali dei giudici popolari;
- (3) Copie di atti giudiziari notificati dal Comune;
- (4) Elenchi dei notai;
- (5) Fascicoli non rilegati del Bollettino dei protesti e del Foglio annunci legali;

CATEGORIA VIII: LEVA E TRUPPA E SERVIZI MILITARI

- (1) Schede personali dei militari da includere nella lista di leva;
- (2) Schede personali dei giovani compresi nella leva di altri comuni o deceduti prima della stessa;
- (3) Corrispondenza relativa alla formazione delle schede personali, alle aggiunte o alle cancellazioni dalle liste;
- (4) Carteggio tra comuni per l'aggiornamento dei ruoli matricolari;
- (5) Carteggio con gli uffici militari per l'aggiornamento dei ruoli matricolari;
- (6) Matrici di richieste di congedi anticipati;
- (7) Certificati degli esami sierologici;
- (8) Corrispondenza per la richiesta e la trasmissione di certificati di esito di leva;
- (9) Richiesta di invio di notizie varie relative ai militari (esclusi i periodi bellici);

CATEGORIA IX: ISTRUZIONE PUBBLICA

- (1) Matrici di buoni acquisto generi di refezione e comunque consumo;
- (2) Copie degli elenchi dei buoni libro concessi e documentazione di supporto (conservando l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali; eventuali fatture dovranno essere conservate per dieci anni);
- (3) Autorizzazioni all'uso di impianti culturali e sportivi (conservando eventuali atti riassuntivi);

- (4) Note di frequenza, ricevute di pagamento di rette e domande di esonero per scuole materne (conservando gli elenchi dei beneficiari; eventuali fatture dovranno essere conservate per dieci anni);
- (5) Moduli per l'accertamento del diritto al trasporto gratuito degli alunni (conservando eventuali relazioni riassuntive);
- (6) Copie di delibere di liquidazioni di contributi per concerti, attività culturali, biblioteca comunale, biblioteche scolastiche (conservando la corrispondenza o la richiesta, una copia dei programmi e dei manifesti e gli elenchi dei libri forniti);
- (7) Atti relativi a concorsi a borse di studio e premi (conservando la seguente documentazione: originale degli atti della commissione o dei comitati, gli eventuali rendiconti speciali; una copia degli stampati e dei manifesti, il registro delle opere esposte in occasione di mostre artistiche e simili);
- (8) Copie di delibere di liquidazioni dei compensi al personale straordinario per corsi serali e carteggio transitorio sui corsi (conservando gli atti di interesse per il personale che ha prestato servizio e relazioni finali, programmi di spesa, altri documenti riassuntivi);

CATEGORIA X: LAVORI PUBBLICI, POSTE E TELEGRAFI, TELEFONI, RADIO, TELEVISIONE

- (1) Matrici di bollettari per l'acquisto materiali di consumo per l'ufficio tecnico;
- (2) Domande di allacciamento all'acquedotto e richieste di concessione di illuminazione, ove le stesse non facciano fede di contratto (in tal caso saranno eliminabili cinque anni dopo l'esaurimento del contratto);
- (3) Note di lavori da eseguirsi dall'officina comunale;
- (4) Libretti dei veicoli;
- (5) Atti di assegnazione di vestiario protettivo ai cantonieri;
- (6) Rapporti delle guardie e dei cantonieri;
- (7) Avvisi di convocazione delle commissioni;
- (8) Copie e minute dei progetti, sia realizzati che non realizzati;

CATEGORIA XI: AGRICOLTURA, INDUSTRIA E COMMERCIO

- (1) Corrispondenza per la richiesta e la concessione di licenze non di pertinenza comunale;
- (2) Domande di commercianti per deroghe all'orario dei negozi;
- (3) Copie degli inviti agli utenti convocati per la verifica biennale dei pesi e delle misure o per altri adempimenti;
- (4) Domande per la concessione dei libretti di lavoro e libretti restituiti al Comune;

CATEGORIA XII: ANAGRAFE, STATO CIVILE, CENSIMENTO, STATISTICA

- (1) Domande per la richiesta di certificati, carteggi per la loro trasmissione e bollettari di pagamento;
- (2) Annotazioni marginali eseguite agli atti di stato civile provenienti da altri comuni e altre assicurazioni di trascrizione relative agli stessi;
- (3) Matrici delle proposte di annotazioni marginali inviate alle Procure;
- (4) Comunicazioni relative a variazioni anagrafiche;
- (5) Matrici o copie di comunicazioni anagrafiche ad altri uffici comunali;
- (6) Delegazioni alla celebrazione di matrimonio in altri comuni;
- (7) Atti relativi all'organizzazione di censimenti;
- (8) Carteggio relativo alla contabilità per registri di stato civile (conservando le fatture per dieci anni);

CATEGORIA XIII: ESTERI

- (1) Lettere di trasmissione di passarti; autorizzazioni alla richiesta degli stessi;
- (2) Lettere di trasmissione di carte d'identità;

CATEGORIA XIV: OGGETTI DIVERSI

- (1) Corrispondenza per la richiesta di licenze di pubblica sicurezza o rilasciate da altri uffici;

B) Documentazione eliminabile dopo sette anni

- (1) Fogli di presenza dei dipendenti;
- (2) Fogli di lavoro straordinario (conservando eventuali prospetti riassuntivi);
- (3) Modelli 740 (copia per il Comune); i sette anni decorrono dall'anno cui si applica la dichiarazione.

C) Documentazione eliminabile dopo dieci anni

CATEGORIA I: AMMINISTRAZIONE

- (1) Carteggi relativi a sottoscrizione di abbonamenti a giornali e riviste e ad acquisto di pubblicazioni amministrative (conservando eventuali carteggi autorizzativi con l'organo di tutela);
- (2) Carteggi per l'acquisto di macchine d'ufficio e di materiale per la loro manutenzione e per la cancelleria (conservando proposte di spesa, verbali d'asta e contratti);
- (3) Carteggi per la fornitura di combustibile per riscaldamento (conservando proposte di spesa, verbali d'asta e contratti);
- (4) Inviti alle sedute del Consiglio e della Giunta (conservando gli ordini del giorno con elenco dei destinatari, fascicoli delle interpellanze ed eventuali progetti e relazioni);
- (5) Atti dei concorsi: copie dei verbali della commissione giudicatrice; domande di partecipazione (conservando per 40 anni i diplomi originali di studio e/o i documenti militari); copie di manifesti inviate ad altri enti e restituite; elaborati scritti e pratici; copie di avvisi diversi; copie di delibere;
- (6) Carteggi di liquidazione delle missioni ai dipendenti e agli amministratori, con relative tabelle di missione e documentazione allegata, salvo, se esistenti, prospetti generali;
- (7) Carteggi per l'acquisto di vestiario per specifiche categorie di dipendenti (conservando proposte di spesa, verbali d'asta e contratti);
- (8) Carteggi per l'acquisto di attrezzature varie, di mobili e di materiale di cancelleria e pulizia per uffici, ambulatori, scuole (conservando proposte di spesa, verbali d'asta e contratti);
- (9) Carteggi per l'acquisto di carburante per gli automezzi (conservando proposte di spesa, verbali d'asta e contratti);
- (10) Carteggi per la pulizia di locali (conservando proposte di spesa, verbali d'asta e contratti);

CATEGORIA II: OPERE PIE E BENEFICIENZA

- (1) Libretti di povertà restituiti al Comune;
- (2) Domande di concessione di sussidi straordinari,
- (3) Ricette di medicinali distribuiti ai poveri;
- (4) Certificazioni di prestazioni mediche fornite ai poveri;
- (5) Richieste di informazioni da parte di ospedali ed enti assistenziali;
- (6) Fascicoli delle spedalità (assunte dal Comune o da altri Enti);
- (7) Domande di ammissione a colonie;
- (8) Domande di iscrizione all'elenco dei poveri (conservando l'elenco);

CATEGORIA III: POLIZIA URBANA E RURALE

- (1) Verbalì delle contravvenzioni di polizia (conservando i registri);
- (2) Bollettari per la riscossione delle contravvenzioni;
- (3) Bollettari per la riscossione dell'imposta sulla pubblicit , pubbliche affissioni e occupazione di suolo pubblico;
- (4) Carteggi relativi all'acquisto di materiali di consumo (conservando proposte di spesa, verbali d'asta e contratti);

