Comune di
Montelupo
Fiorentino

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

(Regolamento adottato ai sensi degli artt. 3 e 5 del DPCM 3.12.2013)

COMUNE DI MONTELUPO FIORENTINO
Area Organizzativa Omogenea: AOOCMF

COMUNE DI MONTELUPO FIORENTINO
VIALE CENTO FIORI, 34 - 50056 MONTELUPO F.NO (FI)
TELEFONO 0571 9174
POSTA CERTIFICATA: comune.montelupo-fiorentino@postacert.toscana.it
P. IVA: 00614510485
www.comune.montelupo-fiorentino.fi.it

Sommario

PRINCIPI GENERALI

1.1. Premessa

Il DPCM 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico", articolo 3, comma 1, lettera d), prevede l'adozione del manuale di gestione per tutte le amministrazioni di cui all'articolo 2, comma 2, del decreto legislativo 7 marzo 2005, n. 82, Codice dell'Amministrazione Digitale. Il manuale di gestione, disciplinato dal successivo art. 5, comma 1, "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".

In questo ambito il Comune di Montelupo F.no ha individuato l'Area Organizzativa Omogenea, all'interno della quale, con Delibera di Giunta 19 del 19/03/2015, è nominato il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 50 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR n. 445 del 28 dicembre 2000).

Il protocollo informatico costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'attività dell'amministrazione.

Il Manuale di gestione ha l'obiettivo di riunire tutte le misure organizzative e tecniche per l'attuazione di un percorso di completa digitalizzazione dell'Ente, a partire dalla fase di protocollazione della corrispondenza fino ad una completa gestione documentale.

Il manuale 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 e archiviazione dei documenti.

Il presente documento, 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.

Il manuale è articolato in due parti: nella prima vengono indicati l'ambito di applicazione, le definizioni usate e i principi generali del sistema, nella seconda sono descritte analiticamente le procedure di gestione dei documenti e dei flussi documentali.

1.2. Ambito di applicazione

Il presente manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'articolo 3, comma 1, lettera d) del decreto del Presidente del Consiglio del 3 dicembre 2013 concernente le "Regole tecniche per il protocollo informatico".

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre alla gestione dei flussi documentali ed archivistici.

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

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intendono le definizioni in "allegato 1"

Di seguito si riportano acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **MdG** - Manuale di Gestione del protocollo informatico, gestione documentale e degli archivi;
- **RPA** - Responsabile Procedimento Amministrativo- il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RGD** - Responsabile della Gestione documentale;
- **SdP** – Servizio di protocollo informatico;
- **UOP** - Ufficio di registrazione di Protocollo;
- **UOR** - Ufficio di Gestione - ufficio dell'AOO che utilizza i servizi messi a disposizione dal servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le norme ed i regolamenti di riferimento vedasi l'elenco riportato in "allegato 2".

1.4. Area Organizzativa Omogenea

Per la gestione dei documenti, l'amministrazione ha istituito con Delibera di Giunta 19 del 19/03/2015 un'unica Area Organizzativa Omogenea (AOO) dove è costituito un unico servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi.
L'AOO, denominata **AOOCMF,** è stata registrata all'IPA (Indice delle Pubbliche Amministrazioni).

All'interno dell'amministrazione il sistema archivistico è unico.

All'interno della AOO il sistema di protocollazione è distribuito: la corrispondenza, in ingresso è gestita da alcune UOP, in uscita è gestita direttamente da tutti gli UOR dell'amministrazione.

La struttura organizzativa dell'Amministrazione è riportata in "allegato 3".

1.5. Servizio per la gestione informatica del protocollo

Nella AOO è costituito 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 Delibera di Giunta 83 del 08/10/2015;
In relazione alla modalità di fruizione del servizio di protocollo adottata dalla AOO, è compito del servizio:

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale sul sito istituzionale dell'amministrazione;
- abilitare gli utenti dell'AOO all'utilizzo del SdP e definire per ciascuno di essi il tipo di funzioni autorizzate;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta conservazione della copia del registro giornaliero di protocollo;
- sollecitare il ripristino del servizio in caso di indisponibilità del medesimo;

- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili nel SdP.

1.6. Firma digitale

Per l'espletamento delle attività istituzionali l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla. In "'allegato 4" viene riportato l'elenco delle persone titolari di firma digitale.

1.7. Conservazione delle copie

Nell'ambito del servizio di gestione informatica del protocollo si individuano due componenti:

- backup della banca dati, assicurato dal piano della sicurezza di cui al capitolo 2;
- conservazione del registro informatico giornaliero di protocollo. Al fine di garantire la non modificabilità delle operazioni di registrazione, al termine della giornata lavorativa il registro viene generato automaticamente dal sistema in formato pdf, e entro il giorno successivo, inviato in conservazione.

1.8. Caselle di Posta Elettronica

L'AOO è dotata di una casella di posta elettronica certificata istituzionale per la corrispondenza, sia in ingresso che in uscita.

La casella ha il seguente indirizzo: comune.montelupo-fiorentino@postacert.toscana.it

Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici dell'Amministrazione.

Il presidio della casella di posta elettronica certificata istituzionale è svolto dall'UOP SEGRETERA GENERALE.

1.9. Sistema di classificazione dei documenti

Nell'ambito dell'utilizzo del sistema di protocollo informatico, viene adottato un unico titolario di classificazione.

Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.

Il titolario di classificazione adottato dall'Amministrazione è quello riportato in "allegato 5"

1.10. Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione stabilisce percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

1.11. Accreditamento dell'AOO all' IPA

L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA), fornendo le informazioni che individuano l'AOO e la sua struttura organizzativa.

Il codice identificativo dell'amministrazione è stato generato e attribuito autonomamente dall'amministrazione. L'indice delle pubbliche amministrazioni (IPA) è accessibile tramite il relativo sito internet da parte di tutti i soggetti pubblici o privati.

L'amministrazione comunica tempestivamente all' IPA ogni successiva modifica delle proprie credenziali di riferimento e la data in cui la modifica stessa sarà operativa, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività l'amministrazione comunica la soppressione, ovvero la creazione di una AOO.

1.12. Il Responsabile della conservazione

Il Responsabile della Conservazione opera d'intesa con il Responsabile della Gestione documentale, con il Responsabile del trattamento dei dati personali e con il Responsabile della sicurezza informatica.

Il Responsabile della Conservazione in particolare:

- definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare;
- 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, 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;
- assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- predispone il manuale di conservazione e ne cura l'aggiornamento periodico in presenza di

cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Il Manuale della conservazione costituisce allegato "ALL. 6" al presente MdG.

2. PIANO DI SICUREZZA

Il presente capitolo riporta le misure di sicurezza adottate nell'ambito della gestione e della conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

2.1. Obiettivi

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattate dall'AOO sono disponibili, integre e riservate;
- i dati personali comuni, sensibili e/o giudiziari vengono custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

2.2. Politiche di sicurezza adottate dalla AOO

"Componente fisica della sicurezza". Questa componente indica la sicurezza delle apparecchiature hardware. Tutti i dispositivi classificati "di sistema" (server, apparati attivi di rete, firewall.) sono coperti da un servizio di manutenzione che garantisce tempi di intervento adeguati per il ripristino degli apparati.

"Componente organizzativa della sicurezza". La componente organizzativa della sicurezza, legata alla gestione del protocollo e della documentazione, si riferisce alle attività svolte per l'erogazione del SdP.

Le qualifiche funzionali coinvolte sono le seguenti:

- responsabile dei sistemi informativi;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali;

"Componente infrastrutturale della sicurezza". La componente infrastrutturale si riferisce alla sicurezza dei locali e dell'infrastruttura hardware dedicata.
Relativamente a queste componenti si deve far riferimento al piano di continuità operativa e disaster recovery adottato presso l'amministrazione ai sensi del c.3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale.

È compito del responsabile della sicurezza e del responsabile della tutela dei dati personali procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.

All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.

"Componente logica della sicurezza". Per componente logica della sicurezza si intende il sottosistema di sicurezza finalizzato alla implementazione dei requisiti di sicurezza all'interno del SdP:

a) Meccanismi per il controllo degli accessi. Il controllo degli accessi consiste nel garantire che tutti gli accessi agli oggetti del sistema informatico documentale avvengano secondo le modalità prestabilite (login, password). Il sistema di database traccia un file di registrazione degli accessi (file di log).

b) Funzioni per la realizzazione dell'integrità logica. Ogni utente, superata la fase di autenticazione, ha accesso solo ai dati residenti nella propria area di lavoro (scrivania virtuale) e non può accedere ad altre aree di lavoro.

I dati personali registrati nel log del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati secondo le vigenti norme e saranno consultati solo in caso di necessità.

2.3. Formazione dei documenti - Aspetti attinenti alla sicurezza

Le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici garantiscono:

- l'identificabilità del soggetto che ha formato il documento;
- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura (text editor) che possiedono i requisiti di leggibilità, interscambiabilità, non alterabilità, immutabilità nel tempo del contenuto e della struttura. Si adottano preferibilmente i formati PDF, PDF/A, XML. I formati utilizzati dall'amministrazione rispettano le "regole tecniche" e sono quelli indicati in allegato "7".

I documenti informatici redatti dall'AOO con altri prodotti di text editor sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF, PDF/A, XML), come previsto dalle regole tecniche per la conservazione dei documenti, al fine di garantire la leggibilità per altri sistemi, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura del documento.

2.3.1. Gestione dei documenti informatici

Il sistema che eroga il SdP è conforme alle specifiche previste dalla normativa vigente.

I file documenti risiedono sul server che è configurato in maniera da consentire:

- l'accesso esclusivamente al server del protocollo informatico in modo che qualsiasi altro utente non autorizzato non possa mai accedere ai documenti al di fuori del sistema di gestione documentale;
- la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni sono protette al fine di non consentire modifiche non autorizzate.

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di

protocollo;

- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- consente il reperimento delle informazioni riguardanti i documenti registrati;
- consente, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di "privacy", con particolare riferimento al trattamento dei dati sensibili e giudiziari;
- garantisce la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

2.3.2. Gestione della sicurezza nelle registrazioni di protocollo

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad esempio: dati, transazioni), presenti o transitate sul SdP che occorre mantenere, sia dal punto di vista regolamentare, sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul SdP, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza sono costituite:

- dai log dei dispositivi;
- dalle registrazioni dell'applicativo SdP, modulo J-IRIDE.

Le registrazioni di sicurezza sono soggette alle seguenti misure di sicurezza:

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del modulo J-IRIDE sono elaborate tramite procedure automatiche dal sistema di autenticazione e di autorizzazione
- i supporti con le registrazioni di sicurezza sono conservati all'interno di un armadio ignifugo in un locale con controllo biometrico per l'accesso;
- i log di sistema sono accessibili al personale incaricato in sola lettura;
- l'operazione di scrittura delle registrazioni del SdP, modulo J-IRIDE è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera di backup;

2.4. Trasmissione dei documenti informatici

Nella AOO gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o 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.

Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi, contengono soltanto le informazioni relative a stati, fatti e qualità personali di cui è consentita la diffusione e che sono strettamente necessarie per il perseguimento delle finalità per le quali vengono trasmesse.

Il sistema di posta certificata del fornitore esterno (*provider*) di cui si avvale l'AOO, oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

- accesso all'indice dei gestori di posta elettronica certificata, allo scopo di verificare l'integrità del messaggio e del suo contenuto;
- tracciamento delle attività nel file di log della posta;
- gestione automatica delle ricevute di ritorno.

Lo scambio per via telematica di messaggi protocollati tra AOO presenta esigenze specifiche in termini di sicurezza, quali quelle connesse con la protezione dei dati personali, sensibili e/o giudiziari come previsto dal decreto legislativo del 30 giugno 2003, n. 196.

Per garantire l'autenticità della provenienza e l'integrità del messaggio viene utilizzata la sottoscrizione del documento con firma digitale.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dal Codice dell'Amministrazione Digitale.

2.5. Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali, pubblica *(UserID)* e privata *(Password)* ed un sistema di autorizzazione basato sulla profilazione degli utenti.

La profilazione consente di definire le abilitazioni/autorizzazioni che possono essere effettuate/rilasciate ad un utente del servizio di protocollo e gestione documentale.

Queste, in sintesi, sono:

- *consultazione,* per visualizzare in modo selettivo, le registrazioni di protocollo eseguite da altri;
- *inserimento,* per inserire gli estremi di protocollo e effettuare una registrazione di protocollo ed associare i documenti;
- *modifica,* per modificare i dati opzionali di una registrazione di protocollo;
- *annullamento,* per annullare una registrazione di protocollo autorizzata dal RSP.

Il SdP:

- consente il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente, o gruppi di utenti;
- assicura il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni sono protette da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, è possibile associare una *Access Control List* (ACL) che consente di stabilire quali utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).

Considerato che il SdP segue la logica dell'organizzazione, ciascun utente può accedere alla visualizzazione completa dei documenti protocollati.

Il sistema consente, altresì, di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'AOO.

I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso.

2.5.1. Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RGD dell'AOO.

Gli utenti creati non sono mai cancellati ma, eventualmente, storicizzati.

2.5.2. Accesso al registro di protocollo per utenti della AOO

La visibilità del registro di protocollo è consentita a tutti i ruoli.

Nel caso in cui sia effettuata una protocollazione riservata, la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza ed eventualmente conoscenza, il RGD e gli appartenenti a quel ruolo (permesso applicativo di protocollazione riservata associato al ruolo).

2.5.3. Utenti esterni alla AOO

Attualmente non sono disponibili funzioni per l'esercizio, per via telematica, del diritto di accesso ai documenti.

2.6. Conservazione dei documenti informatici

Il responsabile della conservazione redige le regole per la conservazione dei documenti informatici.

La conservazione dei documenti informatici avviene sulla base delle disposizioni riportate nel:

- DPCM 13 novembre 2014, per quanto attiene ai documenti informatici presenti nell'archivio corrente
- DPCM 3 dicembre 2013 per i documenti inviati in conservazione.

3. IL DOCUMENTO: MODALITÀ DI UTILIZZO DEGLI STRUMENTI INFORMATICI PER LA FORMAZIONE

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per la formazione del documento.

Prima di entrare nel merito, occorre caratterizzare l'oggetto di scambio: il documento amministrativo.

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

- ricevuto;
- inviato;
- interno formale;
- interno informale.

Il documento amministrativo come oggetto di scambio, in termini tecnologici è così classificabile:

- informatico;

- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e "2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità'.

Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

3.1. Documento ricevuto

La corrispondenza in ingresso può essere acquisita dalla AOO con diversi mezzi e modalità in base alla tecnologia di trasporto utilizzata dal mittente.

Un documento informatico può essere recapitato:

1. a mezzo posta elettronica convenzionale alla casella di posta istituzionale
2. a mezzo posta elettronica certificata;
3. su supporto rimovibile quale, ad esempio, *cd rom, dvd, floppy disk, tape, pen drive,* consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.
4. a mezzo Interpro/Ap@ci
5. direttamente tramite portale (Istanze web)

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telegramma;
4. con consegna diretta da parte dell'interessato o tramite una persona dallo stesso delegata alle UOP

3.2. Documento inviato

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata. La dimensione del documento e/o di eventuali allegati deve essere ottimizzata e allo stesso tempo garantirne la corretta visualizzazione.

3.3. Documento interno formale

I documenti interni formali sono formati con tecnologie informatiche.
La sottoscrizione digitale è a cura del RPA
La protocollazione nel SdP è a cura della UOR mittente e viene assegnato in carico alla UOR destinataria.

3.4. Documento interno informale

Per comunicazione informale tra uffici, si intende lo scambio di informazioni, con o senza documenti allegati.
Questo genere di comunicazioni è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.

3.5. Il documento analogico – cartaceo

Per documento analogico si intende un documento amministrativo formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei).

Viene pertanto fatto riferimento ad un documento amministrativo cartaceo che può essere prodotto sia in maniera tradizionale (come, ad esempio, una lettera scritta a mano o a macchina), sia con strumenti informatici (ad esempio, una lettera prodotta tramite un sistema di videoscrittura o *text editor*) e poi stampata. In questo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.

Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del manuale.

3.6. Formazione dei documenti: Aspetti operativi

I documenti dell'Amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.

Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

- deve trattare un unico argomento, indicato in maniera sintetica ma esaustiva dell'autore nello spazio riservato all'oggetto;
- deve essere identificato univocamente da un solo numero di protocollo;

Le firme *(e le sigle se si tratta di documento analogico)* necessarie alla redazione e perfezione sotto il profilo giuridico del documento in partenza, devono essere apposte prima della sua protocollazione.

Nel caso si tratti di un documento informatico la firma digitale deve essere apposta in fase di protocollazione a cura del RPA.

Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai RPA.

Il documento deve consentire l' identificazione dell' amministrazione mittente attraverso le seguenti informazioni:

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero civico, CAP, città, provincia);
- il numero di telefono della UOR;
- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione;
- il numero di protocollo;
- la data
- l'oggetto;
- il numero degli allegati, se presenti;
- sottoscrizione digitale del RPA e/o del responsabile del provvedimento; se trattasi di documento digitale,
- sottoscrizione autografa del responsabile del procedimento amministrativo (RPA) e/o del responsabile del provvedimento, se trattasi di documento cartaceo

3.7. 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.

I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi Allegato 2 del decreto del Presidente del Consiglio dei Ministri 13 novembre 2014).

La firma digitale soddisfa pienamente l'integrità e la titolarità sia del documento amministrativo che della copia giornaliera del registro di protocollo, o qualsiasi altro file digitale che necessita di valenza giuridico-probatoria.

3.8. Verifica delle firme nel SdP per i formati .p7m

Nel SdP il software applicativo J-Iride consente la verifica in modalità integrata della firma digitale apposta sui documenti.
La verifica visualizza i dati del soggetto firmatario, della Certification authority, della validità del certificato e la chiave pubblica.

4. MODALITA' DI SCAMBIO DEI DOCUMENTI INFORMATICI

4.1. Uso della Posta Elettronica Certificata

La casella di Posta Elettronica Certificata è presidiata, per la ricezione di documenti, solo dall'UOP Segreteria e segue le regole di assegnazione previste al capitolo 6.

Lo scambio dei documenti soggetti alla 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.

La trasmissione di un documento tramite PEC è consentito a tutte le UOR dell'Amministrazione e avviene in base alle seguenti modalità:

- redazione del documento con un sistema di videoscrittura;
- firma digitale del documento da parte del RPA;

- registrazione di protocollo in uscita nel SdP, allegando il documento firmato digitalmente;
- inviare il documento al destinatario dotato di casella di posta elettronica certificata tramite apposita funzione del software applicativo;

L'utilizzo della posta elettronica certificata (PEC) garantisce:
- la conoscenza in modo inequivocabile della data e dell'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;

Le ricevute di ritorno dal gestore di PEC dell'Amministrazione, sono classificati in:
- conferma di ricezione;
- notifica di eccezione;
- avvenuta consegna;

Il servizio di posta elettronica certificata è strettamente correlato all'indice della pubblica amministrazione (IPA), dove sono pubblicati gli indirizzi istituzionali di posta certificata delle Pubbliche amministrazioni.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alla normativa, vigente e alle relative regole tecniche 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.

L'Amministrazione, in base a quanto previsto dalla vigente normativa, deve comunicare con i soggetti dotati di PEC in modalità digitale.

4.2 Uso del sistema di protocollo interoperabile InterPro

L'interoperabilità di protocollo permette a due sistemi di protocollo informatico di trattare in maniera automatica l'uno le informazioni trasmesse dall'altro. Il sistema consente quindi lo scambio di documenti digitali tra amministrazioni e ne permette il trattamento automatico al protocollo.

Il software applicativo J-Iride è conforme alle RFC di Regione Toscana relativamente al sistema InterPRO e consente l'interscambio dei documenti di protocollo e le relative informazioni accessorie con sistemi di altre PP.AA.

Il sistema di protocollo interoperabile InterPRO è presidiato, per la ricezione di documenti, solo dall'UOP Segreteria e segue le regole di assegnazione previste al capitolo 6.

La trasmissione di un documento tramite InterPro è consentito a tutte le UOR dell'Amministrazione e avviene in base alle seguenti modalità:
- redazione del documento con un sistema di videoscrittura;
- firma digitale del documento da parte del RPA;
- registrazione di protocollo in uscita nel SdP, allegando il documento firmato digitalmente;
- inviare il documento al destinatario registrato all'IPAR di Regione Toscana tramite apposita funzione del software applicativo;

L'utilizzo del sistema InterPro garantisce:

- di conoscere in modo inequivocabile la data e l'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna all'AOO dichiarata dal destinatario;
- la ricezione del file XML contenente il numero di protocollo dell'Amministrazione destinataria.

4.3 Uso del sistema di protocollo Ap@ci

Apaci è il sistema che privati cittadini, imprese e associazioni possono usare per inviare documenti all'amministrazione.

Sono accettati documenti con formati adatti alla conservazione. E' possibile inviare anche più allegati alla stessa comunicazione. Il sistema è presidiato da parte dell'UOP Segreteria che provvede alla registrazione nel SdP ed invia al mittente ricevuta nella casella di mail.

L'utilizzo del sistema Apaci garantisce:

- di conoscere in modo inequivocabile la data e l'ora di trasmissione;
- la generazione e l'invio in automatico di "ricevute di ritorno"
- l'avvenuta consegna alla casella mail del mittente;

Il soggetto che scrive all'amministrazione tramite Apaci elegge il proprio domicilio elettronico.

L'Amministrazione, in base a quanto previsto dalla vigente normativa, deve comunicare con tale soggetto in modalità digitale.

5. DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

Il presente capitolo descrive il flusso di lavorazione dei documenti ricevuti, spediti o interni, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.

Le UOP non effettuano fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

5.1. Flusso dei documenti in ingresso alla AOO

5.1.1. Ricezione dei documenti cartacei

I documenti che arrivano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente alla UOP Segreteria.

La consegna "brevi manu" direttamente dall'utenza viene effettuata presso l'Ufficio Unico Amministrativo.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti, e successivamente aperti per gli ulteriori controlli preliminari alla registrazione; la busta o contenitore si allega al documento per la parte relativa ai timbri postali.

La corrispondenza relativa a procedure negoziali aperte o ristrette è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.

La corrispondenza recante la dicitura "RISERVATA" , "SPM" o "PERSONALE" viene trattata con le modalità stabilite al successivo capitolo 11.7.9;

La corrispondenza ricevuta via telegramma o via telefax, per ciò che concerne la registrazione di protocollo, viene trattata con le modalità descritte nei successivi cap. *11.7.1.*

Nel caso di documenti pervenuti direttamente ad una UOR, questa deve consegnarli alla UOP per la protocollazione.

La documentazione cartacea ricevuta, a seguito delle operazioni di registrazione e segnatura di protocollo previste dai cap. 11.3.3 e 11.3.4 del presente MdG a cura delle UOP competenti, viene assegnata alle UOR in originale a seguito della scansione e la conseguente assegnazione telematica.

5.1.2. Documenti cartacei ricevuti e tutela dei dati personali

Il personale preposto all'apertura e alla registrazione della corrispondenza è regolarmente autorizzato al trattamento dei dati personali in qualità di "incaricato al trattamento" seguendo le modalità gestionali descritte nel presente manuale di gestione.

Qualora la corrispondenza riservata personale venga recapitata per errore ad un ufficio dell'Amministrazione quest'ultimo, a tutela dei dati personali eventualmente contenuti, non apre le buste o i contenitori e li rinvia, entro la giornata lavorativa successiva, all'Ufficio Segreteria Generale.

5.1.3. Ricezione di documenti informatici sulla casella PEC istituzionale

Di norma, la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile solo alla UOP Segreteria.

La UOP Segreteria previa verifica della validità e della leggibilità del documento, procede alla registrazione di protocollo e alla assegnazione agli UOR di competenza.

Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.

L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie.

Qualora i messaggi di posta elettronica non siano conformi agli standard indicati dalla normativa vigente, ovvero non siano dotati di firma elettronica e si renda necessario attribuire agli stessi efficacia probatoria, il messaggio, con il formato di origine, è protocollato, smistato, assegnato e inserito nel sistema di gestione documentale. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

Il personale della UOP controlla quotidianamente i messaggi pervenuti nella casella di posta certificata istituzionale e verifica se sono da protocollare.

5.1.4. Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica.

Nei casi in cui con un documento cartaceo siano trasmessi gli allegati su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione.

5.1.5. Ricezione di documenti informatici su casella di posta elettronica ordinaria

I documenti digitali che pervengono alle caselle di posta elettronica ordinaria vengono valutati dagli RPA; qualora il documento venga ritenuto di valenza amministrativa (es. avvio di istanza), questo viene protocollato ed inserito nel flusso di lavorazione.

La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).

5.1.6. Errata ricezione di documenti digitali

Nel caso in cui pervengano sulla casella di posta certificata istituzionale dell'AOO, messaggi dal cui contenuto si rileva che sono stati erroneamente ricevuti, l'operatore rispedisce il messaggio al mittente con la dicitura "Messaggio pervenuto per errore -non di competenza di questa AOO".

5.1.7. Errata ricezione di documenti cartacei

Se la busta è indirizzata ad altra amministrazione ed è ancora chiusa, viene restituita al servizio postale che provvede ad inoltrarla all'indirizzo corretto.

5.1.8. Attività di protocollazione dei documenti

Superati tutti i controlli precedentemente descritti i documenti, digitali o analogici, sono protocollati e gestiti secondo gli standard e le modalità indicate nel dettaglio nel capitolo 11.

5.1.9. Rilascio di ricevute attestanti la ricezione di documenti informatici

Nel caso di ricezione di documenti informatici per via telematica, la notifica al mittente dell'avvenuto recapito del messaggio è assicurata dal servizio di posta elettronica certificata utilizzato dall'AOO con gli standard specifici.

L'Amministrazione provvede inoltre al rilascio di 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.

5.1.10. Rilascio di ricevute attestanti la ricezione di documenti cartacei

Quando il documento cartaceo è consegnato "brevi manu" dal mittente, o da altra persona incaricata, all'Ufficio Unico Amministrativo, ed è richiesto il rilascio di una ricevuta attestante l'avvenuta consegna, l'Ufficio Unico Amministrativo che lo riceve, a seguito delle operazioni di segnatura e di protocollazione, provvede alla stampa della relativa ricevuta tramite specifica funzione del software applicativo.

Nel caso non sia possibile stampare la ricevuta, le UOP possono consegnare al mittente copia del documento con apposizione del timbro, contenente numero del protocollo, data, indicazione della AOO e della UOP.

La semplice apposizione del timbro datario da parte dell'Ufficio Unico Amministrativo per la tenuta del protocollo, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale in merito alla ricezione ed all'assegnazione del documento.

Nel caso di corrispondenza pervenuta direttamente ad una UOR, questa deve consegnarla ad una UOP preposta allo scopo di ottenere una ricevuta valida.

5.1.11. Archiviazione dei documenti informatici

I documenti informatici ricevuti dall'Amministrazione sono archiviati sui supporti di memorizzazione del sistema, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo.

Tali documenti sono resi disponibili agli UOR, attraverso il software applicativo J-Iride all'atto dell'assegnazione.

5.1.12. Archiviazione delle copie per immagine di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine *(copia per immagine di documento analogico)* attraverso un processo di scansione che avviene secondo le fasi di seguito indicate:

- 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;

Le copie per immagine dei documenti cartacei sono archiviate sul sistema, secondo le regole vigenti, in modo non modificabile al termine del processo di scansione.

