Manuale di gestione documentale

1. Principi generali

1.1 Premessa

Il decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica del 20 ottobre 1998[1] n. 428", all'art. 3, comma 1, lettera c), prevede per tutte le amministrazioni di cui all'art. 2 del decreto legislativo 30 marzo 2001, n. 165, l'adozione del Manuale di gestione.

[1] *Il DPR del 20/10/1998 n. 428 è stato abrogato nel DPR del 20 dicembre 2000, n. 445.*

Quest'ultimo, disciplinato dal successivo art. 5, comma 1, "descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio".

In questo ambito è previsto che ogni amministrazione pubblica individui una o più Aree Organizzative Omogenee, all'interno delle quali sia nominato un responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 50, comma 4 del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa - decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 (già art.12 del citato DPR n. 428 del 20 ottobre 1998). Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili agli addetti al servizio e ai soggetti esterni che a diverso titolo interagiscono con l'amministrazione.

Il protocollo informatico, anche con le sue funzionalità minime, costituisce l'infrastruttura di base tecnico-funzionale su cui avviare il processo di ammodernamento e di trasparenza dell'amministrazione.

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. Esso disciplina:

- la migrazione dei flussi cartacei verso quelli digitali, ovvero in via transitoria, i flussi cartacei in rapporto al protocollo informatico;
- i livelli di esecuzione, le responsabilità ed i metodi di controllo dei processi e delle azioni amministrative;
- l'uso del titolario di classificazione e del massimario di selezione e di scarto;
- le modalità di accesso alle informazioni da parte di coloro che ne hanno titolo ed interesse, in attuazione del principio di trasparenza dell'azione amministrativa.

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 del Manuale

Il presente Manuale di gestione del protocollo, dei documenti e degli archivi è adottato ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, recante le regole tecniche per il protocollo informatico.

Esso descrive le attività di formazione, registrazione, classificazione, fascicolazione ed archiviazione dei documenti, oltre che la gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del Comune di San Benedetto del Tronto a partire dal 01/01/2012 in sostituzione del precedente "Sistema di gestione informatica dei documenti del Comune di San Benedetto del Tronto" approvato con Delibera di Giunta Municipale n.440 del 29/11/2004

Attraverso l'integrazione con le procedure di gestione dei procedimenti amministrativi, di accesso agli atti ed alle informazioni e di archiviazione dei documenti, il protocollo informatico realizza le condizioni operative per una più efficiente gestione del flusso informativo e documentale interno dell'amministrazione anche ai fini dello snellimento delle procedure e della trasparenza dell'azione amministrativa.

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

1.3 Definizioni e norme di riferimento

Ai fini del presente Manuale si intende:

- per **"amministrazione"**, il Comune di San Benedetto del Tronto;
- per "**Testo Unico**", il decreto del Presidente della Repubblica 20 dicembre 2000 n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- per **Regole tecniche**, il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 - Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428;
- per **Codice**, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell'amministrazione digitale e s.m.i.

Si riportano, di seguito, gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;

- **MdG** - Manuale di Gestione del protocollo informatico e gestione documentale e degli archivi;
- **RPA** - Responsabile del Procedimento Amministrativo - il dipendente che ha la responsabilità dell'esecuzione degli adempimenti amministrativi relativi ad un affare;
- **RSP** - Responsabile del Servizio per la tenuta del Protocollo informatico, la gestione dei flussi documentali e degli archivi;
- **PdP** - Prodotto di Protocollo informatico – l'applicativo sviluppato o acquisito dall'amministrazione/AOO per implementare il servizio di protocollo informatico;
- **UOP** - Unità Organizzative di registrazione di Protocollo - rappresentano gli uffici che svolgono attività di registrazione di protocollo;
- **UOR** - Uffici Organizzativi di Riferimento - un insieme di uffici che, per tipologia di mandato istituzionale e di competenza, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato;
- **UU** - Ufficio Utente - un ufficio dell'AOO che utilizza i servizi messi a disposizione dal sistema 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 nell'**allegato 2**.

1.4 Aree Organizzative Omogenee e modelli organizzativi

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata Comune di San Benedetto del Tronto e alla quale è stato assegnato il codice identificativo **c_h769** che è composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato nell'**allegato 3**.
All'interno della AOO il sistema di protocollazione è unico.
Nell'unica AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Nel medesimo allegato sono riportati la denominazione, il codice identificativo della AOO e l'insieme degli UOR che la compongono con la loro articolazione in UU.
All'interno della AOO il sistema di protocollazione è parzialmente distribuito per la corrispondenza in entrata e totalmente distribuito per la corrispondenza in uscita e interna; pertanto ogni UOR svolge anche i compiti di UOP per la posta interna e in partenza.
L'allegato 3 è suscettibile di modifica in caso di inserimento di nuove (AOO/)UOP/UOR/UU o di riorganizzazione delle medesime.
Le modifiche sono proposte ai vertici dell'amministrazione dal RSP d'intesa con il responsabile del sistema informativo e con il responsabile della tutela dei dati personali. L'amministrazione si riserva la facoltà di autorizzare, in via transitoria e del tutto eccezionale, altri UOR allo svolgimento dell'attività di protocollazione.
Tale "decentramento" da un punto di vista operativo segue le indicazioni stabilite nel presente Manuale e sarà sottoposto al controllo del responsabile del protocollo informatico. Nelle UOR sarà utilizzato il medesimo sistema di numerazione di protocollo e l'operatore incaricato dell'attività di protocollazione dovrà essere abilitato dal RSP che ha anche il compito di vigilare sulla corretta esecuzione delle attività.

1.5 Servizio per la gestione informatica del protocollo

Nella AOO precedentemente individuata è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Alla guida del suddetto servizio è posto il Responsabile del Servizio di Protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP). Al servizio è preposto un funzionario, in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente. Nel rispetto dell'autonomia organizzativa dell'Ente ed in relazione alle risorse umane disponibili, le competenze individuate in tale servizio possono essere attribuite per le rispettive competenze a differenti unità operative.

È compito del servizio, in coordinamento e collaborazione con il Servizio Sistemi Informativi e con il responsabile dell'U.O. Archivio storico:

- 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 (eventualmente anche sul sito Internet dell'amministrazione);
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli di settore e di reparto, dei protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- predisporre, in collaborazione con il responsabile per la sicurezza informatica, il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici;
- abilitare gli addetti dell'amministrazione all'utilizzo del PdP e definire per ciascuno di essi il tipo di funzioni

disponibili (ad esempio consultazione, modifica ecc.);
• garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
• garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
• garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO attraverso l'adozione dei formati standard previsti dalla normativa vigente;
• curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
• conservare le copie di salvataggio delle informazioni del sistema di protocollo e del registro di emergenza in luoghi sicuri e diversi da quello in cui viene custodito il suddetto sistema;
• garantire il buon funzionamento degli strumenti e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
• autorizzare le operazioni di annullamento della registrazione di protocollo;
• aprire e chiudere il registro di protocollazione di emergenza.

1.6 Conservazione delle copie di riserva

Nell'ambito del servizio di gestione informatica del protocollo, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della settimana lavorativa, va riversato, nel rispetto della normativa vigente, su supporti informatici non riscrivibili.
Tali supporti rimovibili sono conservati dalla stessa persona che ha realizzato il riversamento, diversa dal RSP.
Le procedure di riversamento e custodia delle copie, predisposte dal RSP, sono illustrate nel piano di sicurezza del MdG.

1.7 Firma digitale

Per l'espletamento delle attività istituzionali e per quelle connesse all'attuazione delle norme di gestione del protocollo informatico, di gestione documentale e di archivistica, l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.

1.8 Tutela dei dati personali

L'amministrazione titolare dei dati di protocollo e dei dati personali - comuni, sensibili e/o giudiziari - contenuti nella documentazione amministrativa di propria pertinenza dà attuazione al dettato del decreto legislativo 30 giugno 2003 n. 196 con atti formali aventi rilevanza interna ed esterna.

• Relativamente agli adempimenti interni specifici, gli addetti autorizzati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono stati incaricati dal titolare dei dati e, se nominato, dal responsabile.

• Relativamente agli adempimenti esterni, l'amministrazione si è organizzata per garantire che i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite; inoltre l'amministrazione certificante, in caso di accesso diretto ai propri archivi, rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente

Le regole e le modalità operative stabilite dall'amministrazione sono riportate nel piano di sicurezza di cui al successivo capitolo 2.
In relazione alla protezione dei dati personali trattati al proprio interno l'amministrazione dichiara di aver ottemperato a quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, con particolare riferimento:
• al principio di necessità nel trattamento dei dati;
• al diritto di accesso ai dati personali da parte dell'interessato;
• alle modalità del trattamento e ai requisiti dei dati;
• all'informativa fornita agli interessati ed al relativo consenso quando dovuto;
• alla nomina degli incaricati del trattamento, per gruppo o individualmente;
• alle misure minime di sicurezza.

1.9 Caselle di posta elettronica

L'AOO si dota di una casella di Posta Elettronica Certificata istituzionale per la corrispondenza, sia in ingresso che in uscita, pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA) e sulla homepage del proprio sito istituzionale protocollo@cert-sbt.it .
Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.
Inoltre l'AOO si dota di una casella di posta elettronica - anche di tipo tradizionale – interna, di appoggio, destinata a raccogliere tutti messaggi di posta elettronica *con annessi documenti ed eventuali allegati* destinati ad essere formalmente inviati all'esterno con la casella di posta "istituzionale" della AOO. In attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie sull'impiego della posta elettronica nelle pubbliche amministrazioni, l'amministrazione dota tutti i propri dipendenti, compresi quelli per i quali non sia

prevista la dotazione di un personal computer, di una casella di posta elettronica.

1.10 Sistema di classificazione dei documenti

Con l'inizio della attività operativa del protocollo unico viene adottato anche un unico titolario di classificazione dell'amministrazione per l'AOO che identifica l'amministrazione stessa.
Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base della organizzazione funzionale dell'AOO, permettendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.
La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico.
Il contenuto della classificazione è dettagliatamente illustrato nel successivo **Allegato 12** .

1.11 Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro della Funzione Pubblica sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione ha stabilito percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.
In particolare, considerato che il personale assegnato agli UOP deve conoscere sia l'organizzazione ed i compiti svolti da ciascun UOR/UU all'interno della AOO sia gli strumenti informatici e le norme di base per la tutela dei dati personali, la raccolta, la registrazione e l'archiviazione delle informazioni, sono stati previsti specifici percorsi formativi volti ad assicurare la formazione e l'aggiornamento professionale con particolare riferimento:

- ai processi di semplificazione ed alle innovazioni procedurali inerenti alla protocollazione e all'archiviazione dei documenti della AOO;
- agli strumenti e alle tecniche per la gestione digitale delle informazioni, con particolare riguardo alle politiche di sicurezza definite dall'Amministrazione/AOO;
- alle norme sulla protezione dei dati personali e alle direttive impartite con il documento programmatico della sicurezza.

1.12 Accreditamento dell'amministrazione/AOO all'IPA

L'amministrazione/AOO si è dotata una casella di posta elettronica istituzionale attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; l'UOP medesima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta e adotta gli opportuni metodi di conservazione in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.
L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'Indice delle Pubbliche Amministrazioni (IPA) tenuto e reso pubblico da DigitPA fornendo le seguenti informazioni che individuano l'amministrazione stessa e le AOO in cui è articolata:

- la denominazione della amministrazione;
- il codice identificativo proposto per la amministrazione;
- l'indirizzo della sede principale della amministrazione;
- l'elenco delle proprie Aree Organizzative Omogenee con l'indicazione:

- della denominazione;
- del codice identificativo;
- della casella di posta elettronica;
- del nominativo del RSP;
- della data di istituzione;
- dell'eventuale data di soppressione;
- l'elenco degli UOR e degli UU dell'AOO.

Le informazioni inerenti all'amministrazione sono riportate nell'**allegato 3**. Il codice identificativo della amministrazione associato alla sua AOO, 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.

1.13 Procedure integrative di conservazione sostitutiva

Per l'esecuzione del processo di conservazione sostitutiva dei documenti l'amministrazione si uniforma alle modalità previste dalla deliberazione CNIPA n. 11/2004. Prima di adottare eventuali accorgimenti e procedure integrative, anche successivamente all'avvio del processo di conservazione sostitutiva dei documenti, l'amministrazione comunicherà a DigitPA le procedure integrative che intende adottare ai sensi dell'art. 7 della citata deliberazione.

1.14 Eliminazione dei protocolli diversi dal protocollo informatico

In coerenza con quanto previsto e disciplinato, tutti i documenti inviati e ricevuti dall'amministrazione sono

registrati all'interno del registro di protocollo informatico. Pertanto tutti i registri particolari di protocollo sono aboliti ed eliminati.
Il protocollo informatico è già operativo dal 2004. La revisione del manuale di gestione si è resa necessaria in seguito a sviluppi normativi e alla sostituzione del prodotto di protocollo utilizzato.

2. Piano di sicurezza

Il presente capitolo riporta le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, anche in relazione alle norme sulla protezione dei dati personali.

2.1 Obiettivi del piano di sicurezza

Il piano di sicurezza garantisce che:

- i documenti e le informazioni trattati dall'amministrazione/AOO siano resi disponibili, integri e riservati;
- i dati personali comuni, sensibili e/o giudiziari vengano 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 Generalità

Il RSP ha predisposto il piano di sicurezza in collaborazione con il responsabile del sistema informativo ed il responsabile del trattamento dei dati personali e/o altri esperti di sua fiducia. Il piano di sicurezza, che si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati (personali e non), e/o i documenti trattati e sulle direttive strategiche stabilite dal vertice dell'amministrazione, definisce:

- le politiche generali e particolari di sicurezza da adottare all'interno della AOO;
- le modalità di accesso al servizio di protocollo, di gestione documentale ed archivistico;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, con particolare riferimento alle misure minime di sicurezza, di cui al disciplinare tecnico richiamato nell'allegato b) del decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, in caso di trattamento di dati personali;
- i piani specifici di formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione con cadenza almeno biennale. Esso può essere modificato anticipatamente a seguito di eventi gravi.

Il responsabile del sistema informativo ed il responsabile del trattamento dei dati personali hanno adottato le misure tecniche e organizzative di seguito specificate, al fine di assicurare la sicurezza dell'impianto tecnologico dell'AOO, la riservatezza delle informazioni registrate nelle banche dati, l'univoca identificazione degli utenti interni ed esterni:

- protezione periferica della Intranet dell'amministrazione/AOO;
- protezione dei sistemi di acceso e conservazione delle informazioni;
- assegnazione ad ogni utente del sistema di gestione del protocollo e dei documenti, di una credenziale di identificazione pubblica (user ID), di una credenziale riservata di autenticazione (password), i medesimi del sistema LDAP di autenticazione al dominio, e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno semestrale durante la fase di esercizio;
- piano di continuità del servizio con particolare riferimento, sia alla esecuzione e alla gestione delle copie di riserva dei dati e dei documenti da effettuarsi con frequenza giornaliera, sia alla capacità di ripristino del sistema informativo entro sette giorni in caso di disastro;
- conservazione, a cura del responsabile dei backup delle copie di riserva dei dati e dei documenti, in locali diversi e se possibile lontani da quelli in cui è installato il sistema di elaborazione di esercizio che ospita il PdP;
- impiego e manutenzione di un adeguato sistema antivirus e di gestione dei "moduli" (patch e service pack) correttivi dei sistemi operativi;
- cifratura o uso di codici identificativi (o altre soluzioni ad es. separazione della parte anagrafica da quella "sensibile") dei dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, allo scopo di renderli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità;
- impiego delle misure precedenti anche nel caso di supporti cartacei di banche dati idonee a rilevare lo stato di salute e la vita sessuale;
- archiviazione settimanale delle copie del registro di protocollo.

I dati personali registrati nel log del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il sistema di protocollazione e gestione dei documenti utilizzato saranno consultati solo in caso di necessità dal RSP e dal titolare dei dati e, ove previsto dalle forze dell'ordine.

2.3 Formazione dei documenti – aspetti di sicurezza

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

- l'identificabilità del soggetto che ha formato il documento e l'amministrazione/AOO di riferimento;

- la sottoscrizione dei documenti informatici, quando prescritta, con firma digitale ai sensi delle vigenti norme tecniche;
- l'idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico;
- l'accesso ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti all'interno della stessa AOO e con AOO diverse.

I documenti dell'AOO sono prodotti con l'ausilio di applicativi di videoscrittura o *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-A, XML e TIFF.

I documenti informatici prodotti dall'AOO con altri prodotti di *text editor* sono convertiti, prima della loro sottoscrizione con firma digitale, nei formati standard (PDF-A, XML e TIFF) 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. Per attribuire in modo certo la titolarità del documento, la sua integrità e, se del caso, la riservatezza, il documento è sottoscritto con firma digitale.