CATEGORIA IV: SANITA' ED IGIENE

- (1) Carteggi relativi alla manutenzione ordinaria degli ambulatori (conservando proposte di spesa, verbali d'asta e contratti);
- (2) Denunce mediche di malattie contagiose a carattere non epidemico se trasmesse ad altri uffici;
- (3) Atti relativi alle vaccinazioni e matrici dei certificati relativi, attestati di eseguita vaccinazione (conservando indefinitamente le schede personali, le statistiche e i registri);
- (4) Atti relativi alle contravvenzioni sanitarie (conservando i registri, se esistenti);
- (5) Matrici dei permessi di seppellimento;
- (6) Autorizzazioni al trasporto di salme fuori del comune;
- (7) Certificati delle levatrici (conservando eventuali registri);
- (8) Modelli statici relativi al bestiame macellato (se esistono registri riassuntivi);
- (9) Carteggi relativi all'acquisto di beni mobili per gli ambulatori (conservando proposte di spesa, contratti e verbali d'asta);
- (10) Carteggio vario transitorio con le farmacie comunali;
- (11) Ordini di sequestro di medicinali in commercio eseguiti su direttive superiori;
- (12) Atti per l'acquisto di disinfettanti (conservando proposte di spesa, verbali d'asta e contratti);
- (13) Referti di esami di laboratorio per l'acqua potabile (conservandone campioni a scadenza regolare);
- (14) Copie di atti per lavori ai cimiteri (conservando l'originale del progetto, i verbali d'asta, i contratti, il conto finale dei lavori e tutti i documenti originali);
- (15) Copie di avvisi per esumazione di salme nei cimiteri (conservando per almeno 40 anni il registro delle lettere spedite e degli avvisi consegnati);
- (16) Verbalì di interrimento di animali inadatti all'alimentazione;

CATEGORIA V: FINANZE

- (1) Atti relativi all'alienazione di mobili fuori uso e di oggetti vari;
- (2) Carteggio interlocutorio e copia di atti per mutui estinti ed accettazioni di eredit ;
- (3) Copie dei mandati e delle reversali e dei loro allegati;
- (4) Copie dei preventivi e dei consuntivi (conservando il progetto del bilancio e, caso per caso, i carteggi ad esso relativi);

- (5) Matricole delle imposte (conservando i ruoli restituiti dall'esattoria e, in mancanza di questi, le loro copie);
- (6) Schedari delle imposte;
- (7) Cartelle personali dei contribuenti cessati (conservando i ruoli);
- (8) Bollettari di riscossione delle imposte di consumo e delle sue contravvenzioni (conservando i registri e i prospetti delle contravvenzioni);
- (9) Registri delle riscossioni dei diritti di segreteria e stato civile (conservando eventuali prospetti riassuntivi annuali);
- (10) Atti relativi al riparto dei diritti di segreteria e stato civile, sanitari e tecnici;
- (11) Atti relativi a liquidazione di spese "a calcolo";
- (12) Atti relativi a liquidazione di spese di rappresentanza;
- (13) Avvisi di pagamento per compartecipazione di imposte erariali a favore del comune;
- (14) Fatture liquidate;
- (15) Verifiche di cassa dell'imposta di consumo e registro di carico e scarico dei suoi bollettari;

CATEGORIA VI: GOVERNO

- (1) Carteggio interlocutorio relativo alle associazioni di comuni;
- (2) Atti di liquidazione di lavoro straordinario per elezioni;
- (3) Verbali sezionali dei referendum abrogativi;

CATEGORIA VII: GRAZIA; GIUSTIZIA E CULTO

- (1) Carteggi relativi a ordinaria e straordinaria manutenzione di sedi di uffici giudiziari o carceri (conservando proposte di spesa, progetti originali, verbali d'asta e contratti);

CATEGORIA VII: LEVA E TRUPPA

- (1) Carteggi per l'organizzazione della leva, locali e arredamento, materiali, cancelleria (conservando i contratti relativi a forniture);
- (2) Corrispondenza relativa al personale del consiglio e delle commissioni e alla liquidazione dei loro compensi;

CATEGORIA IX:ISTRUZIONE PUBBLICA

- (1) Carteggi di ordinaria e straordinaria manutenzione delle scuole (conservando proposte di spesa, contratti, verbali d'asta e progetti originali);

CATEGORIA X: LAVORI PUBBLICI

- (1) Carteggi per l'acquisto di materiali per l'Ufficio tecnico e il magazzino comunale (conservando proposte di spesa, verbali d'asta, contratti);
- (2) Atti relativi all'acquisto di autoveicoli e alla loro manutenzione, con depliant pubblicitari (conservando proposte di spesa, verbali d'asta, contratti);
- (3) Carteggi relativi all'acquisto di materiali per illuminazione pubblica, segnaletica stradale, manutenzione di giardini, piazze, vie, argini dei fiumi, fognature (conservando proposte di spesa, verbali d'asta e contratti);
- (4) Matrici di bollettari di riscossione tasse acqua potabile (conservando il registro o ruolo);
- (5) Domande e certificazioni di ditte per essere incluse nell'albo degli appaltatori comunali;
- (6) Stati di avanzamento di lavori pubblici;

CATEGORIA XV: PUBBLICA SICUREZZA

- (1) Cartellini delle carte d'identità scadute e carte scadute e restituite al comune;

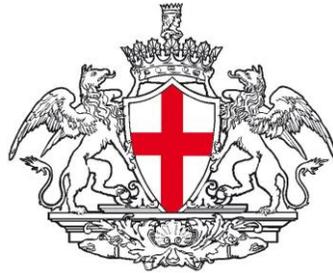
D) Documentazione eliminabile dopo cinquant'anni

- (1) Diplomi originali di studio o militari conservati nella documentazione relativa ai concorsi, eventualmente eliminabili prima dei quarant'anni previa emanazione di un'ordinanza con intimazione al ritiro;
- (2) Registri degli atti notificati per altri uffici;
- (3) Registro delle lettere spedite agli eredi per esumazione di salme nei cimiteri;

E) Documentazione eliminabile dopo cinquant'anni

Mandati di pagamento e riscossione (comprese le eventuali fatture e le cosiddette “pezze d’appoggio”, ma conservando l’eventuale carteggio originale come relazioni, perizie, ecc. che talvolta è rimasto allegato al mandato).

Comune di Genova



Allegato 8 – Accesso agli atti



COMUNE DI GENOVA

Genova, 24 dicembre 2020

Prot. n. 395722

L'accesso agli atti tra novità legislative e nuovi indirizzi giurisprudenziali

Indice:

1. [Scopo della relazione;](#)
2. [Premessa;](#)
3. [Il quadro normativo vigente;](#)
- scheda di sintesi
4. [Le varie tipologie di accesso:](#)
 - 4.1. [L'accesso ai documenti amministrativi di cui alla legge n. 241/1990;](#)
 - [Funzione;](#)
 - [Legittimazione;](#)
 - [Oggetto;](#)
 - [Costi;](#)
 - [Limiti;](#)
 - [Controinteressati;](#)
 - [Conclusione del procedimento;](#)
 - scheda di sintesi
 - 4.2. [L'accesso civico c.d. semplice;](#)
 - [Legittimazione;](#)
 - [Oggetto;](#)
 - [Costi;](#)
 - [Limiti;](#)
 - [Conclusione del procedimento;](#)
 - scheda di sintesi
 - 4.3. [L'accesso civico c.d. generalizzato;](#)
 - [Legittimazione;](#)
 - [Oggetto;](#)
 - [Costi;](#)
 - [Limiti;](#)
 - [Controinteressati;](#)
 - scheda di sintesi
 - 4.4. [I confini tra accesso civico generalizzato e accesso documentale;](#)
5. [L'accesso alle informazioni ambientali;](#)
6. [L'accesso dei Consiglieri Comunali e Provinciali;](#)
7. [La tutela del diritto di accesso;](#)
 - 7.1. [La tutela giustiziale;](#)
 - 7.2. [La tutela giurisdizionale;](#)
 - 7.3. [La tutela penale del diritto di accesso: rapporto tra inerzia della P.A. e art. 328 c.p.;](#)
8. [Note operative per la gestione delle istanze di accesso agli atti](#)
9. [Note operative per il corretto bilanciamento tra accesso e riservatezza;](#)



COMUNE DI GENOVA

1. Scopo della relazione

Scopo della presente relazione è di fornire, tramite riferimenti normativi, massime di giurisprudenza e spunti pratici, uno strumento che possa fungere da orientamento per l'inquadramento, la qualificazione e la gestione delle istanze di accesso agli atti rivolte agli Uffici della civica amministrazione.

2. Premessa

L'istituto dell'accesso agli atti costituisce espressione del principio della trasparenza dell'azione amministrativa e traduce sul piano concreto l'idea di una Pubblica Amministrazione aperta, che operi al servizio del cittadino, in ossequio ai canoni dell'imparzialità e del buon andamento dell'azione amministrativa ai sensi dell'art. 97 Cost.

Un'amministrazione imparziale, infatti, è una amministrazione che, in attuazione del principio di uguaglianza (art. 3 Cost.) e del principio democratico (art. 1 Cost.) consente al cittadino di verificare che la propria attività sia svolta al servizio esclusivo della Nazione (art. 98 Cost.).

Si tratta, come noto, di un'acquisizione recente, posto che l'azione amministrativa è stata tradizionalmente caratterizzata da segretezza, anonimato ed inaccessibilità (art. 15 d.P.R. 10 gennaio 1957, n. 3).