Gli originali dei documenti cartacei ricevuti, di norma vengono ricevuti dalle UOR contestualmente all'assegnazione telematica.

Vengono riprodotti in formato immagine i documenti che contengono dati sensibili secondo la normativa vigente (d.lgs. 196/2003).

5.1.13. Assegnazione, presa in carico dei documenti e classificazione.

Gli addetti alla UOP provvedono ad inviare il documento alla/e UOR responsabile/i.

L'UOR provvede alle seguenti operazioni:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP Segreteria;
- in caso di verifica positiva, esegue l'operazione di presa in carico ed il RPA procede con la corretta fascicolazione e classificazione sulla base delle procedure in essere presso l'AOO.

5.1.14. Conservazione dei documenti e dei fascicoli nella fase corrente

Ciascuna UOR è responsabile della organizzazione e della tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla archiviazione dei documenti al loro interno.

5.2. Flusso dei documenti in uscita dalla AOO

5.2.1. Documento in uscita

Per "documento in uscita" s'intende quel documento amministrativo prodotto da ciascuna UOR dell'Amministrazione nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinato ad essere trasmesso ad un soggetto esterno.

5.2.2. Verifica del documento, registrazione di protocollo e segnatura

E' a cura della UOR provvedere ad eseguire le verifiche di conformità del documento:

- lo standard formale richiamato nel capitolo 3 (logo, descrizione completa dell'amministrazione, etc), la verifica che sia indicato correttamente il destinatario,
- la verifica che il documento sia sottoscritto in modalità digitale o autografa,
- eventuale presenza di allegati.

Superate le verifiche, il documento viene registrato a cura della UOR nel protocollo generale e ad esso viene apposta la segnatura.

5.2.3. Trasmissione di documenti informatici

Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata", conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da 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.

I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica.

La trasmissione avviene secondo quanto indicato al capitolo 4 e con le apposite funzioni del software applicativo J-Iride.

5.2.4. Trasmissione di documenti cartacei, invio alla Segreteria e affrancatura

Le UOR dell'Amministrazione, dopo la registrazione di protocollo, la segnatura e l'imbustamento, consegnano la corrispondenza all'UOP Segreteria che provvede al recapito della stessa all'ufficio postale.

La compilazione dei moduli contenenti i dati delle spedizioni è a cura della UOP Segreteria.

Le attività di affrancatura della corrispondenza inviata per posta, vengono svolte dalla UOP Segreteria.

5.2.5. Inserimento delle ricevute di trasmissione nel fascicolo

Le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo elettronico.

Le UOR curano anche l'archiviazione delle ricevute di ritorno delle raccomandate sulle quali è trascritto il numero di protocollo attribuito al documento a cui esse si riferiscono.

6. REGOLE PER L'ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

Il presente capitolo contiene le regole di assegnazione dei documenti in ingresso adottate dall'AOO.

6.1. Regole disponibili nell'assegnazione

Il SdP per l'assegnazione della documentazione pervenuta all'Amministrazione utilizza l'organigramma in uso presso l'Amministrazione con la descrizione delle relative funzioni.

6.2. Attività di assegnazione

Di seguito viene descritta con maggiore dettaglio l'operazione di assegnazione dei documenti ricevuti illustrata nel flusso di lavorazione del precedente capitolo 5.

L'attività di assegnazione consiste nell'operazione di inviare direttamente dalla UOP il documento protocollato e segnato all'UOR competente e la contestuale trasmissione del materiale documentario oggetto di trattazione.

Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel RPA designato.

Preso atto dell'assegnazione, il RPA verifica la competenza e, se esatta, provvede alla presa in carico del documento che gli è stato assegnato, se errata lo rifiuta; il documento torna all'UOP Segreteria che provvede a riassegnarlo.

L'UOR competente è incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.

Il SdP memorizza tutti i passaggi, tracciando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione. La traccia individua i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità.

L'assegnazione può essere effettuata: per conoscenza o per competenza.

6.3. Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica quindi disponibili unicamente in formato digitale, sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione sul sistema informatico in modo non modificabile.

Le UOR assegnatarie del documento per "competenza" e/o per "conoscenza" lo ricevono esclusivamente in formato digitale.

6.4. Assegnazione dei documenti ricevuti in formato cartaceo

I documenti cartacei gestiti dalla UOP sono di norma assegnati entro le 24 ore.

Al termine delle operazioni di registrazione, segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati al RPA di competenza per via informatica attraverso il software applicativo J-Iride.

L'UOP provvede contestualmente alle seguenti operazioni:

- Acquisizione in formato immagine con *scanner;*
- Trasmissione/ritiro al/dal RPA.

La UOR che ha ricevuto l'assegnazione per "competenza" riceve sia il documento cartaceo che digitale, nel caso vi sia anche assegnazione per "conoscenza" la UOR assegnatarie del documento riceve unicamente copia digitale.

6.5. Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UOR che riceve il documento lo rifiuta; il documento digitale torna tramite il–software applicativo J-iride alla UOP Segreteria e, qualora si tratti di un documento cartaceo originale, anche l'originale stesso.

L'UOP Segreteria procederà ad una nuova assegnazione.

E' in carico alla UOR assegnataria il mancato ritorno alla UOP Segreteria qualora vi sia una assegnazione errata.

Il sistema di gestione informatica del protocollo tiene traccia di tutti i passaggi memorizzando

l'identificativo dell'utente che effettua l'operazione con la data e l'ora di esecuzione.

7. UO RESPONSABILE DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DEI DOCUMENTI

Il presente capitolo individua l'unità organizzativa responsabile delle attività di coordinamento del sistema di protocollo, di organizzazione e di tenuta dei documenti ali' interno della AOO.

In base al modello organizzativo adottato dall'amministrazione, nell'allegato "3" è riportata l'articolazione della AOO in UOR e UOP.

Relativamente alla organizzazione e alla tenuta dei documenti dell'Amministrazione, all'interno della AOO, è stato istituito il servizio archivistico descritto in dettaglio al capitolo 10.

8. DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

8.1. Elenco documenti esclusi

Sono, esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53, comma 5, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 come riportato nell'allegato "8".

8.2. Elenco documenti soggetti a registrazione particolare

Sono esclusi dalla registrazione di protocollo generale e sono soggetti a registrazione particolare le tipologie di documenti riportati nell'allegato "9". Tale tipo di registrazione consente, comunque, di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti. Le funzioni sono coordinate con il RGD.

9. SISTEMA DI FASCICOLAZIONE ELETTRONICA, CLASSIFICAZIONE E PIANO DI CONSERVAZIONE

9.1. Organizzazione del sistema di conservazione

9.1.1. Caratteristiche generali

Il presente capitolo contiene il sistema di formazione del fascicolo, di classificazione dei documenti, di conservazione dell'archivio, con l'indicazione dei tempi e delle modalità di aggiornamento, dei criteri e delle regole di selezione e scarto della documentazione, anche con riferimento all'uso di supporti informatici e di consultazione e movimentazione dei fascicoli.

La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio, è obbligatoria per legge e si avvale del piano di classificazione (titolario), cioè di quello che si suole definire "sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale viene ricondotta la molteplicità dei documenti prodotti".

Il titolario di classificazione disponibile in "allegato 5" e il piano di conservazione in "allegato

10" sono predisposti a cura del RSP, condivisi con tutta la struttura organizzativa dell'Amministrazione e sono adottati con atti formali.

9.1.2. Misure di protezione e conservazione

Gli archivi e i singoli documenti dello Stato, delle regioni, degli altri enti pubblici territoriali, nonché di ogni altro ente ed istituto pubblico sono beni culturali inalienabili.
I singoli documenti sopra richiamati (analogici ed informatici, ricevuti, spediti e interni formali) sono quindi inalienabili, sin dal momento dell'inserimento di ciascun documento nell'archivio dell'Amministrazione, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, e deve essere conservato nella sua organicità.

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della Soprintendenza Archivistica regionale.

Lo scarto dei documenti dell'archivio è subordinato all'autorizzazione della Soprintendenza Archivistica regionale,

9.2. Titolario o piano di classificazione

9.2.1. Titolario
Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'Amministrazione.

Il piano di classificazione si suddivide, di norma, in titoli, classi, sottoclassi, categorie e sottocategorie o, più in generale, in voci di I livello, II livello, III livello.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze (microfunzioni) che rientrano concettualmente nella macrofunzione descritta dal titolo.

Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice dell' amministrazione.
Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'amministrazione, soggette a modifiche in forza delle leggi e dei regolamenti statali. L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RGD.

Dopo ogni modifica del titolario, il RGD 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: non si applica, cioè, ai documenti protocollati prima della sua introduzione.

Il sistema di protocollazione deve garantire la storicizzazione delle variazioni 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.

Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.

Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo titolario e hanno durata almeno per l'intero anno.

9.2.2. Classificazione dei documenti

La classificazione è l'operazione finalizzata alla organizzazione dei documenti, secondo un ordinamento logico, in relazione alle funzioni e alle competenze della AOO.
Essa è eseguita a partire dal titolario di classificazione facente parte del piano di conservazione dell'archivio.
Tutti i documenti ricevuti e prodotti dalle UOR dell'Amministrazione, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.
Mediante la classificazione si assegna al documento, oltre al codice completo dell'indice di classificazione (titolo, classe, sottoclasse), il numero del fascicolo ed eventualmente del sottofascicolo.
Le operazioni di classificazione vengono svolte dalle UOR.

9.3. Fascicoli

9.3.1. Fascicolazione dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, devono essere inseriti nei fascicoli.
Il RPA della UOR stabilisce se il documento assegnatogli dalla UOP debba essere ricollegato ad un affare o procedimento in corso e pertanto debba essere inserito in un fascicolo già esistente oppure se il documento si riferisce a un nuovo affare, o procedimento, per cui è necessario aprire un nuovo fascicolo .

A seconda delle ipotesi, si procede come segue:

- se il documento si ricollega ad un *procedimento in corso,* l'operatore:
  - seleziona il relativo fascicolo;
  - collega la registrazione di protocollo del documento al fascicolo selezionato;
- se il documento da avvio ad un *nuovo fascicolo,* il soggetto preposto:
  - esegue l'operazione di apertura del fascicolo;
  - collega la registrazione di protocollo del documento al nuovo fascicolo aperto;

9.3.2. Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo il RPA provvede all'apertura di un nuovo fascicolo.
La formazione di un nuovo fascicolo avviene attraverso l'operazione di "apertura" che comprende la registrazione di alcune informazioni essenziali:

- indice di classificazione (cioè titolo, classe, sottoclasse);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'AOO;
- data di apertura del fascicolo;
- AOO e UOR;

- livello di riservatezza, se diverso da quello standard applicato dal sistema.

9.3.3. Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'esaurimento dell'affare.

9.3.4. Repertorio dei fascicoli

I fascicoli, sono annotati nel repertorio dei fascicoli.

Il repertorio dei fascicoli, ripartito per ciascuna classe di ogni titolo del titolario, è lo strumento di gestione e di reperimento dei fascicoli.

La struttura del repertorio rispecchia quella del titolario di classificazione e quindi varia in concomitanza con l'aggiornamento di quest'ultimo.

Mentre il titolario rappresenta in astratto le funzioni e le competenze che l'ente può esercitare in base alla propria missione istituzionale, il repertorio dei fascicoli rappresenta in concreto le attività svolte e i documenti prodotti in relazione a queste attività.

Il repertorio dei fascicoli è costantemente aggiornato.

10. MOVIMENTAZIONE E CONSULTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO, STORICO E PIANO DI CONSERVAZIONE

Il servizio archivistico è competente a gestire l'intera documentazione archivistica, ovunque trattata, distribuita o conservata, ai fini della sua corretta collocazione, classificazione, e conservazione. Al servizio archivistico è preposto il responsabile della conservazione.

10.1. Principi generali

Come Archivio si intende il complesso dei documenti prodotti e acquisiti nello svolgimento della attività e l'esercizio delle funzioni dall'amministrazione comunale.
Fanno parte dell'archivio dell'Amministrazione anche gli archivi e i documenti acquisiti per dono, deposito, acquisto o qualsiasi altro titolo.

L'archivio è suddiviso funzionalmente nelle seguenti sezioni:

- ARCHIVIO CORRENTE: il complesso dei documenti relativi a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente;
- ARCHIVIO DI DEPOSITO: il complesso dei documenti relativi a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico;
- ARCHIVIO STORICO: il complesso dei documenti relativi a procedimenti conclusi da oltre 40 anni e destinati, previa operazione di scarto, alla conservazione perenne nella sezione separata d'archivio.

10.2. Funzioni d'archivio

10.2.1. Movimentazione dei fascicoli cartacei

Il RGD cura la procedura di trasferimento dei fascicoli cartacei relativi a procedimenti conclusi e affari esauriti, nell'archivio di deposito dell'Amministrazione, stabilendo modi e tempi del versamento dall' archivio corrente a quello di deposito.
Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

10.2.2. Movimentazione dei fascicoli elettronici

Il RGD insieme al Responsabile della conservazione, al Responsabile della Privacy ed al Responsabile dei sistemi informativi, organizza il trasferimento dei fascicoli elettronici relativi a procedimenti conclusi e affari esauriti, nel sistema di conservazione a norma individuato dall'Amministrazione previa autorizzazione della Soprintendenza archivistica della Toscana.
Il trasferimento deve essere effettuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente.

10.2.3. Procedure di scarto

Sulla base del piano di conservazione di cui all'allegato "10", l'Amministrazione, periodicamente, effettua la procedura di scarto in riferimento alle regole della Soprintendenza archivistica della Toscana.

10.2.4. Consultazione ai fini giuridico-amministrativi

La richiesta di consultazione dei documenti amministrativi, può pervenire dall'interno dell'amministrazione, oppure da utenti esterni per scopi giuridico-amministrativi o per scopi storici.
Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15.

I RPA, in caso di necessità, possono richiedere la documentazione amministrativa tramite registrazione di protocollo con documento interno formale.

Le singole pubbliche amministrazioni individuano, comunque, le categorie di documenti da esse formati o rientranti nella loro disponibilità sottratti all'accesso.

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. Nel caso di documenti contenenti dati sensibili e giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall'articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale "

10.2.5 Consultazione da parte di personale esterno all'amministrazione

La consultazione dei documenti e le richieste di accesso agli atti da parte di personale esterno all'amministrazione, sono disciplinati dal vigente regolamento "Rapporto tra i cittadini e l'amministrazione comunale nello svolgimento delle attività e dei procedimenti amministrativi" - approvato con delibera di Consiglio Comunale n. 27 del 29/09/2010.

La richiesta di accesso ai documenti presentata all'Amministrazione viene protocollata dalla UOP

che la riceve e che provvede ad assegnarla al servizio archivistico.

Nel caso di richieste di accesso ai documenti della sezione storica dell'archivio, le medesime devono essere inviate all'Amministrazione. Analoga richiesta di accesso può essere indirizzata alla Soprintendenza archivistica, utilizzando i moduli predisposti dalla stessa Soprintendenza archivistica, poiché, pur non essendo esplicitamente richiesta dalla normativa, essa è comunque utile a fini statistici e di tutela.

Nel caso di richieste di accesso a documenti digitali il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico. La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.

In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

10.2.6. Consultazione da parte di personale interno all'amministrazione

Le UOR dell'amministrazione, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica previa apposita richiesta.

L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito, o storico, ad un ufficio dell'amministrazione, avviene solamente per il tempo strettamente necessario all'esaurimento di una procedura o di un procedimento amministrativo.

Nel caso di accesso ad archivi convenzionali cartacei, l'affidamento temporaneo avviene solamente mediante richiesta espressa su un apposito modello contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, la UOR di appartenenza e la firma.

Copia della richiesta di consultazione viene conservata nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile del servizio archivistico.
L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, degli stessi rispettandone la sedimentazione archivistica e il vincolo.

Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite nel manuale della conservazione che costituisce l'allegato "6" al presente MdG.

In qualsiasi caso, deve essere garantito l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.

11. MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

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.

11.1. Unicità del protocollo informatico

Nell'ambito della AOO il registro generale di protocollo è unico.

La numerazione si chiude al 31 dicembre di ogni anno e ricomincia dal primo gennaio dell'anno successivo.

Il numero di protocollo individua un unico documento e, di conseguenza, ogni documento reca un solo numero di protocollo.

Il numero di protocollo è costituito da almeno sette cifre numeriche.

Non è consentita l'identificazione dei documenti mediante l'assegnazione manuale di numeri di protocollo che il sistema informatico ha già attribuito ad altri documenti, anche se questi documenti sono strettamente correlati tra loro.

Non è pertanto consentita in nessun caso la cosiddetta registrazione "a fronte", cioè l'utilizzo di un unico numero di protocollo per il documento in arrivo e per il documento in partenza.

La documentazione che non è stata registrata nel SdP viene considerata giuridicamente inesistente presso l'amministrazione.

Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici.

11.2. Registro giornaliero di protocollo

Il registro di protocollo è un atto pubblico originario, che fa fede della tempestività e dell'effettivo ricevimento e spedizione di un documento, indipendentemente dalla regolarità del documento stesso, ed è idoneo a produrre effetti giuridici.

Il registro giornaliero di protocollo è generato automaticamente dal sistema j-iride in formato PDF al termine della giornata lavorativa.

Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, entro la giornata lavorativa successiva, al sistema di conservazione a norma, ai sensi dell'art.7. comma 5, delle Regole tecniche.

11.3. Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i

tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).

Su ogni documento ricevuto, o spedito, dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.

Le registrazioni di protocollo dei documenti pervenuti presso l'AOO destinataria sono, di norma, effettuate nella giornata di arrivo e comunque non oltre le 24 ore dal ricevimento di detti documenti.

La registrazione è eseguita in un'unica operazione, senza possibilità, per l'operatore, di inserire le informazioni in più fasi successive.

Ciascuna registrazione di protocollo contiene, almeno, i seguenti dati obbligatori:

- il numero di protocollo, generato automaticamente dal sistema e registrato in forma non modificabile;
- la data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- il mittente che ha prodotto il documento;
- il destinatario del documento;
- l'oggetto del documento;

In base all'art.8 delle Regole tecniche l'annullamento anche di un solo campo delle informazioni obbligatorie registrate in forma immodificabile, necessario per correggere errori intercorsi in sede di immissione di dati determina l'annullamento della registrazione di protocollo.

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.

Tali dati facoltativi sono descritti nei paragrafi seguenti.

L'operazione di segnatura di protocollo è effettuata contemporaneamente all'operazione di registrazione di protocollo.

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

Essa consente di individuare ciascun documento in modo inequivocabile.

11.3.1. Registrazione di protocollo dei documenti informatici

I documenti informatici sono ricevuti, e trasmessi, in modo formale sulla/dalla scrivania virtuale J-iride di competenza.

La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dall'operatore addetto al protocollo,. che verifica integrità e sottoscrizione con firma digitale. Nel caso di documenti informatici in partenza, l'operatore esegue anche la verifica della validità amministrativa della firma. Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti *i tipi di documento.*

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, che si può riferire sia al corpo del messaggio che ad uno dei *file* ad esso allegati che può assumere la veste di documento principale.

Tali documenti sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

11.3.2. Registrazione di protocollo dei documenti analogici (cartacei e supporti rimovibili)

La registrazione di protocollo di un documento cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.

Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali.

11.3.3. Segnatura dei documenti informatici

I dati della segnatura di protocollo di un documento informatico sono attribuiti, un'unica volta nell'ambito dello stesso messaggio, in *un file* conforme alle specifiche *dell'Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) reso disponibile dagli organi competenti. Le informazioni minime incluse nella segnatura sono le seguenti:

- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del messaggio ricevuto o inviato (art.18 c1)
- l'oggetto
- il mittente
- il destinatario o i destinatari

E' facoltativo riportare le seguenti informazioni:

- denominazione dell'amministrazione;
- codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo.

Per i documenti informatici in partenza possono essere specificate, in via facoltativa, altre informazioni, se ritenuto necessario.

La struttura ed i contenuti del *file* di segnatura di protocollo di un documento informatico sono conformi alle disposizioni tecniche vigenti.

Quando il documento è indirizzato ad altre AOO la segnatura di protocollo può includere tutte le informazioni di registrazione del documento.

L'AOO che riceve il documento informatico può utilizzare tali informazioni per automatizzare le operazioni di registrazione di protocollo del documento ricevuto.

11.3.4. Segnatura dei documenti cartacei

La segnatura di protocollo di un documento cartaceo in arrivo, avviene attraverso l'apposizione di un timbro che riporta le seguenti informazioni relative alla registrazione di protocollo:

- denominazione dell'amministrazione;
- codice identificativo dell'AOO;
- data e numero di protocollo del documento.

L'operazione di segnatura dei documenti in partenza viene integralmente eseguita dalla UOR tramite l'apposizione del timbro o riportando il numero e la data sul documento.

L'operazione di acquisizione dell'immagine dei documenti cartacei viene effettuata solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.

Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo viene apposto sulla prima pagina dell'originale; in caso contrario il "segno" viene apposto sul retro della prima pagina dell'originale.

11.4. Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo.

La registrazione degli elementi facoltativi del protocollo, può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UOR.

In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

Per quanto concerne i campi integrativi, facoltativi presenti nel SdP sono previste specifiche funzionalità che consentono di gestire:

- ulteriori informazioni sul mittente/destinatario, soprattutto se persona giuridica;
- l'indirizzo completo del mittente/destinatario (via, numero civico, CAP, città, provincia, stato civile, sesso);

11.5. Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.

Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal RGD.
In tale ipotesi la procedura riporta la dicitura "annullato" in posizione visibile e tale, da consentire la lettura di tutte le informazioni originarie. Il sistema registra l'avvenuta rettifica, la data ed il soggetto che è intervenuto.

Solo il RGD, o il vicario, sono autorizzati ad annullare, ovvero a dare disposizioni di annullamento delle registrazioni di protocollo.

L'annullamento di una registrazione di protocollo generale deve essere richiesto con specifica nota, adeguatamente motivata, indirizzata al RGD o il vicario.

11.6. Livello di riservatezza

IL SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.

L'UOP se trattasi di documento in arrivo, o la UOR se trattasi di documento in partenza decide se il documento da protocollare è un documento riservato, Il documento riservato è un documento visibile solo al destinatario.

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 invece che hanno un livello di riservatezza superiore lo mantengono.

11.7. Casi particolari di registrazioni di protocollo

Tutta la corrispondenza diversa da quella di seguito descritta viene regolarmente aperta, protocollata e assegnata con le modalità e le funzionalità proprie del SdP.

11.7.1. Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati all'UOP Segreteria, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

11.7.2. Domande di partecipazione a concorsi

La corrispondenza ricevuta con rimessa diretta dall'interessato, viene protocollata al momento della presentazione, dando ricevuta dell'avvenuta consegna con gli estremi della segnatura di protocollo.

Con la medesima procedura deve essere trattata la corrispondenza ricevuta in formato digitale o per posta.

Nell'eventualità che non sia possibile procedere immediatamente alla registrazione dei documenti ricevuti con rimessa diretta, gli stessi saranno accantonati e protocollati successivamente entro le 24 h. In questo caso, al mittente, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

11.7.3. Fatture

Le fatture provenienti dal SDI pervengono al SdP.

Esse sono protocollate sul registro ufficiale di protocollo in modalità automatica e inviate quotidianamente, in originale, alla UOR competente. Il registro delle fatture è costituito sull'apposito software dedicato.

11.7.4. Protocollazione di documenti inerenti gare di appalto (cartacei)

Per motivi organizzativi tutti gli UOR sono tenuti ad informare con congruo anticipo il RSP dell'AOO in merito alle scadenze di concorsi, gare, bandi di ogni genere.

La corrispondenza che riporta l'indicazione "offerta" - "gara d'appalto" - "preventivo", o simili, o dal cui involucro è possibile evincere che si riferisce alla partecipazione ad una gara, non viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede ad inoltrarla alla UOR competente che provvede ai necessari adempimenti.

Dopo l'apertura delle buste, l'UOR che gestisce la gara riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

11.7.5. Documenti non firmati

L'operatore di protocollo, conformandosi alle regole stabilite dal RGD attesta la data, la forma e la provenienza per ogni documento.

Le lettere anonime, sono protocollate su richiesta del RPA e identificate con la dicitura "mittente sconosciuto o anonimo" e "documento non sottoscritto".

Per le stesse ragioni le lettere con mittente, prive di firma, vanno protocollate e vengono identificate come tali.

È poi compito dell'UOR di competenza e, in particolare, del RPA valutare, se il documento privo di firma debba ritenersi valido e come tale trattato dall'ufficio assegnatario.

11.7.6. Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica convenzionale non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata come segue:

- caso di invio, come allegato, di un documento scansionato munito di firma autografa: il RPA valuta, caso per caso, l'opportunità di trattare il documento inviato via *e-mail;*

- caso di invio, in allegato, di un documento munito di firma digitale, o di invio di un messaggio firmato con firma digitale; il documento e/o il messaggio sono considerati come un documento elettronico inviato con qualunque mezzo di posta;

- caso di invio di una *e-mail* contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

11.7.7. Documenti digitali pervenuti erroneamente: annullamento della registrazione

L'addetto al protocollo, previa autorizzazione del RSP, provvede o ad annullare il protocollo stesso o a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

11.7.8. Documenti cartacei pervenuti erroneamente: annullamento della registrazione

Nel caso in cui sia protocollato un documento cartaceo, erroneamente inviato all'AOO, l'addetto al protocollo, previa autorizzazione del RSP, può:
- annullare il protocollo stesso;
- provvedere a protocollare il documento in uscita, indicando nell'oggetto "protocollato per errore"; il documento oggetto della rettifica viene restituito al mittente con la dicitura "protocollato per errore".

11.7.9. Corrispondenza cartacea personale o riservata

La corrispondenza che contiene diciture del tipo "S.P.M." oppure "PERSONALE", oppure "RISERVATA" non viene aperta, ma viene assegnata all'UOR destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati perché attivino una istanza, provvede a trasmetterli alla UOP per la protocollazione.

11.7.10. Integrazioni documentarie

L'addetto al protocollo non è tenuto a controllare la completezza formale e sostanziale della documentazione pervenuta, ma è tenuto a registrare in ogni caso il documento e gli eventuali allegati.

Tale verifica spetta al RPA.

La mancata integrazione della documentazione pervenuta comporta l'interruzione o la sospensione del procedimento.

I documenti pervenuti ad integrazione di quelli già disponibili, sono protocollati dalla UOP sul protocollo generale e, a cura del RPA, vengono classificati ed inseriti nel relativo fascicolo.

11.8 Gestione delle registrazioni di protocollo con il SdP

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 attraverso il SdP.

11.9. Registrazioni di protocollo

11.9.1. Valore giuridico del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente attribuendo valore giuridico-probatorio alla registrazione.

Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale della rete.

Come previsto dalla vigente normativa in materia di protezione dei dati personali le AOO aderenti al SdP sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

12. DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO

La descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'AOO, con particolare riferimento alle modalità di utilizzo dello stesso sono indicate nell'allegato "11"

13. REGISTRO DI EMERGENZA

Il RGD autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo sul registro di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.

Qualora l'impossibilità di utilizzo del sistema informatico di protocollo, si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il RGD può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana.

Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione

La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea.

Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema.