Nel caso si voglia attribuire una data certa a un documento informatico prodotto all'interno di una AOO, si applicano le regole per la validazione temporale e per la protezione dei documenti informatici di cui al decreto del Presidente del Consiglio dei Ministri del 13 gennaio 2004 (regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici).

L'esecuzione del processo di marcatura temporale avviene utilizzando le procedure previste dal certificatore accreditato, con le prescritte garanzie di sicurezza; i documenti così formati, prima di essere inviati a qualunque altra stazione di lavoro interna all'AOO, sono sottoposti ad un controllo antivirus onde eliminare qualunque forma di contagio che possa arrecare danno diretto o indiretto all'amministrazione/AOO.

2.4 Gestione dei documenti informatici

II sistema operativo del PdP utilizzato dall'amministrazione/AOO, è conforme alle specifiche previste dalla classe ITSEC F-C2/E2 o a quella C2 delle norme TCSEC e loro successive evoluzioni (scritture di sicurezza e controllo accessi).

Il sistema operativo del server che ospita i file utilizzati come deposito dei documenti è configurato in modo tale 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;
- garantisce la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornisce informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- 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.

2.4.1 Componente organizzativa della sicurezza

La componente organizzativa della sicurezza legata alla gestione del protocollo e della documentazione si riferisce principalmente alle attività svolte presso il sistema informatico dell'amministrazione/AOO.

Nella conduzione del sistema informativo son stati individuati un responsabile per la sicurezza dei dati ai sensi del D.Lgs 196/2003 e un responsabile delle gestione delle copie di sicurezza dei dati, dei sistemi antivirus e delle autorizzazioni utente a livello di dominio, come da atto di organizzazione del dirigente responsabile, n . 1039 del 12/07/2010 e s.m.i..

Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

Servizio Sviluppo Organizzativo e Sistemi Informativi

- Coordinamento e sviluppo del sistema di gestione documentale
- Coordinamento e sviluppo di sistemi per la conservazione sostitutiva dei documenti
- Formazione interna all'Ente in ambito tecnico-normativo legata all'uso delle tecnologie
- Stesura di regolamenti/manuali per l'utilizzo delle tecnologie nel modello organizzativo dell'ente

- Gestione tecnologica della Server Farm Comunale e della infrastruttura di rete;
- Gestione della sicurezza dei dati ai sensi del d.lgs. 196/2003 e s.m.i.;
- Gestione tecnica del nodo Internet dell'Ente e del sito WEB istituzionale;
- Assistenza agli utenti nell'uso delle attrezzature informatiche e risoluzione problematiche hardware e software di base (788);
- Gestione dei sistemi "antivirus" informatici;
- Gestione backup dei dati;
- Gestione delle autorizzazioni utente e sistemi di posta elettronica

2.4.2 Componente fisica della sicurezza

Il controllo degli accessi fisici ai luoghi in cui sono custodite le risorse del sistema informatico è regolato secondo i seguenti criteri:

- Accesso ai locali tramite tastiera numerica e codice a 6 cifre a conoscenza solo del personale del servizio Sviluppo Organizzativo e Sistemi Informativi
- Gli altri utenti possono accedere solo in presenza del personale del Servizio.
- Business continuity con ridondanza di UPS e gruppo elettrogeno dedicato
- Locali non accessibili
- Sistema antintrusione verificato nelle sue funzionalità ogni 6 mesi
- Sala server protetta da sistema antincendio dedicato controllato con periodicità annuale
- Locali del Servizio Informatica protetti da rilevatori di fumo
- Copie di sicurezza conservate in cassaforte ignifuga

2.4.3 Componente logica della sicurezza

La componente logica della sicurezza garantisce i requisiti di integrità, riservatezza, disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Tale componente, nell'ambito del PdP, è stata realizzata attraverso l'uso di:

- **ACL** (Access Control Listi) per la definizione degli accessi ai documenti (dati strutturati e file);
- Versioning per la gestione delle versioni dei documenti e conseguente tracciatura e storicizzazione delle diverse versioni succedute nel tempo;
- Gestione dei ruoli associati agli utenti
- Sistema di abilitazione all'uso multilivello:
  - Abilitazione di menu
  - Abilitazione di funzione (all'interno del menu)
  - Abilitazione di folder (all'interno della funzione)
  - Abilitazione di bottone (all'interno del folder)
  - Abilitazione di report (all'interno della funzione)
- Autenticazione degli utenti tramite LDAP
- Uso della firma digitale e dell'impronta informatica

  In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura basata su
  - server centralizzati con sistemi operativi aggiornati e protetti da sistemi antivirus
  - Sistema di backup giornaliero (incrementale) e settimanale (FULL)e virtualizzati
- Sistema di autenticazione per la connessione al dominio di rete

2.4.4 Componente infrastrutturale della sicurezza

Il sistema informatico utilizza i seguenti impianti:

- Server farm centralizzata con dispositivi server ridondati nei sistemi di storage
- Storage area network (due) connesse in FC attraverso switch ottici ridondati
- Libreria di backup su nastri e server di backup dedicato
- Sistema di firewalling e proxy clusterizzato
- Virtualizzazione di server con cluster passivo (VMWARE)
- Alimentazioni ridondate, doppio UPS (uno modulare ridondato) e gruppo elettrogeno esterno da 35KVA
- Virtual LAN per la segmentazione della rete
- Switch di rete con porte non usate disabilitate e con sistema di intrusion detection attivato

2.4.5 Gestione delle registrazioni di protocollo e di sicurezza

Le registrazioni di sicurezza sono costituite da informazioni di qualsiasi tipo (ad es. dati o transazioni) - presenti o transitate sul PdP - che è opportuno mantenere poiché possono essere necessarie sia in caso di controversie legali che abbiano ad oggetto le operazioni effettuate sul sistema stesso, sia al fine di analizzare compiutamente le cause di eventuali incidenti di sicurezza. Le registrazioni di sicurezza sono costituite:

- dai log di sistema degli accessi eseguiti dagli amministratori;
- dai log dei dispositivi di protezione periferica del sistema informatico (proxy e firewall);
- dalle registrazioni del PdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- vengono salvate periodicamente, con cadenza settimanale, su supporto non riscrivibile, previa cifratura e firma digitale del responsabile della sicurezza e poi allocate in cassaforte ignifuga ubicata in altro luogo

In questa sede viene espressamente richiamato quanto indicato nell'ultimo capoverso del paragrafo 2.2 del presente Manuale.

2.5 Trasmissione e interscambio dei documenti informatici

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.

Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario. Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre pubbliche amministrazioni, 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 server di posta certificata del fornitore esterno *(provider)* di cui si avvale l'amministrazione, 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 di amministrazioni diverse presenta, in generale, 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.

2.5.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)

Per interoperabilità dei sistemi di protocollo informatico si intende la possibilità di trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare anche le attività ed i processi amministrativi conseguenti (articolo 55, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e articolo 15 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale del 21 novembre 2000, n. 272).

Per realizzare l'interoperabilità dei sistemi di protocollo informatico gestiti dalle pubbliche amministrazioni è necessario, in primo luogo, stabilire una modalità di comunicazione comune, che consenta la trasmissione telematica dei documenti sulla rete. Ai sensi del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000, il mezzo di comunicazione telematica di base è la posta elettronica, con l'impiego del protocollo SMTP e del formato MIME per la codifica dei messaggi.

La trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica è regolata dalla circolare AIPA 7 maggio 2001, n. 28.

2.5.2 All'interno della AOO

Per i messaggi scambiati all'interno della AOO con la posta elettronica non sono previste ulteriori forme di protezione rispetto a quelle indicate nel piano di sicurezza relativo alle infrastrutture.

Gli Uffici dell'amministrazione (UOR) si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica (eventualmente certificata ai sensi del decreto del Presidente della Repubblica n. 68 dell'11 febbraio 2005) in attuazione di quanto previsto dalla direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie concernente l' "impiego della posta elettronica nelle pubbliche amministrazioni".

2.6 Accesso ai documenti informatici

Il controllo degli accessi è assicurato utilizzando le credenziali di accesso (pubblica e privata o PIN nel caso di un dispositivo rimovibile in uso esclusivo all'utente) ed un sistema di autorizzazione basato sulla profilazione degli utenti in via preventiva. La profilazione preventiva 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 elencate per settore/servizio in **Allegato 17**. Si intende ovviamente riferito al personale in organico allo specifico servizio che svolga ruolo impiegatizio e che tratti normalmente procedimenti dell'ente:

Le regole per la composizione delle password e per il blocco delle utenze è il seguente:

- Password lunghe almeno 8 caratteri
- Obbligo di utilizzare maiuscole/minuscole
- Obbligo di utilizzare almeno due cifre
- Blocco dell'account dopo il terzo tentativo errato di connessione

Le relative politiche di composizione, di aggiornamento e, in generale, di sicurezza delle password, in parte riportate di seguito, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo. Il PdP adottato dall'amministrazione/AOO:

- 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 al fine di non consentire modifiche non autorizzate.

Ciascun utente del PdP può accedere solamente ai documenti che sono stati assegnati al suo UOR, o agli Uffici Utente (UU) ad esso subordinati.
Il sistema consente altresì di associare un livello differente di riservatezza per ogni tipo di documento trattato dall'amministrazione. I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio.

2.6.1 Utenti interni alla AOO

I livelli di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti sono attribuiti dal RSP dell'amministrazione/AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i criteri operativi riportati in allegato 17.

2.6.2 Accesso al registro di protocollo per utenti interni alla AOO

La visibilità completa sul registro di protocollo è consentita solo *all'ufficio Gestione Documentale*
L'utente assegnatario dei documenti protocollati è invece abilitato alla loro accettazione/trasferimento ad altro utente e conseguentemente alla visione/modifica/trattamento del contenuto dei documenti assegnati
L'operatore che gestisce lo smistamento dei documenti può *prendere conoscenza del contenuto e smistare*
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa sul documento stesso è possibile solo *al destinatario del documento*
Tutti gli altri utenti possono accedere solo ai dati di registrazione fatto salvo per utenti che siano posizionati superiormente nella scala gerarchica dell'organizzazione i quali, pur non assegnatari devono avere la possibilità di potere prendere visione del contenuto dei documenti (ad es. un Dirigente può accedere in visione a tutti i documenti trattati dal personale del settore da lui diretto e gerarchicamente a lui subordinato*).*

2.6.3 Utenti esterni alla AOO - Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO potrà avvenire, quando sarà possibile attivare tale caratteristica, nel rispetto dei principi della cooperazione applicativa, secondo gli standard e il modello architetturale del Sistema Pubblico di Connettività (SPC) di cui al decreto legislativo 28 febbraio 2005, n. 42.
Le AOO che accederanno ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzeranno funzioni di accesso per ottenere le seguenti informazioni:

- numero e data di registrazione di protocollo del documento inviato/ricevuto, oggetto, dati di classificazione, data di spedizione/ricezione ed eventuali altre informazioni aggiuntive opzionali;
- identificazione dell'UU di appartenenza del RPA.

2.6.4 Utenti esterni alla AOO - Privati

Per l'esercizio del diritto di accesso ai documenti, sono possibili due alternative: l'accesso diretto per via telematica e l'accesso attraverso l'Ufficio Relazioni con il Pubblico (URP). L'accesso per via telematica da parte di utenti esterni all'amministrazione è consentito solo con strumenti tecnologici che permettono di identificare in modo certo il soggetto richiedente, quali: firme elettroniche, firme digitali, Carta Nazionale dei Servizi (CNS), Carta d'Identità Elettronica (CIE), sistemi di autenticazione riconosciuti dall'AOO. L'accesso attraverso l'URP prevede che questo ufficio sia direttamente collegato con il sistema di protocollo informatico e di gestione documentale sulla base di apposite abilitazioni di sola consultazione concesse al personale addetto.
Se la consultazione avviene allo sportello, di fronte all'interessato, a tutela della riservatezza delle registrazioni di protocollo, l'addetto posiziona il video in modo da evitare la diffusione di informazioni di carattere personale.
Nei luoghi in cui è previsto l'accesso al pubblico e durante l'orario di ricevimento devono essere resi visibili, di volta in volta, soltanto dati o notizie che riguardino il soggetto interessato.

2.7 Conservazione dei documenti informatici

La conservazione dei documenti informatici avverrà con le modalità e con le tecniche specificate nella deliberazione CNIPA 19 febbraio 2004, n. 11.

2.7.1 Servizio archivistico

Il responsabile del sistema archivistico dell'AOO individua la sede dell'archivio dell'amministrazione a seguito della valutazione dei fattori di rischio che incombono sui documenti (ad es. rischi dovuti all'ambiente in cui si opera, rischi nelle attività di gestione, rischi dovuti a situazioni di emergenza). Sono state pure regolamentate minutamente le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato
Il responsabile del servizio di gestione archivistica è a conoscenza, in ogni momento, della collocazione del materiale archivistico e ha predisposto degli elenchi di consistenza del materiale che fa parte dell'archivio di deposito e un registro sul quale sono annotati i movimenti delle singole unità archivistiche.
Per il requisito di "accesso e consultazione", l'AOO garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle regole tecniche vigenti, (ovvero altri formati non proprietari di seguito indicati).

2.7.2 Servizio di conservazione sostitutiva

Il responsabile della conservazione sostitutiva dei documenti fornisce le disposizioni, in sintonia con il piano generale di sicurezza e con le linee guida tracciate dal RSP, per una corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile. Per l'archiviazione ottica dei documenti sono utilizzati i supporti di memorizzazione digitale che consentono registrazioni non modificabili nel tempo.

Il responsabile della conservazione digitale:

- adotta le misure necessarie per garantire la sicurezza fisica e logica del sistema preposto al processo di conservazione digitale e delle copie di sicurezza dei supporti di memorizzazione, utilizzando gli strumenti tecnologici e le procedure descritte nelle precedenti sezioni;
- assicura il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti in caso di aggiornamento del sistema di conservazione;
- definisce i contenuti dei supporti di memorizzazione e delle copie di sicurezza;
- verifica periodicamente, con cadenza non superiore ai cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento del contenuto dei supporti.

2.7.3 Conservazione dei documenti informatici e delle registrazioni di protocollo

I luoghi di conservazione previsti per i supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza non sono differenziati e sono custoditi in cassaforte ignifuga.

È compito dell'ufficio che si occupa del servizio di sicurezza del sistema informativo l'espletamento delle seguenti procedure atte ad assicurare la corretta archiviazione, la disponibilità e la leggibilità dei supporti stessi.

L'archiviazione di ogni supporto viene registrata in un specifico file di cui è disponibile la consultazione per le seguenti informazioni:

- descrizione del contenuto;
- responsabile della conservazione;
- lista delle persone autorizzate all'accesso ai supporti, con l'indicazione dei compiti previsti;
- indicazione dell'ubicazione di eventuali copie di sicurezza;
- motivi e durata dell'archiviazione.

È stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle eventuali diverse versioni) necessari alla lettura dei supporti conservati. Presso il sistema informativo sono altresì mantenuti i sistemi con la configurazione hardware necessaria al corretto funzionamento del software.

Nell'archivio di cui al terzo capoverso del presente paragrafo, viene quindi indicato anche:

- il formato del supporto rimovibile;
- il prodotto software col quale è stato generato e la versione della release;
- la configurazione hardware e software necessaria per il suo riuso.

Deve essere inoltre indicata l'eventuale necessità di *refresh* periodico dei supporti.

II personale addetto alla sicurezza del sistema informativo verifica la corretta funzionalità del sistema e dei programmi in gestione e l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento sostitutivo del contenuto su altri supporti.

2.7.4 Conservazione delle registrazioni di sicurezza

Un operatore addetto alla sicurezza dell'amministrazione/AOO, con periodicità settimanale provvede alla memorizzazione su supporto non riscrivibile dei seguenti file di sicurezza:

- Log traffico firewall
- Log traffico proxy
- I Log degli ADS sono conservati a cura del fornitore esterno di tale servizio

I supporti così realizzati sono conservati in cassaforte ignifuga per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

2.7.5 Riutilizzo e dismissione dei supporti rimovibili

È previsto il riutilizzo dei supporti rimovibili riscrivibili (tape). Al termine del periodo di conservazione prestabilito i supporti sono cancellati con una specifica procedura operativa che garantisce la non leggibilità dei dati registrati e verifica la possibilità di un loro corretto ulteriore utilizzo.

2.8 Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza, riportate nell'**allegato 5** stabiliscono sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure per la gestione degli incidenti informatici.

Le politiche illustrate sono corredate dalle procedure sanzionatorie che l'AOO intende adottare in caso di riscontrata violazione delle prescrizioni dettate in materia di sicurezza da parte di tutti gli utenti che, a qualunque titolo, interagiscono con il servizio di protocollo, gestione documentale ed archivistica.

È compito del RSP, assistito dal *responsabile della sicurezza e tutela dei dati personali e dal responsabile del sistema informativo* procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.

II riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti di sicurezza, di variazioni tecnologiche significative, di modifiche all'architettura di sicurezza che potrebbero incidere sulla capacità di

mantenere gli obiettivi di sicurezza o portare alla modifica del livello di sicurezza complessivo, ad aggiornamenti delle prescrizioni minime di sicurezza richieste dal CNIPA o a seguito dei risultati delle attività di *audit*.
In ogni caso, tale attività è svolta almeno con cadenza annuale.

3. Modalità di utilizzo di strumenti informatici per lo scambio di documenti

Il presente capitolo fornisce indicazioni sulle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'AOO.

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 classificabile in:

- ricevuto;
- inviato;
- interno formale;
- interno informale.
- Il documento amministrativo, in termini tecnologici, è classificabile in:
- 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 che "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 o certificata;
2. su supporto rimovibile quale, ad esempio, *CD ROM, DVD, floppy disk, tape, pen drive,* etc, consegnato direttamente alla UOP o inviato per posta convenzionale o corriere.

Un documento analogico può essere recapitato:

1. a mezzo posta convenzionale o corriere;
2. a mezzo posta raccomandata;
3. per telefax o telegramma;
4. con consegna diretta da parte dell'interessato o consegnato tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

3.2 Documento inviato

I documenti informatici, compresi di eventuali allegati, anch'essi informatici, sono inviati, di norma, per mezzo della posta elettronica convenzionale o certificata se la dimensione del documento non supera la dimensione massima prevista dal sistema di posta utilizzato dall'AOO.

In caso contrario, il documento informatico viene riversato, su supporto digitale rimovibile non modificabile e trasmesso con altri mezzi di trasposto al destinatario.

3.3 Documento interno formale

I documenti interni sono formati con tecnologie informatiche.

Lo scambio tra UOR/UU di documenti informatici di rilevanza amministrativa giuridico-probatoria, avviene di norma per mezzo della posta elettronica convenzionale, o, se disponibile, di quella certificata (si può usare quella della posta Raffaello).

II documento informatico scambiato viene prima sottoscritto con firma digitale e poi protocollato.

Nella fase transitoria di migrazione verso la completa gestione informatica dei documenti, il documento interno formale può essere di tipo analogico e lo scambio può aver luogo con i mezzi tradizionali all'interno della AOO. In questo caso il documento viene prodotto con strumenti informatici, stampato e sottoscritto in forma autografa sia sull'originale che sulla minuta e successivamente protocollato.

3.4 Documento interno informale

Per questa tipologia di corrispondenza vale quanto illustrato nel paragrafo precedente ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione. Per la formazione, la gestione e la sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna AOO può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche vigenti. In questa eventualità, le diverse regole adottate saranno pubblicate nel presente MdG.

3.5 Il documento informatico

Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti; l'art. 20 del decreto legislativo del 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" prevede che:

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente codice ed alle regole tecniche di cui all'articolo 71.
2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 che garantiscano l'identificabilità dell'autore e l'integrità del documento.
3. Le regole tecniche per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

3.6 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), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale".

Di seguito faremo 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 quest'ultimo caso si definisce "originale" il documento cartaceo, nella sua redazione definitiva, perfetta ed autentica negli elementi sostanziali e formali comprendente tutti gli elementi di garanzia e di informazione del mittente e destinatario, stampato su carta intestata e dotato di firma autografa.

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

3.7 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 all'esterno o all'interno in modo formale:

- tratta un unico argomento indicato in maniera sintetica ma esaustiva a cura dell'autore nello spazio riservato all'oggetto;
- è riferito ad un solo protocollo;
- può far riferimento a più fascicoli.

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

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

- la denominazione e il logo dell'amministrazione;
- l'indicazione completa della AOO e dell'UOR che ha prodotto il documento;
- l'indirizzo completo dell'amministrazione (via, numero, CAP, città, provincia);
- il numero di telefono della UOR;
- il numero di fax della UOR protocollo;
- il codice fiscale dell'amministrazione.
- Il documento deve inoltre recare almeno le seguenti informazioni:
- luogo di redazione del documento;
- la data, (giorno, mese, anno);
- il numero di protocollo;
- il numero di repertorio (se disponibile);
- il numero degli allegati, se presenti;
- l'oggetto del documento;
- se trattasi di documento digitale, firma elettronica avanzata o qualificata da parte dell'istruttore del documento e sottoscrizione digitale del RPA e/o del responsabile del provvedimento finale;
- se trattasi di documento cartaceo, sigla autografa dell'istruttore e sottoscrizione autografa del Responsabile del Procedimento Amministrativo (RPA) e/o del responsabile del provvedimento finale.

Per agevolare il processo di formazione dei documenti informatici e consentire, al tempo stesso, la trattazione automatica dei dati in essi contenuti, l'AOO rende disponibili per via telematica moduli e formulari elettronici validi ad ogni effetto di legge.

3.8 Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente. L'amministrazione, quando non si configura come autorità di certificazione, si avvale dei servizi di una autorità di certificazione accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto da DigitPA.
I documenti informatici prodotti dall'amministrazione, 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 art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).
Nell'allegato 6 viene riportato l'elenco del documenti prodotti dalla AOO soggetti, o meno, alla sottoscrizione digitale, distinti anche per tipologia di sottoscrizione.

3.9 Requisiti degli strumenti informatici di scambio

Scopo degli strumenti informatici di scambio e degli standard di composizione dei messaggi è garantire sia l'interoperabilità, sia i requisiti minimi di sicurezza di seguito richiamati:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e smistamento dei messaggi all'interno delle AOO;
- l'interconnessione tra AOO, ovvero l'interconnessione tra le UOP/UOR e UU di una stessa AOO nel caso di documenti interni formali;
- la certificazione dell'avvenuto inoltro e ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

3.10 Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 3.9 è la firma digitale utilizzata per inviare e ricevere documenti da e per l'AOO e per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro "file" digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità. Tale processo si realizza in modo conforme a quanto prescritto dalla normativa vigente (si vedano le norme pubblicate sul sito www.cnipa.gov.it)

3.11 Verifica delle firme con il PdP

Nel PdP sono previste funzioni automatiche di verifica della firma digitale apposta dall'utente sui documenti e sugli eventuali allegati da fascicolare. La sequenza delle operazioni previste è la seguente:

- apertura della busta "virtuale" contenente il documento firmato (La busta "virtuale" è costruita secondo la standard PKCS#7 e contiene il documento, la firma digitale ed il certificato rilasciato dalla autorità di certificazione unitamente alla chiave pubblica del sottoscrittore del documento.);
- verifica della validità del certificato. Questa attività è realizzata utilizzando strumenti software gratuiti disponibili presso i siti dei certificatori
- verifica della firma (o delle firme multiple) con le stesse modalità del precedente punto
- verifica dell'utilizzo nella apposizione della firma di un certificato utente emesso da una Certification Authority (CA) presente nell'elenco pubblico dei certificatori accreditati, e segnalazione all'operatore di protocollo dell'esito della verifica;
- aggiornamento della lista delle CA accreditate al DigitPA con periodicità quindicinale;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF-A o XML o TIFF) e attribuzione della segnatura di protocollo;
- inserimento, nel sistema documentale del PdP o dell'AOO, sia del documento originale firmato, sia del documento in chiaro;

. archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del PdP per accelerare successive attività di verifica di altri documenti ricevuti

3.12 Uso della Posta Elettronica Certificata

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.
Il rispetto degli standard di protocollazione, di controllo dei medesimi e di scambio dei messaggi garantisce l'interoperabilità dei sistemi di protocollo
Allo scopo di effettuare la trasmissione di un documento da una AOO a un'altra utilizzando l'interoperabilità dei sistemi di protocollo, è necessario eseguire le seguenti operazioni:

- redigere il documento con un sistema di videoscrittura;
- inserire i dati del destinatario (almeno denominazione, indirizzo, casella di posta elettronica);

- firmare il documento (e eventualmente associare il riferimento temporale al documento firmato) e inviare il messaggio contenente il documento firmato digitalmente alla casella interna del protocollo;
- assegnare il numero di protocollo in uscita al documento firmato digitalmente;
- inviare il messaggio contenente il documento firmato e protocollato in uscita alla casella di posta istituzionale del destinatario.

L'utilizzo della Posta Elettronica Certificata (PEC) consente di:

- firmare elettronicamente il messaggio;
- conoscere in modo inequivocabile la data e l'ora di trasmissione;
- garantire l'avvenuta consegna all'indirizzo di posta elettronica dichiarato dal destinatario;
- interoperare e cooperare dal punto di vista applicativo con altre AOO appartenenti alla stessa e ad altre amministrazioni.

Gli automatismi sopra descritti consentono, in prima istanza, la generazione e l'invio in automatico di "ricevute di ritorno" costituite da messaggi di posta elettronica generati dal sistema di protocollazione della AOO ricevente. Ciascun messaggio di ritorno si riferisce ad un solo messaggio protocollato.

I messaggi di ritorno, che sono classificati in:

- conferma di ricezione;
- notifica di eccezione;
- aggiornamento di conferma;
- annullamento di protocollazione;

sono scambiati in base allo stesso standard SMTP previsto per i messaggi di posta elettronica protocollati in uscita da una AOO e sono codificati secondo lo stesso standard MIME.

II servizio di Posta Elettronica Certificata è strettamente correlato all'Indice della Pubblica Amministrazione, dove sono pubblicati gli indirizzi istituzionali di posta certificata associati alle AOO.

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 notificazione per mezzo della posta nei casi consentiti dalla legge. (gestione delle ricevute elettroniche)

4. Descrizione del flusso di lavorazione dei documenti

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

4.1 Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.

Essi si riferiscono ai documenti:

- ricevuti dalla AOO, dall'esterno o anche dall'interno se destinati ad essere ritrasmessi in modo formale in seno alla AOO;
- inviati dalla AOO, all'esterno o anche all'interno della AOO in modo formale.

Per comunicazione informale tra uffici si intende lo scambio di informazioni, con o senza documenti allegati, delle quali è facoltativa la conservazione. Questo genere di comunicazioni sono ricevute e trasmesse per posta elettronica interna e non interessano il sistema di protocollo.

I flussi dei documenti interni di tipo informale trasmessi e ricevuti vengono descritti nell'allegato 6.

4.2 Flusso dei documenti ricevuti dalla AOO

4.2.1 Provenienza esterna dei documenti

I documenti che sono trasmessi da soggetti esterni all'amministrazione sono, oltre quelli richiamati nel capitolo precedente, i telefax, i telegrammi e i supporti digitali rimovibili. Questi documenti sono recapitati alla/e UOP designata/e previa attestazione, da parte del funzionario responsabile, che assume la responsabilità in ordine alla certezza del mittente e alla necessità di protocollazione dell'atto.

I documenti che transitano attraverso il servizio postale sono ritirati quotidianamente secondo le regole stabilite dal RSP riportate nell'allegato 7.

4.2.2 Provenienza di documenti interni formali

Per sorgente interna dei documenti si intende qualunque RPA che invia formalmente la propria corrispondenza alla UOP della AOO per essere a sua volta nuovamente trasmessa, nelle forme opportune, ad altro UOR o UU della stessa AOO.

II documento è di tipo informatico secondo i formati standard illustrati nel precedente capitolo.

I mezzi principali di recapito della corrispondenza considerati sono la posta elettronica convenzionale o certificata. In tal caso la trasmissione da una UOR/UU ad altra avviene direttamente, previa protocollazione fatta dall'ufficio mittente, tramite il servizio di posta elettronica

Nel caso di trasmissione interna, se al documento sono associati allegati che superano la dimensione della casella di posta elettronica della AOO, si procede ad un riversamento (nelle forme dovute), su supporto rimovibile da consegnare al destinatario del documento.

Nella fase transitoria verso la diffusione della digitalizzazione dell'amministrazione, i documenti interni possono essere anche di tipo analogico e possono essere trasmessi tra UOR/UU anche direttamente, previa protocollazione, tra gli stessi senza necessariamente transitare per la UOP. In questo caso il mezzo di recapito del documento può essere il servizio di posta interna o il telefax o la consegna brevi manu.

4.2.3 Ricezione di documenti informatici sulla casella di posta istituzionale

Di norma la ricezione dei documenti informatici è assicurata tramite la casella di posta elettronica certificata istituzionale che è accessibile in arrivo solo alla UOP in cui si è organizzata l'AOO. Quando i documenti informatici pervengono alle UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento procede alla registrazione di protocollo.

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 comunemente scambiate tra le AOO e associate ai documenti protocollati.

Essa comprende anche i processi di verifica dell'autenticità, della provenienza e dell'integrità dei documenti stessi.

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:

- (alternativa 1) è inserito nel sistema di gestione documentale con il formato di origine apponendo la dicitura "Documento ricevuto via posta elettronica" e successivamente protocollato, smistato, assegnato e gestito. La valenza giuridico-probatoria di un messaggio così ricevuto è assimilabile a quella di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA);
- (alternativa 2) è stampato con l'apposizione della dicitura "Documento ricevuto via posta elettronica". Successivamente esso viene protocollato, smistato, assegnato, gestito e tenuto come un documento originale cartaceo.

L'addetto protocollatore controlla quotidianamente i messaggi pervenuti nella casella di posta istituzionale e verifica

se sono da protocollare.

4.2.4 Ricezione di documenti informatici sulla casella di posta elettronica non istituzionale

Nel caso in cui il messaggio viene ricevuto su una casella di posta elettronica non istituzionale o comunque non destinata al servizio di protocollazione, il messaggio viene inoltrato dal funzionario che la riceve alla casella di posta istituzionale chiedendone la protocollazione e, in questo modo, assumendo la responsabilità dell'autenticità e della provenienza dello stesso. In ogni caso il documento inoltrato deve essere corredato da idonea documentazione relativa all'identità dell'istante ai sensi dell'art. 38 del DPR 445/2000. I controlli effettuati sul messaggio sono quelli sopra richiamati.

4.2.5 Ricezione di documenti informatici su supporti rimovibili

I documenti digitali possono essere recapitati anche per vie diverse dalla posta elettronica. Considerata l'assenza di standard tecnologici e formali in materia di registrazione di file digitali, la AOO si riserva la facoltà acquisire e trattare tutti i documenti informatici ricevuti su supporto rimovibile che riesce a decodificare e interpretare con le tecnologie a sua disposizione.

Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e gli adempimenti del caso.

4.2.6 Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta o ritirati dal personale della UOP dagli uffici postali sono consegnati alla UOP.

Le buste o contenitori sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario sugli stessi apposti.

La corrispondenza relativa a bandi di gara è registrata e successivamente consegnata chiusa all'ufficio responsabile della gara.

La corrispondenza personale non deve essere aperta né protocollata, ma deve essere consegnata al destinatario che ne valuterà il contenuto ed eventualmente, nel caso dovesse riguardare l'istituzione, provvederà a inoltrarla all'ufficio protocollo per la registrazione. La corrispondenza ricevuta via telegramma o via telefax o le ricevute di ritorno della posta raccomandata, per ciò che concerne la registrazione di protocollo, sono trattate come un documento cartaceo. Quando la corrispondenza non rientra nelle categorie da ultimo indicate, si procede all'apertura delle buste e si eseguono gli ulteriori controlli preliminari alla registrazione.

La corrispondenza in arrivo è aperta il giorno lavorativo in cui è pervenuta e contestualmente protocollata. La busta si allega al documento per la parte relativa ai timbri postali.

4.2.7 Documenti cartacei ricevuti a mezzo posta convenzionale e tutela dei dati personali

Qualora la AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UOR aperta al pubblico, oltre, ovviamente alla UOP istituzionale, ovvero se per errore la corrispondenza viene recapitata ad un UOR, quest'ultimo, a tutela dei dati personali eventualmente contenuti nella missiva, non apre le buste o i contenitori ricevuti, ma rilascia ricevuta al mittente nelle forme stabilite dal RSP, e invia, nella stessa giornata, prima della chiusura del protocollo, la posta a una delle UOP abilitate e "incaricate" dell'apertura della corrispondenza e della protocollazione.

Il personale preposto alla apertura della corrispondenza è stato regolarmente autorizzato al trattamento dei dati personali.

Nei casi in cui un UOR o UU non sia stato autorizzato al trattamento dei dati personali, ma sia stato abilitato all'uso del servizio telefax e possa ricevere corrispondenza direttamente dall'esterno, avrà cura di non comunicare ai destinatari della corrispondenza il proprio numero di telefax:

- evitando di inserirlo sulla intestazione, in fase di formazione dei documenti (digitali o cartacei);
- inserendo esplicitamente sul frontespizio dei messaggi di fax, in forma chiara e leggibile, la dicitura "Inviare eventuali risposte via fax al/i numero/i "……" e non al numero sovra impresso automaticamente dal sistema di trasmissione nel documento ricevuto".

In ogni caso i documenti così ricevuti devono essere inviati a cura dell'UOR/UU in busta chiusa, nella stessa giornata, prima della chiusura del servizio di protocollo, a una delle UOP autorizzata all'apertura della corrispondenza.