Solo con la legge n. 15/2005, in modifica degli artt. 1 e 22 della Legge n. 241/1990, la trasparenza è stata espressamente elevata a canone dell'*agere* amministrativo, sebbene, a livello pretorio, fosse un principio già da tempo acquisito in via consolidata.

Con il d.lgs. 150/2009, il legislatore ha poi definito la trasparenza come "*accessibilità totale alle informazioni*" (art. 11), collegandola alla valutazione della *performance* individuale ed organizzativa.

In seguito, con la legge n. 190/2012, la trasparenza ha acquisito un ruolo determinante come strumento di prevenzione e di contrasto ai fenomeni corruttivi che possono insorgere nell'attività amministrativa.

L'art. 1, co. 1 D.Lgs. n. 33/2013 – adottato in attuazione della delega contenuta nell'art. 1 co. 35 L. 190/2012 – ha ridefinito la trasparenza come "*accessibilità totale dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa e favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche*".



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

3. Il quadro normativo vigente

La legge n. 241/1990, agli artt. 22 e ss. disciplina in via generale l'istituto dell'accesso ai documenti amministrativi, cd. **accesso documentale**, ed è attuata con D.P.R. 12 aprile 2006, n. 184, "*Regolamento recante disciplina in materia di accesso ai documenti amministrativi*".

L'evoluzione del concetto di trasparenza ha, tuttavia, inciso profondamente anche sulla conformazione dell'istituto dell'accesso agli atti, favorendo l'introduzione di nuove ulteriori forme di accessibilità rispetto a quella disciplinata dalla legge generale sul procedimento.

In particolare:

- il D.Lgs. 33/2013 ha profondamente innovato la materia della trasparenza, introducendo l'istituto dell'**accesso civico c.d. semplice**;
- il D.Lgs. 97/2016, in senso ancor più ampliativo dell'operatività della trasparenza, ha da ultimo introdotto l'istituto dell'**accesso civico c.d. generalizzato**, sul modello del c.d. FOIA (Freedom of Information Act), di matrice anglosassone.

Accanto a queste ipotesi di applicazione trasversale, esistono poi delle figure di accesso agli atti spiccatamente settoriali, cui la legge dedica una regolamentazione specifica (ad esempio, l'**accesso ambientale** su cui v. infra).

In una prospettiva unitaria e sistematica, tali ipotesi di accesso agli atti denotano la chiara intenzione del legislatore di rafforzare l'ambito di operatività della trasparenza nei rapporti tra cittadini e Pubblica Amministrazione.

L'ambito dell'**accesso agli atti degli enti locali** era già stato oggetto di specifica disposizione normativa ad opera dell'art. 25, c. 1, L. 27 dicembre 1985, n. 816, il quale riconosceva il diritto di tutti i cittadini a prendere visione dei provvedimenti degli enti locali, rinviando alle singole amministrazioni di stabilire, con proprio regolamento, la disciplina dell'esercizio di tale diritto.

Tale disposto è stato poi sostanzialmente trasfuso nel Testo unico degli enti locali di cui al d.lgs. 18 agosto 2000, n. 267, con norme sostanzialmente analoghe a quelle generali nel frattempo introdotte con la legge 241/1990.

In particolare, l'art. 6 del TUEL demanda agli statuti comunali, metropolitani e provinciali la definizione delle forme dell'accesso dei cittadini alle informazioni e ai procedimenti amministrativi (cfr. art. 12 [Statuto del Comune di Genova](#)).



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

A sua volta, il successivo art. 10 TUEL stabilisce che *“Tutti gli atti dell'amministrazione comunale e provinciale sono pubblici, ad eccezione di quelli riservati per espressa indicazione di legge o per effetto di una temporanea e motivata dichiarazione del sindaco o del presidente della provincia che ne vieti l'esibizione, conformemente a quanto previsto dal regolamento, in quanto la loro diffusione possa pregiudicare il diritto alla riservatezza delle persone, dei gruppi o delle imprese”*.

Inoltre demanda ai regolamenti degli enti la disciplina dell'accesso agli atti amministrativi, del rilascio delle relative copie e delle modalità *“per assicurare ai cittadini l'informazione sullo stato degli atti e delle procedure e sull'ordine di esame di domande, progetti e provvedimenti che comunque li riguardino; assicura il diritto dei cittadini di accedere, in generale, alle informazioni di cui è in possesso l'amministrazione”*.

Con specifico riguardo al Comune di Genova, l'accesso agli atti è attualmente disciplinato dagli artt. 29 e ss. del *“Regolamento in materia di procedimento amministrativo, diritto di accesso, disciplina delle dichiarazioni sostitutive e trattamento dei dati personali”* ([Deliberazione del Consiglio Comunale n. 39 del 27.07.2016](#)).

Nell'esame delle istanze di accesso è poi opportuno fare riferimento – per indicazioni di respiro più spiccatamente operativo – ai seguenti provvedimenti:

- artt. 59 e 60, D.lgs., 30 giugno 2003, n. 196 – [“Codice in materia di protezione dei dati personali”](#); .
- Linee Guida sull'accesso civico generalizzato predisposte dell'Autorità Nazionale Anticorruzione - [Delibera ANAC n. n. 1309 del 28 dicembre 2016](#);
- [Circolare n. 2 del 2017 del Ministro per la semplificazione e la pubblica amministrazione](#);
- [Circolare n. 1 del 2019 del Ministro per la Pubblica Amministrazione](#);
- Nota prot. PG/2017/303238 della Segreteria Generale del Comune di Genova con cui è stato introdotto, a decorrere dal 18.09.2017, l'uso del Protocollo Informatico ai fini della estrazione delle informazioni necessarie ad implementare il c.d. Registro degli accessi;
- Nota prot. n. 356723 del 23.11.2020 recante *“Note operative per la registrazione a protocollo delle istanze di accesso”* predisposte dalla Segreteria Generale, da applicare **a partire dal 1° gennaio 2021**.

Con riferimento, infine, alla specifica materia dei **contratti pubblici** è opportuno considerare quanto disposto, in tema di accesso documentale, dall'art. 53 del D.lgs. n. 50/2016 (Codice dei Contratti Pubblici).



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

SCHEDA DI SINTESI - QUADRO NORMATIVO

ACCESSO DOCUMENTALE

- artt. 22 e ss. - Legge, 7 agosto 1990, n. 241 - "[Legge sul procedimento amministrativo e sul diritto di accesso ai documenti amministrativi](#)";
- D.P.R., 12 aprile 2006, n. 184 - "[Regolamento sull'accesso ai documenti amministrativi](#)";
- artt. 6 e 10 - D.lgs., 18 agosto 2000, n. 267 - "[Testo Unico Enti Locali](#)"
- artt. 29 e ss. del "Regolamento in materia di procedimento amministrativo, diritto di accesso, disciplina delle dichiarazioni sostitutive e trattamento dei dati personali" ([Deliberazione del Consiglio Comunale n. 39 del 27.07.2016](#));
- artt. 59 e 60, D.lgs., 30 giugno 2003, n. 196 - "[Codice in materia di protezione dei dati personali](#)";
- art. 53, D.lgs., 18 aprile 2016, n. 50 "[accesso agli atti e riservatezza](#)" - procedure di affidamento e di esecuzione dei contratti pubblici;

ACCESSO CIVICO SEMPLICE e GENERALIZZATO

- D.lgs., 14 marzo 2013, n. 33 - "[diritto di accesso civico, obblighi di pubblicità, trasparenza e diffusione di informazioni](#)";
- Delibera ANAC, 28 dicembre 2016, n. 1309 - "[Linee Guida sull'accesso civico generalizzato](#)";
- Circolare Ministero per la Pubblica Amministrazione, n. 2 del 2017 - "[Attuazione delle norme sull'accesso civico generalizzato](#)";
- Circolare Ministero per la Pubblica Amministrazione, n. 1 del 2019 - "[Attuazione delle norme sull'accesso civico generalizzato \(c.d. FOIA\)](#)";

Regole tecniche:

- Nota prot. PG/2017/303238 della Segreteria Generale del Comune di Genova su "Registro degli accessi";
- Nota prot. n. 356723 del 23.11.2020 recante "Note operative per la registrazione a protocollo delle istanze di accesso" predisposte dalla Segreteria Generale, da applicare a partire dal 1° gennaio 2021;

4. Le varie tipologie di accesso

4.1. L'accesso ai documenti amministrativi di cui alla L. 241/1990

Il diritto di accesso cd. documentale è disciplinato dagli artt. 22 e ss. della legge n. 241/1990 e ss.mm.ii. e consente agli interessati di prendere visione ed estrarre copia di documenti amministrativi, laddove il richiedente sia titolare di un interesse diretto, concreto ed attuale,



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso.