Entro dieci giorni dal ripristino della funzionalità del sistema, le informazioni relative ai documenti protocollati manualmente sono inserite nel sistema informatico associando loro il numero di Protocollo Generale del sistema informatico ordinario. In questo caso il documento sarà registrato con due numeri diversi:

- l'efficacia giuridico-probatoria è garantita dal numero del registro di emergenza
- il numero di Protocollo Generale garantirà l'unicità delle registrazioni.

Questa attività è coordinata dal RGD.

Sul registro di emergenza sono riportate:
a) Causa, data ed ora d'inizio dell'interruzione,
b) Data ed ora del ripristino della funzionalità del sistema
c) Estremi dell'autorizzazione all'uso del **Registro di Emergenza**

Schema del registro di emergenza

Numeri da assegnare alle registrazioni 1-5								
Numero Registr. emergenza	Data	Tipo	Mittente/Destinatario	Oggetto	Classificazione			
					Cat.	Classe	Sotto classe	n. Fascicolo

14. APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, REGOLE TRANSITORIE E FINALI

14.1. Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di Gestione" su proposta del RGD con Deliberazione di Giunta Comunale.

Il presente manuale potrà essere aggiornato 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;
- modifiche apportate negli allegati dal RGD

14.2. 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 dell'AOO e se possibile, viene resa disponibile mediante la rete intranet;
- pubblicato sul sito istituzionale dell'amministrazione.

14.3. Operatività del presente manuale

Il presente manuale è operativo il primo giorno del mese successivo a quello della sua approvazione.

ALLEGATO 1 – DEFINIZIONI

Ai fini del presente manuale di gestione si intende per:
"AMMINISTRAZIONE", il Comune di Montelupo F.no;

"TESTO UNICO", il D.P.R. 20.12.2000, n. 445 recante "Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;

"REGOLE TECNICHE", il D.P.C.M. 3.12.2013 recante "Regole tecniche per il protocollo informatico ai sensi degli articoli 40bis, 41, 47, 57bis e 71 del Codice dell'Amministrazione Digitale";

"C.A.D.", il D. Lgs. 7.3.2005, n. 82 recante "Codice dell'amministrazione digitale";
"AOO", l'Area Organizzativa Omogenea;

"MdG", il Manuale di Gestione;

DOCUMENTO AMMINISTRATIVO ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

PROTOCOLLO l'insieme delle procedure e degli elementi attraverso i quali i documenti vengono trattati sotto il profilo giuridico-gestionale.

SEGNATURA DI PROTOCOLLO l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso.

GESTIONE DEI DOCUMENTI l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dall'amministrazione comunale, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati.

SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dall'amministrazione comunale per la gestione dei documenti.

AMMINISTRATORE DI SISTEMA il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo dell'elaboratore e del sistema di base dati relativi al sistema di gestione informatica dei documenti e di consentirne l'utilizzazione.

SCRIVANIA VIRTUALE è associata ogni unità organizzativa dell'ente ed è un luogo "informatico" dove i documenti stazionano. Nell'ambito del sistema di gestione informatica dei documenti scrivania è, quindi, un "punto" della struttura avente la capacità di movimentare o visionare dei documenti.

FASCICOLO è l'unità archivistica che raccoglie i documenti relativi ad un procedimento amministrativo o ad un affare;

CLASSIFICAZIONE è l'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione;

FASCICOLAZIONE è l'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi;

ARCHIVIAZIONE DIGITALE è il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti digitali, anche informatici, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione;

SUPPORTO OTTICO DI MEMORIZZAZIONE è il mezzo fisico che consente la memorizzazione di documenti digitali mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD);

ARCHIVIO il complesso dei documenti prodotti e acquisiti nello svolgimento della propria attività e l'esercizio delle proprie funzioni dall'amministrazione comunale. Fanno parte dell'archivio del Comune di Pisa anche gli archivi e i documenti acquisiti per dono, deposito, acquisto o qualsiasi altro titolo.

L'archivio è suddiviso funzionalmente in:
ARCHIVIO CORRENTE: il complesso dei documenti relativi a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse corrente;
ARCHIVIO DI DEPOSITO: il complesso dei documenti relativi a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione o comunque verso i quali sussista un interesse sporadico;
ARCHIVIO STORICO: il complesso dei documenti relativi a procedimenti conclusi da oltre 40 anni e destinati, previa operazione di scarto, alla conservazione perenne nella sezione separata d'archivio.

FIRMA DIGITALE un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art. 1 comma 1 lett. s) del d. lgs.7 marzo 2005, n. 82);

MARCA TEMPORALE un'evidenza informatica che consente la validazione temporale (art. 1 comma 1 lett. i) del DPCM 31 gennaio 2004);

POSTA ELETTRONICA CERTIFICATA un sistema di comunicazione simile alla posta elettronica tradizionale a cui si aggiungono delle caratteristiche di sicurezza e di certificazione della trasmissione tali da rendere i messaggi opponibili a terzi.

INTERPRO è il sistema di protocollo interoperabile della Regione Toscana. Il sistema consente a due sistemi di protocollo informatico di amministrazioni della Regione Toscana di scambiarsi documenti informatici con trattamento automatico.

CONSERVAZIONE A NORMA processo di conservazione dei documenti informatici ai sensi della deliberazione CNIPA 19 febbraio 2004, n.11 e dalle "Regole tecniche" DPCM 13/12/2013;

ALLEGATO 2 – NORMATIVA DI RIFERIMENTO

Decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000
Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998, n. 428.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e ss. mm. E
Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

Decreto del Presidente della Repubblica 8 gennaio 2001, n. 37
Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato.

Decreto Legislativo 23 gennaio 2002, n. 10
Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

Ministro per l'innovazione e le tecnologie - 9 dicembre 2002
Direttiva sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

Decreto del Presidente della Repubblica 7 aprile 2003, n. 137
Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10.

Decreto Legislativo 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali.

Ministro per l'innovazione e le tecnologie - 14 ottobre 2003 - Approvazione delle linee guida per l'adozione del protocollo informatico e per i l trattamento informatico dei procedimenti amministrativi.

CNIPA Deliberazione 19 febbraio 2004, n.11 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.

Decreto Legislativo 22 gennaio 2004 n. 42 - Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137.

Decreto Legislativo 7 marzo 2005, n. 82 e ss. mm. e ii. - Codice dell'amministrazione digitale (CAD).

CNIPA Circolare 6 settembre 2005, n.48 - Modalità per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Decreto Legislativo 4 aprile 2006, n.159 - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.

Decreto Legislativo 24 marzo 2006, n.156 - Disposizioni correttive ed integrative al decreto legislativo 22 gennaio 2004, n.42, in relazione ai beni culturali.

Decreto Legge 29 novembre 2008 n. 185 – art. 16 c. 6 convertito in Legge 28 gennaio 2009 n. 2 - Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale - relativo all'utilizzo della posta elettronica certificata.

Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei

Decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 - Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.

CNIPA - Linee guida per l'utilizzo della firma digitale – Versione 1.3 - Aprile 2009.

CNIPA Deliberazione 21 maggio 2009, n. 45 - Regole per il riconoscimento e la verifica del documento informatico.

Deliberazione Garante per la Protezione dei dati personali del 2 marzo 2011, n. 88 - Linee Guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web.

Regole tecniche DigitPA per la consultazione ed estrazione di indirizzi PEC ed elenchi di indirizzi PEC di cui all'art. 6 comma 1-bis del CAD - 22 aprile 2011.

Decreto del Presidente del Consiglio dei Ministri 22 luglio 2011 - Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del CAD.

CIRCOLARE DigitPA 1 dicembre 2011, n. 58 - Attività di DigitPA e delle Amministrazioni ai fini dell'attuazione degli adempimenti previsti dall'articolo 50 -bis (Continuità Operativa) del «Codice dell'Amministrazione Digitale» (D.lgs. n. 82/2005 così come modificato dal D.lgs. 235/2010).

Decreto Legge 9 febbraio 2012 n. 5 convertito nella Legge 4 aprile 2012, n. 35 - Disposizioni urgenti in materia di semplificazione e di sviluppo.

Decreto Legge 22 giugno 2012, n. 83 (cosiddetto "Decreto Sviluppo"), convertito con modificazioni, dalla Legge 7 agosto 2012, n. 134 (in particolare: Art. 19 Istituzione dell'Agenzia per l'Italia digitale).

Decreto del Presidente del Consiglio dei Ministri 6 settembre 2012 - Separati certificati di firma, ai sensi dell'art. 28, comma 3-bis), del CAD, di cui al D.L. 7 marzo 2005 n. 82.

Deliberazione Garante per la Protezione dei dati personali 11 ottobre 2012 n. 280 - Protocollo informatico e protezione dei dati personali dei lavoratori.

Decreto Legge n. D.L. 18 ottobre 2012, n. 179 - Ulteriori misure urgenti per la crescita del Paese - **convertito in Legge 17 dicembre 2012, n. 221** – art. 5, 12, 13 e 13 bis.

Agenzia per l'Italia Digitale - Linee guida per il Disaster Recovery delle Pubbliche Amministrazioni – Aggiornamento 2013.

Circolare Agenzia per l'Italia Digitale n. 60 del 23 gennaio 2013 - Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni. Revisione della Circolare AIPA del 7 maggio 2001, n. 28 relativa agli standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati, ai sensi dell'art. 18, comma 2, del D.P.C.M. 31 ottobre 2000 di cui al D.P.R. 28 dicembre 2000, n. 445.

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.

D.M. 19 marzo 2013 - Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti (INI-PEC).

Decreto del Presidente del Consiglio dei Ministri 21 marzo 2013 - Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni.

Circolare Agenzia per l'Italia Digitale n. 61 del 29 marzo 2013 - Disposizioni del D.L. 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012, 221 in tema di accessibilità dei siti web e servizi informatici. Obblighi delle Pubbliche Amministrazioni.

Circolare Agenzia per l'Italia Digitale n. 62 del 30 aprile 2013 - Linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD.

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

Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

ALLEGATO 3 – STRUTTURA ORGANIZZATIVA

SERVIZI E UFFICI	UOP	UOR
SERVIZIO COMUNICAZIONE E SERVIZI DI SUPPORTO		si
Segreteria Generale	si	si
Sportello Unico Amministrativo	si	si
Anagrafe e Stato civile		si
Elettorale		si
URP	si	si
SERVIZIO AFFARI GENERALI		si
Attività Educative e Formative		si
Mmbab		si
Risorse strumentali e innovazione tecnologica		si
Risorse economiche e programmazione finanziaria		si
Ragioneria - Uff_eFatturaPA		si
Economato		si
Tributi		si
Ufficio Associato del Personale		si
SERVIZIO ASSETTO DEL TERRITORIO		si
Sportello Unico Attività tecniche		si
Ambiente		si
Edilizia Privata		si
Suap		si
Urbanistica		si
SERVIZIO LAVORI PUBBLICI		si
Attività amministrative e contrattuali		si
Manutenzioni		si
Progettazioni		si
SERVIZIO DI POLIZIA MUNICIPALE		si
ATTIVITA' DI PROGETTAZIONE		si
CENTRO COMUNALE PER L'ARCHEOLOGIA CERAMICA		si
SEGRETARIO GENERALE		si
SINDACO		si
VICE-SINDACO		si
ASSESSORI		si

ALLEGATO 4 - ELENCO DEI TITOLARI DI FIRMA DIGITALE

ANNA	GRANELLI	SPORTELLO UNICO AMMINISTRATIVO
BENEDETTA	FALTERI	MMBAB
CHIARA	BOLLINI	SPORTELLO UNICO AMMINISTRATIVO
CLAUDIO	BALDUCCI	SPORTELLO UNICO AMMINISTRATIVO
CRISTINA	TRINCI	SPORTELLO UNICO AMMINISTRATIVO
DANIELA	MANETTI	SPORTELLO UNICO AMMINISTRATIVO
DANIELA	CERBAI	LAVORI PUBBLICI – ATTIVITA' AMMINISTRATIVE
EMANUELE	ROMOLI	LAVORI PUBBLICI
GIOVANNI	VINCI	LAVORI PUBBLICI
GIUSEPPA	MARUCCIO	ECONOMATO
LORENZO	NESI	VICE-SINDACO
LORENZO	SORDI	SUAP
LUCIO	FABBRIZZI	ASSETTO DEL TERRITORIO
LUISA	BUGETTI	AFFARI GENERALI
MANUELA	SCALI	SEGRETERIA GENERALE
MARIA TERESA	MIGLIORI	RISORSE ECONOMICHE E PROGRAMMAZIONE FINANZIARIA
MASSIMO	ALDERIGHI	MMBAB
PAOLA	ANZILOTTA	SEGRETARIO
PAOLA	GIANI	TRIBUTI
PAOLO	MASETTI	SINDACO
PAOLO	NIGI	POLIZIA MUNICIPALE
PAOLO	VAGLINI	ASSETTO DEL TERRITORIO
PARIDE	MATINI	UFFICIO PERSONALE
RICCARDO	MANETTI	ASSETTO DEL TERRITORIO
ROSA	FUSCO	ASSETTO DEL TERRITORIO
SANDRA	BONFANTI	LAVORI PUBBLICI – ATTIVITA' AMMINISTRATIVE
SARA	NALDINI	ASSETTO DEL TERRITORIO
SIMONETTA	ROMANELLI	ATTIVITA' EDUCATIVE E FORMATIVE
STEFANIA	ORSINI	SPORTELLO UNICO AMMINISTRATIVO
UMBERTO	SANTINI	LAVORI PUBBLICI - MANUTENZIONI
VALENTINA	SPAGLI	SERVIZIO COMUNICAZIONE E SERVIZI DI SUPPORTO

ALLEGATO 5 – TITOLARIO DI CLASSIFICAZIONE

dic. 2005	Schema riassuntivo del piano di classificazione per l'archivio comunale
I	Amministrazione generale 1. Legislazione e circolari esplicative 2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica 3. Statuto 4. Regolamenti 5. Stemma, gonfalone, sigillo 6. Archivio generale 7. Sistema informativo 8. Informazioni e relazioni con il pubblico 9. Politica del personale; ordinamento degli uffici e dei servizi 10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale 11. Controlli interni ed esterni 12. Editoria e attività informativo-promozionale interna ed esterna 13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti 14. Interventi di carattere politico e umanitario; rapporti istituzionali 15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni 16. Area e città metropolitana 17. Associazionismo e partecipazione
II	Organi di governo, gestione, controllo, consulenza e garanzia 1. Sindaco 2. Vice-Sindaco 3. Consiglio 4. Presidente del Consiglio 5. Conferenza dei capigruppo e Commissioni del Consiglio 6. Gruppi consiliari 7. Giunta 8. Commissario prefettizio e straordinario 9. Segretario e Vice-segretario 10. Direttore generale e dirigenza 11. Revisori dei conti 12. Difensore civico 13. Commissario *ad acta* 14. Organi di controllo interni 15. Organi consultivi 16. Consigli circoscrizionali 17. Presidente dei Consigli circoscrizionali 18. Organi esecutivi circoscrizionali 19. Commissioni dei Consigli circoscrizionali 20. Segretari delle circoscrizioni 21. Commissario *ad acta* delle circoscrizioni 22. Conferenza dei Presidenti di quartiere
III	Risorse umane 1. Concorsi, selezioni, colloqui 2. Assunzioni e cessazioni 3. Comandi e distacchi; mobilità 4. Attribuzione di funzioni, ordini di servizio e missioni 5. Inquadramenti e applicazione contratti collettivi di lavoro 6. Retribuzioni e compensi 7. Trattamento fiscale, contributivo e assicurativo 8. Tutela della salute e sicurezza sul luogo di lavoro 9. Dichiarazioni di infermità ed equo indennizzo 10. Indennità premio di servizio e trattamento di fine rapporto, quiescenza 11. Servizi al personale su richiesta 12. Orario di lavoro, presenze e assenze 13. Giudizi, responsabilità e provvedimenti disciplinari 14. Formazione e aggiornamento professionale 15. Collaboratori esterni
IV	Risorse finanziarie e patrimonio 1. Bilancio preventivo e Piano esecutivo di gestione (PEG) 2. Gestione del bilancio e del PEG (con eventuali variazioni) 3. Gestione delle entrate: accertamento, riscossione, versamento 4. Gestione della spesa: impegno, liquidazione, ordinazione e pagamento 5. Partecipazioni finanziarie 6. Rendiconto della gestione; adempimenti e verifiche contabili 7. Adempimenti fiscali, contributivi e assicurativi 8. Beni immobili 9. Beni mobili 10. Economato 11. Oggetti smarriti e recuperati 12. Tesoreria 13. Concessionari ed altri incaricati della riscossione delle entrate 14. Pubblicità e pubbliche affissioni

V	Affari legali 1. Contenzioso 2. Responsabilità civile e patrimoniale verso terzi; assicurazioni 3. Pareri e consulenze
VI	Pianificazione e gestione del territorio 1. Urbanistica: piano regolatore generale e varianti 2. Urbanistica: strumenti di attuazione del piano regolatore generale 3. Edilizia privata 4. Edilizia pubblica 5. Opere pubbliche 6. Catasto 7. Viabilità 8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi 9. Ambiente: autorizzazioni, monitoraggio e controllo 10. Protezione civile ed emergenze
VII	Servizi alla persona 1. Diritto allo studio e servizi 2. Asili nido e scuola materna 3. Promozione e sostegno delle istituzioni di istruzione e della loro attività 4. Orientamento professionale; educazione degli adulti; mediazione culturale 5. Istituti culturali (Musei, Biblioteche, Teatri, Scuola comunale di musica, etc.) 6. Attività ed eventi culturali 7. Attività ed eventi sportivi 8. Pianificazione e accordi strategici con enti pubblici e privati e con il volontariato sociale 9. Prevenzione, recupero e reintegrazione dei soggetti a rischio 10. Informazione, consulenza ed educazione civica 11. Tutela e curatela di incapaci 12. Assistenza diretta e indiretta, benefici economici 13. Attività ricreativa e di socializzazione 14. Politiche per la casa 15. Politiche per il sociale
VIII	Attività economiche 1. Agricoltura e pesca 2. Artigianato 3. Industria 4. Commercio 5. Fiere e mercati 6. Esercizi turistici e strutture ricettive 7. Promozione e servizi
IX	Polizia locale e sicurezza pubblica 1. Prevenzione ed educazione stradale 2. Polizia stradale 3. Informative 4. Sicurezza e ordine pubblico
X	Tutela della salute 1. Salute e igiene pubblica 2. Trattamento Sanitario Obbligatorio 3. Farmacie 4. Zooprofilassi veterinaria 5. Randagismo animale e ricoveri
XI	Servizi demografici 1. Stato civile 2. Anagrafe e certificazioni 3. Censimenti 4. Polizia mortuaria e cimiteri
XII	Elezioni ed iniziative popolari 1. Albi elettorali 2. Liste elettorali 3. Elezioni 4. Referendum 5. Istanze, petizioni e iniziative popolari
XIII	Affari militari 1. Leva e servizio civile sostitutivo 2. Ruoli matricolari 3. Caserme, alloggi e servitù militari 4. Requisizioni per utilità militari
XIV	Oggetti diversi

ALL. 6)

Manuale della Conservazione di Maggioli S.p.A.

EMISSIONE DEL DOCUMENTO

Azione	Data	Nominativo	Funzione
Redazione	01/06/2015	F. Tiralongo	Responsabile sviluppo e manutenzione del sistema di conservazione
Verifica		B. Pacassoni	Responsabile Qualità Gruppo Maggioli
Approvazione		M. Villa	Responsabile del servizio di conservazione

REGISTRO DELLE VERSIONI

N°Ver/Rev/Bozza	Data emissione	Modifiche apportate	Osservazioni
1 – 0 – Bozza	01/06/2015	Prima stesura	
1 – 1 – Rilasciato	05/06/2015	Verifica della struttura del documento e stralcio delle ridondanze	
1 – 2 – Rilasciato	10/07/2015	Integrazioni al Manuale di conservazione	
1 – 3 – Rilasciato	14/07/2015	Reintroduzione delle tabelle e degli schemi XSD omessi in prima stesura	Capitolo 6

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini, C.F. e P.IVA 02066400405
R.E.A. n. 219107
C.A. 0810883901 50

Capitale sociale:
Euro 2.215.200
interamente versato

INDICE DEL DOCUMENTO

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini + R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

INDICE DELLE TABELLE

INDICE DELLE FIGURE

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini n. R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

1 SCOPO E AMBITO DEL DOCUMENTO

Il presente manuale descrive la struttura e la gestione del sistema di conservazione, la definizione dei ruoli e delle interazioni con i soggetti esterni con i quali interagisce.

Nella redazione del documento e dei suoi allegati, come nella scelta e nell'*assesment* del software utilizzato per la componente *core* del servizio, si è tenuto conto di quanto previsto dal documento "Requisiti di qualità e sicurezza per l'accreditamento e la vigilanza" limitatamente, ma non solo, alle indicazioni sui contenuti del manuale di conservazione e dettaglia gli elementi elencati all'articolo 8, comma 2, del suddetto DPCM.:

- la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- la struttura organizzativa, comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione; riportata nel presente manuale e richiamata nelle condizioni di fornitura del servizio allegate;
- la descrizione delle tipologie degli oggetti sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di documenti e delle eventuali eccezioni è riportata in Allegato 1 al Manuale – "Modalità e Condizioni di fornitura del servizio";
- la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento è riportata nel presente documento e dettagliata nelle specifiche di integrazione in Allegato 2 al Manuale – "Specifiche di interoperabilità ed integrazione applicativa del servizio";
- la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- la descrizione delle procedure per la richiesta di duplicati o copie;
- le normative in vigore nei luoghi dove sono conservati i documenti.

Si fa presente che alcuni argomenti che riguardano aspetti delle specifiche forniture del servizio di conservazione, come alcune delle informazioni previste all'interno del manuale, sono state enucleate dal presente documento per motivi di privacy e/o sicurezza e per i quali è richiesta la non pubblicazione. Tali informazioni vengono già depositate all'atto della domanda di accreditamento:

- Le specificità del contratto di si sviluppano nel già citato Allegato 1 "Modalità e Condizioni di fornitura del servizio";
- i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, sono disponibili su richiesta tramite estrazione dell'apposito report dal sistema di conservazione stesso. Le deleghe, gli incarichi e le nomine interne al Conservatore sono descritte in modo puntuale, nell'allegato *N* alla domanda di accreditamento;
- la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione e di evoluzione delle medesime sono citate nel manuale ed approfondite nell'allegato *O "copia del piano per la sicurezza";*

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

- la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie è dettagliata nel piano della sicurezza allegato;

Ogni modifica al presente Manuale prevede una nuova versione del manuale stesso, in base alle policy di gestione documentale in uso presso il Conservatore, e il suo invio all'Agenzia dell'Italia Digitale entro 20 giorni dalla sua pubblicazione.

La verifica delle diverse versioni del Manuale e della loro conservazione sono oggetto dell'attività di vigilanza ed eseguite sotto il diretto controllo del Responsabile del servizio di conservazione.

Torna al sommario

2 TERMINOLOGIA (GLOSSARIO, ACRONIMI e DEFINIZIONI)

Rimandando al DPCM 3 dicembre 2013 allegato I, pubblicato sul sito www.gazzettaufficiale.it, si riportano qui di seguito i termini e gli acronimi ricorrenti nel testo o comunque giudicati significativi in relazione alla materia trattata.

Glossario dei termini e Acronimi	
Accesso	operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici
Accreditamento	riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Aggregazione documentale informatica	aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente
AgID	Agenzia per l'Italia Digitale
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
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
AIP	Archival Information package (Pacchetto di archiviazione) - pacchetto informative composto dalla trasformazione di uno o più pacchetti di versamento all'interno del sistema di conservazione
AOO	Area Organizzativa Omogenea
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
CA	Certification Authority

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini + R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

CAD	Codice dell'amministrazione digitale
certificatore accreditato	soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza
ciclo di gestione	arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo
Classificazione	attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuare attraverso specifici metadati
Codice	decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni
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
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
Conservazione	L'insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione
copia analogica del documento informatico	documento analogico avente contenuto identico a quello del documento informatico da cui è tratto
copia di sicurezza	copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle presenti regole tecniche per il sistema di conservazione
CRL	Certificate Revocation List, è la lista dei certificati revocati o sospesi, ovvero lista di certificati che sono stati resi non validi prima della loro naturale scadenza
Destinatario	identifica il soggetto/sistema al quale il documento informatico è indirizzato
DIP	Dissemination Information Package (Pacchetto di distribuzione) - pacchetto informativo generato dal sistema di conservazione su espressa e specifica richiesta effettuata da un utente precedentemente autorizzato dal Soggetto Produttore
duplicazione dei documenti informatici	produzione di duplicati informatici
Esibizione	Operazione atta a generare un pacchetto di distribuzione, solitamente necessario in sede di contenzioso, che consente di esibire una copia conforme di un documento conservato e delle sue informazioni di rappresentazione necessarie alla fruibilità dei dati in esso contenuti
evidenza informatica	una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.210.200
interamente versato

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
IdC	Indice di Conservazione - È l'evidenza di avvenuta conservazione e garantisce la possibilità di verificare la validità del dato conservato al momento dell'esibizione del documento
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 (funzione di hash)	funzione matematica riproducibile e verificabile che, partendo da un documento informatico, genera una sequenza univoca di byte non invertibile
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	caratteristiche di un documento informatico che ne attestano la completezza e la conformità all'originale
Interoperabilità	capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi
IR	Informazioni sulla rappresentazione
ISO	International organization for Standardization
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
Metadati	Informazioni, associate ad un documento informatico all'atto del versamento, necessarie alla sua successiva identificazione univoca in fase di ricerca ed esibizione.
Memorizzazione	processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici
Metadati	insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del presente decreto

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggioli@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini - R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

OAIS	ISO 14721:2012; Space Data information transfer system,.....
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
PDI	Preservation description information (informazioni sulla conservazione)
PEC	Posta Elettronica Certificata
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 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
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.
RdV	Rapporto (o Verbale) di Versamento - Indica la presa in carico del SIP da parte del sistema di conservazione. Riporta l'elenco dei documenti versati e i metadati forniti dal SP o dal sistema applicativo di versamento.
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
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

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale Sociale:
Euro 2.216.200 i.v.

SC	Soggetto Conservatore - Maggioli S.p.A.
Scarto	operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e di interesse storico culturale
SdC	Sistema di Conservazione - Il sistema (o servizio) di conservazione offerto dal SC
SdV	Sistema di Versamento - il sistema (o l'applicazione) che costruisce i SIP e li inoltra alla conservazione
SIP	Submission Information Package (Pacchetto di versamento) - pacchetto informativo inviato dal produttore al sistema di conservazione secondo modalità e specifiche concordate
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
SP	Soggetto Produttore - il proprietario del dato e colui che è responsabile del versamento dei dati nel sistema di conservazione
SMTP	Simple Mail Transfer Protocol (SMTP) - Standard per la trasmissione messaggi (e-mail) in internet
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
TSA	Time Stamping Autorithy – Soggetto Certificato/Certificatore autorizzato a rilasciare riferimenti temporali certi
transazione informatica	particolare evento caratterizzato dall'atomicità, consistenza, 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
UNI SInCRO	UNI 11386:2010 - Supporto all'Interoperabilità nella conservazione e nel Recupero del documento informatico
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

Tabella 1 - Acronimi e Definizioni

Torna al sommario

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.218.200
interamente versato

3 NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Si riporta qui di seguito la principale normativa di riferimento considerata per l'attività di conservazione già inclusa nel documento "Modalità e Condizioni di fornitura del servizio", aggiornato a cura del Responsabile Sicurezza dei sistemi per la conservazione:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

3.2 Standard di riferimento

Si riportano qui di seguito gli standard a cui l'attività di conservazione si riferisce, già inclusi nel documento "Modalità e Condizioni di fornitura del servizio", aggiornato a cura del Responsabile Sicurezza dei sistemi per la conservazione e che sono richiamati nel 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);

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

- 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

Presso il Conservatore, a seguito dell'incarico ricevuto dal conservatore, sono designai i seguenti responsabili, i cui dettagli e curricula sono depositati presso AgID all'atto dell'accreditamento.