4.2.8 Errata ricezione di documenti digitali

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

4.2.9 Errata ricezione di documenti cartacei

Nel caso in cui pervengano erroneamente alla UOP dell'amministrazione documenti indirizzati ad altri soggetti. Possono verificarsi le seguenti possibilità:

a) si restituisce alla posta;
b) se la busta viene aperta per errore, il documento è protocollato in entrata e in uscita inserendo nel campo oggetto una nota del tipo "documento pervenuto per errore" e si invia al mittente apponendo sulla busta la

dicitura “Pervenuta ed aperta per errore”.

4.2.10 Attività di protocollazione dei documenti

Superati tutti i controlli precedenti, i documenti, digitali o analogici, sono protocollati e “segnati” nel protocollo generale o particolare (riservato) secondo gli standard e le modalità dettagliate nel capitolo 9.

4.2.11 Rilascio di ricevute attestanti la ricezione di documenti informatici

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

Il sistema di protocollazione informatica dei documenti, in conformità alle disposizioni vigenti, provvede alla formazione e all’invio al mittente di uno dei seguenti messaggi:

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

4.2.12 Rilascio di ricevute attestanti la ricezione di documenti cartacei

Gli addetti alle UOP non possono rilasciare ricevute per i documenti che non sono soggetti a regolare protocollazione.

La semplice apposizione del timbro datario dell’UOP per la tenuta del protocollo sulla copia, non ha alcun valore giuridico e non comporta alcuna responsabilità del personale dell’UOP in merito alla ricezione ed all’assegnazione del documento. Quando il documento cartaceo è consegnato direttamente dal mittente o da altra persona incaricata ad una UOP di protocollo ed è richiesto il rilascio di una ricevuta attestante l’avvenuta consegna, la UOP che lo riceve è autorizzata a:

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

4.2.13 Conservazione dei documenti informatici

I documenti informatici sono archiviati su supporti di memorizzazione, in modo non modificabile, contestualmente alle operazioni di registrazione e segnatura di protocollo. I documenti ricevuti per via telematica sono resi disponibili agli UU, attraverso la rete interna dell’amministrazione/AOO, subito dopo l’operazione di smistamento e di assegnazione.

4.2.14 Conservazione delle rappresentazioni digitali di documenti cartacei

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, possono essere acquisiti in formato immagine attraverso un processo di scansione.

II processo di scansione avviene in diverse fasi:

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

Le rappresentazioni digitali dei documenti cartacei sono archiviate, secondo le regole vigenti, su supporti di memorizzazione, in modo non modificabile al termine del processo di scansione. L’addetto alla UOP che effettua la scansione deve siglare digitalmente, con Firma digitale, il documento informatico ottenuto dalla scansione.

I documenti cartacei dopo l’operazione di riproduzione in formato immagine e conservazione sostitutiva ai sensi della delibera CNIPA 19 febbraio 2004 n.11 vengono inviati agli UOR/UU/RPA destinatari per le operazioni di fascicolazione e conservazione.

I documenti con più destinatari, sono riprodotti in formato immagine ed inviati solo in formato elettronico. *(*- Il documento cartaceo originale viene inviato al primo destinatario).

Qualora effettuata, la riproduzione dei documenti cartacei in formato immagine viene eseguita sulla base dei seguenti criteri:

- se il documento ricevuto in formato A4 o A3 non supera le 20 pagine viene acquisito direttamente con le risorse, umane e strumentali, interne all'AOO;
- se il documento ha una consistenza maggiore o formati diversi dai precedenti, viene acquisito in formato

immagine solo se esplicitamente richiesto dagli UOR/UU/RPA di competenza, avvalendosi eventualmente dei servizi di una struttura esterna specializzata. In questo caso il RSP, insieme al RPA, individua i documenti da sottoporre al processo di scansione e ne fissa i tempi, diversi da quelli ordinari, e le modalità esecutive.

In ogni caso non vengono riprodotti in formato immagine i seguenti documenti:

- i certificati medici contenenti la diagnosi,
- Planimetrie allegate a progetti edili o di urbanizzazione, dei quali non sia stata richiesta la loro forma digitale.
- Allegati rilegati dei quali sia impossibile la scansione senza la destrutturazione degli stessi.

4.2.15 Classificazione, assegnazione e presa in carico dei documenti

Gli addetti alla UOP eseguono la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione adottato presso l'AOO e provvedono ad inviarlo all'UOR di destinazione che:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore, il documento è ritrasmesso alla UOP di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA.

4.2.16 Conservazione dei documenti nell'archivio corrente

Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

1. classificazione di livello superiore sulla base del titolario di classificazione adottato dall'AOO;
2. fascicolazione del documento secondo le procedure previste dall'AOO;
3. inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

4.2.17 Conservazione dei documenti e dei fascicoli nella fase corrente

All'interno di ciascun ufficio utente di ciascun UOR della AOO sono stati individuati e formalmente incaricati gli addetti alla organizzazione e tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla conservazione dei documenti al loro interno. Generalmente i responsabili della conservazione dei documenti e dei fascicoli nella fase corrente sono gli stessi RPA.

4.3 Flusso dei documenti inviati dalla AOO

4.3.1 Sorgente interna dei documenti

Per sorgente interna (all'AOO) dei documenti si intende l'unità organizzativa mittente interna all'AOO che invia, tramite il RPA, la corrispondenza alla UOP della AOO stessa affinché sia trasmessa, nelle forme e nelle modalità più opportune, ad altra amministrazione, ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Per documenti in partenza s'intendono quelli prodotti dal personale degli uffici dell'AOO nell'esercizio delle proprie funzioni avente rilevanza giuridico-probatoria e destinati ad essere trasmessi ad altra amministrazione ovvero ad altro ufficio (UU o UOR) della stessa AOO.

Il documento è in formato digitale formato secondo gli standard illustrati nei precedenti capitoli.

Nel caso di trasmissione interna di allegati al documento di cui sopra che possono superare la capienza della casella di posta elettronica si procede ad un riversamento (con le modalità previste dalla normativa vigente), su supporto rimovibile da consegnare al destinatario contestualmente al documento principale.

I documenti in partenza contengono l'invito al destinatario a riportare i riferimenti della registrazione di protocollo della lettera alla quale si da riscontro.

Durante la fase transitoria di migrazione verso l'utilizzo di un sistema di gestione documentale interamente digitale, il documento può essere in formato analogico. I mezzi di recapito della corrispondenza in quest'ultimo caso sono il servizio postale, nelle sue diverse forme, ed il servizio telefax.

4.3.2 Verifica formale dei documenti

Ogni UOR è autorizzata dall'AOO per il tramite del RSP, a svolgere attività di registrazione di protocollo e apposizione della segnatura per la corrispondenza in uscita e/o interna formale. Di conseguenza tutti i documenti originali da spedire, siano essi informatici o analogici, sono direttamente protocollati e spediti dagli UOR.

Gli UOR provvedono ad eseguire al loro interno le verifiche di conformità della documentazione predisposta per essere trasmessa con le stesse modalità descritte nel capitolo precedente.

Se la verifica da esito positivo, il documento viene registrato nel registro di protocollo generale o particolare; in caso contrario è restituito al mittente UU/RPA con le osservazioni del caso.

4.3.3 Registrazione di protocollo e segnatura

La spedizione è centralizzata

La compilazione di moduli se prevista (ad es. nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere) è a cura degli UOR/UU/RPA mittenti.

La protocollazione e la segnatura della corrispondenza in partenza, sia essa in formato digitale che in formato analogico, è effettuata direttamente dai singoli RPA/UU/UOR abilitati in quanto collegati al sistema di protocollo informatico della AOO a cui appartengono. Le attività di registrazione degli elementi obbligatori e degli elementi accessori del protocollo e la relativa segnatura della missiva da inviare sono effettuate dal RPA. Il documento registrato presso il protocollo riservato è contrassegnato anteponendo al numero della segnatura una sigla (ad es. "RIS").

4.3.4 Trasmissione di documenti informatici

Le modalità di composizione e di scambio dei messaggi, il formato della codifica e le misure di sicurezza sono conformi alla circolare AIPA 7 maggio 2001, n. 28.
I documenti informatici sono trasmessi all'indirizzo elettronico dichiarato dai destinatari, ovvero abilitato alla ricezione della posta per via telematica (il destinatario può essere anche interno alla AOO).
Per la spedizione dei documenti informatici l'AOO si avvale dei servizi di autenticazione e marcatura temporale offerti da un certificatore accreditato iscritto nell'elenco pubblico tenuto dal CNIPA.
Per la spedizione dei documenti informatici, l'AOO si avvale di un servizio di "Posta Elettronica Certificata", conforme al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che può essere offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio di ricevute di ritorno elettroniche.
L'Ente si avvale dei servizi di "Postecom spa".
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, dell'esistenza o del contenuto della corrispondenza, delle comunicazioni o dei messaggi trasmessi per via telematica, salvo che si tratti di informazioni che per loro natura o per espressa indicazione del mittente sono destinate ad essere rese pubbliche.

4.3.5 Trasmissione di documenti cartacei a mezzo posta

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza, operando anche in base agli accordi contrattuali in essere con il soggetto terzo che provvederà alla trasmissione fisica della posta, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici . L'UOP conserva, temporaneamente, la minuta da restituire al mittente.

4.3.6 Affrancatura dei documenti in partenza

L'UOP provvede alle operazioni necessarie, se non diversamente disposto da apposite convenzioni con il soggetto affidatario del servizio di spedizione, per l'invio della corrispondenza in partenza.
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP secondo le regole richiamate nell'allegato 7.

4.3.7 Conteggi spedizione corrispondenza

L'UOP effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

4.3.8 Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno, e comunque in numero maggiore di tre, può essere autorizzata la spedizione di copie dell'originale. L'elenco dei destinatari, in formato cartaceo, è allegato alla minuta.

4.3.9 Trasmissione di documenti cartacei a mezzo telefax

Sul documento trasmesso via fax può essere apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale". Solo su richiesta del destinatario verrà trasmesso anche l'originale.
Le ricevute della avvenuta trasmissione sono trattenute dagli UOR/UU/RPA che hanno effettuato la trasmissione.

4.3.10 Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.
Le UOP di protocollo che effettuano la spedizione centralizzata di documenti informatici o cartacei curano anche l'invio delle ricevute di ritorno al mittente che si fa carico di archiviarle nel fascicolo logico o fisico.
Gli UOR che effettuano la spedizione di documenti informatici o cartacei direttamente curano anche l'archiviazione delle ricevute di ritorno.

5. Regole di smistamento ed assegnazione dei documenti ricevuti

Il presente capitolo riporta le regole di smistamento ed assegnazione dei documenti ricevuti.

5.1 Regole disponibili con il PdP

Le AOO che fruiscono del servizio di protocollo con il proprio PdP eseguono lo smistamento e l'assegnazione dei documenti protocollati e segnati adottando le funzionalità di seguito illustrate:
L'attività di smistamento consiste nell'operazione di inviare un documento protocollato e segnato all'UOR competente in base alla classificazione di primo livello del titolario, o della relativa competenza o per indirizzamento diretto all'UOR del documento stesso. Con l'assegnazione si provvede al conferimento della responsabilità del procedimento amministrativo ad un soggetto fisico e alla trasmissione del materiale documentario oggetto di lavorazione.
Effettuato lo smistamento e l'assegnazione, il RPA provvede alla presa in carico del documento allo stesso assegnato.
L'assegnazione può essere effettuata per conoscenza o per competenza. L'UOR competente è incaricato della gestione del procedimento a cui il documento si riferisce e prende in carico il documento.
I documenti che sono immediatamente riconducibili ad una specifica UOR e/o materia, vengono inoltrati direttamente dalla UOP.
I termini per la definizione del procedimento amministrativo che prende avvio dal documento, decorrono comunque dalla data di protocollazione.
Il sistema di gestione informatica dei documenti memorizza tutti i passaggi, conservando, per ciascuno di essi, l'identificativo dell'utente che effettua l'operazione, la data e l'ora di esecuzione.
La traccia risultante definisce, ai fini normativi e regolamentari, i tempi del procedimento amministrativo ed i conseguenti riflessi sotto il profilo della responsabilità. Nell'allegato 17 sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.
Lo smistamento iniziale eseguito dalla/e UOP recapita ai dirigenti di ciascuna UOR, attraverso funzioni specifiche del sistema di protocollo informatico, i documenti indirizzati all'UOR medesimo.
Quest'ultimi, dopo averne preso visione, provvedono ad accettarli e ad assegnarli ai propri UU/RPA, oppure in caso di errore, ad informare il mittente (UOP) e a smistare la notifica ad altro UOR.
L'UOR del procedimento amministrativo indica, sul documento in arrivo, il nominativo del RPA. Qualora non sia diversamente specificato il RPA coincide con il dirigente dell'UOR.

5.2 Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione al direttore generale , o in sua assenza/mancanza di nomina, al segretario generale, che provvede ad individuare l'UOR competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

5.3 Assegnazione dei documenti ricevuti in formato digitale

I documenti ricevuti dall'AOO per via telematica, o comunque disponibili in formato digitale, sono assegnati all'UOR competente attraverso i canali telematici dell'AOO al termine delle operazioni di registrazione, segnatura di protocollo, memorizzazione su supporti informatici in modo non modificabile.
L'UOR competente ha notizia dell'arrivo della posta ad esso indirizzata tramite un messaggio di posta elettronica
Il responsabile dell'UOR può visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente per la materia a cui si riferisce il documento.

La "presa in carico" dei documenti informatici viene registrata dal PdP in modo automatico e la data di ingresso dei documenti negli UOR competenti coincide con la data di assegnazione degli stessi. I destinatari del documento per "competenza" lo ricevono esclusivamente in formato digitale.

5.4 Assegnazione dei documenti ricevuti in formato cartaceo

I documenti ricevuti dall'amministrazione in formato cartaceo, se successivamente acquisiti in formato immagine con l'ausilio di scanner, una volta concluse le operazioni di registrazione, di segnatura e di assegnazione, sono fatti pervenire al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione/AOO. L'originale cartaceo può essere successivamente trasmesso al RPA oppure essere conservato dalla UOP. L'UOR competente ha notizia dell'arrivo del documento ad essa indirizzata t**ramite un messaggio di posta elettronica.**
Il responsabile dell'UOR può visualizzare i documenti, attraverso l'utilizzo dell'applicazione di protocollo informatico e in base alle abilitazioni previste potrà:

- visualizzare gli estremi del documento;
- visualizzare il contenuto del documento;
- individuare come assegnatario il RPA competente sulla materia oggetto del documento.

La “presa in carico” dei documenti informatici viene registrata dal sistema in modo automatico e la data di ingresso dei documenti negli UOR di competenza coincide con la data di assegnazione degli stessi.
Il ritiro giornaliero della corrispondenza cartacea in arrivo da parte degli UOR/UU/RPA avviene presso la UOP ricevente/i.

5.5 Modifica delle assegnazioni

Nel caso di assegnazione errata, l’UOR/UU che riceve il documento, se è abilitato all’operazione di smistamento, provvede a trasmettere l’atto all’UOR competente, in caso contrario comunica l’errore alla UOP che ha erroneamente assegnato il documento, che procederà ad una nuova assegnazione.
Nel caso in cui un documento assegnato erroneamente ad un UU afferisca a competenze attribuite ad altro UU dello stesso UOR, l’abilitazione al relativo cambio di assegnazione è attribuita al dirigente della UOR medesima o a persona da questi incaricata. 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.

6. UO responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti

Il presente capitolo individua le unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e di tenuta dei documenti all'interno della AOO. In base al modello organizzativo adottato dall'Amministrazione/AOO, nell'allegato 3 è riportato l'elenco delle unità organizzative responsabili delle attività di registrazione del protocollo (UOP). Relativamente alla organizzazione e alla tenuta dei documenti dell'amministrazione all'interno della AOO, sono istituiti il servizio archivistico e eventualmente il servizio per la conservazione sostitutiva e sono definite le strutture dedicate alla conservazione dei documenti.

I servizi in argomento sono stati identificati e formalizzati prima di rendere operativo il servizio di gestione informatica del protocollo, dei documenti e degli archivi.

6.1 Servizio archivistico

L'amministrazione ha istituito il servizio archivistico.

6.2 Servizio della conservazione elettronica dei documenti

Il servizio in parola è realizzato al fine di trasferire su supporto informatico rimovibile le informazioni:

- del protocollo informatico;
- della gestione dei documenti:

- relative ai fascicoli che fanno riferimento a procedimenti conclusi;
- riversamento su nuovi supporti informatici per garantire nel tempo la leggibilità dei medesimi.

Il ruolo di pubblico ufficiale per la chiusura dei supporti rimovibili è svolto dal dirigente dell'ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per i casi nei quali si richiede l'intervento di soggetto diverso della stessa amministrazione.