- Funzione

Come chiarito dall'art. 24 co. 3 L. 241/1990 non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni. È pertanto necessario che l'istanza sia strumentale alla realizzazione e alla tutela di una situazione giuridica tutelata dall'ordinamento e connessa al documento richiesto.

Benché la domanda di accesso debba essere finalizzata alla cura di un interesse diretto, concreto e attuale e, quindi, non meramente emulativo o potenziale, connesso alla disponibilità dell'atto o del documento del quale si richiede l'accesso, la nozione di strumentalità va, tuttavia, intesa in senso ampio.

Il carattere strumentale non ne implica, per conseguenza, la riduzione ad una situazione meramente servente rispetto alla difesa in giudizio della situazione sottostante (così T.A.R Lazio, sez. I, 2.03.2020, n. 2704).

La finalità dell'accesso documentale è, infatti, quella di porre i soggetti interessati in grado di esercitare al meglio le facoltà partecipative, oppositive e difensive che l'ordinamento attribuisce loro, nell'ambito di un procedimento amministrativo, di un giudizio o anche di un rapporto tra privati, a tutela delle posizioni giuridiche di cui sono titolari.

In tal senso, volendo citare degli esempi, in giurisprudenza è stato affermato che *“sussiste il diritto di un esercente un'attività commerciale ad accedere alla documentazione relativa ai titoli abilitativi rilasciati ad un soggetto diretto concorrente. Infatti (...) il soggetto ha certamente un interesse diretto, concreto e attuale, corrispondente a una situazione giuridicamente rilevante e tutelata, a verificare la legittimità dei titoli abilitativi rilasciati ad un'impresa concorrente, esercente analogo attività commerciale in posizione frontistante”* (T.A.R Puglia, sez. II, 27.11.2014, n. 2933).

Ancora, in altra vicenda, è stato riconosciuto *“il diritto del coniuge di accedere agli atti detenuti dall'INPS relativi al reddito percepito dalla ex moglie, divenuta titolare – dopo il momento della cessazione del rapporto matrimoniale, di un reddito da pensione quale casalinga; l'interesse in vista del quale è stato chiesto l'accesso (modificazione delle condizioni economiche conseguenti alla cessazione degli effetti civili del matrimonio) si rivela senz'altro tutelato dall'ordinamento, mentre non è dato rinvenire, in capo*



COMUNE DI GENOVA

alla controinteressata, una situazione giuridica avente carattere di preminenza o prevalenza, ovvero tale da rendere necessaria la compressione e/o il sacrificio del diritto di accesso” (T.A.R Calabria, sez. I, 16.03.2015, n. 281).

Nell’ambito delle procedure di evidenza pubblica, in relazione alla fase di esecuzione del contratto pubblico, l’Adunanza Plenaria del Consiglio di Stato ha, infine, osservato che: *“gli operatori economici che abbiano preso parte alla gara sono legittimati ad accedere agli atti della fase esecutiva, con le limitazioni di cui all’art. 53 del d.lgs. n. 50 del 2016, purché abbiano un interesse diretto, concreto e attuale a conoscere tali atti (...) laddove funzionale, ad esempio, a dimostrare, attraverso la prova dell’inadempimento delle prestazioni contrattuali, l’originaria inadeguatezza dell’offerta vincitrice della gara”*. Si chiarisce, tuttavia, in relazione a tale ipotesi, che ai fini dell’accesso, l’interesse dell’istante, affinché possa considerarsi concreto, attuale e diretto, debba essere preesistente all’istanza di accesso e non esserne conseguenza *“per il verificarsi, ad esempio, di una delle situazioni che legittimerebbe o addirittura imporrebbe la risoluzione del rapporto con l’appaltatore ai sensi dell’art. 108, commi 1 e 2, del d.lgs. n. 50 del 2016, e potrebbero indurre l’amministrazione a scorrere la graduatoria”* (Cons. Stato, Ad. Plen., 2.04.2020, n. 10).

- Legittimazione

La legittimazione all’accesso in esame è, dunque, riconosciuta ai soggetti che dimostrino che i documenti amministrativi oggetto dell’accesso abbiano spiegato o siano idonei a spiegare effetti diretti o indiretti nei loro confronti.

È per tale ragione che grava in capo al richiedente un onere di motivazione, per l’assolvimento del quale non è sufficiente addurre un generico e indistinto interesse alla legalità o al buon andamento dell’amministrazione.

Come chiarito dalla giurisprudenza, l’istanza di accesso è reiterabile a fronte di una diversa prospettazione dell’interesse giuridicamente rilevante (T.A.R. Emilia Romagna, sez. I, 22.01.2015, n. 41).

- Oggetto

Sul piano oggettivo, l’accesso di cui si tratta è riferito ai *“documenti amministrativi”*, definiti dall’art. 22 co. 1 lett. d) L. 241/90 come *“ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura*



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

pubblicistica o privatistica della loro disciplina sostanziale”.

Non sono accessibili, per contro, le informazioni “*che non abbiano forma di documento amministrativo*” (co. 4 del medesimo art. 22). In particolare, l’art. 2 co. 2 DPR n. 184 del 2006 specifica che il diritto di accesso si esercita “*con riferimento ai documenti amministrativi materialmente esistenti al momento della richiesta*” e “*nei confronti dell’autorità competente a formare l’atto conclusivo o a detenerlo stabilmente*”.

Di tal guisa si intende evitare che la P.A. possa essere obbligata a formare nuovi documenti contenenti le informazioni richieste, al fine di non creare eccessivi aggravii all’attività amministrativa.

- Costi

L’art. 25 co. 1 dispone che “*L’esame dei documenti è gratuito. Il rilascio di copia è subordinato soltanto al rimborso del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura*”. L’amministrazione deve dal proprio canto sostenere, quali costi generali il cui finanziamento ricade sulla fiscalità generale, le spese relative alla predisposizione di uffici e personale dedicati al riscontro delle istanze di accesso.

A riguardo, si segnala che la giurisprudenza considera illegittimo l’eventuale diniego fondato su eventuali carenze di risorse umane e strumentali dell’amministrazione: i limiti organizzativi e di struttura non sono in alcun caso da considerare limiti oggettivi all’ostensione (cfr. Cons. Stato, sez. IV, 10.04.2009, n. 2243, relativo ad un caso di accesso ad elaborati grafici in materia urbanistica non fotocopiabili dall’ente locale con mezzi propri nel formato più idoneo).

- Limiti

Il diritto di accesso, per quanto teso ad un principio di massima ostensione, incontra due ordini di limiti:

A) i **limiti tassativi** individuati dall’art. 24 co. 1 L. 241/1990

- per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;

- nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;

- nei confronti dell’attività della pubblica amministrazione diretta all’emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari

norme che ne regolano la formazione;



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

- nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

B) i **limiti eventuali** individuati con regolamento governativo al fine di tutelare alcuni interessi primari, enucleati dalla legge: sicurezza nazionale, politica monetaria e valutaria, ordine pubblico, riservatezza (art. 24 co. 6).

La medesima disposizione demanda inoltre alle singole amministrazioni la facoltà di individuare le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso.

In tutte queste fattispecie, il legislatore attribuisce una rilevanza maggiore all'interesse generale alla segretezza che a quello dell'interessato all'ostensione.

Resta fermo il "controlimite" del c.d. accesso difensivo: ai sensi dell'art. 24 co. 7 L. 241/1990 "Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici".

- Controinteressati

L'art. 22 L. 241/1990 definisce come controinteressati "*tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza*".

Secondo giurisprudenza, sono controinteressati tutti coloro i quali, anche se non sono nominati o coinvolti nel documento che incorpora le informazioni cui si vuole accedere, potrebbero vedere pregiudicato il loro diritto alla riservatezza (Cons. Stato, sez. III, 21.02.2013, n. 1065).

Per la qualifica di controinteressato, rispetto al diritto di accesso a documenti, non è, però, sufficiente che un soggetto sia, in qualche modo nominato nel documento richiesto, essendo necessario, invece, che costui sia titolare di un diritto alla riservatezza dei dati racchiuso nello stesso documento (così Cons. Stato, sez. IV, 4.10.2019).

Ai sensi dell'art. 3 D.P.R. 184/2006, la pubblica amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, è tenuta a dare comunicazione agli stessi, mediante raccomandata con avviso di ricevimento o per via telematica.

Tale comunicazione consente la partecipazione dei controinteressati al procedimento relativo all'esame dell'istanza di accesso, anche mediante la possibilità di presentare una motivata opposizione alla richiesta di accesso, nel termine di dieci giorni decorso il quale la P.A. provvede sulla richiesta.