Ruoli	nominativo	attività di competenza	periodo nel ruolo
Responsabile del servizio di conservazione	*M. Villa - Direttore di divisione Maggioli Modulgrafica*	• 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	*oltre 8 anni in ruolo analogo*
Responsabile Sicurezza dei sistemi per la conservazione	*B. Paccassoni - Impiegato a tempo indeterminato Maggioli S.p.A.; Responsabile della Qualità per il Gruppo Maggioli*	• 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	*oltre 5 anni in ruolo analogo*
Responsabile funzione archivistica di conservazione	*E. Bruno - Consulente esterno con contratto di tre anni, rinnovabile*	• Definizione e gestione del processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; • Definizione del set di metadati di conservazione dei documenti e dei fascicoli	*Laurea Magistrale e esperienza di oltre 3 anni in ruolo analogo*

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (FN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.216.200
interamente versato

		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	
Responsabile trattamento dati personali	*M. Villa - Direttore di divisione Maggioli Modulgrafica*	• Garanzia del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali; • garanzia che il trattamento dei dati affidati dai Clienti avverrà nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza	*oltre 8 anni in ruolo analogo*
Responsabile sviluppo e manutenzione del sistema di conservazione	*F. Tiralongo - Impiegato a tempo indeterminato Maggioli S.p.A.;*	• 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	*oltre 5 anni in ruolo analogo*
Responsabile sistemi informativi per la conservazione	*O. Bevoni – Direttore Responsabile dei Sistemi Informativi del Gruppo Maggioli*	• Gestione dell'esercizio delle componenti hardware e software del sistema di conservazione; • monitoraggio del mantenimento dei livelli di servizio (SLA) concordati con l'ente produttore; • segnalazione delle eventuali difformità degli SLA al Responsabile del servizio di conservazione e individuazione e pianificazione delle necessarie azioni correttive; • pianificazione dello sviluppo delle infrastrutture tecnologiche del sistema di conservazione; • controllo e verifica dei livelli di servizio erogati da terzi con segnalazione delle eventuali difformità al Responsabile del servizio di conservazione.	*oltre 10 anni in ruolo analogo*

Tabella 2 - Nomine in capo al Conservatore

Il sistema di conservazione digitale dei documenti informatici opera secondo i modelli tecnici ed organizzativi pubblicati nel presente manuale di conservazione e, a tutela dei soggetti coinvolti, si determina entità distinta logicamente e fisicamente dal sistema di gestione documentale o do versamento che resta sotto la completa responsabilità del Cliente o del Soggetto Produttore delegato.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolisp@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

Il servizio di conservazione, coerentemente con lo standard OAIS, tiene conto dei 3 attori principali coinvolti nei flussi di input/output (I/O) della conservazione:

Il Producer del cliente ovvero il **Soggetto Produttore**, responsabile del versamento per conto del cliente (nel caso in cui le due figure non coincidano) che invece mantiene la proprietà e la responsabilità dei dati trasmessi delegando l'Outsourcer al trattamento di tali dati per le sole attività previste dalla conservazione e nominando MAGGIOLI S.p.A. quale Responsabile esterno del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali (D.Lgs. 196/2003 e s.m.i.).

Il Soggetto Conservatore: MAGGIOLI S.p.A., con sede legale in Santarcangelo di Romagna (RN) Via del Carpino, 8 iscritta al Registro delle Imprese di Rimini al n. 06188330150, al R.E.A. di Rimini al n. 219107, C.F. 06188330150 e Partita IVA 02066400405; numero telefono 0541/628111 e numero fax 0541/622100, casella di posta elettronica maggiolispa@maggioli.it, in persona dell'Amministratore Delegato dott. Paolo Maggioli, di seguito denominata, per brevità, **"Outsourcer"** o **"Conservatore"**.

Il Consumer, il cliente, nella persona dei suoi delegati, identificato con colui che è autorizzato ad accedere ai dati conservati, secondo le specifiche condivise e rispetto a quanto riportato nelle condizioni generali di fornitura del servizio.

4.1 Suddivisione dei ruoli

L'immagine qui sotto rappresenta lo schema di riferimento dei flussi I/O del sistema di conservazione ed i campi di responsabilità/azione di ciascuno degli attori citati in precedenza:

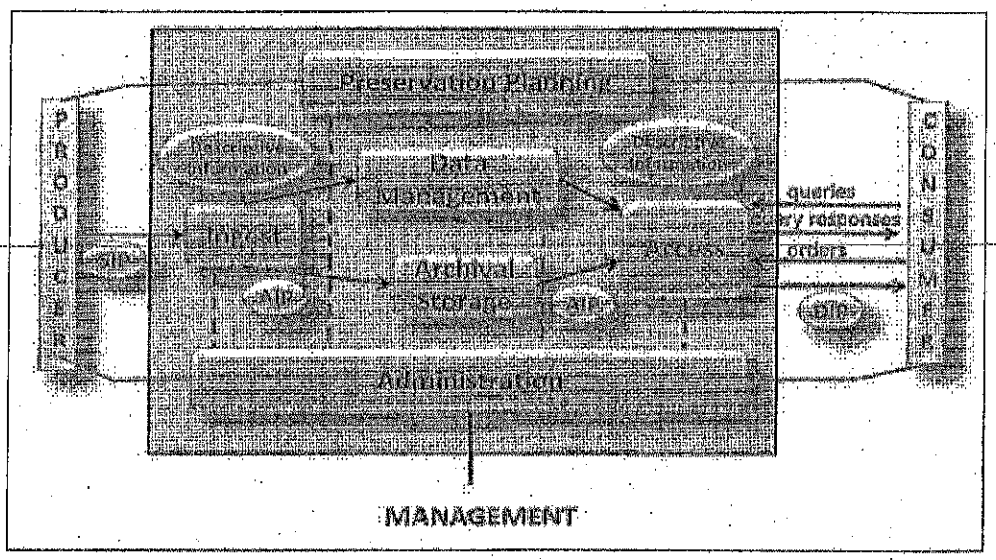


Figura 1 - Flussi OAIS

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini n. R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

- Il sistema documentale o comunque il Soggetto Produttore genera i Pacchetti di Versamento (SIP) secondo le specifiche del servizio di conservazione e le direttive di interoperabilità dell'AgID;
- Il Sistema di Conservazione elabora e verifica i SIP generando un rapporto/verbale di versamento (RdV), atto a certificare la corretta presa in carico del volume versato;
- Terminata la trascrizione dei dati da conservare e dei metadati, utili a garantire la reperibilità del documento informatico in futuro, il Sistema di conservazione genera un indice di conservazione (IdC) firmato digitalmente dal Conservatore e marcato temporalmente;
- Controlli periodici, sia automatici, sia operativi e manuali, verificheranno che i dati conservati non abbiano subito alterazioni, confrontando i dati in archivio con i dati registrati nell'indice di conservazione;
- Gli utenti, autorizzati dal Responsabile della conservazione del cliente, potranno accedere ai dati conservati per richiedere la generazione di pacchetti di distribuzione (DIP), utili all'esibizione del documento informatico in sede di contenzioso legale.

La conservazione a norma del documento informatico garantisce il mantenimento della validità legale del documento conservato "congelando" lo stato del documento e delle firme digitali e delle marche temporali che lo accompagnano, dal momento del versamento per tutta la sua permanenza all'interno del flusso di conservazione.

4.2 Obblighi e responsabilità

Il Titolare dei documenti informatici inviati in conservazione è **il Cliente,** che attraverso il proprio **Responsabile della Conservazione**, delega all'Outsourcer la gestione del servizio di conservazione secondo le politiche complessive ed il sistema di gestione in uso presso il Conservatore.

Il Conservatore, MAGGIOLI S.p.A., nomina i delegati ed i responsabili individuati nel suo organico secondo le direttive di legge ed il CAD di riferimento, indicando Mauro Villa, Direttore di Divisione, come **Responsabile del Servizio di Conservazione**, al momento della stesura del presente manuale. Lo storico dei nominativi dei vari responsabili in capo al conservatore, i delegati del conservatore e del Responsabile del servizio ed i loro CV, sono depositati presso AgID all'atto di richiesta dell'accreditamento. Il report dei Responsabili di conservazione che si sono succeduti nel tempo in riferimento ai versamenti degli specifici Soggetti Produttori è disponibile, a richiesta, nel sistema di conservazione stesso. Le nomine sono pubbliche e comunicate ad AgID in fase di richiesta di accreditamento. La stessa agenzia, si occuperà delle eventuali verifiche e il Soggetto Conservatore dell'aggiornamento di tali dati.

4.2.1 Obblighi del Cliente

Il processo di conservazione impone al Cliente l'istituzione di un'organizzazione interna idonea, che garantisca la piena osservanza delle disposizioni normative in tema di gestione documentale e delle procedure da osservare per la corretta produzione, formazione, emissione e sottoscrizione dei documenti informatici destinati alla conservazione digitale in conformità alle regole tecniche di cui all'art. 71 del CAD ed a quanto stabilito nel presente documento.

Ogni Cliente, identificato con uno o più Soggetti Produttori (SP o AOO), adotta il manuale di conservazione del conservatore e definisce le sue DA (Descrizioni Archivistiche) compilando il modulo di attivazione. Il Cliente dichiara di aver letto il presente documento e di voler procedere al versamento in conservazione utilizzando le DA scelte e qui descritte, secondo le modalità concordate, riportate nel "Manuale di conservazione – Maggioli" e riassunte nelle condizioni di fornitura allegate alla richiesta di attivazione.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

4.2.2 Obblighi del Conservatore

Rispetto a quanto già indicato il conservatore, limitatamente alle attività ad essa delegate, è responsabile verso il Cliente per l'adempimento degli obblighi discendenti dall'espletamento delle attività previste dalla normativa vigente in materia di conservazione digitale dei documenti informatici versati da Soggetto Produttore nei modi e nei termini specificati nel presente documento, negli allegati e nei manuali ad esso relativi.

Pertanto è obbligo del Conservatore conservare digitalmente i documenti informatici del Cliente allo scopo di assicurare, dalla presa in carico e fino all'eventuale cancellazione, la loro conservazione a norma, garantendone, tramite l'adozione di regole, procedure e tecnologie, le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità.

Il Sistema di conservazione è in grado di esibire tutti i documenti informatici in esso conservati in qualsiasi momento del periodo di conservazione, secondo le richieste di accesso, esibizione o consegna dei documenti conservati, effettuate dai soggetti debitamente autorizzati.

Oltre alla restituzione dei documenti informatici trasferiti e conservati, viene garantita anche la restituzione dei relativi indici di conservazione (ex "evidenze") che garantiscono la corretta conservazione degli stessi, fornendo gli elementi necessari per valutare la loro autenticità e validità giuridica.

Restano a carico del Conservatore:

- La definizione delle caratteristiche ed i requisiti del sistema di conservazione;
- L'attuazione di procedure di sicurezza e tracciabilità che consentano di risalire in ogni momento alle attività effettuate durante l'esecuzione operativa di conservazione;
- La gestione delle procedure informatiche ed organizzative per la corretta tenuta dei supporti su cui vengono memorizzati i documenti informatici oggetto di conservazione
- Il funzionamento delle procedure informatiche atte ad esibire la documentazione conservata, in caso di richieste formulate da chi ne abbia titolo
- Il mantenimento di un registro cronologico del software di conservazione
- L'adozione di un registro cronologico degli eventi (di gestione, accessi, attività, ecc.) del sistema di conservazione
- Il monitoraggio dei sistemi software ed hardware coinvolti
- L' analisi del log di sistema e di sicurezza
- Verificare la validità delle firme digitali e delle marche temporali utilizzate dal sistema di conservazione ed emesse da Certification Authority italiane, accreditate e riconosciute

4.3 Trattamento dei dati

Con l'affidamento del servizio il **Soggetto Produttore** nomina e delega a **MAGGIOLI S.p.A.** le seguenti cariche:

- **Responsabile del servizio di conservazione**
- **Responsabile esterno del trattamento dei dati**

Maggioli S.p.A. garantisce la tutela degli interessati in ottemperanza a quanto disposto del D.Lgs. 196/2003 e s.m.i. Il Cliente è informato sui diritti di accesso ai dati personali ed altri diritti (art. 7, D.Lgs. 196/2003 e s.m.i.).

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini n. R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.215.200
(interamente versato

4.3.1 Trattamento dei dati personali

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. I dati raccolti sono utilizzati per il perfezionamento del Contratto e per l'attivazione del Servizio di conservazione a norma dei documenti informatici. Maggioli S.p.A. utilizzerà i dati raccolti per lo svolgimento dell'attività connessa e/o derivante dal Servizio di conservazione dei documenti informatici del Cliente.

4.3.2 Trattamento dei dati conservati

Come previsto dalle norme vigenti in materia, il Conservatore adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo: i rischi di distruzione o perdita, anche accidentale, dei documenti informatici, di danneggiamento delle risorse hardware su cui i documenti informatici sono registrati ed i locali ove i medesimi vengono custoditi; l'accesso non autorizzato ai documenti stessi; i trattamenti non consentiti dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

- l'integrità dei documenti informatici, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;
- la disponibilità dei dati e dei documenti informatici da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei documenti informatici, evitando la perdita o la riduzione dei dati anche accidentale utilizzando un sistema di backup;
- la riservatezza dei documenti informatici da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

Per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e la difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i documenti informatici ed i dati forniti potranno essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità Pubbliche e Autorità Giudiziaria per lo svolgimento delle attività di loro competenza. Come previsto dalle norme vigenti in materia, il Conservatore adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo: i rischi di distruzione o perdita, anche accidentale, dei documenti informatici, di danneggiamento delle risorse hardware su cui i documenti informatici sono registrati ed i locali ove i medesimi vengono custoditi; l'accesso non autorizzato ai documenti stessi; i trattamenti non consentiti dalla legge o dai regolamenti aziendali.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini n. R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

4.3.3 Accesso ai dati conservati

Il Cliente detiene la proprietà del dato conservato e ne autorizza l'accesso, secondo le modalità previste per la conservazione a norma, al suo **Responsabile della Conservazione** e **agli altri utenti** identificati dal responsabile stesso.

I dati conservati sono catalogati per DA, quindi in base alla **Descrizione Archivistica** a cui sono associati. La DA di appartenenza di un documento è quindi **un attributo logico del dato versato** che ne determina i vari aspetti, dettagliati nel documento "Modalità e Condizioni di fornitura del servizio", ma non la proprietà del dato stesso che è invece sempre associata al solo SP (Soggetto Produttore).

L'accesso ai dati conservati, come il versamento dei dati in conservazione, **avviene sempre tramite canale criptato.** In particolare le applicazioni o gli utenti, interagiscono con il sistema di conservazione solo via HTTPS ed in alcuni casi via SFTP, secondo le specifiche fornite dal conservatore e sempre con l'utilizzo di credenziali personali e personalizzate, secondo le regole in uso presso il conservatore ed in relazione alla segregazione dei ruoli, e del minimo privilegio. Ogni Soggetto Produttore nomina quindi le persone ed eventualmente le applicazioni autorizzati all'accesso ai documenti informatici posti in conservazione e associati al Soggetto Produttore medesimo.

Figure di riferimento

In ognuna delle 3 macrostrutture indicate, si identificano precise figure di riferimento oggetto di deleghe e nomine secondo quanto previsto dalla vigente normativa e riportato nelle condizioni di fornitura del servizio:

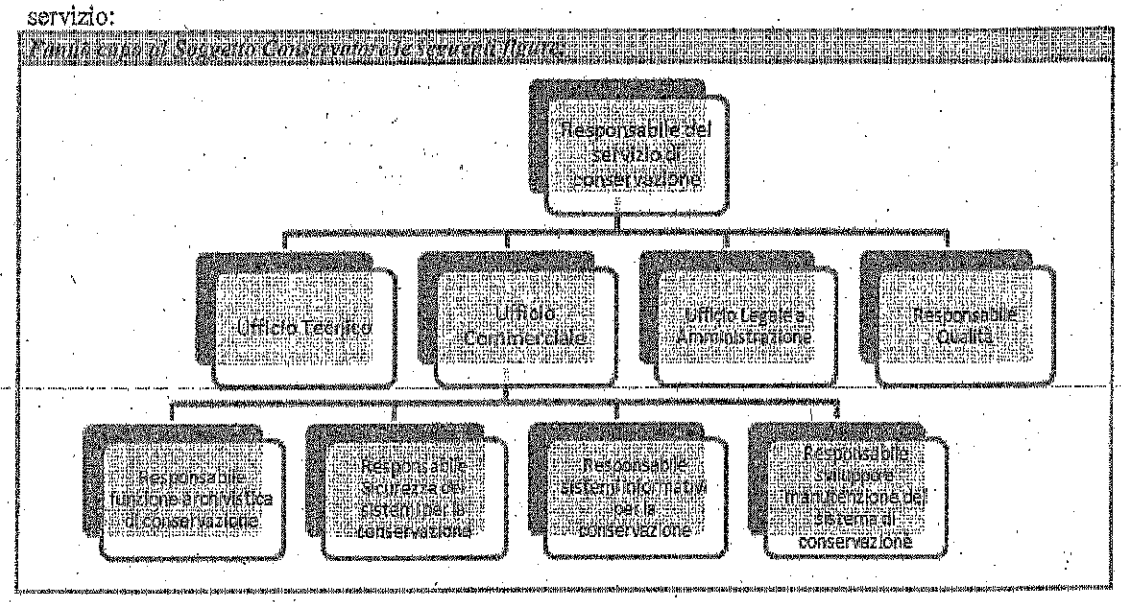


Tabella 3 - Struttura SC

Maggioli SpA
via del Carpino, 8
47922 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

Si identificano tra Soft Cliente i seguenti riferimenti	
Referente Contrattuale	Firma l'ordine di attivazione e riceve: • le comunicazioni di attivazione effettuata e di fatturazione • le notifiche di superamento delle soglie di utilizzo del servizio configurate • le richieste di rinnovo o estensione del contratto
Referente Tecnico	Collabora con i tecnici del Conservatore all'avvio delle procedure di versamento/integrazione. Ad attività avviata è il riferimento per: • l'invio di eventuali aggiornamenti alle specifiche di integrazione • le eventuali comunicazioni di disservizio programmato
Responsabile della conservazione	Affidando in outsourcing il servizio di conservazione adotta il manuale di conservazione del conservatore e delega le attività correlate: • definizione delle caratteristiche e i requisiti del sistema di conservazione, in conformità alla normativa vigente; • gestione del processo di conservazione in aderenza, nel tempo, alla normativa vigente; • generazione del rapporto di versamento, secondo le modalità previste dal manuale di conservazione; • generazione e sottoscrizione del pacchetto di archiviazione con firma digitale e riferimento temporale certificato (marcatura) • monitorare la funzionalità del sistema di conservazione; • verificare periodicamente l'integrità degli archivi e della leggibilità degli dati conservati; • adottare le misure necessarie a rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e, ove necessario, a ripristinare la corretta funzionalità; • adottare analoghe misure con riguardo all'obsolescenza dei formati provvedendo, se necessario, alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico; • adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12; • assicurare 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; • assicurare e organizzare l'espletamento delle attività periodiche di verifica e di vigilanza; • provvedere a predisporre il manuale di conservazione di cui all'art. 8 e curandone l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
Utente	Riceve le credenziali utili alla fruizione dei dati conservati (Ricerca, Esibizione, Download e richiesta di generazione dei pacchetti di distribuzione)

Tabella 4 - Referenti Cliente

Delegato dal cliente all'atto dell'attivazione del servizio fa fede su Soggetto Produttore	
Responsabile del versamento	Indicato nella scheda di richiesta di attivazione del servizio è responsabile dei dati e dei metadati rispetto all'estrazione dall'eventuale sistema documentale in uso presso il cliente ed al loro consolidamento e successivo versamento al sistema di conservazione. Il responsabile del versamento è tenuto a mantenere copia dei dati versati fino a corretta verifica del rapporto di versamento generato dal sistema di conservazione e resta a disposizione per eventuali comunicazioni relative a disservizi, anomalie nei dati versati, superamento delle soglie di versamento previste, ecc..

Tabella 5 - Referenti SP

Altre figure coinvolte nel processo di conservazione in capo al Conservatore	
Direttore di Divisione	Supervisione ed approvazione delle procedure in atto e della documentazione rilasciata
Incaricato Commerciale	• Primo contatto con il Produttore e supporto alle attività propedeutiche alla richiesta di attivazione. • Esegue il monitoraggio dei livelli di soddisfazione dei clienti e riferimento del produttore per gli eventuali dubbi su possibili disservizi
Responsabile Ufficio Tecnico	• monitora, gestisce e coordina le attività di registrazione, verifica e validazione relative alle procedure di attivazione e disattivazione dei clienti • riceve le richieste di attivazione ed avvia l'iter di fatturazione • monitora gli indicatori di riferimento per le soglie di utilizzo del servizio da parte della clientela avviando e gestendo le eventuali richieste di rinnovo/estensione dei contratti in scadenza o prossimi alle soglie di utilizzo configurate

Tabella 6 - Ruoli a supporto del processo di conservazione

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.218.200 i.v.
Interamente versato

I riferimenti del Responsabile della conservazione sono indicati anche nell'allegato 1 nel quale sono anche riportate le attività affidate al Conservatore, al Produttore e al Responsabile del servizio di conservazione.

Nell'allegato *N*, depositato all'atto della richiesta di accreditamento, sono riportati l'organigramma dettagliato, le referenze e il riepilogo dei curriculum vitae dei vari responsabili delegati dal Conservatore.

Si allegano anche gli atti di nomina interni, ed i contratti di collaborazione citati nell'allegato stesso.

Nelle procedure di gestione documentale in uso presso il conservatore si terrà conto di ogni variazione riportata al presente manuale come a tutti gli allegati presentati all'atto dell'accreditamento con conseguente versioning e registrazione di ogni variazione, nel caso specifico, in riguardo alle nomine, alle deleghe o/o alle mansioni ad esse correlate.

Torna al sommario

5 STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Le attività relative alle varie procedure e pratiche in uso presso il soggetto conservatore sono applicate, in riferimento al servizio in oggetto, secondo il seguente organigramma, nel rispetto delle deleghe e delle nomine già citate e alle disposizioni tecniche e normative di AgID.

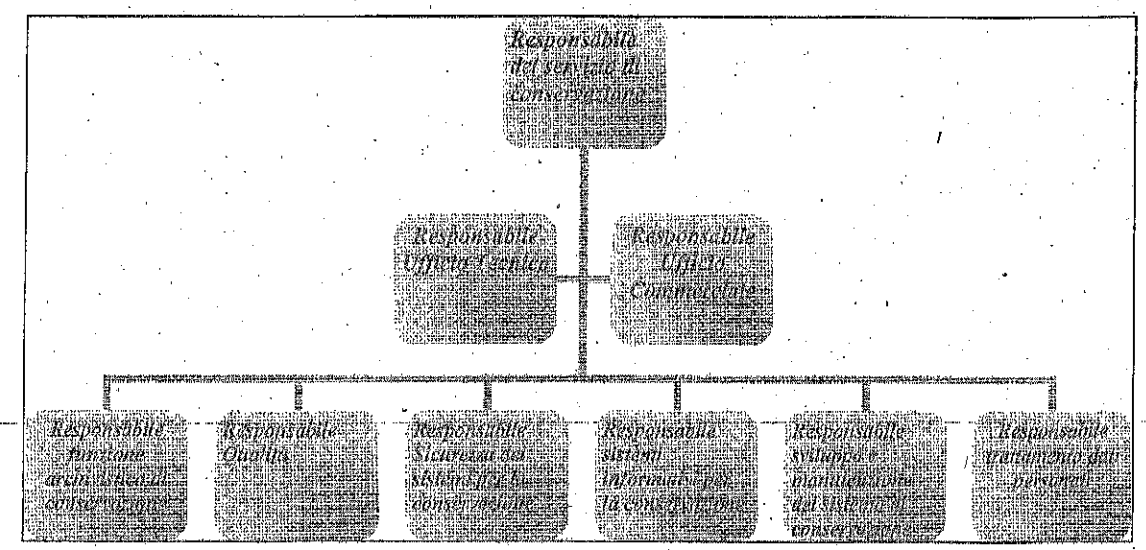


Figura 2 - Organigramma di servizio

Ognuno dei responsabili, indicati nell'organigramma del servizio e dettagliati nell'allegato *N* alla domanda di accreditamento, appartiene ad una delle aree riportate nello schema seguente, in cui sono indicate anche le strutture che a vario titolo collaborano attivamente alla definizione, alla gestione ed all'erogazione del servizio.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini - R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400406

Capitale sociale:
Euro 2.216.200
interamente versato

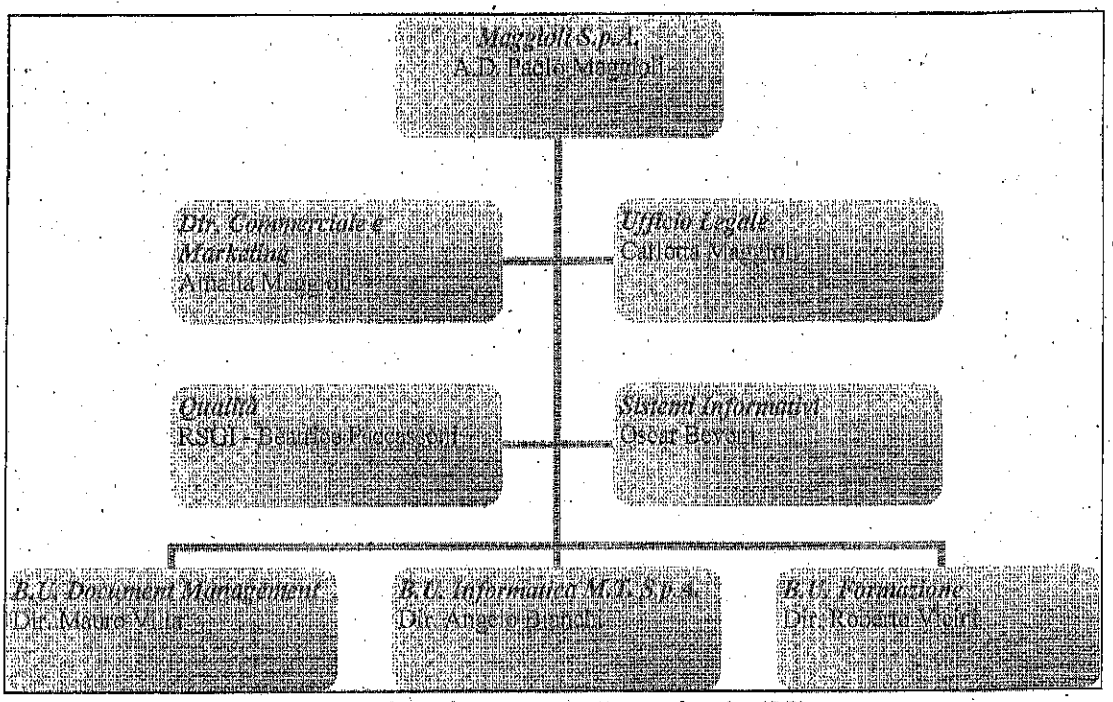


Figura 3 - Organigramma strutture coinvolte (SC)

Torna al sommario

5.2 Strutture organizzative

Le strutture organizzative interne, che intervengono nelle principali funzioni che riguardano il servizio di conservazione, si possono raggruppare in 5 aree principali, quali:

1. Direzione
2. Area Tecnica
3. Area Commerciale
4. Area Operativa
5. Sistemi Informativi

Le seguenti tabelle riportano le 5 procedure principali della conservazione, così come identificate da AgID per la redazione del presente manuale.