Il responsabile delle procedure di conservazione sostitutiva, può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone dell'AOO che, per competenza ed esperienza, garantiscano la corretta esecuzione di tali operazioni. L'amministrazione si riserva la facoltà di affidare, in tutto o in parte, ad altri soggetti, pubblici o privati, il procedimento di conservazione e di riversamento; questi sono tenuti ad osservare quanto previsto dalle norme vigenti in materia di protocollo e protezione dei dati personali (integrate, all'occorrenza, da specifici richiami contrattuali).

Nel caso di affidamento a "soggetto esterno", l'amministrazione provvede ad incaricare formalmente tale soggetto (ad esempio Società di servizi, Consulente, ecc) delle attività di conservazione e riversamento e nel contempo lo diffida dal comunicare o diffondere, anche accidentalmente, gli eventuali dati personali comuni, sensibili e/o giudiziari presenti nei supporti oggetto di copia e di riversamento.

6.2.1 Archiviazione ottica dei documenti analogici

Il RSP, o il responsabile del servizio archivistico, se distinto dal primo, valutati i costi ed i benefici, può proporre l'operazione di conservazione sostitutiva dei documenti analogici su supporti di memorizzazione sostitutivi del cartaceo in conformità alle disposizioni vigenti.

6.2.2 Archiviazione ottica dei documenti digitali

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

Qualora il processo riguardi documenti informatici sottoscritti è richiesta anche l'apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d'origine.

7. Elenco dei documenti esclusi dalla protocollazione e dei documenti soggetti a registrazione particolare

7.1 Documenti esclusi

Sono esclusi dalla registrazione di protocollo, le tipologie di documenti riportati nell'allegato 9.
Sono inoltre esclusi dalla registrazione di protocollo tutti i documenti di cui all'art. 53 comma 5 del decreto del Presidente della Repubblica 20 dicembre 2000, n. 445.

7.2 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 10.
Tale tipo di registrazione consente comunque di eseguire su tali documenti tutte le operazioni previste nell'ambito della gestione dei documenti, in particolare la classificazione, la fascicolazione, la repertoriazione.
Questi documenti costituiscono comunque delle serie di interesse archivistico, ciascuna delle quali deve essere corredata da un repertorio contenente le seguenti informazioni:

- dati identificativi di ciascun atto (persona fisica o giuridica che adotta il documento, data di adozione, oggetto….);
- numero di repertorio, un numero progressivo;
- dati di classificazione e di fascicolazione.

8. Sistema di classificazione, fascicolazione e piano di conservazione

8.1 Protezione e conservazione degli archivi pubblici

8.1.1 Generalità

Il presente capitolo riporta il sistema di classificazione dei documenti, di formazione del fascicolo e 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 sostitutivi 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 piano di conservazione, collegato con il titolario ed elaborato tenendo conto dei flussi documentali dipendenti dai procedimenti e dalle prassi seguiti dall'AOO nell'espletamento delle funzioni istituzionali, definisce i tempi di conservazione dei documenti e dei fascicoli nella sezione di deposito dell'archivio. Il piano di conservazione preso in considerazione, riportato nell'allegato 11, è quello formulato nel 2005 dal Gruppo di lavoro all'uopo costituitosi all'interno del Ministero per i Beni e le Attività culturali.

8.1.2 Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici **territoriali** e non 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'AOO, di norma mediante l'attribuzione di un numero di protocollo e di un codice di classificazione.

L'archivio non può essere smembrato, a qualsiasi titolo, e deve essere conservato nella sua organicità. Il trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.

L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della Soprintendenza archivistica per la Regione Marche.

Lo scarto dei documenti degli archivi delle amministrazioni/AOO statali è subordinato all'autorizzazione della Soprintendenza archivistica per la Regione Marche.

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

8.2 Titolario o piano di classificazione

8.2.1 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'ente. 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, etc. Il titolo (o la voce di I livello) individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni (classi, sottoclassi, etc.) corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato 12.

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 della funzione di governo dell'amministrazione.

Il titolario è uno strumento suscettibile di aggiornamento: esso deve infatti descrivere le funzioni e le competenze dell'ente, soggette a modifiche in forza delle leggi e dei regolamenti statali e/o regionali.

L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP (oppure, su proposta del responsabile dell'archivio generale dell'amministrazione e/o dalle autorità competenti per materia).

La revisione anche parziale del titolario viene proposta dal RSP quando è necessario ed opportuno.

Dopo ogni modifica del titolario, il RSP 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.

Viene garantita 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 modifica di una voce viene riportata la data di introduzione 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 valgono almeno per l'intero anno. Rimane possibile, se il sistema lo consente, registrare documenti in fascicoli già aperti fino alla conclusione e chiusura degli stessi.

8.2.2 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 dagli UOR dell'AOO, indipendentemente dal supporto sul quale vengono formati, sono classificati in base al sopra citato titolario.
Qualora l'ente lo ritenga opportuno, le operazioni di classificazione possono essere svolte in momenti diversi: l'addetto alla registrazione di protocollo può inserire la voce di livello più alto, mentre l'attribuzione delle voci di dettaglio è demandata all'incaricato della trattazione della pratica.

8.3 Fascicoli e dossier

8.3.1 Fascicolazione dei documenti

Ogni documento, dopo la sua classificazione, viene inserito nel fascicolo di riferimento. I documenti sono archiviati all'interno di ciascun fascicolo o, all'occorrenza, sottofascicolo o inserto, secondo l'ordine cronologico di registrazione.

8.3.2 Apertura del fascicolo

Qualora un documento dia luogo all'avvio di un nuovo procedimento amministrativo, in base all'organizzazione dell'ente, il soggetto preposto (quale, ad esempio, RPA, RSP, responsabile del servizio archivistico addetto alla protocollazione, etc.) 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, etc);
- numero del fascicolo;
- oggetto del fascicolo, individuato sulla base degli standard definiti dall'amministra-zione/AOO;
- data di apertura del fascicolo;
- AOO e UOR;
- collocazione fisica, di eventuali documenti cartacei;
- collocazione logica, dei documenti informatici;
- livello di riservatezza, se diverso da quello standard applicato dal sistema.

Il fascicolo di norma viene aperto all'ultimo livello della struttura gerarchica del titolario. Le informazioni di cui sopra, compaiono sulla camicia del fascicolo. Un esempio di "camicia di fascicolo" è riportato nell'allegato 13.

8.3.3 Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o all'esaurimento dell'affare.
La data di chiusura si riferisce alla data dell'ultimo documento prodotto.
Esso viene archiviato rispettando l'ordine di classificazione e la data della sua chiusura.
Gli elementi che individuano un fascicolo sono gestiti dal soggetto di cui al paragrafo 8.3.2, primo capoverso, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

8.3.4 Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'amministrazione, l'UOR abilitato all'operazione di fascicolazione stabilisce, con l'ausilio delle funzioni di ricerca del sistema di protocollo informatizzato, se il documento stesso 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 *affare o procedimento in corso,* l'addetto:
    - seleziona il relativo fascicolo;
    - collega la registrazione di protocollo del documento al fascicolo selezionato;
    - invia il documento all'UOR cui è assegnata la pratica. (Se si tratta di un documento su supporto cartaceo, assicura l'inserimento fisico dello stesso nel relativo fascicolo).
- Se il documento dà 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;
    - assegna il documento ad un istruttore su indicazione del responsabile del procedimento;
    - invia il documento con il relativo fascicolo al dipendente che dovrà istruire la pratica per competenza.

8.3.5 Modifica delle assegnazioni dei fascicoli

Quando si verifica un errore nella assegnazione di un fascicolo, l'ufficio abilitato all'operazione di fascicolazione provvede a correggere le informazioni inserite nel sistema informatico e ad inviare il fascicolo all'UOR di competenza.
Il sistema di gestione informatizzata dei documenti tiene traccia di questi passaggi, memorizzando per ciascuno di essi l'identificativo dell'operatore di UU che effettua la modifica con la data e l'ora dell'operazione.

8.3.6 Repertorio dei fascicoli

I fascicoli sono annotati nel repertorio dei fascicoli.

Il repertorio dei fascicoli, ripartito per ciascun 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. Nel repertorio sono indicati:

- la data di apertura;
- l'indice di classificazione completo (titolo, classe, sottoclasse, etc);
- il numero di fascicolo (ed altre eventuali partizioni in sottofascicoli e inserti);
- la data di chiusura;
- l'oggetto del fascicolo (ed eventualmente l'oggetto dei sottofascicoli e inserti);
- l'annotazione sullo status relativo al fascicolo, se cioè sia ancora una "pratica" corrente, o se abbia esaurito la valenza amministrativa immediata e sia quindi da mandare in deposito, oppure, infine, se sia da scartare o da passare all'archivio storico;
- l'annotazione sullo stato della pratica a cui il fascicolo si riferisce (pratica in corso da inserire nell'archivio corrente, pratica chiusa da inviare all'archivio di deposito, pratica chiusa da inviare all'archivio storico o da scartare).

Il repertorio dei fascicoli è costantemente aggiornato.

8.3.7 Apertura del dossier

La formazione di un nuovo dossier avviene attraverso l'operazione di "apertura" che prevede l'inserimento delle seguenti informazioni essenziali:

- il numero del dossier;
- la data di creazione;
- il responsabile del dossier;
- la descrizione o oggetto del dossier;
- la sigla della AOO e dell'UOR;
- l'elenco dei fascicoli contenuti;
- il livello di riservatezza del dossier (viene, di norma, assegnato dal livello di riservatezza del fascicolo a più alto livello di riservatezza).

8.3.8 Repertorio dei dossier

I dossier, di norma, sono annotati nel repertorio dei dossier.

II repertorio dei dossier è lo strumento di gestione e reperimento dei dossier. Nel repertorio sono indicati:

- il numero del dossier;
- la data di creazione;
- la descrizione o oggetto del dossier;
- il responsabile del dossier.

Il repertorio dei dossier è costantemente aggiornato.

8.4 Serie archivistiche e repertori

8.4.1 Serie archivistiche

La serie archivistica consiste in un raggruppamento di unità archivistiche (documenti, fascicoli, registri) riunite o per caratteristiche omogenee, quali la natura e la forma dei documenti (es. le determinazioni, i contratti, i registri di protocollo) oppure in base alla materia trattata, all'affare o al procedimento al quale afferiscono (es. i fascicoli personali, le pratiche di finanziamento e in generale le pratiche attivate dall'amministrazione nello svolgimento dell'attività istituzionale).

Le serie documentarie sono formate dai registri e dai relativi fascicoli compresi in un arco d'anni variabile.

I fascicoli subiscono il processo di selezione e scarto dei documenti; le serie così composte, faranno parte, successivamente, della sezione storica dell'archivio. [Riferimento: art. 41 comma 3 D. Lgs. 42/2004; DPR 8 gennaio 2001 n. 37, art.10, *regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di vigilanza sugli archivi e per lo scarto dei documenti degli uffici dello Stato* (entrambe le disposizioni si riferiscono agli Archivi di Stato e dunque agli archivi statali, ma per prassi si applicano anche agli archivi pubblici non statali, per i quali non esiste una norma analoga; lo scarto dei documenti degli archivi pubblici e degli archivi privati dichiarati di interesse storico particolarmente importante è disciplinato dall'art. 21, comma 1, lett. *d)* dello stesso decreto legislativo 42/2004)].

8.4.2 Repertori e serie archivistiche

I documenti soggetti a registrazione particolare, come i verbali, le delibere degli organi di governo dell'amministrazione, o i contratti, costituiscono una serie archivistica. Tali documenti sono organizzati nel registro di repertorio.

Con riguardo alla gestione dei documenti cartacei, è previsto che per ogni verbale, delibera, determinazione, decreto, ordinanza e contratto siano, di norma, prodotti almeno due originali, di cui:

- uno viene inserito nel registro di repertorio con il numero progressivo di repertorio;
- l'altro, viene conservato nel relativo fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Per quanto concerne la gestione dei documenti informatici, ogni verbale, delibera, determinazione, decreto, ordinanza e contratto è, di norma, associato:

- al registro di repertorio con il numero progressivo di repertorio;
- al fascicolo, insieme ai documenti che afferiscono al medesimo affare o procedimento amministrativo.

Nel repertorio generale sono riportati gli elementi obbligatori del documento (data, classifica e numero di repertorio) che identificano il documento all'interno del repertorio stesso.
II repertorio è costantemente aggiornato.
All'interno dell'amministrazione sono istituiti i repertori generali indicati nell'Allegato 14.

8.4.3 Versamento dei fascicoli nell'archivio di deposito

La formazione dei fascicoli (virtuali o tradizionali), delle serie e dei repertori è una funzione fondamentale della gestione archivistica.
Periodicamente, e comunque almeno una volta all'anno, il RSP provvede a trasferire i fascicoli e le serie documentarie relativi ai procedimenti conclusi in un apposita sezione di deposito dell'archivio generale costituito presso l'amministrazione/AOO. Per una regolare e costante "alimentazione" dell'archivio di deposito lo stesso responsabile dell'archivio stabilisce tempi e modi di versamento dei documenti, organizzati in fascicoli, serie e repertori, dagli archivi correnti dei diversi UOR/UU dell'amministrazione/AOO all'archivio di deposito.
Con la stessa metodologia vengono riversati nell'archivio di deposito anche gli altri repertori generali.
La regolare periodicità dell'operazione è fondamentale per garantire l'ordinato sviluppo (o il regolare accrescimento) dell'archivio di deposito.
Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente. Prima di effettuare il conferimento di cui sopra, il RPA/UU procede alla verifica:

- dell'effettiva conclusione ordinaria della pratica;
- dell'avvenuta annotazione dell'esaurimento della pratica nel registro di repertorio dei fascicoli;
- della corretta indicazione della data di chiusura sulla camicia del fascicolo;

Il RPA/UU provvede inoltre:

- allo scarto di eventuali copie e fotocopie di documentazione di cui è possibile l'eliminazione al fine di garantire la presenza di tutti e soli i documenti relativi alla pratica trattata senza inutili duplicazioni;
- a verificare che il materiale da riversare sia correttamente organizzato e corredato da strumenti che ne garantiscano l'accesso organico.

Ricevuti i fascicoli e controllato l'aggiornamento del relativo repertorio, il RSP predispone un elenco di "versamento" da inviare al servizio archivistico. Copia di detto elenco viene conservata dal responsabile che ha versato la documentazione.
I fascicoli che riguardano il personale devono essere trasferiti dall'archivio corrente all'archivio di deposito l'anno successivo a quello di cessazione dal servizio.

8.4.4 Verifica della consistenza del materiale riversato nell'archivio di deposito

L'ufficio ricevente esegue il controllo del materiale riversato.
II servizio archivistico dell'amministrazione/AOO riceve agli atti soltanto i fascicoli con materiale ordinato e completo.
Il fascicolo che in sede di controllo risulta mancante di uno o più documenti ovvero presenti delle incongruenze deve essere restituito agli UOR/UU tenutari dell'archivio corrente, affinché provvedano alla integrazione e/o correzioni necessarie.
Nell'eventualità che non sia stato possibile recuperare uno o più documenti mancanti, il responsabile degli UOR deposita il fascicolo dichiarando ufficialmente che è incompleto e si assume la responsabilità della trasmissione agli atti.
Ricevuti i fascicoli e controllato il relativo elenco, il responsabile del servizio archivistico dell'amministrazione firma per ricevuta l'elenco di consistenza.

8.5 Piano di conservazione

L'art. 68 del DPR 445/2000 prevede che ogni amministrazione debba dotarsi di un «piano di conservazione degli archivi, integrato con il sistema di classificazione, per la definizione dei criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti»..
L'adozione del titolario, studiato alla luce della interoperabilità tra sistemi informativi diversi, comporta come conseguenza l'adozione del piano di conservazione che da esso discende.
In merito allo scarto archivistico, è opportuno ricordare che gli enti pubblici – e tra questi i Comuni – devono ottenere per tale intervento l'autorizzazione del Ministero per i beni e le attività culturali, ai sensi dell'art. 21, comma 1, lettera d) del Codice dei beni culturali e del paesaggio (D. lgs. 22 gennaio 2004, n. 42).

8.5.1 -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.

Il materiale non archivistico non viene preso in considerazione dal Piano di Classificazione, 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.In genere, salvo poche eccezioni, tutti i repertori devono essere conservati permanentemente.

 Il Comune non deve scartare i documenti considerati "vitali" (quelli che in caso di disastro, sono necessari a ricreare lo 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).

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.…

Documenti originali e copia sfoltimento dei fascicoli

È 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.

8.6 Scarto, selezione e riordino dei documenti

8.6.1 Operazione di scarto

Nell'ambito della sezione di deposito dell'archivio viene effettuata la selezione della documentazione da conservare perennemente e lo scarto degli atti che l'amministrazione non ritiene più opportuno conservare ulteriormente, allo scopo di conservare e garantire il corretto mantenimento e la funzionalità dell'archivio, nell'impossibilità pratica di conservare indiscriminatamente ogni documento.

Un documento si definisce scartabile quando ha perso totalmente la sua rilevanza amministrativa e non ha assunto alcuna rilevanza storica.

La legge impone all'amministrazione/AOO l'uso di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio.