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

L'amministrazione non può legittimamente assumere quale unico fondamento del diniego di accesso agli atti la mancanza del consenso all'accesso da parte dei soggetti controinteressati, in quanto spetta sempre all'amministrazione il potere-dovere di valutare la fondatezza della richiesta stessa, anche in contrasto con l'opposizione eventualmente manifestata dai controinteressati (T.A.R Calabria, sez. I, 16.05.2015, n. 281). In assenza di contro interessati, secondo quanto previsto dall'art. 5 del D.P.R. n. 184/2006, disciplinante il c.d. accesso informale " *il diritto di accesso può essere esercitato in via informale mediante richiesta, anche verbale, all'Ufficio dell'amministrazione competente a formare l'atto conclusivo del procedimento o a detenerlo stabilmente*" (vedasi anche l'art. 33 del Regolamento comunale).

- Conclusione del procedimento

Ai sensi dell'art. 25, comma 3, L. 241/1990, il rifiuto, il differimento e la limitazione dell'accesso devono essere motivati. Decorsi inutilmente trenta giorni dalla richiesta, questa si intende, tuttavia, respinta.

Secondo l'opinione prevalente, che fa leva sul dato letterale dell'art. 25 L. 241/1990, l'inerzia serbata dall'amministrazione sull'istanza di accesso agli atti assume il significato di provvedimento tacito di rigetto dell'istanza.

Pertanto, decorsi 30 giorni dalla presentazione dell'istanza, l'istanza si intende rifiutata.

SCHEDA DI SINTESI - ACCESSO DOCUMENTALE

- **Legittimazione passiva:** i titolari di un interesse diretto, concreto e attuale corrispondente ad una situazione giuridicamente tutelata e collegata al documento richiesto (obbligo di motivazione dell'istanza);
- **Oggetto:** documenti amministrativi materialmente esistenti;
- **Limiti tassativi:** segreto di Stato; procedimenti tributari; atti normativi, amministrativi generali, di pianificazione e di programmazione, procedimenti selettivi e informazioni psico-attitudinali;
- **Limiti eventuali:** sicurezza nazionale, politica economica, monetaria, valutaria, ordine pubblico e riservatezza;
- **Controinteressati:** soggetti individuabili sulla base del documento richiesto titolari di un diritto alla riservatezza (obbligo di preventiva comunicazione) – in difetto accesso informale;

4.2 L'accesso civico c.d. semplice

L'art. 5 D.Lgs. 33/2013, nella sua prima formulazione, ha introdotto l'istituto dell'accesso civico c.d. semplice, direttamente connesso agli obblighi di pubblicità gravanti sulla pubblica amministrazione.



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

Si tratta, nello specifico, di una sorta di sanzione che l'ordinamento ha previsto al fine di garantire il rispetto degli obblighi di trasparenza imposti dalla legge.

- Legittimazione

La titolarità della pretesa alla esibizione documentale è attribuita dalla legge in capo a "chiunque".

Non sussiste, dunque, alcun limite soggettivo di legittimazione, non essendo necessario dimostrare alcuno specifico interesse alla pretesa ostensiva.

Ciò è coerente con la *ratio* stessa dell'istituto di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali.

- Oggetto

L'accesso civico ha ad oggetto dati, informazioni o documenti di cui sia obbligatoria la pubblicazione ed è connesso al diritto di chiunque di richiedere i medesimi nei casi in cui sia stata omessa la loro pubblicazione. In tale prospettiva, si spiega dunque l'assenza dell'obbligo di motivare la relativa istanza.

- Costi

Questa *species* di accesso – a differenza di quello disciplinato dalla L. 241/1990 – è caratterizzata dalla totale gratuità del servizio di esibizione, "*salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali*" (art. 5 co. 4 D.Lgs. 33/2013).

Secondo quanto indicato dalla Circolare Ministeriale n. 2/2019, è possibile addebitare al richiedente i soli costi di riproduzione e di spedizione dei documenti (se superiori a 20 pagine), mentre la consultazione in loco e l'accesso elettronico o tramite i registri è gratuita.

L'importanza fondamentale del diritto di accesso civico generalizzato esclude, in definitiva, che il rimborso possa costituire un ostacolo economico all'esercizio del diritto.

La citata Circolare – a cui si rinvia per ulteriori approfondimenti sul regime dei costi – suggerisce, infine, di predeterminare i costi mediante un tariffario e comunque di prospettarli al richiedente prima delle attività di riproduzione.

Non si esclude, infine, che ai costi addebitabili al richiedente possano cumularsi – come avviene per l'accesso procedimentale alla documentazione urbanistica e/o edilizia – gli oneri in materia di bollo e i diritti di ricerca e visura.



COMUNE DI GENOVA

- Limiti

La latitudine dell'accesso civico semplice coincide con l'ambito degli obblighi di legge che l'amministrazione è tenuta a rispettare in tema di trasparenza, così come delineati dagli artt. 13 e ss. D.Lgs. 33/2013.

- Conclusione del procedimento

Secondo quanto previsto dall'art. 5, comma 6 del D.lgs. n. 33/2013, il procedimento deve concludersi con un **provvedimento espresso e motivato** entro il termine di trenta giorni dalla presentazione dell'istanza con una comunicazione trasmessa a richiedente e eventuali controinteressati.

Non è, dunque, prevista la disciplina del silenzio-diniego, in caso di inerzia dell'amministrazione.

In caso di diniego, il richiedente può presentare istanza di **riesame** al responsabile della prevenzione della corruzione e della trasparenza che decide, con provvedimento motivato, entro venti giorni.

SCHEDA DI SINTESI – ACCESSO CIVICO SEMPLICE

-**Legittimazione:** chiunque

-**Oggetto:** dati, informazioni o documenti di cui sia obbligatoria la pubblicazione, nei casi in cui la stessa sia stata omessa.

-**Limiti:** obblighi di trasparenza di cui agli artt. 13 e ss. D.Lgs. n. 33/2013

-**Costi:** totale gratuità, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali

4.3 L'accesso civico c.d. generalizzato

Tale tipologia di accesso è stata introdotta con D. Lgs. 97/2016, a modifica ed integrazione del D. Lgs. 33/2013, *“allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico”*.

- Legittimazione

l'art. 5 co. 2 D.Lgs. 33 cit. attribuisce a *“chiunque”* il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, secondo quanto previsto dall'articolo 5-bis.

Come l'accesso civico semplice, si traduce in un diritto di accesso non condizionato dalla titolarità di situazioni giuridicamente rilevanti, non essendo preordinato alla tutela di una propria posizione giuridica soggettiva.



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

Non essendo dunque richiesta la prova di un interesse specifico, la relativa istanza non richiede motivazione. Conseguentemente, lo strumento in esame può essere utilizzato solo per evidenti ed esclusive ragioni di tutela di interessi propri della collettività generale dei cittadini, non anche a favore di interessi riferibili, nel caso concreto, a singoli individui od enti associativi particolari (Cons. Stato, sez., 12.02.2020, n. 1121).

In altri termini, l'accesso civico generalizzato può avere ad oggetto dati, informazioni e documenti la cui ostensione si palesi come espressiva di un interesse conoscitivo generale, in coerenza con la finalità dell'istituto di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

- Oggetto

L'istanza può riguardare *“tutti i dati e i documenti e informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione”* e, come chiarito dalle Linee guida ANAC sopra richiamate, i limiti e le esclusioni previste dall'art. 5-*bis* rappresentano eccezioni e, come tali, non possono che essere interpretati restrittivamente.

Il riferimento ai “dati” o alle “informazioni” è, quindi, espressione di un obbligo informativo più ampio rispetto all'accesso documentale, in quanto esula dal supporto fisico su cui potrebbe essere incorporato il dato conoscitivo posseduto dall'amministrazione.

Si evidenzia, in ogni caso, che secondo le Linee Guida ANAC *“resta escluso che (...) l'amministrazione sia tenuta a formare o raccogliere o altrimenti procurarsi informazioni che non siano già in suo possesso. Pertanto, l'amministrazione non ha l'obbligo di rielaborare i dati ai fini dell'accesso generalizzato, ma solo a consentire l'accesso ai documenti nei quali siano contenute le informazioni già detenute e gestite dall'amministrazione stessa”*.

Le richieste, inoltre, non devono essere generiche, ma consentire l'individuazione del dato, del documento o dell'informazione, con riferimento, almeno, alla loro natura e al loro oggetto.

Ancora, sempre secondo le citate Linee Guida ANAC, *“nei casi particolari in cui venga presentata una domanda di accesso per un numero manifestamente irragionevole di documenti, imponendo così un carico di lavoro tale da paralizzare, in modo molto sostanziale, il buon funzionamento dell'amministrazione, la stessa può ponderare, da un lato, l'interesse dell'accesso del pubblico ai documenti e, dall'altro, il carico di lavoro che ne deriverebbe, al fine di salvaguardare, in questi casi particolari e di stretta interpretazione, l'interesse ad un buon andamento dell'amministrazione”*.