1. Attività preliminari
2. Attivazione del servizio
3. Versamento
4. Elaborazione
5. Gestione dei sistemi informativi

Maggioli SpA
via del Carpino, 8
47922 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini e C.F. n. 219107
C.F. 06188330150
P.IVA 02066400405
Capitale sociale
Euro 2.216.200
interamente versato

Ogni procedura è stata scomposta in attività (operative e di controllo) a cui è assegnata la struttura competente ed il responsabile della singola attività.

Le combinazioni di attività operative e attività di controllo, insieme alla doppia assegnazione e (struttura competente e persona responsabile) garantiscono un monitoraggio continuo delle attività e degli standard di servizio da parte di almeno 2 soggetti per ogni attività.

5.2.1 Attività preliminari propedeutiche all'attivazione del servizio

Attività	Area competente	Responsabile
Analisi dei requisiti tecnico-normativi per la definizione del servizio	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione
Definizione dell'offerta e dei requisiti funzionali	Direzione	Responsabile del servizio di conservazione
Assessment del software di conservazione	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione
Redazione della pianificazione e della progettazione	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione
Predisposizione dell'infrastruttura hardware e software ed analisi dei costi di manutenzione	Sistemi Informativi	Responsabile sistemi informativi per la conservazione
Definizione delle procedure operative	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione
Verifica sezione audit e monitoraggio dei vincoli e dei requisiti tecnico-normativi nel tempo	Direzione	Responsabile Qualità
Verifica e autorizzazione delle implementazioni	Direzione	Responsabile Sicurezza dei sistemi per la conservazione
Validazione delle implementazioni proposte	Area Tecnica	Responsabile funzione archivistica di conservazione
Validazione delle attività e delle autorizzazioni ad alto impatto	Direzione	Responsabile del servizio di conservazione
Monitoraggio e gestione dell'operatività ordinaria	Area Operativa	Responsabile sviluppo e manutenzione del sistema di conservazione
Capacity planning e monitoraggio dei sistemi applicativi	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione

Tabella 7 – Attività 1

5.2.2 Attivazione del servizio

Attività	Area Competente	Responsabile
Supporto pre-sales al cliente per la definizione delle tipologie documentarie, delle modalità di utilizzo del servizio e delle possibili integrazioni	Area Commerciale	Dir. Commerciale e Marketing
Raccolta dei requisiti e della documentazione necessaria all'attivazione del servizio	Area Commerciale	Dir. Commerciale e Marketing
Riconoscimento e nomina dei delegati per l'erogazione del servizio e l'accesso ai dati conservati	Cliente	Responsabile della Conservazione
Verifica ed inoltro della richiesta di attivazione all'area tecnica e monitoraggio delle attività di provisioning	Area Commerciale	Dir. Commerciale e Marketing
Verifica delle richieste di attivazione in merito all'assolvimento degli obblighi contrattuali preliminari	Area Tecnica	Dir. Document Management
Inoltro della pratica di attivazione e della pratica di fatturazione agli uffici competenti	Area Tecnica	Dir. Document Management
Provisioning delle attivazioni: - Censimento Clienti e Referenti - Setup dell'ambiente di conservazione secondo le richieste dei clienti - Configurazione ed invio delle credenziali di accesso	Area Operativa	Responsabile sviluppo e manutenzione del sistema di conservazione
Interfacciamento con i clienti per la messa in esercizio delle eventuali integrazioni applicative	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione

Tabella 8 – Attività 2

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

5.2.3 Versamento

Attività	Area competente	Responsabile
Generazione automatica dei pacchetti di versamento secondo le specifiche concordate	Soggetto Produttore	Responsabile del Versamento
Acquisizione dei pacchetti di versamento a cadenza concordata e programmata	Sistema di Conservazione	Responsabile sviluppo e manutenzione del sistema di conservazione
Generazione del rapporto di versamento	Sistema di Conservazione	Responsabile del servizio di conservazione
Segnalazione al Responsabile del versamento di anomalie e/o eventuali errori e/o rifiuti	Area Tecnica	Responsabile Sicurezza dei sistemi per la conservazione

Tabella 9 – Attività 3

5.2.4 Elaborazione

Attività	Area Competente	Responsabile
Generazione dei pacchetti di archiviazione secondo le modalità di conservazione definite, previamente armonizzate con il cliente	Sistema di Conservazione	Responsabile sviluppo e manutenzione del sistema di conservazione
Gestione dei pacchetti di archiviazione secondo le specifiche del servizio	Area Operativa	Responsabile del servizio di conservazione
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	Sistema di Conservazione	Responsabile del servizio di conservazione
Scarto dei pacchetti di archiviazione	Area Tecnica	Responsabile del servizio di conservazione

Tabella 10 – Attività 4

5.2.5 Gestione dei sistemi informativi

Attività	Area competente	Responsabile
Conduzione e manutenzione del sistema di conservazione	Sistemi Informativi	Responsabile sistemi informativi per la conservazione
Monitoraggio del sistema di conservazione	Area Tecnica	Responsabile sviluppo e manutenzione del sistema di conservazione
Change management	Area Operativa	Responsabile del servizio di conservazione
Verifica periodica di conformità a normativa e standard di riferimento	Direzione	Responsabile Sicurezza dei sistemi per la conservazione

Tabella 11 – Attività 6

Torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.218.200
interamente versato

6 OGGETTI SOTTOPOSTI A CONSERVAZIONE

La descrizione delle tipologie degli oggetti e dei pacchetti in essi contenuti sottoposti a conservazione è riportata per i clienti nel documento "Modalità e Condizioni di fornitura del servizio" in cui sono riportate anche le "Specificità del contratto". Per l'accreditamento, le medesime informazioni sono state inserite in Allegato 1 al Manuale – "Registro dei dati e dei metadati gestiti", in riferimento alla tipologia degli oggetti che possono essere posti in conservazione e dei loro metadati, mentre le specifiche di generazione dei pacchetti di versamento e di distribuzione e degli indici generati dal sistema di conservazione sono dettagliati in Allegato 2 al Manuale – "Specifiche di interoperabilità ed integrazione applicativa del servizio".

Torna al sommario

6.1 Oggetti conservati

Il Sistema di conservazione gestisce Documenti Informatici con i metadati ad essi associati in base alla Descrizione Archivistica a cui appartengono.

Contratti	Ordinanze
Decreti	OU
Delibere (Generico)	PEC
Delibere di Consiglio	Protocollo (Altri Documenti)
Delibere di Giunta	Pratiche SUAP
Determinazioni	Pratiche SUE
Documenti Generici	Registri di Protocollo
Fascicoli Elettorali	Registri Contabili
Fatture Attive	Verbali di Consiglio
Fatture Passive	Verbali di Giunta
Mandati SdI	

Tabella 12 - Classi Documentali

Per ogni Descrizione Archivistica Gestita è possibile, negli allegati indicati verificare il periodo di retention impostato e il set di metadati definito. Il sistema gestisce gli oggetti sottoposti a conservazione distinti per ogni singolo soggetto produttore ed anche per singola struttura (generalmente corrispondenti alle Aree Organizzative Omogenee), consentendo di definire configurazioni e parametrazioni ad hoc per ogni Soggetto Produttore, in base agli accordi stipulati all'atto della sottoscrizione del servizio, fin'anche all'eventuale titolario o piano di classificazione in uso presso il cliente.

Riguardo ai formati degli oggetti sottoposti in conservazione, si rimanda alle raccomandazioni già riportate negli allegati citati. I formati ammessi, di cui segue un elenco schematico sono stati scelti in base alle loro caratteristiche di:

- **Diffusione** Intesa come l'estensione dell'impiego di uno specifico formato, affinché sia più probabile che esso venga supportato nel tempo
- **Sicurezza** Tenendo conto del grado di modificabilità del contenuto e della capacità di essere immune dall'inserimento di codice maligno
- **Apertura** Intesa come la disponibilità di specifiche pubbliche a chiunque abbia interesse ad utilizzare quel formato
- **Portabilità** Ossia, la facilità con cui i formati possano essere usati su piattaforme diverse
- **Funzionalità** Intesa come la possibilità da parte di un formato di essere gestito da prodotti informatici
- **Supporto allo sviluppo** Considerando le modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini + R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale:
Euro 2.216.200
interamente versato

A garanzia della fruibilità del dato conservato è necessario che ogni documento sia associato ad un proprio viewer definito a monte dell'attivazione e conservato a sua volta prima dell'inizio dei caricamenti. Il sistema di conservazione verifica il mime-type dei dati inviati in conservazione ed accetta solo i file per i quali il Produttore ha definito il software di visualizzazione.
Si riportano qui di seguito, in via meramente esemplificativa, alcune possibili configurazioni di default:

Estensione	Mime-Type	Publisher	Standard	Viewer	Produttore	Versione	S.O.
PDF	application/pdf application/x-pdf application/acrobat applications/vnd.pdf text/pdf text/x-pdf	Adobe Systems Inc.	ISO 32000	Adobe Acrobat Reader	Adobe Systems Software Ireland Ltd	11	Windows 8 Windows 7 Mac OS X
EML (PEO o PEC)	message/rfc822	CNR	RFC 6109	Mozilla Thunderbird	Mozilla Found.	31.6	Windows 8 Windows 7 MacOSX10 Ubuntu10 Ubuntu12
MP3 (video) MPEG MPG (video)	video/mpeg	Moving Picture Experts Group	ISO/IEC 14496	VLC Media Player	VideoLAN Org.	2.2.1	Windows7 Windows8 MacOSX10
AVI	video/avi video/msvideo video/x-msvideo	Microsoft	RFC 2361	VLC Media Player	VideoLAN Org.	2.2.1	Windows7 Windows8 MacOSX10
MP3 (audio)	audio/mpeg3	Moving Picture Experts Group	RFC 3003	VLC Media Player	VideoLAN Org.	2.2.1	Windows7 Windows8 MacOSX10
MPA MPG (audio)	audio/mpeg	Moving Picture Experts Group	RFC 3003	VLC Media Player	VideoLAN Org.	2.2.1	Windows7 Windows8 MacOSX10
JPG JPEG	image/jpeg	CCITT	RFC 2045 RFC 2046	Wega2 Stand Alone	Wega2/Exposureplot	11.0.5	Windows7 Windows8
TIF	image/tiff	Adobe Systems Inc.	RFC 3302	Wega2 Stand Alone	Wega2/Exposureplot	11.0.5	Windows7 Windows8
GIF	image/gif	CCITT	RFC 2045 RFC 2046	Wega2 Stand Alone	Wega2/Exposureplot	11.0.5	Windows7 Windows8

L'elenco completo di tutti i formati gestiti, i relativi mime-type, i viewer e le restanti informazioni di rappresentazione, peculiari di ogni formato, sono riportati nel dettaglio nell'allegato 1 "Modalità e Condizioni di fornitura del servizio".

Nei pacchetti di distribuzione saranno riportate le informazioni descrittive sintattiche e semantiche di ogni documento conservato e, al momento della generazione del DIP, sarà sempre incluso il visualizzatore corrispondente al mime-type di riferimento che il Soggetto Produttore avrà posto in conservazione prima di procedere al versamento dei documenti stessi

I formati già citati, firmati o firmati e marcati temporalmente, saranno anch'essi accettati e corredati del viewer necessario all'apertura del file firmato.

Eventuali altri formati, purché compatibili con le caratteristiche indicate nel manuale di conservazione, potranno essere gestiti, previa richiesta di fattibilità tecnica al conservatore e solo in relazione ad una nuova offerta commerciale in cui sia specificata la personalizzazione richiesta. In questo caso il cliente dovrà porre in conservazione una copia di backup del software, già disponibile o in uso presso il Soggetto Produttore stesso, necessario alla visualizzazione dei file al momento dell'esibizione, indicandone almeno il sistema operativo supportato, la versione e la lingua.

Torna al sommario

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405
Capitale sociale
Euro 2.216.200
interamente versato

6.2 Pacchetto di versamento

Le informazioni tecniche necessarie all'alimentazione dei moduli che andranno a costruire il pacchetto di versamento, come pure le possibili personalizzazioni, sono riportate nel documento "Specifiche di interoperabilità ed integrazione applicativa del servizio, mentre nell'allegato 1 sono riportati i metadati gestiti e, più in generale le descrizioni archivistiche che possono essere attivate, rispetto a quanto già riportato riguardo alle classi documentali.

Rispetto alla pluralità di situazioni documentarie possibili, il sistema si comporterà applicando le regole d'ingresso che definite nelle condizioni generali di fornitura che, esattamente come avviene in un archivio di deposito tradizionale, stabiliscono:

- le caratteristiche minime che la documentazione deve possedere per poter essere accettata in ingresso;
- i tempi di versamento della documentazione dotata di tali caratteristiche;
- le modalità di versamento;
- i metadati di ciascun documento.

In particolare, per quanto riguarda il primo punto, il sistema può gestire due ordini di caratteristiche:

- caratteristiche tecnologiche, riferite ai singoli oggetti digitali;
- caratteristiche archivistiche, ossia la presenza di alcuni metadati di contesto.

Le caratteristiche archivistiche possono riguardare, ad esempio, l'appartenenza di ciascun documento, ad un fascicolo, o la possibilità di ricondurre un fascicolo all'attività di un determinato ufficio.

Le caratteristiche tecnologiche possono riguardare il formato dei documenti versati, la validità della firma, e/o della marca temporale, la completezza e la correttezza formale dei metadati versati ovvero, in definitiva, la sussistenza dei requisiti di base per la conservazione.

Una volta che la documentazione avrà superato i controlli di qualità previsti, il sistema procederà alla costruzione dei pacchetti di archiviazione a partire dai SIP inviati dal soggetto produttore.

È importante ricordare che il sistema di conservazione definisce ed arricchisce le informazioni di ogni dato versato durante ogni fase del ciclo di conservazione; dal momento della connessione al sistema per la prima fase di upload, dove viene identificata la proprietà e la provenienza del dato digitale; ai metadati di contesto, utili a conservare le informazioni secondo il titolario a cui appartengono; fino alle registrazioni delle verifiche periodiche, come delle visualizzazioni o delle esibizione.

A garanzia della tenuta dell'impianto documentale e delle informazioni in esso contenute si è quindi definito un insieme di metadati comune a tutte le descrizioni archivistiche gestite dal sistema di conservazione:

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini n. REA n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

1. Anno *	10. Oggetto/Descrizione *
2. Titolario/Classificazione *	11. UOR/UU (Responsabile) *
3. TIPO_DOC/Sottoclasse*	12. Rif_Allegati
4. Fascicolo	13. RIF_DocPrecedenti
5. Numero_Protocollo	14. Rif_DocSussegnenti
6. DOC_ID *	15. Rif_Mittente
7. DATA_DOC*	16. Rif_Destinatario
8. Versione *	17. Data_Invio
9. Impronta	18. Data_Ricezione

Tabella 13 - Metadati trasversali

Questi metadati sono quindi utili, come metodo di ricerca trasversale all'intero archivio di deposito del cliente, per recuperare interi fascicoli o serie documentali, anche quando queste vengono distribuite in più classi, sottoclassi o anche in descrizioni archivistiche diverse, purché afferenti allo stesso titolario, AOO o Soggetto Produttore.

Ogni Descrizione Archivistica prevede poi la possibilità di arricchire il dato conservato con altre informazioni utili a ricercarlo in futuro ed a contestualizzarlo con maggior dovizia di particolari. Come già detto, si forniranno al cliente tutte la informazioni necessarie, rispetto alle DA già definite, ma il Conservatore si rende disponibile fin d'ora a rivedere i metadati associati alle nuove classi che si andranno a gestire, secondo le richieste che potranno pervenire dai potenziali clienti.

Torna al sommario

6.3 Pacchetto di archiviazione

Il sistema gestisce gli oggetti sottoposti a conservazione distinti per ogni singolo soggetto produttore anche per singola struttura (generalmente corrispondenti alle aree organizzative omogenee), consentendo di definire configurazioni e parametri ad hoc per ogni soggetto produttore, in base agli accordi stipulati all'atto della sottoscrizione del contratto di affidamento del servizio di conservazione.

Per mantenere anche nel sistema le informazioni relative alla struttura dell'archivio e dei relativi vincoli archivistici, le unità documentarie possono essere versate corredate di un set di metadati di profilo archivistico che include gli elementi identificativi e descrittivi del fascicolo, con riferimento alla voce di classificazione e l'eventuale articolazione in sotto fascicoli. Inoltre è gestita la presenza di classificazioni, fascicoli e sotto fascicoli secondari e collegamenti tra le diverse unità archivistiche e documentarie presenti nel sistema.

Le serie ed i fascicoli possono essere versati nel sistema quando sono completi e dichiarati chiusi, descritte da un set di metadati che include obbligatoriamente, oltre alle informazioni di identificazione, classificazione e descrizione, anche il tempo di conservazione previsto. Nel caso delle serie la chiusura può avvenire a cadenza annuale o comunque secondo una definizione temporale definita dal soggetto produttore.

I documenti informatici (unità documentarie), e i fascicoli informatici, possono essere suddivisi secondo un piano di classificazione, che identifica gruppi documentali omogenei per natura e/o funzione giuridica (titolo, classe, sottoclasse), modalità di registrazione o di produzione.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.800
interamente versato

6.3.1 Struttura del pacchetto di archiviazione

Si riporta la rappresentazione grafica della struttura dell'indice del pacchetto di archiviazione

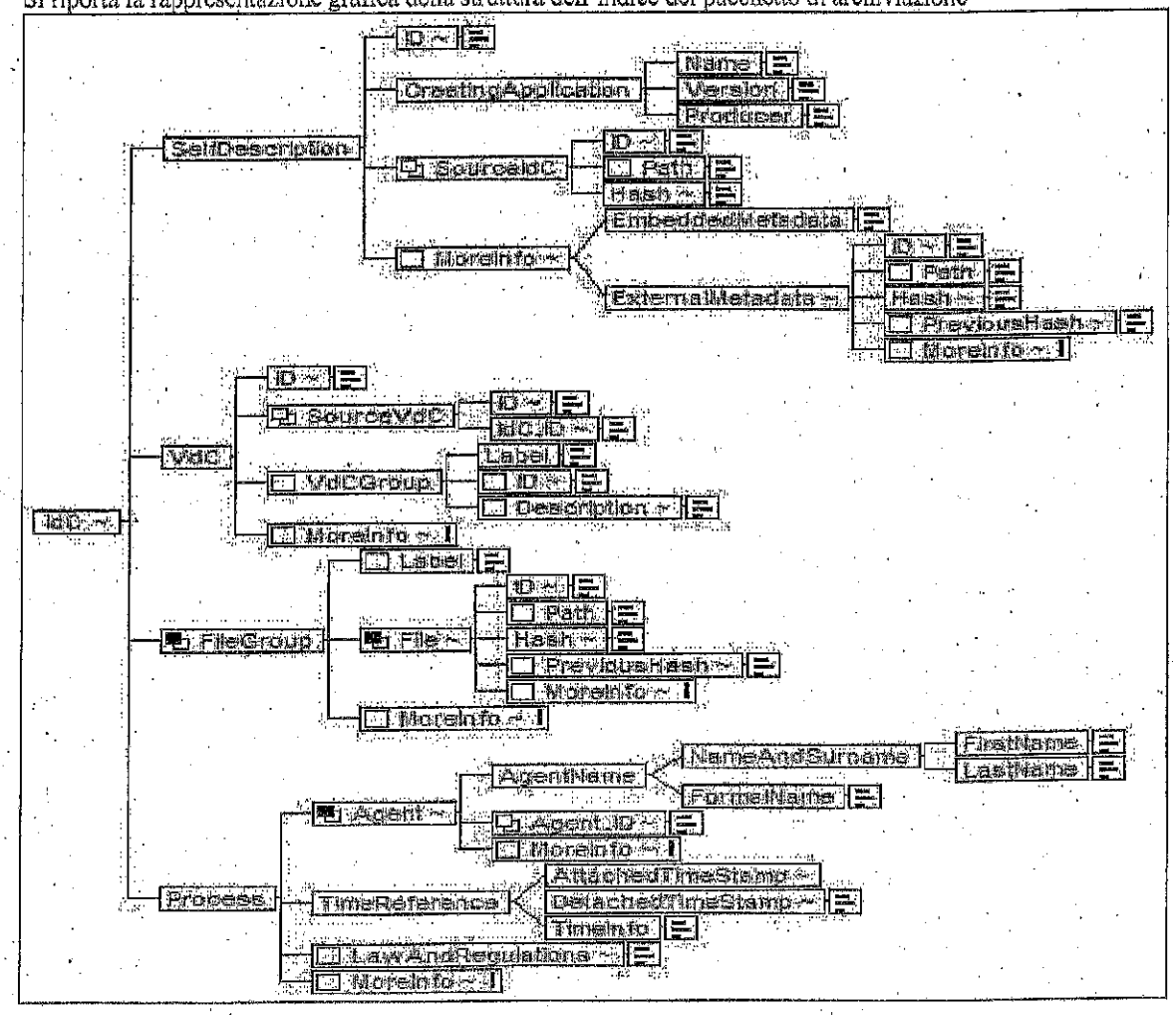


Figura 4 - Indice UNISInCRO

Per il dettaglio di ogni singola voce si rimanda alle specifiche tecniche pubblicate sul sito http://www.gazzettaufficiale.it/ del 12-1-2015 Serie generale - n. 8 "SPECIFICHE TECNICHE DEL PACCHETTO DI ARCHIVIAZIONE", mentre per quanto riguarda le "MoreInfo" (metadati, viewer, ecc…) si rimanda all'allegato 2 di cui alle specifiche di interoperabilità tra i conservatori accreditati ed al riferimento, più avanti nel presente manuale, al file metadata.xml che le ospita.

Lo standard OAIS prevede che, ad ogni oggetto portato in conservazione, vengano associate un insieme di informazioni (metadati) che ne permetta in futuro una facile reperibilità e le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

Classifichiamo quindi le informazioni sulla rappresentazione in:

- **Strumenti per la leggibilità:** tipicamente legati al formato dell'oggetto conservato (viewer);
- **Informazioni sulla rappresentazione sintattica:** tipicamente legate al formato dell'oggetto conservato (per esempio il documento di specifiche tecniche del formato del file);
- **Informazioni sulla rappresentazione semantica:** tipicamente legate alla descrizione archivistica dell'oggetto conservato (per esempio come leggere il contenuto di una fattura).

Nell'insieme dei metadati, definito per ogni descrizione archivistica attivata in accordo con il soggetto produttore, troviamo le informazioni sulla rappresentazione (IR), classificabili in sintattiche (IRsi) e semantiche (IRse), il cui obiettivo è fornire tutte le informazioni necessarie per poter leggere ed interpretare la sequenza di bit dell'oggetto conservato.

Concretamente, all'interno di un medesimo pacchetto informativo, si troveranno le seguenti componenti, codificate in un XML:

- l'oggetto digitale possibilmente in un formato standard non proprietario;
- l'impronta del documento generata con funzione di hash;
- il riferimento temporale (rappresentato dalla marca temporale o altro riferimento temporale opponibile a terzi, come la segnatura di protocollo);
- il set di metadati per la conservazione:
  - metadati identificativi (per esempio possono essere utilizzati i metadati dello standard ISAD);
  - metadati descrittivi (per esempio possono essere utilizzati i metadati dello standard ISAD);
  - metadati gestionali (UNI SInCRO);
  - metadati tecnologici (per esempio possono essere utilizzati i metadati dello standard METS);
- il viewer necessario per la visualizzazione del documento stesso, o in alternativa, si inserisce il puntatore/riferimento al viewer comune a più pacchetti informativi per quel formato di file del documento;
- la documentazione tecnica necessaria alla comprensione del viewer stesso (anch'esso può essere un puntatore/riferimento che rimanda alla componente digitale descritta per più pacchetti informativi) oppure la documentazione per la comprensione del documento digitale e/o della classe documentale di riferimento.

Tutte le informazioni esterne o non previste dall'indice di conservazione UNISinCRO (External metadata Info) sono quindi riportate per esteso nel file metadata.xml, anch'esso incluso in ogni AIP o DIP in cui troveremo i link ai viewer necessari ad interpretare i dati conservati ed i metadati già riportati nel verbale di versamento.