Le operazioni di selezione e scarto sono effettuate, sotto la vigilanza del RSP (o da persona delegata, ad esempio il responsabile dell'archivio), a cura degli addetti del servizio archivistico.

8.6.2 Conservazione del materiale presso la sezione di deposito dell'archivio

L'operazione di riordino della sezione di deposito dell'archivio viene effettuata con la periodicità stabilita dall'amministrazione/AOO e consiste nella schedatura dei materiali e nell'organizzazione delle schede.

L'operazione si conclude con la sistemazione fisica del materiale, mediante l'inserimento in unità di condizionamento (scatole, pallets, etc.) che riportano all'esterno l'indicazione del contenuto, la classificazione e i tempi di conservazione dei documenti.

E' possibile affidare la conservazione dei documenti versati all'archivio di deposito anche ad aziende terze che garantiscano la perfetta conservazione, sia fisica che logica, e allo stesso tempo garantiscano la possibilità di prendere visione, ottenere copia o trasformazione del cartaceo in originale informatico, in qualsiasi momento e in tempi inferiori alle 24/48 ore.

8.6.3 Versamento dei documenti nell'archivio storico

Gli enti pubblici, territoriali e non, trasferiscono al proprio archivio storico i documenti relativi agli affari esauriti da oltre quarant'anni unitamente agli strumenti che ne garantiscono la consultazione.

I trasferimenti vengono effettuati dopo il completamento delle operazioni di scarto.

Presso l'archivio storico i documenti vengono inventariati al fine della conservazione, consultazione e valorizzazione.

8.7 Consultazione e movimentazione dell'archivio corrente, di deposito e storico

8.7.1 Principi generali

La richiesta di consultazione, che può comportare la movimentazione dei fascicoli, può pervenire dall'interno dell'amministrazione/AOO oppure da utenti esterni all'amministrazione, per scopi giuridico-amministrativi o per scopi storici.

8.7.2 Consultazione ai fini giuridico-amministrativi

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 e s.m.i. che qui di seguito si riporta.

Esclusione dal diritto di accesso.

1. Il diritto di accesso è escluso:

a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;

b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;

c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;

d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.

2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.

3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:

e) quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione;

f) Quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;

g) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini;

h) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono;

i) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. 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".

8.7.3 Consultazione per scopi storici

La richiesta di consultazione ai fini di ricerca per scopi storici è disciplinata dal regolamento emanato da ciascuna amministrazione/AOO. Per le amministrazioni/AOO non statali il regolamento è emanato sulla base degli indirizzi generali stabiliti dal Ministero per i beni e le attività culturali (a norma dell'art. 124 del decreto legislativo 22 gennaio 2004, n. 42). La ricerca per scopi storici è

- gratuita;
- libera riguardo ai documenti non riservati per legge, per declaratoria del Ministero dell'interno (a norma dell'art. 125 del decreto legislativo 22 gennaio 2004, n. 42) o per regolamento emanato dalla stessa amministrazione/AOO. È possibile l'ammissione alla consultazione dei documenti riservati, previa autorizzazione rilasciata dal Ministero dell'interno, su conforme parere dell'autorità archivistica competente (Archivio di Stato o soprintendenza archivistica, a seconda che si tratti di archivi statali o non statali);
- condizionata all'accettazione integrale del "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" da parte del soggetto consultatore.

8.7.4 Consultazione da parte di personale esterno all'amministrazione

La domanda di accesso ai documenti viene presentata al servizio archivistico o all'Ufficio Relazioni con il Pubblico (URP), che provvede a smistarla al servizio archivistico. Presso il servizio archivistico e l'URP sono disponibili appositi moduli come quelli riportati nell'allegato 8.

Le richieste di accesso ai documenti della sezione storica dell'archivio vengono compilate dagli utenti direttamente presso la sede dell'Archivio Storico (Palazzo Piacentini).

In caso di richieste di consultazione di materiale documentale che comportano ricerche complesse, il termine di evasione della richiesta, di norma, non può essere immediata ma richiede tempi e modalità da concordare con l'utenza.. L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico.

La consultazione dei documenti è possibile esclusivamente in locali appositamente predisposti (aula di studio o di consultazione) sotto la diretta sorveglianza del personale addetto.

Il rilascio di copie dei documenti dell'archivio 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 in rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione entro il termine di 30 giorni.

8.7.5 Consultazione da parte di personale interno all'amministrazione

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica. L'affidamento temporaneo di un fascicolo già versato all'archivio di deposito o storico ad un ufficio del medesimo UOR/UU od altro UOR/UU 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 redatta in duplice copia su un apposito modello, contenente gli estremi identificativi della documentazione richiesta, il nominativo del richiedente, il suo UOR/UU e la sua firma.

Un esemplare della richiesta di consultazione viene conservato all'interno del fascicolo, l'altro nella posizione fisica occupata dal fascicolo in archivio.

Tale movimentazione viene registrata a cura del responsabile del servizio archivistico in un apposito registro di carico e scarico, dove, oltre ai dati contenuti nella richiesta, compaiono la data di consegna/invio e quella di restituzione, nonché eventuali note sullo stato della documentazione in modo da riceverla nello stesso stato in cui è stata consegnata.

Il responsabile del servizio archivistico verifica che la restituzione dei fascicoli affidati temporaneamente avvenga alla scadenza prevista.

L'affidatario dei documenti non estrae i documenti originali dal fascicolo, né altera l'ordine, 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 dall'amministrazione/AOO.

In ogni 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.

8.7.6 organizzazione del sistema archivistico

Concettualmente l'archivio è un tutt'uno e convenzionalmente si suole suddividerlo in archivio storico (per la fase inattiva della documentazione) e di deposito (per la fase semiattiva della documentazione).

9. 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.

9.1 Unicità del protocollo informatico

Nell'ambito della AOO il registro di protocollo è unico e la numerazione progressiva delle registrazioni di protocollo è unica indipendentemente dal modello organizzativo, centralizzato o distribuito delle UOP, adottato dall'AOO medesima.

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 presso una UOP viene considerata giuridicamente inesistente presso l'amministrazione.

Non è consentita la protocollazione di un documento già protocollato. 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 di protocollo è soggetto alle forme di pubblicità e di tutela di situazioni giuridicamente rilevanti previste dalla normativa vigente.

9.2 Registro giornaliero di protocollo

Il RSP provvede alla produzione del registro giornaliero di protocollo, costituito dall'elenco delle informazioni inserite con l'operazione di registrazione di protocollo nell'arco di uno stesso giorno.
Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro giornaliero informatico di protocollo è riversato, al termine della giornata lavorativa, su supporti di memorizzazione non riscrivibili i quali sono conservati in luogo sicuro a cura di un soggetto (responsabile della conservazione delle copie) appositamente nominato dall'amministrazione/AOO diverso dal RSP ai sensi dell'art. 7 comma 5 del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000. Tale operazione di riversamento viene espletata all'interno del Servizio Informatico>.
È a carico del RSP conservare in modalità sicura la copia del registro giornaliero di protocollo.

9.3 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.
Tale 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, registrato in forma non modificabile;
- il destinatario del documento, registrato in forma non modificabile;
- l'oggetto del documento, registrato in forma non modificabile;
- la classificazione.

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.

9.3.1 Documenti informatici

I documenti informatici sono ricevuti e trasmessi in modo formale dalla casella di posta elettronica certificata istituzionale dell'amministrazione.
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore addetto al protocollo ne ha accertato l'autenticità, la provenienza, l'integrità ed ha verificato la validità della firma.
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 file allegati al messaggio di posta elettronica ricevuto o inviato.
La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio sia ad uno o più file ad esso allegati. I documenti informatici sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.

9.3.2 Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza, (il servizio postale pubblico e/o privato o con consegna diretta alla UOP). La registrazione di protocollo di un documento analogico 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 competente esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

9.4 Elementi facoltativi delle registrazioni di protocollo

II RSP, con proprio provvedimento e al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, può modificare e integrare gli elementi facoltativi del protocollo. La registrazione degli elementi facoltativi del protocollo, con determinazione del RSP può essere modificata, integrata e cancellata in base alle effettive esigenze delle UOR o degli UOP. I dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registri tali modifiche. Di seguito vengono riportati gli elementi facoltativi finalizzati alla conservazione e gestione della documentazione:

- ora e minuto di registrazione;
- luogo di provenienza o di destinazione del documento;
- tipo di documento;
- mezzo di ricezione/spedizione (ordinaria, espressa, corriere, raccomandata con ricevuta di ritorno, telefax, ecc.);
- collegamento a documenti precedenti e susseguenti;
- numero degli allegati;
- riferimenti agli allegati su supporto informatico;
- nominativo dei destinatari delle copie per conoscenza;
- UOR/UU competente;
- identificativo del RPA;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- classificazione del documento (titolo, categoria e fascicolo; eventuale sottofascicolo e inserto);
- data di istruzione del fascicolo;
- numero del fascicolo;
- numero del sottofascicolo;
- numero dell'inserto;
- data di chiusura del fascicolo;
- repertorio dei fascicoli;
- identificativo del fascicolo e/o del documento;
- numero di repertorio della serie (delibere, determinazioni, verbali, circolari e contratti);
- tipologia del documento con l'indicazione dei termini di conservazione e di scarto;
- scadenzario.

9.5 Segnatura di protocollo dei documenti

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.

9.5.1 Documenti informatici

I dati della segnatura di protocollo di un documento informatico sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un file conforme alle specifiche *dell'Extensìble Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) . Le informazioni minime incluse nella segnatura sono quelle di seguito elencate:

- codice identificativo dell'amministrazione;
- codice identificativo dell'area organizzativa omogenea;
- data e numero di protocollo del documento.

È facoltativo riportare anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il 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, anche le seguenti informazioni:

- persona o ufficio destinatario;
- identificazione degli allegati;
- informazioni sul procedimento e sul trattamento.

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. Qualora l'AOO decida di scambiare con altre AOO informazioni non previste tra quelle definite come facoltative, può estendere il file di cui sopra, nel rispetto delle regole tecniche dettate dal CNIPA, includendo le informazioni specifiche stabilite di comune accordo con l'AOO con cui interagisce.

9.5.2 Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico (etichetta autoadesiva), sul quale vengono riportate le seguenti informazioni relative alla registrazione di protocollo:

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

Facoltativamente possono essere riportate anche le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- il codice identificativo dell'UOR a cui il documento è destinato/assegnato o che ha prodotto il documento;
- numero di fascicolo;
- ogni altra informazione utile o necessaria, se già disponibile al momento della registrazione di protocollo.

Il "segno" grafico di norma è realizzato con una etichetta autoadesiva corredata di codice a barre o, in alternativa, con un timbro tradizionale.
L'AOO ha optato per il "segno" riportato nell'allegato 15.
L'operazione di segnatura dei documenti in partenza viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita; in alternativa l'operazione viene integralmente eseguita dalla UOP.
L'operazione di acquisizione dell'immagine dei documenti cartacei è eseguibile 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 deve essere apposto sulla prima pagina dell'originale; in caso contrario il "segno" viene apposto sul retro della prima pagina dell'originale.

9.6 Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo *tra quelli obbligatori della registrazione di protocollo, registrati 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 RSP.
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 RSP è autorizzato 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 RSP.
A tal fine è istituito un registro (informatico o cartaceo) per le richieste di annullamento delle registrazioni e dei dati obbligatori delle registrazioni.
Il registro riporta i motivi dell'annullamento e, se il documento è stato protocollato nuovamente, il nuovo numero di protocollo assegnato.

9.7 Livello di riservatezza

L'operatore che effettua la registrazione di protocollo di un documento attribuisce allo stesso il livello di riservatezza che ritiene necessario, se diverso da quello standard applicato automaticamente dal sistema.
In modo analogo, il RPA che effettua l'operazione di apertura di un nuovo fascicolo ne fissa anche il livello di riservatezza.
Il livello di riservatezza applicato ad un fascicolo è acquisito automaticamente da tutti i documenti che vi confluiscono, se a questi è stato assegnato un livello di riservatezza minore od uguale. I documenti che invece hanno un livello di riservatezza superiore lo mantengono.

9.8 Casi particolari di registrazioni di protocollo

9.8.1 Registrazioni di protocollo particolari (riservate)

All'interno dell'AOO è istituito il protocollo riservato - sottratto alla consultazione da parte di chi non sia espressamente abilitato - nel quale sono riportati:

- documenti relativi a vicende di persone o a fatti privati o particolari;
- documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- le tipologie di documenti individuati dalla normativa vigente richiamati nell'allegato 10.

La registrazione nel protocollo particolare, quando non sia palesemente evidente la necessità, può essere disposta dal RSP con l'apposizione, sul documento, della seguente dicitura: "Da registrare sul protocollo particolare".
I documenti (informatici o cartacei) anonimi, *come tali individuati ai sensi dell'art. 8, comma 4, e 141 del codice di*

procedura penale, vengono inviati al RSP che ne effettua una valutazione:

- se ritiene che contengano dati o informazioni di interesse dell'amministrazione/AOO, provvede ad inviarli agli uffici competenti per le ulteriori eventuali determinazioni. Questi decidono se farli registrare nel protocollo generale;
- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo particolare.

9.8.2 Circolari e disposizioni generali

Le circolari, le disposizioni generali e tutte le altre comunicazioni che abbiano più destinatari si registrano con un solo numero di protocollo generale.

I destinatari sono indicati in appositi elenchi da associare alla minuta del documento e alla registrazione di protocollo secondo le modalità previste dalla gestione anagrafica del sistema.

9.8.3 Documenti cartacei in partenza con più destinatari

Qualora i destinatari siano in numero maggiore di uno, la registrazione di protocollo è unica e viene riportata solo sul documento originale

9.8.4 Documenti cartacei ricevuti a mezzo telegramma

I telegrammi vanno di norma inoltrati al servizio protocollo come documenti senza firma, specificando tale modalità di trasmissione nel sistema di protocollo informatico.

9.8.5 Documenti cartacei ricevuti a mezzo telefax

II documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.

Il documento trasmesso da chiunque ad una pubblica AOO tramite telefax, qualora ne venga accertata la fonte di provenienza, soddisfa il requisito della forma scritta e la sua trasmissione non deve essere seguita dalla trasmissione dell'originale. L'accertamento della fonte di provenienza spetta al RPA e avviene, di norma, per le vie brevi o con l'uso di sistemi informatici.

Qualora non sia possibile accertare la fonte di provenienza, sul telefax viene apposta la dicitura "Documento ricevuto via telefax" e successivamente il RPA provvede ad acquisire l'originale.

Nel caso che al telefax faccia seguito l'originale, poiché ogni documento viene individuato da un solo numero di protocollo, indipendentemente dal supporto e dal mezzo di trasmissione, l'addetto alla registrazione a protocollo, dopo aver registrato il telefax, deve attribuire all'originale la stessa segnatura del documento pervenuto via telefax ed apporre la seguente dicitura: "**Già pervenuto via fax il giorno……..".**

Il RSP accerta comunque che si tratta del medesimo documento ricevuto via fax: qualora dovesse riscontrare una differenza, anche minima, deve procedere alla registrazione con un nuovo numero di protocollo in quanto si tratta di un documento diverso. Il fax ricevuto con un terminale telefax dedicato (diverso da un PC) è fotocopiato dal ricevente qualora il supporto cartaceo non fornisca garanzie per una corretta e duratura conservazione. Su di esso o sulla sua foto-riproduzione va apposta, a cura del ricevente, la dicitura "Documento ricevuto via telefax". Il documento in partenza reca una delle seguenti diciture:

- " Anticipato via telefax" se il documento originale viene successivamente inviato al destinatario;
- " La trasmissione via fax del presente documento non prevede l'invio del documento originale" nel caso in cui l'originale non venga spedito. Il RPA è comunque tenuto a spedire l'originale qualora il destinatario ne faccia motivata richiesta;

La segnatura viene apposta sul documento e non sulla copertina di trasmissione. La copertina del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

Il fax ricevuto direttamente su una postazione di lavoro (esempio un PC con l'applicativo per invio e ricezione di fax) è la rappresentazione informatica di un documento che può essere, sia stampato e trattato come un fax convenzionale come è stato descritto nei paragrafi precedenti, sia visualizzato e trattato interamente con tecniche informatiche. In questo secondo caso il "file" rappresentativo del fax, viene inviato al protocollo generale, per essere sottoposto alle operazioni di protocollazione e segnatura secondo gli standard XML vigenti e poi, trattato secondo le regole precedentemente specificate per la gestione dei documenti informatici.

9.8.6 Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (es. scadenza gare o concorsi) che in uscita, deve esserne data comunicazione all'ufficio protocollo con almeno due giorni lavorativi di anticipo, onde concordare tempi e modi di protocollazione e di spedizione.