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

Secondo la circolare n. 2.2017 del Ministero della Pubblica Amministrazione, la ragionevolezza della richiesta va, infine, valutata tenendo conto dei seguenti criteri:

- l'eventuale attività di elaborazione (ad es. oscuramento di dati personali) che l'amministrazione dovrebbe svolgere per rendere disponibili i dati e documenti richiesti;
- le risorse interne che occorrerebbe impiegare per soddisfare la richiesta, da quantificare in rapporto al numero di ore di lavoro per unità di personale;
- la rilevanza dell'interesse conoscitivo che la richiesta mira a soddisfare;

- Costi

cfr. in accesso civico semplice

- Limiti

L' art. 5-bis D.Lgs. n. 33/2013 prevede tre ordini di limiti:

- A) limiti a tutela di interessi pubblici inerenti alla sicurezza pubblica e all'ordine pubblico, alla sicurezza nazionale, alla difesa, alle relazioni internazionali, alla politica e alla stabilità finanziaria ed economica dello Stato, alla conduzione di indagini sui reati e il loro perseguimento, al regolare svolgimento di attività ispettive (co. 1);
- B) limiti a tutela di interessi privati inerenti alla protezione dei dati personali, alla libertà e alla segretezza della corrispondenza, agli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali (co. 2);
- C) limiti assoluti, nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, "ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990" (art. 5-bis co. 3).

I limiti sub A) e B) presentano carattere relativo e, pertanto, l'eventuale applicazione degli stessi è rimessa ad una valutazione dell'amministrazione che tenga conto di eventuali interessi contrapposti.

Diversamente, i limiti sub C) sono considerati assoluti e, come tali, non suscettibili di bilanciamento: l'accesso generalizzato è sempre escluso nei casi di segreto di Stato e negli altri casi in cui una norma di legge abbia espressamente disposto la non ostensibilità di dati, documenti, informazioni.

Negli altri casi, si rinvia, invece, ad un'attività valutativa dell'amministrazione tenuta a compiere un bilanciamento, caso per caso, tra interesse pubblico all'accesso generalizzato e la tutela di altrettanto



COMUNE DI GENOVA

rilevanti interessi presi in considerazione dall'ordinamento.

La legge specifica, inoltre, che i suindicati limiti trovano esclusiva applicazione per il periodo nel quale la protezione è giustificata in relazione alla natura del dato e che in ogni caso l'accesso civico non può essere negato ove, per la tutela di tali interessi, sia sufficiente fare ricorso al potere di differimento.

Le richiamate linee guida ANAC, adottate in attuazione di quanto disposto dall'art. 5 bis, comma 6 del D.lgs. n. 33/2103, d'intesa con il Garante per la Privacy, assolvono la funzione di fornire alcune prime indicazioni utili a dare supporto alle amministrazioni nella identificazione degli interessi pubblici considerati dal citato art. 5 bis.

- Controinteressati

In base all'art. 5, comma 5, del D.lgs. n. 33/2013, *«Fatti salvi i casi di pubblicazione obbligatoria, l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione».*

Sono qualificabili come controinteressati tutti i soggetti che possono subire un pregiudizio concreto agli interessi privati indicati dall'art. 5-bis, comma 2, del citato decreto, quali protezione dei dati personali (riferibili a persone fisiche identificate o identificabili), libertà e segretezza della corrispondenza, interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali.

Due sono le possibili modalità di comunicazione ai controinteressati: *“con raccomandata con avviso di ricevimento”* o *“per via telematica per coloro che abbiano consentito tale forma di comunicazione”*.

La finalità di questa disposizione è consentire ai controinteressati di esercitare il diritto di difesa nell'ambito del procedimento amministrativo di accesso e la comunicazione deve, pertanto, essere effettuata anche quando il numero di controinteressati sia elevato (eventualmente ricorrendo all'utilizzo di posta elettronica certificata (PEC)).

Qualora non sia possibile procedere a mezzo PEC e il numero di controinteressati sia così elevato da rischiare di arrecare un pregiudizio economico e/o organizzativo all'attività amministrativa, la citata Circolare Ministeriale suggerisce di consentire l'accesso parziale, oscurando i dati personali o le parti dei documenti richiesti che possano ledere gli interessi privati coinvolti.



COMUNE DI GENOVA

SCHEDE DI SINTESI - ACCESSO CIVICO GENERALIZZATO

-Legittimazione: chiunque;

-Oggetto: tutti i dati e i documenti e informazioni detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli per i quali è stabilito un obbligo di pubblicazione;

-Limiti a tutela dell'interesse pubblico: sicurezza pubblica e ordine pubblico, sicurezza nazionale, difesa, relazioni internazionali, politica e stabilità finanziaria ed economica dello Stato, conduzione di indagini sui reati e il loro perseguimento, regolare svolgimento di attività ispettive (art. 5-bis co. 1 D.Lgs. n. 33/2013);

-Limiti a tutela dell'interesse privato: protezione dei dati personali (riferibili a persone fisiche identificate o identificabili), libertà e segretezza della corrispondenza, interessi economici e commerciali di una persona fisica o giuridica, ivi compresi proprietà intellettuale, diritto d'autore e segreti commerciali (art. 5-bis co. 2 D.Lgs. n. 33/2013);

-Controinteressati: tutti i soggetti che possono subire un pregiudizio concreto agli interessi privati indicati dall'art. 5-bis, comma 2, del decreto citato.

4.4. I confini tra accesso civico generalizzato e accesso documentale

Tenere ben distinte le due fattispecie è essenziale per calibrare i diversi interessi in gioco allorché si renda necessario contemperare interessi in conflitto.

Come evidenziato dalle Linee guida ANAC, l'accesso di cui alla legge n. 241/90 può consentire una conoscenza maggiormente approfondita limitata però a specifici documenti, mentre nel caso dell'accesso generalizzato, le esigenze di controllo diffuso del cittadino devono consentire un accesso che assicuri – da un punto di vista quantitativo – una larga conoscibilità di dati, documenti e informazioni, seppure meno approfondito sul piano qualitativo.

L'accesso documentale di cui agli artt. 22 e ss L. 241/1990, pur essendo finalizzato a garantire l'imparzialità e la trasparenza dell'azione amministrativa e a favorirne lo svolgimento imparziale, non si configura, infatti, come un'azione popolare, esercitabile da chiunque, stante l'inammissibilità di istanze preordinate ad un controllo generalizzato dell'operato della pubblica amministrazione (art. 24, comma 3, L. 241/1990).

L'accesso civico, invece, è riconosciuto proprio allo scopo di favorire forme diffuse di controllo sulle funzioni istituzionali delle amministrazioni e sull'utilizzo delle relative risorse patrimoniali, economiche e lavorative.

Si segnala, inoltre, che secondo la recente decisione dell'Adunanza Plenaria, in materia di accesso civico e documentale, *“la pubblica amministrazione ha il potere-dovere di esaminare l'istanza di accesso agli atti e ai documenti pubblici, formulata in modo generico o cumulativo dal richiedente senza riferimento ad una specifica disciplina, anche alla stregua della disciplina dell'accesso civico generalizzato, a meno che l'interessato non abbia inteso fare esclusivo, inequivocabile, riferimento alla disciplina dell'accesso*



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

documentale, nel qual caso essa dovrà esaminare l'istanza solo con specifico riferimento ai profili della l. n. 241 del 1990, senza che il giudice amministrativo, adito ai sensi dell'art. 116 c.p.a., possa mutare il titolo dell'accesso, definito dall'originaria istanza e dal conseguente diniego adottato dalla pubblica amministrazione all'esito del procedimento" (Cons. Stato, Ad. Plen., 2.04.2020, n. 10).

Solo ove l'istante abbia inteso, espressamente e inequivocabilmente, limitare l'interesse ostensivo ad uno specifico profilo, quello documentale o quello civico, la pubblica amministrazione dovrà, dunque, limitarsi ad esaminare quello specifico profilo, senza essere tenuta a pronunciarsi sui presupposti dell'altra forma di accesso, non richiesta dall'interessato.

5. L'accesso alle informazioni ambientali

Il D.Lgs. 195/2005, in attuazione della Direttiva 2003/4/CE, disciplina l'accesso del pubblico all'informazione ambientale, disponendo che l'autorità pubblica rende disponibile l'informazione ambientale detenuta a chiunque ne faccia richiesta, senza che questi debba dichiarare il proprio interesse.

Si tratta dunque di una fattispecie che, discostandosi nettamente dall'accesso documentale di cui alla L. 241/1990, si pone piuttosto come una forma *ante litteram* di accesso generalizzato, al fine di assicurare una più pervasiva tutela dell'interesse ambientale.

Il novero delle notizie accessibili riguarda le "informazioni ambientali" che possono quindi implicare anche un'attività elaborativa da parte dell'Amministrazione debitrice delle comunicazioni richieste.