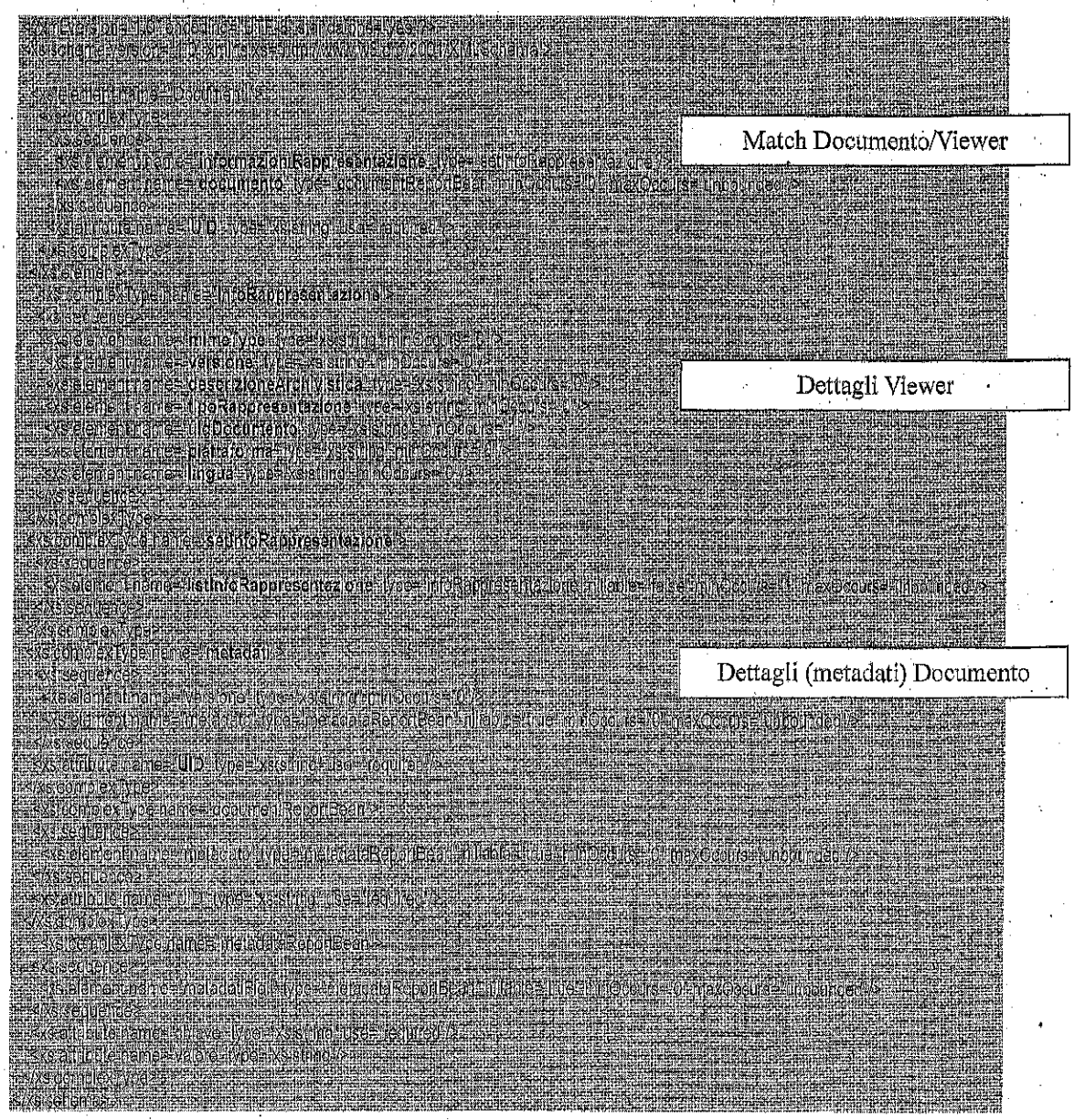
Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale
Euro 2.216.200
interamente versato

La struttura di riferimento del file dei metadati è descritta nel suo XSD di riferimento, fornito come sempre unitamente ad ogni XML prodotto dal sistema di conservazione:



Torna al sommario

6.4 Pacchetto di distribuzione

Nel modello OAIS, adottato dal sistema di conservazione, il pacchetto di distribuzione (DIP) è strutturato nel modello dati come il pacchetto di archiviazione. La differenza sta nella sua destinazione in quanto esso viene concepito per essere fruito ed utilizzato dall'utente finale (esibizione). I DIP sono il frutto di più AIP che vengono "spacchettati" e re-impacchettati per un più fruibile utilizzo da parte dell'utente.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

In risposta alla richiesta iniziale di esibizione, da parte dell'utente, il sistema risponderà restituendo un DIP che nel caso più completo conterrà:

- I documenti richiesti nel formato previsto per la loro visualizzazione.
- Un'estrazione dei metadati associati ai documenti.
- L'indice di conservazione firmato e marcato.
- I viewer necessari alla visualizzazione dei documenti del pacchetto.

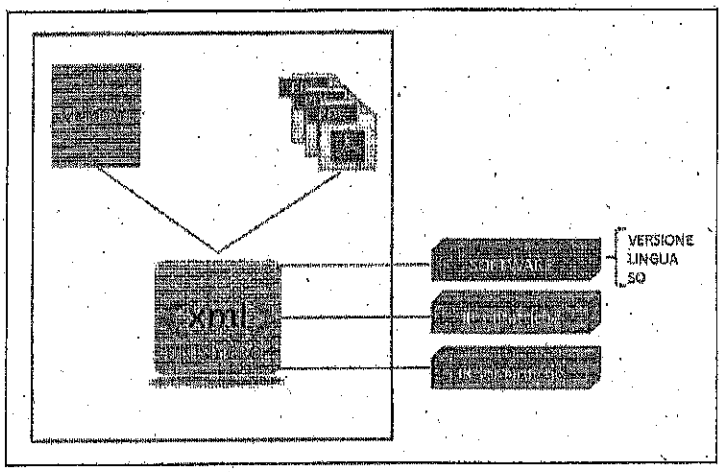


Tabella 14 - Struttura DIP

Inoltre, nei pacchetti di distribuzione, è possibile inserire tutta la catena di documentazione necessaria a rispondere alle esigenze dello standard OAIS.

Torna al sommario

7 IL PROCESSO DI CONSERVAZIONE

Al capitolo 5.2 del presente manuale sono riportati gli schemi delle attività principali previste per la conservazione ed i responsabili identificati all'interno della struttura organizzativa che ha in carico la singola attività.

Nel piano della sicurezza si farà riferimento alle procedure interne previste anche in merito agli standard di qualità e di sicurezza adottati nel trattamento dei dati, delle informazioni e dei documenti da parte del conservatore, già riportati nelle condizioni di fornitura del servizio stesso.

Torna al sommario

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

Ogni soggetto produttore può scegliere una modalità di utilizzo del servizio tra quelle proposte dal conservatore e riepilogate nella seguente tabella:

Modalità di utilizzo	Descrizione	Periodicità di versamento
Manuale	*Utilizzo del servizio tramite la web user interface (Web-App)*	**Chiusura quindicinale** delle conservazioni

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini + R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.218.800
interamente versato

Gestionali Maggioli	*Integrazione completa nei gestionali Maggioli* *+ Web-App per la sola esibizione online e l'eventuale versamento di documenti aggiuntivi*	**Chiusura settimanale** delle conservazioni
Integrazione altro gestionale	*Disponibilità della Web-App per le operazioni di esibizione e versamento* *+ Utenza Applicativa da destinare ai versamenti via Web-Services (SOAP) o per l'upload dei pacchetti di versamento via SFTP* *+ Manuali e specifiche di integrazione in base al canale di versamento predefinito.* *Il canale "SOAP-WS" è utilizzabile anche per ricercare e scaricare dati ed informazioni dal sistema di conservazione.*	**Chiusura settimanale** delle conservazioni

Tabella 15 - Modalità di utilizzo/Versamento

Le funzionalità di versamento ed esibizione sono sempre disponibili anche in modalità manuale, accedendo al servizio di conservazione tramite un'apposita web-app con l'utenza personale dell'utente delegato dal cliente. L'utilizzo delle funzionalità web "end-user" è descritto nell'apposito manuale utente, mentre le istruzioni per l'integrazione delle funzionalità applicative sono riportate nell'allegato 2 al presente manuale.

Tutte le comunicazioni, inteso come il trasferimento dei dati da e per il sistema di conservazione avviene tramite canale criptato (HTTPS o SFTP), sia nel caso di utilizzo manuale del servizio, sia per tutte le integrazioni applicative previste. Ad ogni buon conto, nella definizione del SIP, è richiesto al Produttore il rispetto dei seguenti massimali:

- Massimo 4 GB per ogni SIP, allegati ed indici inclusi;
- Massimo 20 mila documenti per lotto (50 mila, allegati inclusi)
- Massimo 5 MB per ogni file versato.

Inoltre, così come definito dall'art 22 del Decreto Legislativo 196/2003, i dati sensibili e giudiziari vengono trattati con tecniche di cifratura dipendenti dal sistema di database utilizzato, e sono resi illeggibili anche a chi è autorizzato ad accedervi.

Tipo Dato	Cifratura	Tracciabilità
Dato Generico	Opzionale	opzionale
Dato Personale	Opzionale	obbligatoria
Dato Sensibile	Obbligatoria	obbligatoria
Dato Giudiziario	Obbligatoria	obbligatoria

Tabella 16 - Cifratura dei metadati

Nel sistema di conservazione la definizione di un metadato di tipo generico o personale fornisce la possibilità di essere comunque gestito con tecniche di cifratura se impostate nella configurazione della descrizione archivistica e fornisce anche la possibilità di tracciare l'utente che ha visualizzato il dato personale e i documenti ad esso associato. L'identificazione dell'interessato da parte di un utente autorizzato, viene tracciato in appositi log dal sistema di conservazione.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiollispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

A prescindere dalla modalità di utilizzo del servizio, selezionata al momento dell'attivazione, il processo di conservazione seguirà il preservation planning, così come definito dallo standard OAIS.

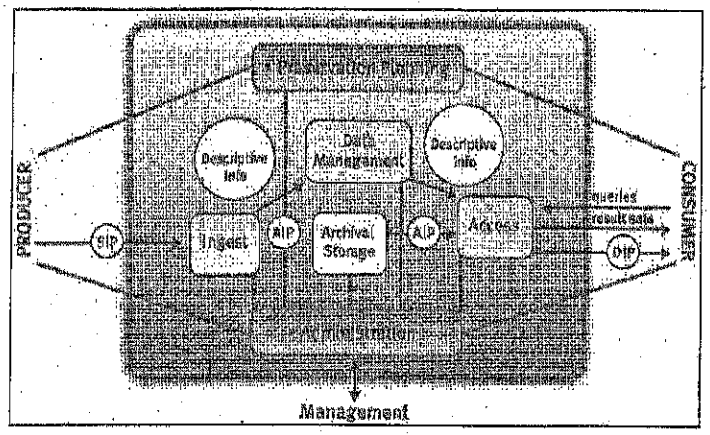


Figura 5 - Perimetro di applicazione

Il sistema di versamento mette a disposizione del soggetto produttore una serie di funzionalità di validazione che gli consentono, se necessario, di correggere la composizione dei pacchetti di versamento prima della sua acquisizione da parte del conservatore. Il produttore potrà correggere i metadati descrittivi e le relazioni con il contesto archivistico laddove queste non fossero state correttamente impostate in fase di prima produzione dei singoli SIP.

Il work flow degli stati di validazione/elaborazione di un SIP è il seguente:

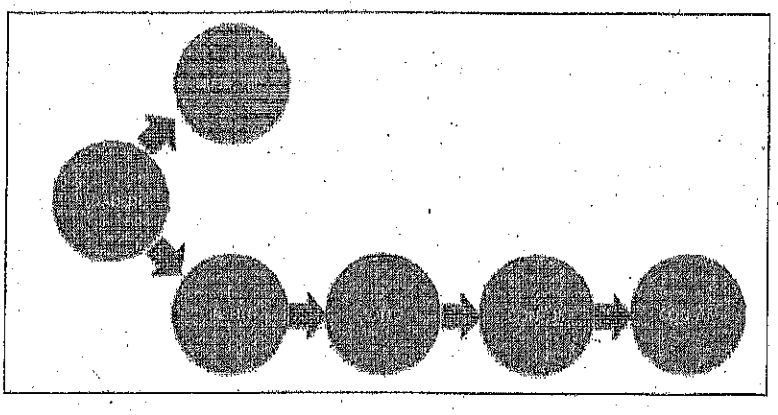


Figura 6 - Flow di elaborazione

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

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

Il Produttore è incaricato dal Cliente di fornire al Conservatore i Pacchetti di versamento, così come indicato nelle condizioni di fornitura. Il sistema di conservazione, verificherà il rispetto degli stessi requisiti analizzando i pacchetti di versamento sottomessi e ne potrà validare o rigettare il contenuto, ad esempio se i metadati sono formalmente errati o se il file inviato non è in un formato (mime-type) tra quelli abilitati per la specifica Descrizione Archivistica.

La prima verifica avviene contestualmente al tentativo di accesso dell'utente o dell'applicazione che intende tentare il caricamento di un pacchetto in conservazione e tende a garantire non solo che l'accesso avvenga in modalità sicura e da un soggetto riconosciuto ma, contestualmente al riconoscimento, definisce anche la proprietà del dato versato che potrà quindi attestarsi in conservazione sono in una posizione gerarchicamente inferiore rispetto all'alberatura di classi e privilegi definita per l'operatore (es.: Soggetto Conservatore → Soggetto Produttore Padre → Soggetto Produttore Figlio → AOO → Descrizione Archivistica). In caso di esito negativo si ottiene un errore di log-in tracciato nei log di sistema.

Il secondo step intende verificare che il dato versato sia compatibile con quanto definito per la Descrizione Archivistica (DA) a cui è stato destinato. Vengono verificati in questo passaggio i metadati, i mime-type, l'univocità dei dati, e quant'altro definito in fase di attivazione del servizio tra il Produttore ed il Conservatore. In caso di esito negativo si ottiene un errore di validazione e la distruzione del pacchetto per il quale si è tentato l'invio. L'evento, a prescindere dal suo esito, è tracciato nel log specifico del Soggetto Produttore che è portato in conservazione a cadenza periodica.

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

All'atto del versamento sono eseguiti i seguenti controlli:

- il soggetto produttore non è bloccato (su segnalazione del Cliente o come procedura di sicurezza);
- non siano stati raggiunti i limiti di contratto (plafond acquistato, durata del contratto, versamenti annui, ecc...);
- sia definito almeno un certificato di firma (implica la delega al Responsabile del Servizio di Conservazione);
- sia definito un responsabile della conservazione per il soggetto produttore;
- sia definito un account di marca temporale per la descrizione archivistica;
- siano definite delle informazioni di rappresentazione valide (formato dei dati versati)
- siano riportati correttamente i metadati obbligatori e gli eventuali facoltativi inviati.

Superati i controlli, secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettere d) ed e), il sistema di conservazione genera un rapporto di versamento, firmato dal Responsabile del Servizio di Conservazione, che attesta la presa in carico del SIP e riporta, nel formato pubblicato nelle specifiche tecniche, l'elenco dei file versati, i metadati comunicati all'atto del versamento, l'identificativo (UID) del documento all'interno del sistema di conservazione, le impronte HASH (sha256/HEX) dei file versati già verificate con il metadato HASH fornito all'atto del versamento e la data e l'ora della presa in carico del

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

SIP da parte del sistema di conservazione.

Il caricamento di file corrotti o non conformi a quanto definito per la DA, la presenza di duplicati non precedentemente dichiarati, i tentativi di caricamenti successivi a blocchi imposti per superamento delle soglie di contratto, implicano il rifiuto dei pacchetti di versamento.

I log delle attività e dei processi, così come tutti i rapporti di versamento, restano in disponibilità del cliente, all'interno del sistema di conservazione per tutta la durata del contratto e sono visionabili e scaricabili al pari di ogni dato conservato.

Le notifiche delle anomalie di validazione sono inviate al sistema produttore come (ERR-V), mentre, in caso di conservazioni manuali l'utente ha pronta evidenza del motivo del rifiuto. Oltre a queste segnalazioni, gli operatori e gli amministratori del sistema di conservazione, ricevono specifiche notifiche sulle cause del problema riscontrato ed il dettaglio del processo in errore. È in carico al Conservatore assicurarsi di informare il produttore del problema rilevato e supportarlo adeguatamente nelle procedure di rientro che potranno essere concordate.

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

Eventuali errori di validazione dei DIP, evidenziati da un riscontro positivo ai check di cui sopra, genera una segnalazione al conservatore che, eseguita una serie di controlli preliminari, potrà indicare al referente tecnico del cliente e/o al Produttore la procedura di rientro corretta.

Tale procedura potrà consistere in un nuovo versamento, dopo aver risolto l'anomalia in capo al Produttore o ad una variazione/integrazione del servizio acquistato, ad esempio aggiungendo una DA o ulteriore plafond alla disponibilità del Cliente.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Di seguito si riporta l'elenco delle funzioni e delle procedure di preparazione e di gestione del pacchetto di archiviazione :

- Per ogni SIP vengono creati dei sottoprocessi per migliorare le performance di conservazione
- Caricamento nel database dei metadati del pacchetto di versamento
- Creazione del pacchetto di archiviazione
- Creazione del file di metadati per il pacchetto di archiviazione
- Creazione dell'indice di conservazione secondo lo standard UNI SINCRO
- Firma digitale dell'indice di conservazione
- Marcatura Temporale dell'indice firmato
- Memorizzazione nel database tutte le informazioni inerenti al pacchetto di archiviazione
- Copia il pacchetti di archiviazione nel repository di destinazione
- Verifica che la copia sia andata a buon fine (controllo di hash)
- Collegamento del pacchetto di archiviazione alle Informazioni sulla rappresentazione
- Cancellazione dei dati di input e delle tabelle e delle cartelle temporanee
- Crittografia dei metadati con tipo di privacy impostato a giudiziario o sanitario

Periodicamente, con Job separati da quelli di generazione dei pacchetti di archiviazione, questi vengono sottoposti a verifiche periodiche, almeno ogni 5 anni. Tale procedura automatica entra nel merito dei pacchetti conservati e verifica l'hash del dato conservato con l'informazione memorizzata all'atto del versamento. Eventuali file mancanti, corrotti o alterati, genereranno un'eccezione nella verifica degli hash

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405
Capitale sociale
Euro 2.215.200 i.v.

con conseguente registrazione dell'anomalia e l'invio della relativa notifica al gruppo di lavoro competente. La procedura di rientro prevede un'analisi delle cause che hanno portato a tale situazione, escludendo da principio eventuali anomalie nella verifica stessa, per poi passare al controllo puntuale dei file segnalati. I file effettivamente compromessi saranno ripristinati dal sistema di backup ed il pacchetto sarà poi sottoposto nuovamente al processo di verifica per convalidarne lo stato nel sistema di conservazione.

I log delle attività e dei processi restano in disponibilità del cliente, all'interno del sistema di conservazione, per tutta la durata del contratto e sono visionabili e scaricabili al pari di ogni dato conservato.

Torna al sommario

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

Il cliente delega le persone e gli utenti autorizzati ad accedere ai dati conservati, così come codificato nelle condizioni di fornitura del servizio.

Ogni utente potrà quindi procedere alla richiesta di generazione del DIP per conto del Cliente.

Le richieste vengono inoltrate accedendo all'interfaccia web del servizio e selezionando i file che si intende esibire. La richiesta viene sottoposta al sistema di conservazione che, viste le autorizzazioni riservate all'utente e le correlazioni, file, allegati, indici, viewer, genererà il pacchetto di distribuzione.

Terminata la generazione l'utente ne riceverà notifica e potrà procedere al download del DIP, sempre tramite l'interfaccia web del servizio (https).

In caso di errori l'utente troverà la richiesta in stato "pending", mentre il conservatore riceverà una notifica nell'evento anomalo. Il conservatore potrà sanare l'anomalia o annullare l'operazione errata contattando l'utente per fornire il giusto supporto.

I log delle attività eseguite sia dall'utente, sia dall'operatore, sono tracciati e registrati e restano in disponibilità del cliente, all'interno del sistema di conservazione, per tutta la durata del contratto e sono visionabili e scaricabili al pari di ogni dato conservato.

Si fa presente che nel caso in cui il cliente richieda l'utilizzo di supporti fisici rimovibili per la trasmissione dei pacchetti di distribuzione, il personale incaricato del trasporto dei supporti fisici viene scelto sulla base dei requisiti definiti dal responsabile del servizio di conservazione.

Inoltre:

- i supporti fisici non devono presentare riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti, della loro tipologia, ecc.;
- i dati trasmessi devono essere protetti con sistemi crittografici.

Nel caso in cui il cliente richieda la consegna dei pacchetti di distribuzione via email si dovrà valutarne la fattibilità tecnica e dovrà essere utilizzata la sola posta certificata per permettere di tracciare l'intera trasmissione. In questo caso dovranno essere conservate le ricevute di invio e consegna.

Torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini • R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

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

In merito alla produzione delle copie sarà cura del soggetto produttore produrre le copie conformi e richiedere, quando necessario, la presenza di un pubblico ufficiale. L'attestazione di conformità, anche nel caso si necessiti un cambio di formato, rimarrà a carico del soggetto produttore.

7.8 Scarto dei pacchetti di archiviazione

L'art. 9 comma 2, lett. K del DPCM 3 dicembre 2013 stabilisce che deve essere effettuato lo scarto dal sistema di conservazione, alla scadenza dei termini di conservazione previsti dalla norma, dandone informativa al soggetto produttore. Il sistema di gestione dati, grazie alla propria concezione, permette di gestire al meglio lo scarto del materiale documentario non destinato alla conservazione permanente, ma caratterizzato invece da tempi di conservazione limitati e diversificati. Negli archivi correnti gestiti secondo criteri aggiornati è presente, nel piano di classificazione e conservazione, un metadato, definibile per ciascuna tipologia documentaria o fascicolo (descrizione archivistica), che stabilisce i tempi di conservazione. Sarà dunque il sistema di gestione dati (SGD) ad incaricarsi di avvisare il responsabile del servizio di conservazione attraverso una o più notifiche impostabili, circa la scadenza dei tempi di conservazione dei documenti, e a supportarlo nell'effettuazione materiale dello scarto, a mantenere al proprio interno, ove richiesto, i metadati della documentazione fisicamente scartata.

Il sistema di conservazione produrrà quotidianamente un elenco dei pacchetti di archiviazione che hanno superato il tempo di conservazione, così come definito le massimario di selezione e scarto. Tale elenco di scarto, dopo una verifica da parte del Conservatore, viene comunicato al soggetto produttore che, utilizzando apposite funzionalità del sistema, può rifiutarlo (perché non intende procedere allo Scarto) o validarlo.
Nei casi previsti dalla legge, l'elenco di scarto così validato viene trasmesso dal soggetto produttore all'autorità di vigilanza che, in base alle norme vigenti, deve fornire il nulla-osta per lo scarto. Il soggetto produttore, una volta ricevuto il nulla-osta (che può essere concesso anche solo su una parte dell'elenco proposto), provvede ad adeguare, se necessario, l'elenco di scarto presente sul sistema alle decisioni dell'autorità. Una volta che l'elenco di scarto definitivo viene predisposto, il soggetto produttore lo valida e trasmette al Conservatore la richiesta di procedere allo scarto. Solo dopo aver ricevuto l'autorizzazione, il conservatore provvederà alla cancellazione dei pacchetti di archiviazione, contenuti nell'elenco di scarto.

Il sistema di conservazione, è quindi dotato di un processo di scarto che si occupa di controllare quotidianamente se esistono pacchetti di archiviazione che devono scartati. Alla presenza di uno o più pacchetti, il processo avvisa il responsabile del servizio di conservazione, che avrà a disposizione una interfaccia che gli permetterà di decidere se scartare o meno i documenti. In caso affermativo, il processo di selezione e scarto provvederà ad eliminare fisicamente i file presenti nel file system e a cancellare tutti i riferimenti nel database, mantenendo però l'indice di conservazione (in quanto contiene la lista dei file scartati) e aggiungendo automaticamente ai metadati del volume, una nota che indichi il fatto che il volume è stato sottoposto a processo di scarto, includendo data e ora di esecuzione.

Torna al sommario

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

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

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale:
Euro 2.215.800
interamente versato

Allo stesso modo il sistema di conservazione è in grado di importare e archiviare pacchetti di distribuzione generati da altri sistemi OAIS compliant.

L'esportazione dei volumi di conservazione (pacchetti di archiviazione) può essere effettuata su supporto elettronico in formato ZIP oppure in formato ISO. Tali file, saranno messi a disposizione del cliente su server SFTP oppure memorizzati su supporto fisico e consegnati da personale autorizzato. Per rispondere ai requisiti richiesti dalla norma ISO27001, in quest'ultimo caso, i file memorizzati su supporto fisico trasportabile saranno criptati.

Le strutture XML e XSD di riferimento sono riportate nell'allegato 2 al presente manuale, unitamente alla descrizione dei metodi di interoperabilità applicativa tra i sistemi, anche conservatori, che dovranno trattare i dati versati.

Torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.215.200
interamente versato

8 IL SISTEMA DI CONSERVAZIONE

I prossimi paragrafi descrivono l'architettura generale del sistema di conservazione dei documenti informatici e nel caso specifico, gli applicativi software utilizzati, le componenti del sistema installato presso il Conservatore.

Il dettaglio dei sistemi utilizzati è approfonditamente tracciato nel piano della sicurezza depositato all'atto dell'accreditamento.

Il sistema di conservazione tiene traccia del versioning del suo proprio software e la gestione dei tali aggiornamenti è in carico al Responsabile delegato allo sviluppo, manutenzione ed operation per la Conservazione a Norma.

L'aggiornamento dei sistemi, degli impianti e delle infrastrutture, così come la manutenzione e gli adeguamenti tecnico-normativi sono a carico della struttura "Sistemi Informativi" interna al Conservatore stesso, secondo le modalità previste.

Torna al sommario

8.1 Componenti Logiche

Schema e descrizione delle entità funzionali relative al sistema di conservazione:

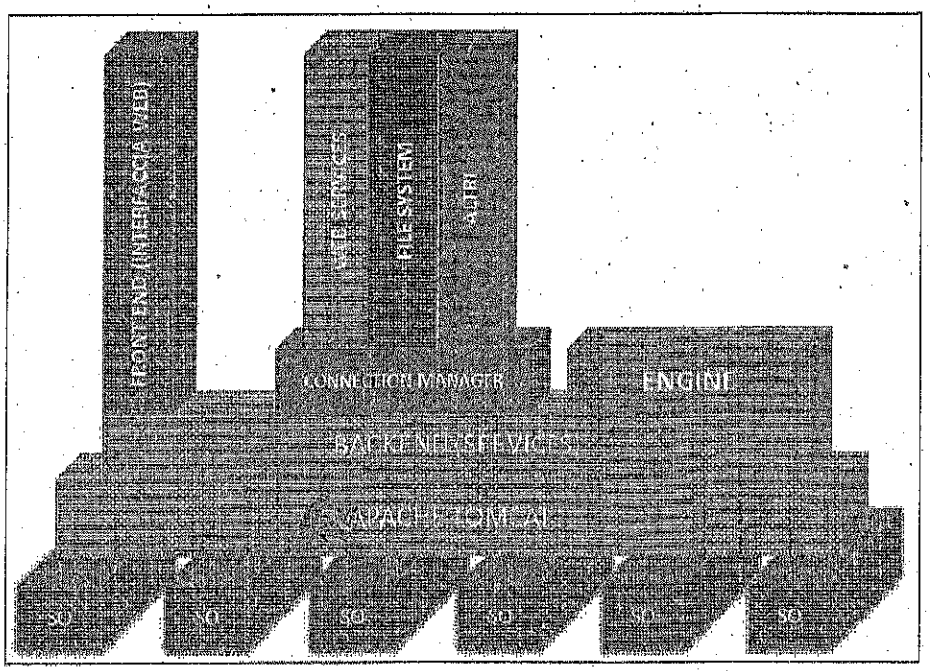


Figura 7 – Pila

Come si può notare il sistema di conservazione è modulare ed altamente scalabile, sia nelle componenti logiche, sia per le componenti fisiche, pure virtualizzate e parallelizzate come si vedrà in seguito, in modo da far fronte alle richieste di incremento di potenza di calcolo derivante dall'attivazione di più clienti o dal versamento di più dati.

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)
tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it
iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405
Capitale sociale:
Euro 2.216.200
interamente versato

Tali modifiche ed incrementi possono essere attivati in continuità operativa ed in modo totalmente trasparente per i sistemi esterni che accedono al servizio.