9.8.7 Domande di partecipazione a concorsi, avvisi, selezioni, corsi e borse di studio

La corrispondenza ricevuta con rimessa diretta dall'interessato o da persona da questi delegata, 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, essi saranno accantonati e protocollati successivamente (come di seguito descritto). In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

9.8.8 Fatture, assegni e altri valori di debito o credito

Le buste contenenti fatture, assegni o altri valori di debito o credito sono immediatamente separate dall'altra posta in arrivo e inviate quotidianamente all'UOR competente.

9.8.9 Protocollazione di documenti inerenti a gare di appalto confezionati su supporti cartacei

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 deve essere aperta, ma protocollata in arrivo con l'apposizione della segnatura, della data e dell'ora e dei minuti di registrazione direttamente sulla busta, plico o simili, e deve essere inviata all'UOR competente.

È compito dello stesso UOR provvedere alla custodia delle buste o dei contenitori protocollati, con mezzi idonei, sino all'espletamento della gara stessa.

Dopo l'apertura delle buste l'UOR che gestisce la gara d'appalto riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti. Per motivi organizzativi tutti gli UOR sono tenuti ad informare preventivamente il RSP dell'amministrazione in merito alle scadenze di concorsi, gare, bandi di ogni genere.

9.8.10 Protocolli urgenti

La richiesta di protocollare urgentemente un documento è collegata ad una necessità indifferibile e di tipo straordinario.

Solo in questo caso il RSP si attiva garantendo, nei limiti del possibile, la protocollazione del documento con la massima tempestività a partire dal momento della disponibilità del documento digitale o cartaceo da spedire.

Tale procedura viene osservata sia per i documenti in arrivo che per quelli in partenza, raccomandando, per questi ultimi, che non devono essere protocollati anticipatamente documenti diversi dall'originale (ad esempio bozze del documento), fatti pervenire all'UOP.

9.8.11 Documenti non firmati

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

Le lettere anonime, pertanto, devono essere protocollate e identificate come tali, 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.

9.8.12 Protocollazione dei messaggi di posta elettronica convenzionale

Considerato che l'attuale sistema di posta elettronica non certificata non consente una sicura individuazione del mittente, questa tipologia di corrispondenza è trattata nei seguenti modi:

- in caso di invio, come allegato, di un documento scansionato e munito di firma autografa, quest'ultimo è trattato come un documento inviato via fax fermo restando che l'RPA deve verificare la provenienza certa dal documento; in caso di mittente non verificabile, l'RPA valuta caso per caso l'opportunità di trattare il documento inviato via e-mail;
- in 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;
- in caso di invio di una e-mail contenente un testo non sottoscritto quest'ultima sarà considerata come missiva anonima.

9.8.13 Protocollo di documenti digitali pervenuti erroneamente

Nel caso in cui sia protocollato un documento digitale erroneamente inviato all'amministrazione non competente, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede a protocollare il documento in uscita indicando nell'oggetto "protocollato per errore" e rispedisce il messaggio al mittente.

9.8.14 Ricezione di documenti cartacei pervenuti erroneamente

Nel caso in cui sia protocollato un documento cartaceo erroneamente inviato all'amministrazione, l'addetto al protocollo provvede o ad annullare il protocollo stesso o provvede 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".

9.8.15 Copie per conoscenza

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 9.8.3. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, inserisce nel registro di protocollo i nominativi di coloro ai quali sono state inviate le suddette copie per conoscenza. Tale informazione è riportata anche sulla segnatura di protocollo.

9.8.16 Differimento delle registrazioni

Le registrazioni di protocollo dei documenti pervenuti presso l'amministrazione destinataria sono effettuate nella giornata di arrivo e comunque non oltre le 48 ore dal ricevimento di detti documenti.

Qualora non possa essere effettuata la registrazione di protocollo nei tempi sopra indicati si provvede a protocollare, in via prioritaria, i documenti che rivestono una particolare importanza previo motivato provvedimento del RSP, che

autorizza l'addetto al protocollo a differire le operazioni relative agli altri documenti.
Il protocollo differito consiste nel differimento dei termini di registrazione. Il protocollo differito si applica solo ai documenti in arrivo e per tipologie omogenee che il RSP descrive nel provvedimento sopra citato.

9.8.17 Registrazioni di documenti temporaneamente riservati

Quando si è in presenza di documenti che per la loro natura richiedono una temporanea riservatezza delle informazioni in essi contenute (ad esempio gare e appalti, verbali di concorso, etc), è prevista una forma di accesso riservato al protocollo generale

9.8.18 Corrispondenza personale o riservata

La corrispondenza personale è regolarmente aperta dagli uffici incaricati della registrazione di protocollo dei documenti in arrivo, a meno che sulla busta non sia riportata la dicitura "riservata" o "personale".
In quest'ultimo caso, la corrispondenza con la dicitura "riservata" o "personale" non è aperta ed è consegnata in busta chiusa al destinatario, il quale, dopo averne preso visione se reputa che i documenti ricevuti devono essere comunque protocollati provvede a trasmetterli al più vicino ufficio abilitato alla registrazione di protocollo dei documenti in arrivo.

9.8.19 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 ed eventuali allegati.
Tale verifica spetta al Responsabile del Procedimento Amministrativo (RPA) che, qualora reputi necessario acquisire documenti che integrino quelli già pervenuti, provvede a richiederli al mittente indicando con precisione l'indirizzo al quale inviarli e specificando che 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, sono inseriti nel fascicolo relativo.

9.9 Gestione delle registrazioni di protocollo con il PdP

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 PdP.
Il sistema di sicurezza adottato dall'AOO garantisce la protezione di tali informazioni sulla base dell'architettura del sistema informativo, sui controlli d'accesso e sui livelli di autorizzazione previsti.

9.10 Registrazioni di protocollo

9.10.1 Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il servizio di protocollo è realizzato dall'applicativo PdP attraverso l'apposizione di un riferimento temporale come previsto dalla normativa vigente.
Il sistema informativo assicura in tal modo la precisione del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.
Come previsto dalla normativa in materia di tutela dei dati personali, gli addetti al protocollo adottano tutti gli accorgimenti necessari per la tutela dei dati sensibili e giudiziari non inserendoli nel campo "oggetto" del registro di protocollo.

9.10.2 Registro informatico di protocollo

Al fine di assicurare l'integrità e la disponibilità dei dati contenuti nel registro di protocollo generale della AOO si provvede, in fase di chiusura dell'attività di protocollo, ad effettuare le seguenti operazioni:

- estrazione delle registrazioni del giorno corrente (o precedente) dal file del registro generale di protocollo;
- applicazione della firma digitale e di un riferimento temporale al file così realizzato;
- copia del file estratto, del file di firma e del riferimento temporale su supporto rimovibile non riscrivibile;
- salvataggio del file di firma e del riferimento temporale sul sistema di esercizio del PdP.

L'ufficio incaricato di eseguire l'operazione di riversamento dei file in parola su due supporti rimovibili non riscrivibili è stato individuato nell'ufficio " Gestione Infrastruttura Tecnologica Centrale – Sicurezza dei dati – numero unico 788" del servizio Sviluppo Organizzativo e Sistemi Informativi.
L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo.
È inoltre disponibile, all'occorrenza, per i gestori del PdP una funzione applicativa di "stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.
Al termine delle operazioni giornaliere o, comunque entro il giorno successivo sono effettuate le seguenti operazioni di garanzia:

- Backup dei dati del sistema informativo inclusi gli archivi del protocollo.

9.10.3 Tenuta delle copie del registro di protocollo

È compito del responsabile della conservazione dei documenti provvedere alla verifica del contenuto dei supporti prodotti dall'ufficio o dall'addetto incaricato e provvedere alle operazioni relative al trasferimento su supporto non rimovibile delle copie del registro di protocollo.

Una copia dei supporti è conservata *nella cassaforte* in dotazione del responsabile del Servizio Sviluppo Organizzativo e Sistemi Informativi, mentre la seconda copia è custodita presso la sede della Polizia Municipale (ubicata in luogo diverso e distante) Le modalità di gestione di tali supporti sono definite e regolamentate direttamente dal RSP dell'AOO.

I dati contenuti su tali supporti sono conservati con le modalità previste dalla normativa vigente.

10. Descrizione funzionale ed operativa del sistema di protocollo informatico

Il presente capitolo contiene la descrizione funzionale ed operativa del sistema di protocollo informatico adottato dall'amministrazione con particolare riferimento alle modalità di utilizzo dello stesso.

10.1 Descrizione funzionale ed operativa

Di seguito viene fornita una elencazione sintetica delle principali funzioni del PdP. Nell'allegato 16 è riportata, per motivi di opportunità, la descrizione dettagliata di dette funzioni.

In esso è presente una descrizione completa che tuttavia non tratta delle modalità operative perché quest'ultime sono trattate dettagliatamente nel Manuale utente del PdP. I manuali utente operativi sono allegati esterni al presente Manuale

11. Rilascio delle abilitazioni di accesso alle informazioni documentali

Il presente capitolo riporta i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali gestite dal PdP.

11.1 Generalità

Il controllo degli accessi è il processo che garantisce l'impiego degli oggetti/servizi del sistema informatico di protocollo esclusivamente secondo modalità prestabilite. Il processo è caratterizzato da utenti che accedono ad oggetti informatici (applicazioni, dati, programmi) mediante operazioni specifiche (lettura, aggiornamento, esecuzione). Gli utenti del servizio di protocollo, in base agli UU di appartenenza, ovvero in base alle rispettive competenze (UOP, UOR, UU) hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni stabilite dall'ufficio di appartenenza. Ad ogni utente è assegnata:

- una credenziale di accesso, costituita, ad esempio, da una componente:
  - pubblica che permette l'identificazione dell'utente da parte del sistema *(userID);*
  - privata o riservata di autenticazione *(password);*
- una autorizzazione di accesso (profilo) al fine di limitare le operazioni di protocollo e gestione documentale alle sole funzioni necessarie e indispensabili a svolgere le attività di competenza dell'ufficio a cui l'utente appartiene.

I diversi livelli di autorizzazione sono assegnati agli utenti dal RSP, che si avvale di un utente così detto privilegiato (amministratore). Gli utenti del servizio di protocollo una volta identificati sono suddivisi in 8 profili d'accesso, sulla base delle rispettive competenze.

In particolare possiamo individuare le seguenti profilature

1. registrazione di protocollo dei documenti in arrivo (A);
2. registrazione di protocollo dei documenti in partenza (P);
3. classificazione dei documenti (C);
4. presa in carico e assegnazione interna dei documenti ricevuti (PC);
5. fascicolazione dei documenti (F);
6. protocollazione dei documenti nel registro di emergenza (PE);
7. versamento dei fascicoli chiusi nell'archivio di deposito (VAD);
8. consultazione della banca dati documentale (CBD).

Le abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti, ovvero l'identificazione degli UU e del personale abilitato allo svolgimento delle operazioni di registrazione di protocollo, organizzazione e tenuta dei documenti all'interno dell'AOO, sono riportate nell'allegato 17 e sono costantemente aggiornate a cura del RSP.

11.2 Abilitazioni interne ad accedere ai servizi di protocollo

Gli utenti abilitati accedono al PdP attraverso l'immissione di credenziali di rete.

Le informazioni raccolte per controllare l'accesso al servizio sono quelle strettamente necessarie per l'identificazione dell'utente abilitato.

Il "file delle password" utilizzato dal servizio di accesso è una struttura LDAP crittografata e accessibile soltanto da un processo di sistema.

Tutte le utenze del PdP dell'AOO sono configurate con un timeout che provvede a disconnettere automaticamente l'applicazione dopo 120 minuti di inattività.

Le sessioni multiple con la stessa user ID non sono proibite e impedite dal PdP

11.3 Profili di accesso

La realtà tecnico operativa dell'amministrazione/AOO su questo aspetto si articola attraverso l'attività dei seguenti soggetti:

- Utente amministratore di PdP
- Operatore di protocollo
- Utente ordinario

11.4 Modalità di creazione e gestione delle utenze e dei relativi profili di accesso

Al fine di procedere alla creazione delle utenze il RSP, in accordo con la dirigenza, definisce i profili di autorizzazione del personale abilitato all'uso del Pdp. Tale elenco di profili deve essere trasmesso al servizio Sviluppo Organizzativo e Gestione Sistema Informativo per l'effettiva creazione di tali profili

In caso di smarrimento della password, sarà il dirigente competente, per e-mail interna, a richiedere al servizio Sviluppo Organizzativo e Gestione Sistema Informativo l'attribuzione di nuove credenziali all'utente in causa.

11.5 Ripristino delle credenziali private d'accesso

La stessa procedura indicata al paragrafo precedente secondo comma deve essere utilizzata per richiedere il ripristino delle credenziali private di accesso per un utente che abbia il profilo bloccato dal sistema di sicurezza

11.6 Abilitazioni esterne

Le modalità di accesso qui illustrate riguardano i soggetti esterni (privati) all'AOO. L'accesso al sistema di gestione del protocollo informatico e documentale da parte di utenti esterni all'AOO sarà realizzato mediante l'impiego di sistemi sicuri di identificazione ed autenticazione quali la carta d'identità elettronica, la carta nazionale dei servizi o i dispositivi di firma digitale o elettronica avanzata.

Agli utenti esterni riconosciuti ed abilitati alla consultazione dei dati propri presenti all'interno dell'amministrazione saranno fornite tutte le informazioni necessarie per accedere a detti documenti amministrativi.

11.7 Abilitazioni esterne concesse ad altre AOO

L'accesso al sistema di gestione informatica e documentale da parte di altre amministrazioni, o da parte di altre AOO della stessa amministrazione, avverrà secondo le modalità di interconnessione previste dalle norme e dai criteri tecnici emanati per la realizzazione del SPC.

In questi casi, le pubbliche amministrazioni accedono ai sistemi di gestione informatica dei documenti utilizzando al momento il SPC al fine di ottenere le seguenti informazioni:

- il numero e la data di protocollo del documento inviato;
- il numero e la data di protocollo del documento ricevuto.

11.8 Consultazione delle registrazioni di protocollo particolari

Il complesso dei documenti per i quali è stata attivata la registrazione di protocollo particolare costituisce l'archivio particolare.

I documenti e i fascicoli dell'archivio particolare sono consultabili nel rispetto delle seguenti norme:

- art. 24 della legge 7 agosto 1990, n. 241, e successive modificazioni;
- art. 8 del decreto del Presidente della Repubblica 27 giugno 1992, n. 352;
- artt. 107 e 108 del decreto legislativo 29 ottobre 1999, n. 490.

12. Modalità di utilizzo del registro di emergenza

Il presente capitolo illustra le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente, prevista dal PdP.

12.1 Il registro di emergenza

Qualora non fosse disponibile fruire del PdP per una interruzione accidentale o programmata, l'AOO è tenuta ad effettuare le registrazioni di protocollo sul registro di emergenza. Il registro di emergenza si rinnova ogni anno solare e, pertanto, inizia il primo gennaio e termina il 31 dicembre di ogni anno.

Qualora nel corso di un anno non venga utilizzato il registro di emergenza, il RSP annota sullo stesso il mancato uso.

Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite su registro di protocollo generale.

Il registro di emergenza si configura come un repertorio del protocollo generale. Ad ogni registrazione recuperata dal registro di emergenza viene attribuito un nuovo numero di protocollo generale, continuando la numerazione del protocollo generale raggiunta al momento dell'interruzione del servizio.

A tale registrazione è associato anche il numero di protocollo e la data di registrazione riportati sul protocollo di emergenza.

I documenti annotati nel registro di emergenza e trasferiti nel protocollo generale recano, pertanto, due numeri: quello del protocollo di emergenza e quello del protocollo generale. La data in cui è stata effettuata la protocollazione sul registro di emergenza è quella a cui si fa riferimento per la decorrenza dei termini del procedimento amministrativo.

In tal modo è assicurata la corretta sequenza dei documenti che fanno parte di un determinato procedimento amministrativo

12.2 Modalità di apertura del registro di emergenza

II RSP assicura che, ogni qualvolta per cause tecniche non è possibile utilizzare la procedura informatica, le operazioni di protocollo sono svolte manualmente sul registro di emergenza, sia esso cartaceo o informatico, su postazioni di lavoro operanti fuori linea. Prima di autorizzare l'avvio dell'attività di protocollo sul registro di emergenza, il RSP imposta e verifica la correttezza della data e dell'ora relativa al registro di emergenza su cui occorre operare. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione del funzionamento del protocollo generale.

Per semplificare e normalizzare la procedura di apertura/chiusura del registro di emergenza il RSP ha predisposto il modulo (cartaceo o digitale) riportato di seguito.

L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 3.

Servizio di gestione informatica del protocollo, dei documenti e degli archivi

Scheda di apertura/chiusura del registro di emergenza

Comune di San Benedetto del Tronto >

AOO:c_h - UOP Ufficio Gestione Documentale

Causa dell'interruzione: _____

_____

_____

_____

Data inizio/fine Interruzione ___/_____/_____ Ora Inizio/fine evento _____:_____

Numero di protocollo di emergenza _____ iniziale/finale

Pagina n_____

Firma del responsabile del servizio di protocollo

Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre le ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di non più di una settimana.