In giurisprudenza, è stato osservato che a fronte della particolare ampiezza delle informazioni ambientali, non osta alla loro divulgazione una eventuale "copiosa mole" dei dati richiesti, posto che si tratta di una condizione intrinseca alla qualità delle informazioni stesse che, per loro natura, hanno ad oggetto molteplici e complessi indicatori di natura tecnica e specialistica; del resto, è proprio la particolare complessità della informazione ambientale che, nell'interesse di una conoscenza diffusa delle condizioni degli elementi costitutivi dell'ecosistema e dei fenomeni antropici, richiede la condivisione con gli interessati di tutti i dati scientifici relativi agli elementi fisici, chimici e biologici che ne determinano l'assetto (così T.A.R Lazio, sez. II-ter, 27.02.2018, n. 2141).

Sono escluse solo le richieste manifestamente irragionevoli e formulate in termini eccessivamente generici, ma in un'ottica di massima cooperazione, l'autorità che detiene l'informazione ambientale di fronte a una domanda formulata in maniera eccessivamente generica "*può chiedere al richiedente, al più*



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

presto e, comunque, entro 30 giorni dalla data del ricevimento della richiesta stessa, di specificare i dati da mettere a disposizione, prestandogli a tale scopo la propria collaborazione” (art. 3, comma 3 del decreto).

6. L'accesso dei Consiglieri Comunali e Provinciali

L'art. 43 co. 2 TUEL attribuisce ai consiglieri comunali e provinciali il diritto di ottenere dagli uffici, rispettivamente, del comune e della provincia, nonché dalle loro aziende ed enti dipendenti, tutte le notizie e le informazioni in loro possesso, utili all'espletamento del proprio mandato.

Fermo restando che gli stessi sono tenuti al segreto nei casi specificamente determinati dalla legge.

Si tratta di una fattispecie che presenta carattere derogatorio rispetto alla disciplina generale dell'accesso, in quanto funzionale alla cura di un interesse pubblico connesso al mandato democratico di cui è portatore.

In questo caso l'accesso è infatti volto a consentire al consigliere comunale di poter esercitare il proprio munus verificando e controllando il comportamento degli organi istituzionali decisionali dell'Ente.

Si tratta, quindi, di un diritto molto più ampio rispetto a quello disciplinato dalla legge n. 241/1990: il diritto di accesso, infatti, prescinde da un interesse diretto, concreto e attuale del Consigliere Comunale e risulta esperibile nei confronti di qualsiasi atto/documento ritenuto utile per l'espletamento del proprio mandato; è esente da particolari obblighi di motivazione e/o formalità.

Al pari dell'accesso documentale, però, la richiesta di accesso agli atti del Consigliere Comunale non può obbligare l'amministrazione alla formazione di un documento allo stato non ancora materialmente esistente (così Cons. Stato, sez. IV, 12.02.2013, n. 846).

7. La tutela del diritto di accesso

7.1. La tutela giustiziale

Avverso il diniego o il differimento di accesso (sia civico che documentale) è, anzitutto, possibile esperire, tramite ricorso, una tutela di tipo giustiziale che nel caso di amministrazioni comunali si svolge dinanzi al

Difensore Civico.

Tale ricorso non esclude la possibilità di avvalersi della tutela giurisdizionale: i termini per il ricorso al giudice amministrativo sono, infatti, sospesi fino alla conclusione del procedimento avviato innanzi al Difensore Civico.



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

L'istanza al difensore civico deve essere presentata entro il termine di trenta giorni dal diniego e se nei successivi trenta giorni non interviene una decisione, essa si intende rigettata.

Qualora, invece, il difensore civico ritenga illegittimo il diniego o il differimento, ne dà immediata comunicazione all'istante e all'amministrazione coinvolta, la quale, nei successivi trenta giorni, deve confermare la propria precedente decisione, ovvero, consentire l'accesso.

In caso di mancata pronuncia da parte dell'amministrazione interessata, l'accesso si intende consentito (silenzio-assenso).

7.2. La tutela giurisdizionale

Il ricorso al **giudice amministrativo** avverso le determinazioni sulle istanze di ostensione documentale è disciplinato dall'art. 116 c.p.a. (la cui applicazione è estesa anche alla tutela del diritto di accesso civico semplice e generalizzato) e deve essere promosso, a pena di decadenza, nel termine di 30 giorni dal provvedimento espresso di rigetto o dal formarsi del silenzio diniego sull'istanza.

Ancorché configurato come impugnatorio, il giudizio che ne scaturisce è sostanzialmente volto ad accertare la sussistenza o meno del diritto di accesso del ricorrente ai documenti amministrativi di cui ha chiesto l'ostensione, indipendentemente dalla maggiore o minore correttezza delle ragioni addotte dall'Amministrazione per giustificare il diniego ovvero dal silenzio da questa serbato sull'istanza.

Ne consegue che il giudice amministrativo, nel contraddittorio con l'amministrazione ed eventuali controinteressati, può ordinare in caso di accoglimento del ricorso, l'esibizione e, ove previsto, la pubblicazione dei documenti richiesti.

Il controinteressato che intenda tutelare il proprio interesse alla riservatezza è legittimato ad impugnare il provvedimento che accolga la richiesta di ostensione.

7.3 La tutela penale del diritto di accesso: rapporto tra inerzia della P.A. e art. 328 c.p.

L'art. 328 c.p. punisce il fatto del pubblico ufficiale o dell'incaricato di pubblico servizio che, entro trenta giorni dalla richiesta di chi vi abbia interesse, non compie l'atto del suo ufficio o non risponde per esporre le ragioni del ritardo.

Ai fini della rilevanza penale dell'inerzia della P.A. a fronte di un'istanza di accesso agli atti, occorre distinguere tra accesso documentale e accesso civico.

Nel primo caso, secondo l'opinione prevalente l'inerzia non integrerebbe il reato di omissione di atti d'ufficio, alla luce del significato di provvedimento negativo tacito che l'art. 25 L. 241/90 attribuisce al silenzio della P.A..



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

In altri termini, il silenzio diniego è considerato concettualmente incompatibile con la nozione penalistica di omissione.

Seguendo questa impostazione, potrebbe assumere, per contro, rilevanza penale il silenzio serbato sulle istanze di accesso civico, per le quali il D.Lgs. 33/2013 espressamente esclude il formarsi di un silenzio significativo valutabile come provvedimento tacito, con la conseguenza che non vi sarebbero particolare ostacoli alla configurabilità dell'azione penale.

8. Note operative per la gestione delle istanze di accesso agli atti

Per una corretta gestione delle istanze di accesso agli atti si ritiene opportuno considerare la scansione temporale delle seguenti fasi:

- ricezione della domanda;
- comunicazione di avvio del procedimento;
- individuazione di eventuali controinteressati;
- individuazione di eventuali limiti o divieti e valutazione della fondatezza della domanda di accesso;
- accoglimento totale o parziale dell'istanza;
- diniego dell'istanza.

Ricezione della domanda. Ricevuta la richiesta di accesso agli atti, per via telematica ovvero per posta, anche ordinaria, è necessario procedere alla sua protocollazione. La richiesta può pervenire direttamente all'Ufficio che detiene il documento richiesto, ovvero all'U.R.P., ovvero ancora essere indirizzata genericamente al Comune di Genova.

A decorrere dal gennaio 2021, come indicato nelle note operative trasmesse dalla Segreteria Generale, le istanze di accesso civico semplice, civico generalizzato e documentale, devono essere oggetto di registrazione nell'apposito "Registro Accessi".

In questa prima fase, è opportuno esaminare l'istanza al fine di individuare la disciplina applicabile (accesso civico o accesso documentale) con particolare attenzione all'eventuale motivazione della richiesta e agli eventuali riferimenti normativi indicati dallo stesso richiedente, in quanto, come già osservato, solo ove l'istante abbia espressamente e inequivocabilmente voluto limitare l'interesse all'accesso ad uno specifico profilo (civico o documentale), l'amministrazione dovrà limitarsi ad esso (così Cons. Stato, Ad. Plen. n.10/2020).



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

Comunicazione di avvio del procedimento. Ricevuta e protocollata l'istanza di accesso agli atti, è poi opportuno procedere con le comunicazioni di avvio del procedimento ex art. 7, legge n. 241/1990, con indicazione della data di ricezione e protocollazione dell'istanza e individuazione dell'Ufficio responsabile.

In caso di istanze generiche o incomplete potrebbe essere opportuno richiedere integrazioni o chiarimenti, specie qualora non siano identificati in modo preciso i dati, le informazioni o i documenti richiesti.

Individuazione di eventuali limiti o divieti e valutazione della fondatezza della domanda di accesso.

Nell'esaminare la fondatezza dell'istanza, opportunamente qualificata e individuata la disciplina applicabile, anche all'esito di eventuali controdeduzioni dei controinteressati, occorre verificare la sussistenza della legittimazione all'accesso e la presenza di eventuali limiti tassativi o eventuali imposti dalla relativa disciplina, oltre a valutare la necessità o meno di attività di rielaborazione del dato o informazione richiesti, in relazione ad esempio alla necessità di oscurare dati sensibili, in considerazione anche del carico di lavoro che la richiesta possa imporre, nel rispetto del principio di buon andamento della pubblica amministrazione.