I moduli logici che concorrono a definire l'architettura logica del servizio sono di 7 tipi:

- Connettore SOAP-WS (erogato dal layer di front-end; è utilizzato per le integrazioni applicative)
- Web-App (eroga la web user interface; dal fron-tend per le attività di versamento, ricerca ed esibizione dei clienti, dal back-end per le attività di amministrazione del servizio.
- Back-end Application (Veicola le informazioni tra i vari moduli e il DB e dall'Engine agli Storage; si attesa nel layer di back-end)
- Engine (Esegue le conservazioni ed evade le richieste di generazione dei DIP e tutte le procedure che coinvolgono i dati conservati; si attesta al back-end)
- Storage (accoglie i dati per la conservazione a lungo termine; si attesta al 2° livello di back-end)
- NTFS .(utilizzato per il transito dei dati e le elaborazioni temporanee; è erogato da un'infrastruttura apposita all'interno del data center)
- Data Base dedicato (erogato da server specifici, virtualizzati e clusterizzati; si attesa al back-end)

8.2 Infrastruttura

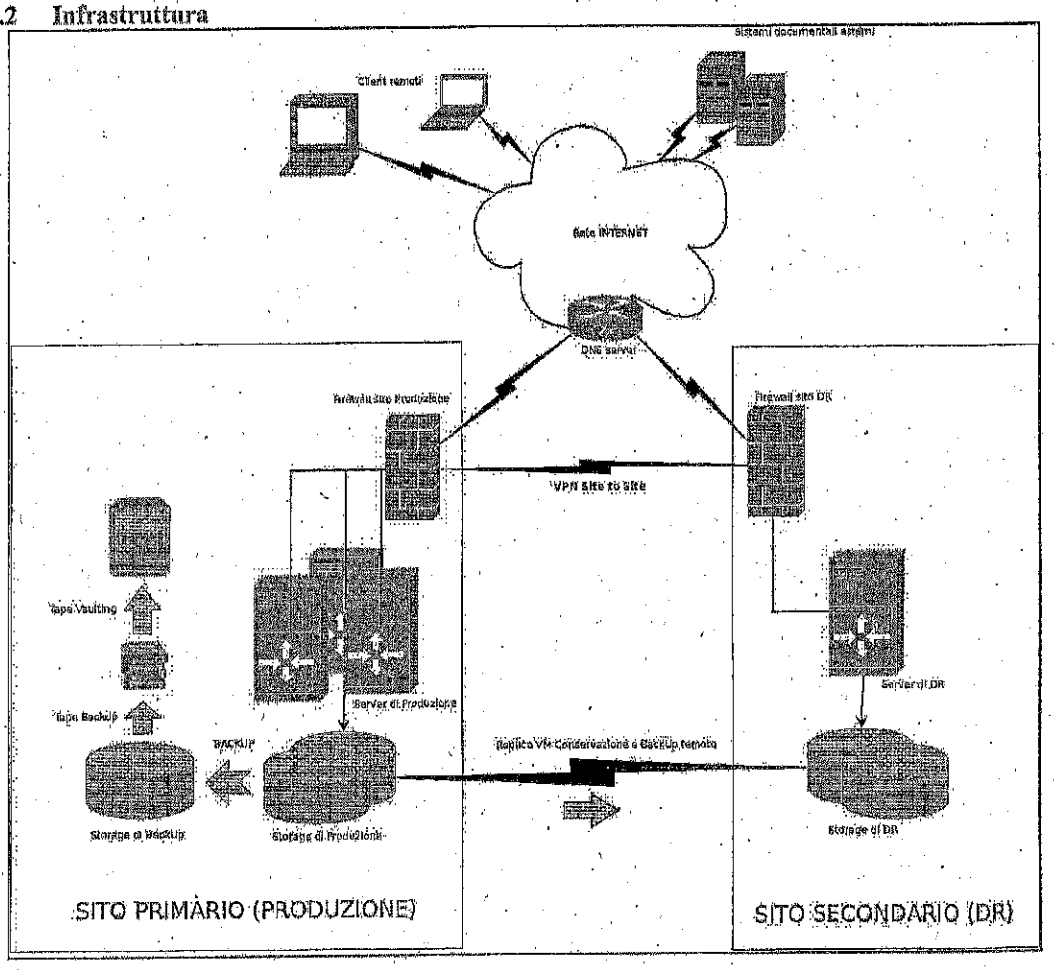


Figura 8 – Infrastruttura

Torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

Le comunicazioni tra i vari moduli avvengono sempre in modalità protetta ed attraverso appositi firewall, diversi per ogni layer di attestazione del nodo di erogazione. Le comunicazioni tra front-end e back-end avvengono solo tramite canali interni all'applicativo di conservazione. Presso il sito primario vengono effettuate:

1. procedure quotidiane di backup verso storage di backup locale
2. replica delle VM deputate alla conservazione verso il sito DR
3. backup remoto verso il sito DR
4. tape vaulting settimanale dello storage di backup

La procedura di replica per DR sfrutta la possibilità di replicare interamente il sistema virtuale, con frequenza giornaliera, verso il sito di DR in cui si trova una infrastruttura di virtualizzazione compatibile.

Parallelamente, sul sito di DR vengono inviati anche i backup, questo consente di avere sul sito di DR:

- una replica del sistema già disponibile per essere attivata
- il datastore di backup contenente i "recovery point" degli ultimi 30 giorni

Sia il data center che ospita il sito primario ed il sito di test, sia i locali dedicati al Disaster Recovery sono in Italia, di proprietà e sotto la gestione diretta del Conservatore che ha deciso, a tutela del servizio e dei suoi clienti, di non affidarsi a servizi di cloud o hosting esterni. Questo garantisce l'efficacia del monitoraggio, la disponibilità delle risorse necessaria agli interventi e la disponibilità del miglior servizio garantito.

8.3 Componenti Tecnologiche

Gli ambienti server deputati alla conservazione sono ospitati all'interno di una infrastruttura di virtualizzazione, questo consente di "astrarre" i sistemi dall'hardware su cui sono ospitati.

La soluzione adottata prevede l'erogazione di nodi di erogazione dei moduli applicativi tramite un'infrastruttura che opera di fatto in alta affidabilità, garantendo la Business Continuity anche nel caso di fault di una o più macchine reali e, attraverso i backup periodico dell'intera infrastruttura, mette a disposizione dei clienti un sito di DR attivabile in caso di disastro.

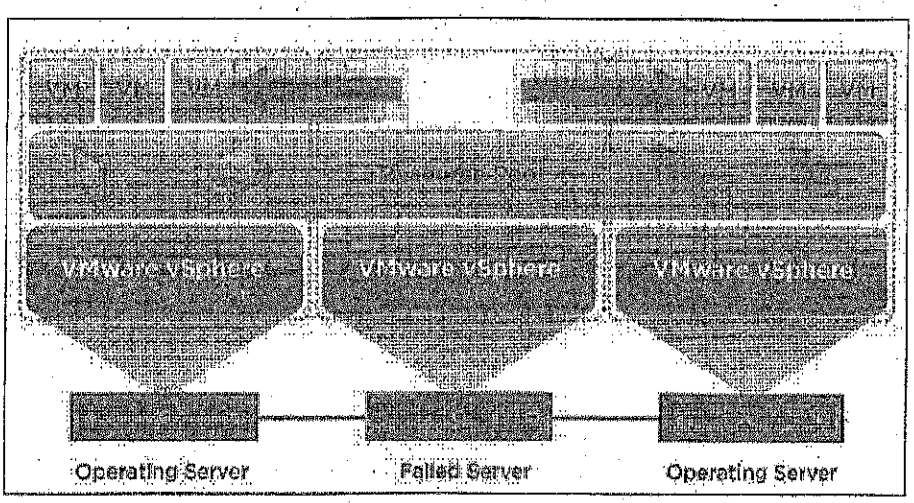


Figura 9 - Virtualizzazione

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini + R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

In questo scenario l'evoluzione e l'aggiornamento dell'hardware della infrastruttura non ha impatto sulla configurazione dei sistemi, che possono così beneficiare in modo "trasparente" delle modifiche e migliorie introdotte.

Per gli approfondimenti: si rimanda al piano per la sicurezza

Torna al sommario

8.4 Componenti Fisiche

Come già indicato al paragrafo precedente, il sistema di conservazione è erogato in Alta Affidabilità grazie al sistema di virtualizzazione dei server che è stato adottato presso il Data Center di proprietà del conservatore. Tale sistema, implementato anche in rispetto della certificazione ISO:270001, dispone di gruppi di continuità per la doppia alimentazione elettrica e connessioni di rete in fibra ottica tra i server e dai server agli storage. Gli storage utilizzano un sistema RAID6 per garantirne la consistenza anche in caso di rottura dei supporti fisici. I dati ed i server virtuali sono sottoposti a backup incrementali ogni notte e ad un backup totale ogni settimana. Una copia dei server di esercizio e dello storage di conservazione è mantenuta allineata presso una seconda sede sempre di proprietà del conservatore, ad oltre 190 Km dalla prima, sempre in territorio italiano. Questa disponibilità, applicando la procedura di rientro prevista in caso di fault o disastro presso il sito primario, consente l'erogazione del servizio con l'utilizzo del Disaster Recovery.

Nel piano per la sicurezza sono dettagliate le procedure, l'architettura e fin'anche i modelli di hardware utilizzati, come pure i sistemi, i dispositivi e le policy di monitoraggio dei sistemi eroganti il servizio. Tali dettagli sono volutamente omessi dal presente per motivi di sicurezza e concorrenza, ma sono richiedibili a ragione al Conservatore in fase di valutazione dell'offerta.

Torna al sommario

Procedure di gestione e di evoluzione

Si rimanda al piano per la sicurezza per la descrizione delle procedure di gestione e di evoluzione, e della relativa documentazione prevista, inerenti le componenti logiche, tecnologiche e fisiche del sistema di conservazione relativamente a:

- conduzione e manutenzione del sistema di conservazione;
- gestione e conservazione dei log (anche in accordo con l'ente Produttore);
- monitoraggio del sistema di conservazione;
- change management;
- verifica periodica di conformità a normativa e standard di riferimento.

9 MONITORAGGIO E CONTROLLI

Descrizione generale della strategia della conservazione e dei conseguenti obiettivi di monitoraggio e controllo (Regole Tecniche: art. 8, comma 2, lettera h).

Torna al sommario

Maggioli SpA
Via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P.IVA 02066400405

Capitale sociale
Euro 2.215.200
interamente versato

9.1 Procedure di monitoraggio

I servizi ed i sistemi di conservazione sono controllati in modo automatico con diversi sistemi di monitoraggio che operano a seconda del range di applicazione (infrastruttura, sistemi, servizi, applicazioni, ecc...).
Tutti i sistemi centralizzati e gestiti dal data center prevedono monitoraggi e alert automatici ai dispositivi di controllo in uso presso la divisine informatica del conservatore.
Le notifiche e gli alert dell'applicazione di conservazione, invece riguardano la struttura operativa dedicata al servizio specifico e si concretizzano nell'invio di mail e notifiche agli operatori, agli utenti o ai responsabili a seconda del tipo di evento da segnalare.

La rilevazione di qualsiasi anomalia viene registrata e successivamente risolta dal personale autorizzato.

Torna al sommario

9.2 Verifica dell'integrità degli archivi e sistemi di allerta preventiva

La funzionalità di verifica di integrità degli archivi, permette di verificare l'integrità del documento informatico dal momento della sua conservazione, confrontando l'impronta attuale con quella contenuta nell'Indice di Conservazione. Tale funzionalità viene applicata durante il processo di conservazione subito dopo la fase di memorizzazione nel file system, e risulta poi utile, nell'assolvimento dei requisiti di verifica periodica della leggibilità dei documenti, come richiesto dalla normativa.

Questa funzionalità è schedulata con cadenza periodica, almeno ogni 5 anni, o più di frequente, in relazione al volume di dati versato da ogni Soggetto Produttore. Ogni verifica effettuata genera un report in formato xml che può essere consultato da parte del responsabile del servizio di conservazione per attestare la corretta esecuzione della verifica o per diagnosticare eventuali anomalie.

In aggiunta o congiuntamente a questa verifica sono previste delle procedure operative "umane" atte a verificare l'effettiva fruibilità dei dati conservati; in concreto il conservatore può definire un campione di dati da ricercare e di cui simulare un'esibizione, scaricando il relativo DIP e procedendo alla verifica del file conservato tramite il viewer ad esso associato.

Ogni riscontro anomalo è prontamente segnalato al cliente ed al produttore vi mail.

Nel piano della sicurezza si approfondirà quanto già trattato nel presente manuale con particolare riguardo alla tenuta dei sistemi informativi di storage ed ai loro backup. Ogni anomalia o manomissione è verificata e segnalata secondo le procedure aziendali previste, mentre resta a carico del sistema di conservazione entrare nel merito della relazione tra dato versato e dato conservato; diversamente parleremmo di un archivio non riscrivibile, pure in disponibilità del sistema ed utilizzabile per particolari casistiche contrattuali eventualmente definibili tra il conservatore ed il produttore.

Torna al sommario

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

9.3 Soluzioni adottate in caso di anomalie

Le anomalie vengono affrontate con diverse metodologie, secondo la natura dell'anomalia stessa e la collocazione dell'evento che l'ha generata nel processo di Conservazione:

Anomalia	Casistica	Procedura di rientro
Versamenti non conformi alle regole concordate	Firma non valida, Formato file non previsto, file corrotto, mancanza di Metadati obbligatori, ecc..	Il conservatore contatta i referenti del soggetto produttore, con i quali viene concordata la soluzione del problema.
Mancata risposta al Versamento	Versamento avvenuto con successo, ma senza rilevazione da parte del produttore, che lo reputa non fallito e replica l'operazione *n* volte.	Il sistema di conservazione, di default, è programmato a tutela del produttore per rifiutare i versamenti duplicati con un ritorno specifico. Una risposta in tal senso può essere utilizzata per attestare l'avvenuto versamento..
Errori temporanei	È il caso di errori dovuti a problemi temporanei che pregiudicano il versamento, ma si presume non si ripresentino a un successivo tentativo di Versamento. Il caso più frequente è l'impossibilità temporanea di accedere alle CRL degli enti certificatori. In questi casi il sistema di conservazione dopo aver riprovato 10 volte, genera un messaggio di errore perché non riesce a completare le verifiche previste e il versamento viene rifiutato.	Il soggetto produttore deve provvedere a rinviare l'unità documentaria in un momento successivo. L'operazione potrebbe dover essere ripetuta più volte qualora il problema, seppur temporaneo, dovesse protrarsi nel tempo.
Errori interni o dovuti a casistiche non previste o non gestite	In alcuni casi è possibile che il sistema di Conservazione risponda con un messaggio di errore generico o non gestibile dal sistema di conservazione.	I referenti del soggetto produttore segnalano il problema via e-mail al soggetto conservatore, che si attiverà per la sua risoluzione.

Tabella 17 - Gestione anomalie

10 Ulteriori informazioni ed approfondimenti

10.1 Altri Allegati

Costituiscono parte integrante degli accordi di fornitura :

- **Modalità e Condizioni di fornitura del servizio**
- **Modulo di richiesta attivazione del servizio**
- **Specifiche di interoperabilità ed integrazione applicativa del servizio**

Le procedure di attivazione, disattivazione, scarto e restituzione dei dati conservati sono riportate e firmate per accettazione dai clienti all'atto della richiesta di attivazione del servizio.

Torna al sommario

10.2 Delega a Maggioli S.p.A. per la nomina del Responsabile del Servizio di conservazione

Con l'affidamento del servizio il Soggetto Produttore nomina e delega a MAGGIOLI S.p.A. le seguenti cariche:

- Responsabile del servizio di conservazione
- Responsabile esterno del trattamento dei dati

Maggioli SpA
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini * R.E.A. n. 219107
C.F. 06188330150
P. IVA 02066400405

Capitale sociale:
Euro 2.216.200
interamente versato

Le nomine e le deleghe necessarie all'attivazione ed all'erogazione del servizio sono riportate nelle condizioni di fornitura che vengono firmate dal cliente e riconsegnate al conservatore all'atto della richiesta di attivazione.

Il Modulo di richiesta di attivazione del servizio costituisce il documento nel quale sono sintetizzati gli elementi peculiari del servizio attivato e, unitamente alle sue istruzioni ed alle condizioni di fornitura del servizio, integra il presente manuale. Il modulo di attivazione firmato, se accettato dal conservatore mediante effettiva attivazione del servizio, costituisce riferimento per gli impegni contrattuali fra le parti.

10.3 Protezione dei dati e delle procedure informatiche

Il Conservatore è garante nei confronti del Cliente che lo ha nominato dell'applicazione delle misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione, comprensivo della copie di sicurezza dei supporti di memorizzazione, al fine di proteggere le informazioni da possibili violazioni in termini di riservatezza, integrità e disponibilità delle informazioni. Maggioli S.p.A. ha stabilito attraverso un analisi del rischio gli appropriati controlli di sicurezza delle informazioni da adottare. Approfonditi nell'allegato o depositato presso AgID all'atto del accreditamento

Il cliente è consapevole che l'accreditamento sottintende il rispetto di adeguati standard di implementazione e gestione del servizio, così come la certificazione ISO 27001 del data center ne garantisce la qualità operativa. Gli SLA e le modalità di erogazione del servizio sono riportate nelle condizioni di servizio sottoscritte al momento della richiesta di attivazione.

Maggioli S.p.A.
via del Carpino, 8
47822 Santarcangelo
di Romagna (RN)

tel. 0541 628111
fax 0541 622100
maggiolispa@maggioli.it
www.maggioli.it

Iscritta al Registro delle Imprese
di Rimini e R.E.A. n. 219107
C.F. 06188330150
e IVA 02066400405

Capitale Sociale:
Euro 2.215.200
Interamente versato

ALLEGATO "7" – I FORMATI IDONEI PER LA FORMAZIONE E PER LA CONSERVAZIONE

1. Introduzione

Il presente documento fornisce indicazioni iniziali sui formati dei documenti informatici che per le loro caratteristiche sono, al momento attuale, da ritenersi coerenti con le regole tecniche del documento informatico, del sistema di conservazione e del protocollo informatico.
I formati descritti sono stati scelti tra quelli che possono maggiormente garantire i principi dell'interoperabilità tra i sistemi di conservazione e in base alla normativa vigente riguardante specifiche tipologie documentali.
Il presente allegato, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e allineato con la pubblicazione dell'Agenzia per l'Italia digitale.

2. I formati

La leggibilità di un documento informatico dipende dalla possibilità e dalla capacità di interpretare ed elaborare correttamente i dati binari che costituiscono il documento, secondo le regole stabilite dal formato con cui esso è stato rappresentato.
Il formato di un file è la convenzione usata per interpretare, leggere e modificare il file.

2.1 Le tipologie di formato

L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità più specializzate per renderne più facile la creazione, la modifica e la manipolazione.
Questo fenomeno porta all'aumento del numero dei formati disponibili e dei corrispondenti programmi necessari a gestirli nonché delle piattaforme su cui questi operano.
Per esigenze lavorative gestionali possono essere trattati documenti in formati diversi da quelli indicati al paragrafo 2.3, come ad esempio in formato WORD (.doc), EXCEL (.xls), POWER POINT (.ppt), purchè accompagnati dalla versione dello stesso documento in uno dei formati accettati, preferibilmente PDF/A.

2.2 Caratteristiche generali dei formati

L'informazione digitale è facilmente memorizzata, altrettanto facilmente accedere e riutilizzarla, modificarla e manipolarla, in altre parole, elaborarla ed ottenere nuova informazione.
In particolare devono soddisfare quanto previsto da AGID

- apertura
- sicurezza
- portabilità
- funzionalità
- supporto allo sviluppo
- diffusione

2.2.1 Apertura

Un formato si dice "aperto" quando è conforme a specifiche pubbliche, cioè disponibili a chiunque abbia interesse ad utilizzare quel formato. La disponibilità delle specifiche del formato rende sempre possibile la decodifica dei documenti rappresentati in conformità con dette specifiche, anche in assenza di prodotti che effettuino tale operazione automaticamente.
Questa condizione si verifica sia quando il formato è documentato e pubblicato da un produttore o da un consorzio al fine di promuoverne l'adozione, sia quando il documento è conforme a formati definiti da organismi di standardizzazione riconosciuti.
Nelle indicazioni di questo documento si è inteso privilegiare i formati già approvati dagli Organismi di standardizzazione internazionali quali ISO e ETSI.

2.2.2 Sicurezza
La sicurezza di un formato dipende da due elementi il grado di modificabilità del contenuto del file e la capacità di essere immune dall'inserimento di codice maligno.

2.2.3 Portabilità
Per portabilità si intende la facilità con cui i formati possano essere usati su piattaforme diverse, sia dal punto di vista dell'hardware che del software, inteso come sistema operativo. Di fatto è indotta dall'impiego fedele di standard documentati e accessibili.

2.2.4 Funzionalità
Per funzionalità si intende la possibilità da parte di un formato di essere gestito da prodotti informatici, che prevedono una varietà di funzioni messe a disposizione dell'utente per la formazione e gestione del documento informatico.

2.2.5 Supporto allo sviluppo
E' la modalità con cui si mettono a disposizione le risorse necessarie alla manutenzione e sviluppo del formato e i prodotti informatici che lo gestiscono (organismi preposti alla definizione di specifiche tecniche e standard, società, comunità di sviluppatori, ecc.).

2.2.6 Diffusione
La diffusione è l'estensione dell'impiego di uno specifico formato per la formazione e la gestione dei documenti informatici.
Questo elemento influisce sulla probabilità che esso venga supportato nel tempo, attraverso la disponibilità di più prodotti informatici idonei alla sua gestione e visualizzazione.
Inoltre nella scelta dei prodotti altre caratteristiche importanti sono la capacità di occupare il minor spazio possibile in fase di memorizzazione (a questo proposito vanno valutati, in funzione delle esigenze dell'utente, gli eventuali livelli di compressione utilizzabili) e la possibilità di gestire il maggior numero possibile di metadati, compresi i riferimenti a chi ha eseguito modifiche o aggiunte.

2.3 Formati idonei per la conservazione
La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche suddette deve essere strumentale a che il documento assuma le caratteristiche di immodificabilità e di staticità previste dalle regole tecniche.
In particolare è necessario tener conto nella scelta dei seguenti elementi:

- non devono poter contenere macroistruzioni o codici eseguibili, ovvero devono essere disponibili gli strumenti capaci di rilevarne la presenza con sufficiente sicurezza;
- devono essere standard e documentati, ovvero le relative specifiche devono essere pubblicamente accessibili, complete ed esaustive;
- devono essere robusti, accurati, ampiamente adottati ed usabili
- devono essere indipendenti dalle piattaforme tecnologiche, in modo da poter visualizzare un documento senza particolari vincoli di natura informatica o il pagamento di royalty;
- devono essere conformi alle disposizioni emanate dalle autorità competenti in materia di archiviazione e conservazione digitale.

Per quanto fin qui considerato, è opportuno privilegiare i formati che siano standard internazionali (de jure e de facto) o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche, dandone opportuna evidenza nel manuale di conservazione dei documenti informatici.
Ulteriore elemento di valutazione nella scelta del formato è il tempo di conservazione previsto dalla normativa per le singole tipologie di documenti informatici.
I formati di seguito indicati sono un primo elenco di formati da usare per la conservazione:

- **PDF/A (Portable Document Format/Archive)** formato sviluppato con l'obiettivo specifico di rendere possibile la conservazione documentale a lungo termine su supporti digitali.

- **ODF (Open Document Format)** è uno standard aperto, basato sul linguaggio XML, sviluppato dal consorzio OASIS per la memorizzazione di documenti corrispondenti a testo, fogli elettronici, grafici e presentazioni. Secondo questo formato, un documento è descritto da più strutture XML, relative a contenuto, stili, metadati ed informazioni per l'applicazione.
- **XML (Extensible Markup Language)** formato di testo flessibile. E' un linguaggio di markup, ovvero un linguaggio marcatore basato su un meccanismo sintattico che consente di definire e controllare il significato degli elementi contenuti in un documento o in un testo.
- **OOXML (Office Open XML)** è un formato di file, sviluppato da Microsoft, basato sul linguaggio XML per la creazione di documenti di testo, fogli di calcolo, presentazioni, grafici e database.
- **TXT** è un file che contiene solo caratteri di scrittura semplici, che compongono un testo leggibile direttamente dagli utenti senza bisogno di installare programmi appositi.
- **RTF (Rich Text Format)** è un file ASCII con stringhe di comandi speciali in grado di controllare le informazioni riguardanti la formattazione del testo: il tipo di carattere e il colore, i margini, i bordi del documento, ecc.
- **TIFF (Tagged Image File Format)** formato immagine di tipo raster.
- **DXF (Drawing Interchange Format, o Drawing Exchange Format),** un formato simile al DWG(Autocad) , di cui sono state rilasciate le specifiche tecniche.
- **Shapefile** un formato vettoriale proprietario per sistemi informativi geografici (GIS) con la caratteristica di essere interoperabile con con i prodotti che usano i precedenti formati. Il formato è stato sviluppato e regolato da ESRI, allo scopo di accrescere l'interoperabilità fra i sistemi ESRI e altri GIS. Di fatto è diventato uno standard per il dato vettoriale spaziale, e viene usato da una grande varietà di sistemi GIS.
- **SVG (Scalable Vector Graphics)**, un formato aperto, basato su XML, in grado di visualizzare oggetti di grafica vettoriale, non legato ad uno specifico prodotto.

Come già indicato nelle premesse questo elenco sarà periodicamente aggiornato, sulla base delle nuove tecnologie e dei nuovi standard definiti da AGID.

Qualora detta documentazione debba possedere specifiche valenze giuridiche, tra cui ad esempio l'opponibilità a terzi, deve essere prodotta nei formati indicati nei punti precedenti, o altri che offrano analoghe o maggiori garanzie a motivo dell'evoluzione tecnologica, e firmata digitalmente. Per i formati indicati deve essere garantita dagli applicativi informatici, , la corretta visualizzazione dei contenuti.

Date le caratteristiche richieste per i documenti informatici in tema di inalterabilità e immutabilità, non sono accettati né trasmessi file compressi, come ad esempio i file con estensione ".ZIP" oppure ".RAR".

I documenti informatici prodotti dall'Amministrazione su formati diversi (ad esempio, in estensione ".doc" di Microsoft Word, ".xls" di Microsoft Excel) prima della loro sottoscrizione con firma elettronica o comunque nel momento che si considerano perfezionati, sono convertiti nel formato PDF/A - o nei formati sopraindicati se maggiormente confacenti al tipo di documento considerato - al fine di garantirne la leggibilità, la non alterabilità durante le fasi di accesso e conservazione e l'immutabilità nel tempo del contenuto e della struttura.

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO,
DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

ALLEGATO N. 8 – ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

Si riporta, innanzitutto, il testo del comma 5 dell'art. 53 del D.P.R. 28.12.2000, n. 445, che recita:

"Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e 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 e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

Inoltre, sono escluse dalla protocollazione le seguenti categorie di documenti:

- Le comunicazioni d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
- Le richieste di ferie ed altri permessi;
- Le richieste di rimborso spese e missioni;
- Gli allegati, se accompagnati da lettera di trasmissione, compresi gli elaborati tecnici;
- I certificati di malattia;
- I certificati di infortunio;
- La pubblicità conoscitiva di convegni;
- La pubblicità in generale;
- Le offerte, i listini prezzi e i preventivi di terzi non richiesti;
- Le richieste di copia o visione di atti amministrativi pubblicati;
- Le ricevute di ritorno delle raccomandate A.R.;
- Le convocazioni ad incontri o riunioni interne;
- I curricula non richiesti;
- I cosiddetti "ritorni", cioè le risposte alle richieste di certificazioni varie avanzate dall'Amministrazione a vari enti, i quali rispondono apponendo semplicemente sulla richiesta medesima diciture o timbri quali "Nulla" o "Nulla osta", ecc.;
- Tutti i documenti che, per loro natura, non rivestono alcuna rilevanza giuridico-amministrativa presente o futura.