Accoglimento totale o parziale dell'istanza. In caso di accoglimento totale o parziale dell'istanza, comunicato il provvedimento di accoglimento anche agli eventuali controinteressati, occorre individuare i documenti/dati/informazioni cui si concede l'accesso, concordando le modalità ostensive (visione o estrazione di copia), informando adeguatamente il richiedente degli eventuali costi.

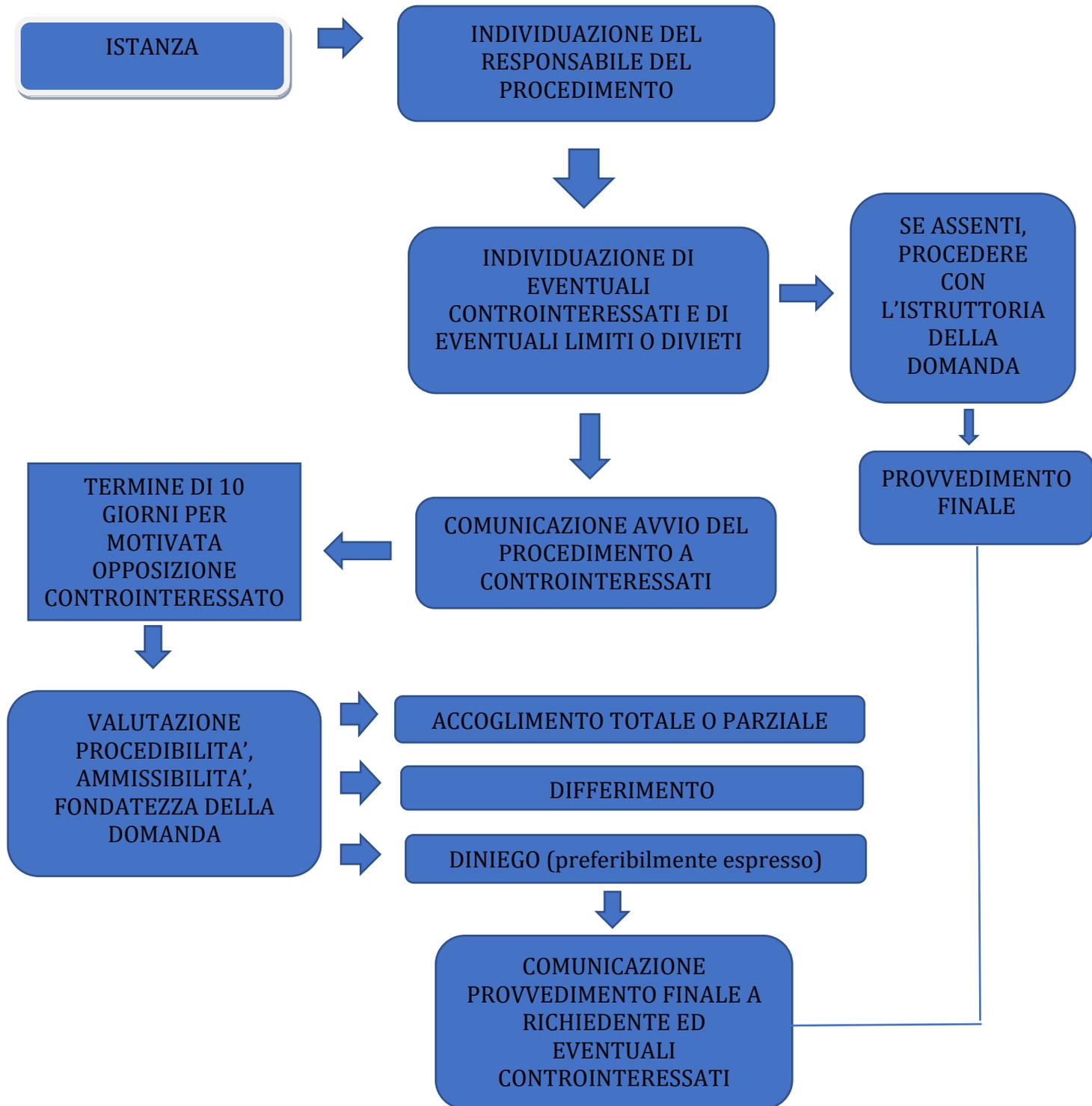
Si suggerisce, quindi, di predisporre un elenco della documentazione che sarà consegnata (in visione o in copia), unitamente ad un verbale delle operazioni di accesso, che dovrà essere sottoscritto anche dal richiedente.

Diniego dell'istanza. In caso di diniego dell'istanza, da adottarsi, per ragioni di trasparenza, preferibilmente in forma espressa, il provvedimento dovrà essere adeguatamente motivato, indicando i presupposti di fatto e le ragioni di diritto giustificanti il diniego.

In relazione all'accesso documentale, si evidenzia che, in caso di inerzia, trascorsi trenta giorni dalla presentazione della domanda, la stessa si intende respinta.



COMUNE DI GENOVA





COMUNE DI GENOVA

9. Note operative per un corretto bilanciamento tra accesso e riservatezza

Come detto, l'accesso documentale e l'accesso civico documentale sono suscettibili di interferire sulla posizione di soggetti che vedrebbero compromesso il proprio diritto alla riservatezza.

Sul piano operativo, occorre dunque sempre porsi il problema dell'esistenza di eventuali controinteressati in sede di esame di un'istanza di accesso.

In primo luogo, la presenza di controinteressati:

- impedisce alla P.A. di accettare istanze di accesso informali;
- impone di notificarli dell'istanza con le modalità previste dal D.P.R. 184/2006, al fine di consentire la loro partecipazione al procedimento e di presentare entro il termine di 10 giorni motivata opposizione;
- obbliga la P.A. a valutare le deduzioni dagli stessi eventualmente formulate;
- può suggerire l'opportunità di limitare l'accesso alla sola presa visione, omettendo le parti di documento riferite a soggetti terzi (cfr. art. 37 co. 2 Regolamento comunale) o in alternativa di utilizzare in via preferenziale il potere di differimento dell'ostensione degli atti alla conclusione del procedimento, in applicazione dell'art. 23 co. 4 L. 241/90 e dell'art. 9 D.P.R. 12 aprile 2006 n. 184, adeguatamente motivando in ordine a tale scelta.

L'art. 25 co. 3 L. 241/90 dispone infatti che "Il rifiuto, il differimento e la limitazione dell'accesso sono ammessi nei casi e nei limiti stabiliti dall'articolo 24 e debbono essere motivati".

In proposito, si segnala tuttavia che la giurisprudenza è molto rigorosa nell'affermare che la scelta di differimento "... deve figurare come il risultato di una consona, pertinente e motivata valutazione, espressamente riportata nel provvedimento di riscontro alla richiesta di accesso o, comunque, facilmente desumibile dai contenuti di quest'ultimo, che si presti a dare atto della sussistenza di negative interferenze tra un eventuale accesso e lo svolgimento della funzione amministrativa, così come prescritto dall'art. 24, ultimo comma, della legge n. 241/90, ovvero della necessità di assicurare una temporanea tutela degli interessi di cui all'art. 24, comma 2, della medesima legge.

Ne consegue che l'atto che dispone il differimento dell'accesso deve indicare la sussistenza delle predette circostanze legittimanti, che devono essere rapportate alle concrete esigenze organizzative dell'amministrazione e non possono risolversi in mere "formule di stile", attraverso un generico richiamo al principio di buon andamento dell'azione amministrativa" (fra le più recenti, T.A.R Lazio, Roma, sez. I, 11.12.2020, n. 13331).



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |





COMUNE DI GENOVA

L'Avvocatura rimane a disposizione per fornire tutti gli ulteriori chiarimenti che si renderanno necessari. Il presente documento verrà pubblicato sulla INTRANET del Comune, Area Direzioni, Avvocatura, Linee Guida su applicazione istituti giuridici, per una maggiore visibilità.

Genova, 24 dicembre 2020

avv. Gabriella Bozzone

Firmato digitalmente da: Gabriella Bozzone
Data: 24/12/2020 10:33:24

avv. Nicola Rossi

Firmato digitalmente da: ROSSI NICOLA
Ruolo: 4.6 Avvocato
Organizzazione: ORDINE DEGLI AVVOCATI DI GENOVA
Data: 24/12/2020 10:28:53

Il Dirigente del Settore di Diritto Amministrativo

avv. Maria Paola Pessagno

PESSAGNO MARIA PAOLA
2020.12.24 10:59:51
CN=PESSAGNO MARIA PAOLA
C=IT
O=COMUNE DI GENOVA
2.5.4.97=VATTI-00866930102
RSA/2048 bits



Comune di Genova | Direzione Avvocatura |
Via Garibaldi 9 | 16124 Genova |
Tel 0105572470/5572596 – Fax 0105572695 |
avvocatura@comune.genova.it |