ALL. 9 – Elenco tipologie documentarie soggette a registrazione particolare nel sistema di gestione documentale o in altri sistemi gestionali di settore

- deliberazioni del Consiglio Comunale
- deliberazioni della Giunta Comunale
- decisioni/direttive della Giunta Comunale
- decreti del Sindaco /del Responsabile di Servizio
- ordinanze del Sindaco
- ordinanze dei Dirigenti
- determinazioni dei Dirigenti
- atti rogati o autenticati dal Segretario Comunale
- verbali delle adunanze del Consiglio Comunale
- verbali delle Commissioni Consiliari
- atti di stato civile
- pubblicazioni all'Albo Pretorio
- pubblicazioni di matrimonio
- carta di identità
- tessere elettorali
- certificazioni anagrafiche e di stato civile rilasciate direttamente al richiedente
- verbali di violazione del codice della strada
- richieste permessi di transito e sosta
- fatture attive
- mandati di pagamento
- reversali
- atti da notificare e relata di notifica
- certificati catastali rilasciati direttamente al richiedente
- autorizzazioni edilizie
- autorizzazioni SUAP
- concessione per l'occupazione di spazi ed aree pubbliche
- avvisi accertamento tributari

ALLEGATO 10 – PIANO DI CONSERVAZIONE

Come disciplinato dal MdG, di seguito si ripropone, integralmente, il testo del piano di conservazione per i Comuni elaborato dal Ministero per i beni culturali e riportato dalla Soprintendenza Archivistica per la Toscana sul proprio sito.

Ovviamente, l'Amministrazione comunale di Montelupo Fiorentino farà riferimento ad esso, per le operazioni di scarto, soltanto relativamente alle voci che interessano.

SOPRINTENDENZA ARCHIVISTICA PER LA TOSCANA

PIANO DI CONSERVAZIONE

Premessa

L'individuazione del materiale documentario da scartare è un'operazione delicata, da effettuarsi con la dovuta attenzione e con il controllo degli organi direttivi comunali, subordinata comunque, in base all'art. 21, comma 1/d del Decreto Legislativo 22 gennaio 2004, n. 41 (Codice dei beni culturali e del paesaggio) all'autorizzazione della Soprintendenza Archivistica per la Toscana di Firenze.

In linea generale va tenuto presente che, quanto più in passato l'archivio ha subito dispersioni o scarti indiscriminati, tanto più le operazioni di selezione del materiale da eliminare andranno eseguite con prudenza e oculatezza.

Gli atti compresi nella sezione separata (archivio storico) non sono, di regola, proponibili per lo scarto, salvo diverse specifiche indicazioni della Soprintendenza Archivistica per la Toscana.

I Comuni, qualora intendano procedere allo scarto di documenti, dovranno inviare alla Soprintendenza Archivistica (Via Ginori n. 7 – 50123 Firenze, Tel 055/271111 – fax 055/2711142) n. 3 originali o copie conformi della proposta di scarto (cioè l'elenco dei documenti che si intendono eliminare: si veda il modello di cui all'allegato n. 1), firmati dal Sindaco o da un suo delegato; tali esemplari dovranno avere le pagine numerate ed essere provvisti del bollo tondo del Comune. Ad essi dovrà essere allegata una lettera di accompagnamento, debitamente protocollata e firmata dal Sindaco o da un suo delegato, attestante la volontà del Comune di procedere allo scarto, nonché certificante il numero dei fogli di cui si compone la proposta di scarto medesima: La proposta di scarto potrà eventualmente essere accompagnata anche da una delibera di Giunta, oppure da un provvedimento dirigenziale, contenenti gli stessi elementi sopra richiesti. In caso di dubbi sul materiale da proporre per l'eliminazione si consiglia di consultare preventivamente la Soprintendenza Archivistica per la Toscana.

Si ricorda che, in base al DPR 854/1975, la Soprintendenza Archivistica, una volta valutato l'elenco, deve trasmetterlo all'Ispettorato Centrale per i Servizi archivistici del Ministero degli Interni, per il controllo sulla eventuale presenza di atti riservati, contenenti o dati relativi alla politica interna o estera dello Stato o i cosiddetti dati sensibili (Artt. 20 e 26 della legge 196/03 "Codice in materia di protezione dei dati personali").

Una volta pervenuta la lettera di risposta dell'Ispettorato (cosa che richiede mediamente 1 mese) la Soprintendenza Archivistica restituisce al Comune un esemplare della proposta di scarto munito di nulla osta.

Nella compilazione dell'elenco si raccomanda la massima chiarezza e precisione nella descrizione di ciascuna tipologia documentaria, evitando locuzioni generiche, abbreviazioni, sigle, acronimi.

In base all'art. 8 del DPR n. 37/2001 l'ente pubblico stabilisce in proprio le modalità di cessione dei documenti d'archivio di cui è stato disposto lo scarto; esso può anche rivolgersi sia alla Croce Rossa Italiana, sia alle organizzazioni di volontariato.

Si sottolinea in ogni caso la necessità di garantire la distruzione (con qualunque mezzo ritenuto idoneo) della documentazione da eliminare, allo scopo di impedirne usi impropri, e l'obbligo di trasmettere alla Soprintendenza Archivistica l'attestazione dell'avvenuta distruzione medesima, quale atto conclusivo della pratica.

Si rileva che il piano di conservazione 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.

Per ogni tipologia documentaria non compresa nei sotto indicati elenchi, si rimanda pertanto alla consulenza diretta della Soprintendenza Archivistica per la Toscana (tel. 055/271111 – fax 055/2711142 – e-mail: sa-tos@beniculturali.it

Il presente documento si compone di due parti:

-la prima nella quale vengono definiti i principi generali e le indicazioni di massima

-la seconda che contiene nello specifico per ogni Categoria e classe del Titolario l'indicazione delle tipologie documentarie prodotte e dei relativi tempi di conservazione. Per quanto riguarda le tipologie documentarie, si fa riferimento alle «Linee guida per l'organizzazione dei fascicoli e delle serie dei documenti prodotti dai Comuni italiani in riferimento al piano di classificazione» proposte da Giorgetta Bonfiglio-Dosio al Gruppo e disponibili per la sperimentazione.

Principi generali

Ambito e criteri generali di applicazione

- Il presupposto per il corretto utilizzo di questo strumento è l'organizzazione dell'archivio basata sul Piano di classificazione prodotto dal Gruppo di lavoro.
- Lo scarto della documentazione prodotta e classificata sino all'adozione del nuovo titolario deve essere valutato sulla base del massimario precedente.
- I termini cronologici indicati devono essere conteggiati dalla chiusura dell'affare per i fascicoli oppure dall'ultima registrazione effettuata, nel caso dei registri.
- In generale, si sono ridotti, rispetto a quelli indicati dal massimario di scarto precedentemente in vigore, i termini di conservazione dei documenti, in linea con la normativa generale civilistica e con la normativa specifica ove contempli termini per la conservazione degli atti.
- Il materiale non archivistico non viene preso in considerazione dal presente Piano, in quanto non devono essere considerati documenti gli stampati in bianco, la modulistica, le raccolte normative o altro materiale analogo (ad esempio, copie della normativa da consegnare all'utenza).
- L'applicazione del piano di conservazione non può comunque essere automatica, ma deve valutare caso per caso le eventuali particolarità adottate dal Comune nell'organizzazione dei documenti prodotti.
- Lo scarto, se non viene effettuato regolarmente ogni anno e su un archivio organizzato, potrà essere deciso e valutato solo dopo che l'intero complesso archivistico sia stato analizzato e almeno sommariamente riordinato.

I fondamenti della conservazione permanente

- In genere, salvo poche eccezioni, tutti i repertori devono essere conservati permanentemente.
- Il Comune non deve scartare i documenti considerati "vitali" (quelli che – mutuando una definizione formulata da Luciana Duranti[1] – in caso di disastro, sono necessari a ricreare lo

1 L. DURANTI, *I documenti archivistici. La gestione dell'archivio da parte dell'ente produttore*, Roma 1997 (Pubblicazioni degli Archivi di Stato. Quaderni della «Rassegna degli Archivi di Stato», 82), p. 93

stato giuridico dell'ente e la sua situazione legale e finanziaria, a garantire i diritti dei dipendenti e dei cittadini, a soddisfare i suoi obblighi e a proteggere i suoi interessi esterni).

Alcune considerazioni sulla dimensione culturale degli archivi

- Lo scarto si effettua di norma sui documenti dell'archivio di deposito.
- Non vanno scartati i documenti prodotti durante la prima e la seconda guerra mondiale e vanno vagliati con estrema attenzione quelli degli anni del dopoguerra e della ricostruzione, perché tali archivi costituiscono una miniera di informazioni e di dati ancora sconosciuti e finora inesplorati dagli storici, oltre che un serbatoio di informazioni rilevanti dal punto di vista giuridico..

Documenti originali e documenti prodotti in copia

- Lo scarto dei documenti in copia può essere facilmente effettuato qualora sia prevista la conservazione permanente dei documenti in originale e qualora le copie non contengano annotazioni amministrative o visti essenziali per ricostruire il procedimento nella sua correttezza.
- È opportuno prevedere repertori di documenti di interesse generale per tutte le UO del Comune, resi disponibili sul sito interno del Comune, che quindi diventano depositi di documenti ad alto carattere informativo, in modo da evitare copie multiple, superflue, che contribuiscono ad appesantire inutilmente la conservazione documentale nelle diverse UOR, a scapito dei documenti essenziali e specifici.
- È altresì opportuno che ciascun RPA, durante la formazione dell'archivio corrente, abbia cura di non inserire nel fascicolo copie superflue di normative o atti repertoriati di carattere generale, facilmente reperibili in un sistema informatico-archivistico ben organizzato.
- Sarebbe anche auspicabile che il fascicolo venisse organizzato in sottofascicoli nei quali inserire i documenti soggetti a scarto periodico, in modo da facilitare, a tempo debito, le operazioni di scarto.

Avvertenze per la lettura del piano di conservazione

- Quando si usa la formula "previo sfoltimento del carteggio di carattere transitorio e strumentale" si allude all'operazione che estrae dal fascicolo le copie e i documenti, che hanno appunto carattere strumentale e transitorio, utilizzati dal RPA per espletare il procedimento, ma che esauriscono la loro funzione nel momento in cui viene emesso il provvedimento finale oppure non sono strettamente connessi al procedimento (ad esempio, appunti, promemoria, copie di normativa e documenti di carattere generale).
- Se i documenti sono inseriti integralmente o per estratto in una banca dati, l'archivio dispone solo degli esemplari più aggiornati e perde memoria delle fasi storiche. In certi casi, nei quali la memoria è ritenuta essenziale, si suggerisce nel corso del Piano di eseguire periodicamente, a cadenza prestabilita, un salvataggio (copia di back-up) o una stampa della banca dati.

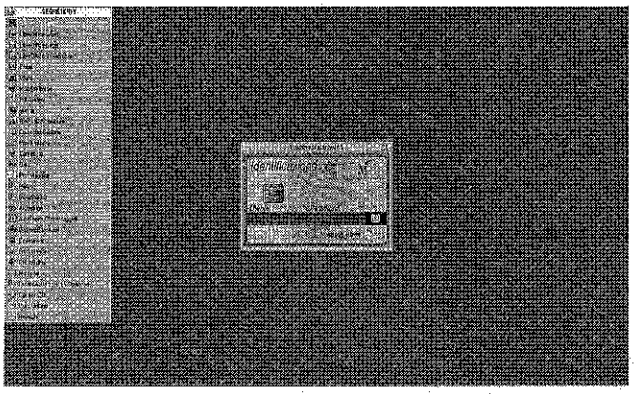
ALLEGATO N. 11 **DESCRIZIONE DELLE FUNZIONI E DELLE MODALITÀ' OPERATIVE DEL SISTEMA DI PROTOCOLLO INFORMATICO**

LOGIN E INGRESSO A J-IRIDE

Per accedere al programma è necessario lanciare l'icona seguente che troverete sul vostro desktop all'interno dell'icona " Procedure".

PROCEDURE_2013.lnk

All'interno del menù troverete l'icona per accedere a J-iride.
Prima di iniziare qualsiasi tipo di operazione in J-Iride, è necessario che l'Utente si identifichi all'interno del pagina principale.



Per l'ingresso è necessario indicare:
• **Utente**: cognome – iniziale del nome (es. Mario Rossi ha come utente rossi-m).
• **Password**: password di J-Iride, che non ha nulla a che vedere con la password di rete, ed è necessario inserirla tenendo presente le lettere maiuscole e minuscole.
Per cambiarla, una volta entrati nel sistema, aprire "Affari Generali" – opzioni e selezionare ***Cambio Password***.

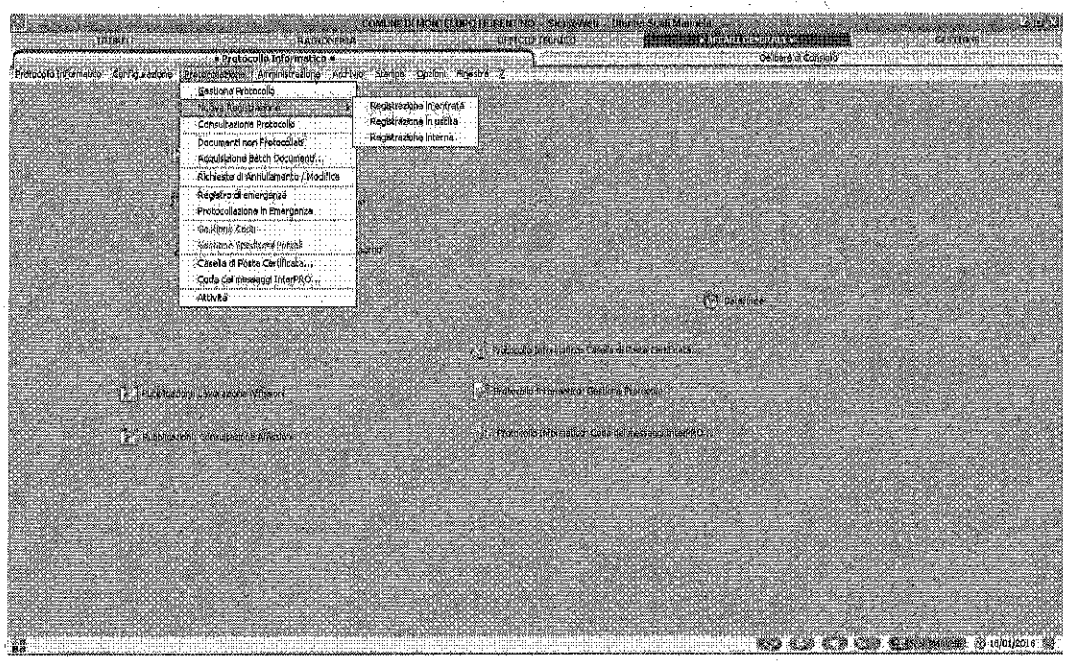
• **Ruolo**: il ruolo indica la "funzione" con la quale si lavora in j-iride.
Nel caso in cui ad un utente sia associato più di un ruolo, questo dalla propria scrivania, deve selezionarlo tra quelli disponibili. In base al ruolo l'Utente svolge funzioni diverse e automaticamente vengono impostate le funzionalità del sistema.

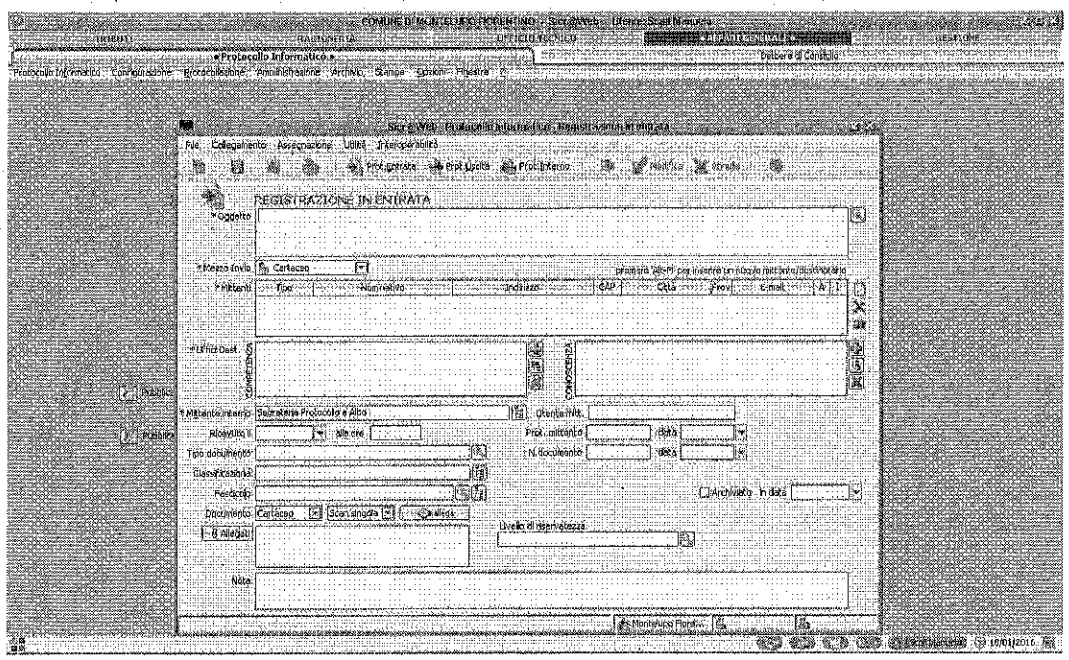
Per accedere al protocollo bisogna cliccare su Affari Generali – Protocollo informatico

La gestione del Protocollo Generale avviene in J-IRIDE, dove è possibile:
• protocollare nuovi documenti;
• gestire il contenuto delle pratiche;
• compiere ricerche sui documenti protocollati e trarre le informazioni relative;
• allegare testi e note ai documenti protocollati.

INSERIMENTO NUOVO PROTOCOLLO

Una volta entrati nella sezione protocollo selezionando il "Protocollazione" in alto a sinistra, sarà possibile protocollare un nuovo documento.





La procedura assegna automaticamente l'anno e la data di protocollazione, mentre il numero e l'identificativo vengono anch'essi attribuiti automaticamente ma solo a conferma effettuata. Una volta

registrato il protocollo, i dati relativi all'identificativo dell'anno, del numero, della data di protocollazione, del mittente o del destinatario sono immodificabili.

L'ORIGINE DOCUMENTO

I possibili tipi di protocollo sono tre:

• protocollo **in entrata**: sono tali i documenti che provengono dall'esterno e vengono indirizzati ad una specifica unità operativa. Essi ammettono quindi uno o più mittenti esterni, un destinatario per **competenza** e uno o più destinatari per **conoscenza**;
• protocollo **in uscita**: sono tali i documenti che nascono all'interno dell'Ente, tipicamente da un ufficio e sono diretti a soggetti esterni all'Ente. Essi ammettono quindi un mittente interno e uno o più destinatari esterni.
• protocollo **interno**: sono tali i documenti che nascono all'interno dell'Ente e viaggiano sempre all'interno dell'Ente da una unità operativa ad un'altra. Essi ammettono quindi un mittente interno e un destinatario interno.

L'OGGETTO

L'oggetto di un documento serve ad individuare a prima vista il contenuto di un documento.
Può essere utile utilizzare l'oggettario per agevolare la protocollazione, l'assegnazione e la classificazione del documento.
L'uso dell'oggettario è consigliato per una standardizzazione degli oggetti.

CARATTERISTICHE DEL DOCUMENTO E MEZZO INVIO

Il documento può essere:
- cartaceo
- elettronico
- informatico

Il tipo di invio del protocollo in entrata e in uscita può essere: cartaceo, raccomandata, atto giudiziario, interoperabile, interpro, apaci, pec.

MITTENTE/DESTINATARIO

Ad ogni documento protocollato deve sempre essere associato almeno un mittente o un destinatario con indicazione di: cognome, nome, indirizzo e recapiti di contatto.
In particolare per ogni documento **protocollato in arrivo** sarà necessario specificare uno o più mittenti.
In caso di un **protocollo in partenza** è necessario specificare l'Ufficio mittente e uno o più destinatari del documento.
Nel caso di un **protocollo interno** è necessario specificare sia l'unità operativa mittente, sia l'unità operativa destinataria del documento.
Mittenti e destinatari vengono quindi divisi in due categorie:
• **mittenti e destinatari esterni**: rappresentano persone fisiche o giuridiche esterne che scrivono o a cui viene scritto dal Comune di Montelupo Fiorentino
• **mittenti e destinatari interni**: rappresentano gli uffici codificati all'interno della struttura dell'Ente che per competenza specifica risultano essere depositari in un qualsiasi momento di un documento protocollato. Essi saranno depositari e responsabili del documento fintanto che un movimento interno non provochi lo spostamento ad un destinatario interno diverso.

ASSEGNAZIONE DEL DOCUMENTTO

L'ufficio UOP che riceve il documento lo assegna per competenza ad un solo ufficio, per conoscenza a uno o più uffici. In caso di documento cartaceo, l'originale è consegnato all'ufficio che lo ha in carico per competenza.

CLASSIFICA DEL DOCUMENTO

Ad ogni documento protocollato deve essere assegnata obbligatoriamente una classifica che qualifichi il documento protocollato in base all'argomento in esso trattato.
Tale classificazione permette una fascicolazione (utile soprattutto in fase di archiviazione) che rende più agevole un'eventuale necessità di reperimento del documento una volta che questo sia stato archiviato.
Non solo, la classificazione permette di suddividere i documenti per aree di appartenenza e quindi consente di individuare l'unità operativa che tratta tale materia.
La classificazione e la fascicolazione sono obbligatorie per qualsiasi tipo di protocollo e spettano al servizio al quale il documento è assegnato per competenza.
La classificazione è modificabile anche successivamente all'attribuzione del numero di protocollo.

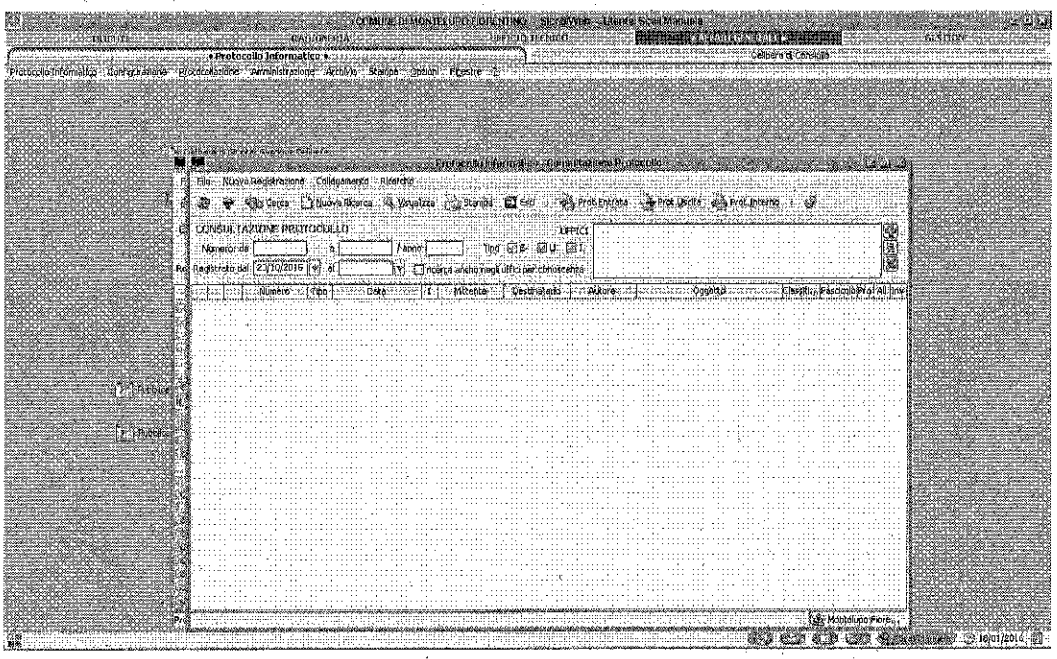
GESTIONE DEGLI ALLEGATI

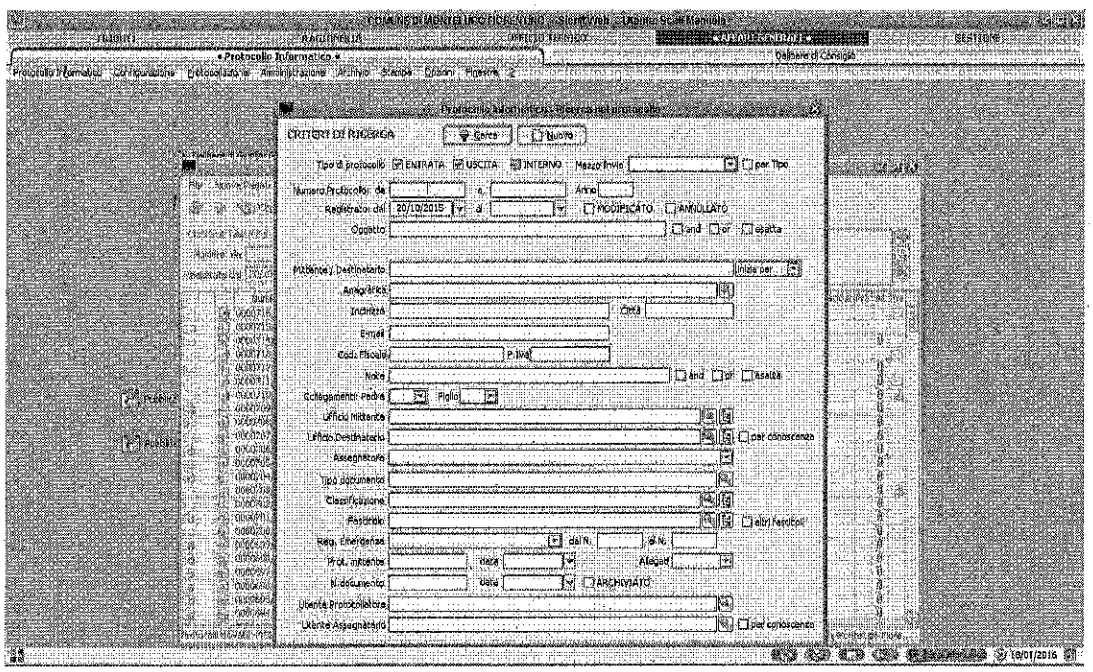
I documenti allegati al protocollo devono essere allegati in formato elettronico o informatico.
In caso di documenti cartacei, gli stessi devono essere scannerizzati integralmente con il timbro contenente i dati del protocollo.
Se vengono consegnati degli allegati in fase successiva al protocollo di origine è necessario: - creare un nuovo protocollo e collegarlo al protocollo padre (iniziale)

CONSULTAZIONE DI UN PROTOCOLLO

La consultazione di un protocollo può essere fatta in J-IRIDE come segue:
- Affari Generali
- Protocollazione
- Consultazione Protocollo (vedi maschere sotto), accedendo con "cerca- icona del cannocchiale" o "filtro attivo icona marrone e gialla).

Tanti più dati di ricerca sono inseriti tanto sarà più facile individuare il documento di interesse.





GESTIONE DEL PROTCOLLO ASSEGNATO

Ogni ufficio provvederà a gestire i protocolli sulla propria scrivania e a verificare la competenza dei documenti ricevuti;
In caso di:

- documenti assegnati e di competenza: l'ufficio deve prenderli in carico, **classificarli, fascicolarli** infine evaderli come completati.
- documenti non di competenza dell'ufficio: l'ufficio deve rifiutarli indicando nelle note alla motivazione.