12.3 Modalità di utilizzo del registro di emergenza

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

La sequenza numerica utilizzata su un registro di emergenza è progressiva nell'anno e anche a seguito di successive interruzioni garantisce comunque l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.

Il formato delle registrazioni di protocollo, ovvero i campi obbligatori delle registrazioni, sono quelli stessi previsti

dal protocollo generale.
Durante il periodo di interruzione del servizio di protocollo informatico generale, il responsabile del sistema informatico (o persona da lui delegata) provvede a tener informato il RSP sui tempi di ripristino del servizio

12.4 Modalità di chiusura e recupero del registro di emergenza

È compito del RSP verificare la chiusura del registro di emergenza. È compito del RSP, o suo delegato, riportare dal registro di emergenza al sistema di protocollo generale (PdP) le protocollazioni relative ai documenti protocollati manualmente, entro cinque giorni dal ripristino delle funzionalità del sistema.
Una volta ripristinata la piena funzionalità del PdP, il RSP provvede alla chiusura del registro di emergenza annotando, sullo stesso il numero delle registrazioni effettuate e la data e ora di chiusura.
Per semplificare la procedura di chiusura del registro di emergenza il RSP ha predisposto un modulo (cartaceo o digitale) analogo a quello utilizzato nella fase di apertura del registro di emergenza (vedi punto 12.2).

13. Procedimenti Amministrativi

Quanto di seguito riportato in termini di base informativa dei procedimenti amministrativi dell'amministrazione/AOO, costituisce il riferimento per qualsiasi successivo impiego delle tecnologie informatiche di gestione dei flussi documentali *(work flow)*.

13.1 Matrice delle correlazioni

I procedimenti amministrativi saranno descritti nel "Catalogo dei procedimenti amministrativi", di cui il RSP curerà la realizzazione e l'aggiornamento, estemporaneo o periodico.
I procedimenti amministrativi costituiscono i processi attraverso i quali si esplica l'attività istituzionale dell'amministrazione/AOO.
All'interno del catalogo i procedimenti sono individuati mediante la definizione dei riferimenti riportati al successivo paragrafo 13.2.
La definizione del singolo procedimento amministrativo rappresenterà il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.
II risultato concreto di questa attività saranno i documenti opportunamente aggregati in fascicoli, ognuno dei quali è relativo a un singolo affare.
L'individuazione del RPA e del responsabile dell'adozione del provvedimento finale sarà effettuata sulla base delle competenze assegnate a ciascuna figura interna agli UOR/UU.

13.2 Catalogo dei procedimenti amministrativi

La gestione delle attività e dei procedimenti amministrativi, il loro iter, l'individuazione del responsabile del provvedimento finale e i termini entro i quali il procedimento deve essere concluso sono definiti così come previsto da norme di rango legislativo, regolamentare nonché dal regolamento interno emanato dall'amministrazione. A tal fine l'AOO, per favorire la trasparenza dell'azione amministrativa, per semplificare i procedimenti e per schematizzare le descrizioni, costituirà una base informativa dei procedimenti amministrativi registrando, per ciascuno di essi, almeno, le seguenti informazioni:

- la denominazione del procedimento;
- il codice del procedimento;
- i fondamenti giuridici del procedimento;
- le fasi operative del procedimento (e, all'occorrenza, dei sub-procedimenti) e la relativa sequenza;
- UOR/UU competenze per ciascuna fase;
- il tempo massimo di definizione dell'intero procedimento;
- il tempo di svolgimento di ciascuna fase;
- la forma e il contenuto dei documenti intermedi e del provvedimento finale;
- il responsabile dell'adozione del provvedimento finale;
- il responsabile del procedimento amministrativo;
- il funzionario incaricato dell'istruttoria;
- il titolario a cui il procedimento si riferisce, se disponibile.

13.3 Avvio dei procedimenti e gestione degli stati di avanzamento

Mediante l'assegnazione dei fascicoli agli UOR/UU di volta in volta competenti, le UOP o i RPA provvedono a dare avvio ai relativi procedimenti amministrativi selezionandoli dalla base informativa di cui al paragrafo precedente.
La registrazione degli stati di avanzamento dei procedimenti amministrativi sulla base informativa sopra richiamata può avvenire in modalità manuale o automatica.
Nel primo caso, gli stati di avanzamento sono aggiornati dal RPA.
Nel secondo caso, è il software che registra automaticamente i passaggi dei documenti contenuti nei fascicoli e lo stato di avanzamento del procedimento.

14. Approvazione e aggiornamento del Manuale, norme transitorie e finali

14.1 Modalità di approvazione e aggiornamento del Manuale

La Giunta Municipale adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico (RSP).
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 RSP.

14.2 Regolamenti abrogati

Con l'entrata in vigore del presente Manuale sono annullati tutti i regolamenti interni all'amministrazione/AOO nelle parti contrastanti con lo stesso.

14.3 Pubblicità del presente Manuale

Il presente Manuale, a norma dell'art. 22 della legge 7 agosto 1900, n. 241, è reso 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 resa disponibile mediante la rete intranet;
- inviata all'organo di revisione;
- inviata, per opportuna conoscenza, al CNIPA, Centro di competenza sul protocollo informatico;
- pubblicata sul sito internet dell'amministrazione.

14.4 Operatività del presente Manuale

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

15. Allegati

Allegato 1 - Definizioni

Oggetto/Soggetto	Descrizione
AMMINISTRAZIONI CERTIFICANTI	Le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti *(art. 1, comma 1, lett. p) del DPR n. 445/2000);*
AMMINISTRAZIONI PROCEDENTI	Le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive ovvero provvedono agli accertamenti d'ufficio *(art. 1, comma 1 lett. o) DPR n. 445/2000);*
AMMINISTRAZIONI PUBBLICHE	Per amministrazioni pubbliche si intendono quelle indicate nell'art. 1, comma 2 del d. lgs. 30 marzo 2001, n. 165;
AMMINISTRAZIONI PUBBLICHE CENTRALI	Le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300 *(art. 1, comma 1 lett. z) del d. lgs.7 marzo 2005, n. 82);*
ARCHIVIO	L'archivio è la sedimentazione naturale e ordinata degli atti spediti, inviati o comunque formati dall'Amministrazione nell'esercizio delle funzioni attribuite per legge o regolamento, per il conseguimento dei propri fini istituzionali. Gli atti formati e/o ricevuti dall'Amministrazione (Area Organizzativa Omogenea) sono collegati tra loro da un rapporto di interdipendenza, determinato dal procedimento o dall'affare al quale si riferiscono (il cosiddetto "vincolo archivistico"). Essi sono ordinati e conservati in modo coerente e accessibile alla consultazione; l'uso degli atti può essere amministrativo, legale o storico. L'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, l'archivio viene suddiviso in tre sezioni: corrente, di deposito e storica;
ARCHIVIO CORRENTE	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque verso i quali sussista un interesse attuale (corrispondente con la fase attiva);
ARCHIVIO DI DEPOSITO	Costituito dal complesso dei documenti relativi ad affari e a procedimenti amministrativi conclusi, per i quali non risulta più necessaria una trattazione per il corrente svolgimento del procedimento amministrativo o comunque verso i quali sussista un interesse sporadico (corrispondente con la fase semiattiva);
ARCHIVIO STORICO	Costituito da complessi di documenti relativi ad affari e a procedimenti amministrativi conclusi da oltre 40 anni e destinati, previa l'effettuazione delle operazioni di scarto, alla conservazione perenne (corrispondente con la fase inattiva);
ARCHIVIAZIONE ELETTRONICA	Processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione *(art. 1 della Deliberazione CNIPA 19 febbraio 2004 n. 11);*
AREA ORGANIZZATIVA OMOGENEA (**AOO**)	Un insieme di funzioni e di strutture, individuate dall'Amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato *(art. 2, lett. n) del DPCM 31 ottobre 2000);*
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive *(art. 1, comma 1, lett. i) del DPR 28 dicembre 2000, n. 445);*
AUTENTICAZIONE INFORMATICA	La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso; *(art. 1, comma 1 lett. b) del d. lgs.7 marzo 2005, n. 82);*
BANCA DI DATI	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti *(art. 4 comma 1 lett. o) del d. lgs. 30 giugno 2003 n.196);*
BLOCCO	La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento *(art. 4, comma 1, lett. d) del d. lgs. 30 giugno 2003 n.196);*
CARTA NAZIONALE	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica

DEI SERVIZI	ai servizi erogati dalle pubbliche amministrazioni *(art. 1 del d. lgs.7 marzo 2005, n. 82);*
CARTA D'IDENTITÀ ELETTRONICA	Il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare *(art. 1 comma 1, lett. c) del d. lgs.7 marzo 2005, n. 82) ;*
CASELLA DI POSTA ELETTRONICA ISTITUZIONALE	La casella di posta elettronica istituita da una AOO, attraverso la quale vengono ricevuti i messaggi da protocollare (ai sensi del DPCM 31 ottobre 2000, articolo 15, comma 3). *(art. 1 dell'allegato A alla circolare AIPA 7 maggio 2001 n. 28);*
CERTIFICATI ELETTRONICI	Gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi *(art. 1, comma 1 lett. e) del d. lgs.7 marzo 2005, n. 82);*
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva *(art. 1 comma 1 lett. f) del d. lgs.7 marzo 2005, n. 82);*
CERTIFICATO	Il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione o partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche *(art. 1 comma I lett. f) del DPR 28 dicembre 2000, n. 445);*
CERTIFICATORE	II soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime *(art. 1, comma 1 lett. g) del d. lgs. 7 marzo 2005, n. 82);*
CLASSIFICAZIONE	L'operazione che consente di organizzare i documenti in relazione alle funzioni e alle modalità operative dell'Amministrazione.
COMUNICAZIONE	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione *(art. 4 comma 1 lett. l) del d. lgs. 30 giugno 2003 n.196);*
CONSERVAZIONE SOSTITUTIVA	Processo effettuato con le modalità di cui agli articoli 3 e 4 della deliberazione CNIPA 19 febbraio 2004, n.11;
CREDENZIALI DI AUTENTICAZIONE	I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica *(art. 4 comma 3 lett. d) del d. lgs. 30 giugno 2003 n. 196);*
DATI GIUDIZIARI	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale *(art. 4, comma 1 lett. e) del d. lgs. 30 giugno 2003 n. 196;*
DATI IDENTIFICATIVI	I dati personali che permettono l'identificazione diretta dell'interessato *(art. 4, comma 1 lett. c) del d. lgs. 30 giugno 2003 n. 196);*
DATI SENSIBILI	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale *(art. 4 comma 1, lett. ddd) del d. lgs. 30 giugno 2003 n. 196);*
DATO ANONIMO	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile *(art. 4 comma 1 lett. n) del d. lgs. 30 giugno 2003 n. 196);*
DATO PERSONALE	Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale *(art. 4 comma 1 lett. b) del d. lgs. 30 giugno 2003 n. 196);*
DATO PUBBLICO	Il dato conoscibile da chiunque *(art. 1 comma 1 lett. n) del d. lgs. 7 marzo 2005, n. 82);*
DATO A CONOSCIBLITÀ LIMITATA	l dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti *(art. 1 comma 1 lett. l) del d. lgs.7 marzo 2005, n. 82);*
DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ	Il documento sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dall' *art. 1 comma 1 lett. h) del DPR 28 dicembre 2000, n. 445;*
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato *(art. 1 comma 1 lett. g) del DPR 28 dicembre 2000, n. 445);*
DIFFUSIONE	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione *(art. 4 del d. lgs. 30 giugno 2003 n.*

	196);
DOCUMENTO	Rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica *(art. 1 comma 1 lett. a) Deliberazione CNIPA del 19 febbraio 2004 n.11);*
DOCUMENTO AMMINISTRATIVO	Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa *(art. 1 comma 1 lett. a) del DPR 28 dicembre 2000, n. 445);*
DOCUMENTO ANALOGICO	Documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia *(art. 1 comma 1 lett. b) Deliberazione CNIPA del 19 febbraio 2004, n.11);*
DOCUMENTO ANALOGICO ORIGINALE	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi *(art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica *(art. 1 comma 1 lett. h) Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO CONSERVATO	Documento sottoposto al processo di conservazione sostitutiva *(art. 1 Deliberazione CNIPA del 19 febbraio 2004 n. 11);*
DOCUMENTO DI RICONOSCIMENTO	Ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare. *(art. 1 comma 1 lett. c) del DPR 28 dicembre 2000, n. 445);*
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare *(art. 1 comma 1 lett. d) del DPR 28 dicembre 2000, n. 445);*
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti *(art. 1 comma 1 lett. t) del d. lgs.7 marzo 2005, n. 82);*
DOSSIER	È una aggregazione di più fascicoli che può essere costituita a seguito di esigenze operative dell'Amministrazione, *come ad esempio, dossier riferiti ad un Ente o ad una persona che contengono fascicoli relativi a diversi procedimenti che riguardano lo stesso Ente o la stessa persona;*
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia *(art. 1 comma 1 lett. n) della deliberazione AIPA 19 febbraio 2004 n. 11);*
EVIDENZA INFORMATICA	Una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica *(art. 1 comma 1, lett. f) del DPCM 13 gennaio 2004);*
FASCICOLAZIONE	L'operazione di riconduzione dei singoli documenti classificati in tanti fascicoli corrispondenti ad altrettanti affari o procedimenti amministrativi.
FASCICOLO	Insieme ordinato di documenti, che può fare riferimento ad uno stesso affare/procedimento/processo amministrativo, o ad una stessa materia, o ad una stessa tipologia documentaria, che si forma nel corso delle attività amministrative del soggetto produttore, allo scopo di riunire, a fini decisionali o informativi tutti i documenti utili allo svolgimento di tali attività. Nel fascicolo possono trovarsi inseriti documenti diversificati per formati, natura, contenuto giuridico, ecc., anche se è non è infrequente la creazione di fascicoli formati di insieme di documenti della stessa tipologia e forma raggruppati in base a criteri di natura diversa (cronologici, geografici, ecc.). Il fascicolo rappresenta l'unità base dell'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);*
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica *(art. 1, comma 1, lett. q) del d. lgs.7 marzo 2005, n. 82);*
FIRMA ELETTRONICA QUALIFICATA	La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con

	mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica *(art. 1 comma 1 lett. r) del d. lgs.7 marzo 2005, n. 82);*
FORMAZIONE DEI DOCUMENTI INFORMATICI	Il processo di generazione del documento informatico al fine di rappresentare atti, fatti e dati riferibili con certezza al soggetto e all'amministrazione che lo hanno prodotto o ricevuto. Esso reca la firma digitale, quando prescritta, ed è sottoposto alla registrazione del protocollo o ad altre forme di registrazione previste dalla vigente normativa *(art. 2 della deliberazione AIPA 23 novembre 2000 n. 51);*
FUNZIONE DI HASH	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) per le quali la funzione generi impronte uguali *(art. 1 comma 1 lett. e) del DPCM 13 gennaio 2004);*
GARANTE (della Privacy)	L'autorità di cui all'articolo 153 del d. lgs. 30 giugno 2003 n. 196, istituita dalla legge 31 dicembre 1996, n. 675 *(art. 4 comma 1 lett. q) del d. lgs. 30 giugno 2003 n. 196);*
GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici *(art. 1 comma 1 lett. l) del d. lgs. 7 marzo 2005, n. 82);*
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di *hash (art. 1 del DPCM 13 gen 2004);*
INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI	Le persone fisiche autorizzate a compiere operazioni di trattamento di dati personali dal titolare o dal responsabile;
INSERTO	È un sottoinsieme omogeneo del sottofascicolo che può essere costituito a seguito di esigenze operative dell'Amministrazione;
LEGALIZZAZIONE DI FIRMA	L'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa *(art. 1 comma 1 lett. l) del DPR 28 dicembre 2000, n. 445);*
LEGALIZZAZIONE DI FOTOGRAFIA	L'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato *(art. 1 comma 1 lett. n) del DPR 28 dicembre 2000, n. 445);*
MARCA TEMPORALE	Un'evidenza informatica che consente la validazione temporale *(art. 1 comma 1 lett. i) del DPCM 31 gennaio 2004);*
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	Il massimario di selezione e scarto (Piano di Conservazione) è lo strumento che consente di effettuare razionalmente lo scarto archivistico dei documenti prodotti e ricevuti dalle pubbliche amministrazioni. Il massimario riproduce l'elenco delle partizioni e sottopartizioni del titolario con una descrizione più o meno dettagliata dei procedimenti/procedure attivate per le funzioni a cui ciascuna partizione si riferisce e della natura dei relativi documenti; indica per ciascun procedimento/procedura, quali documenti debbano essere conservati permanentemente (e quindi versati dopo quarant'anni dall'esaurimento degli affari nei competenti archivi di Stato per gli uffici dello Stato o per la sezione degli archivi storici per gli Enti pubblici) e quali invece possono essere destinati al macero dopo cinque anni, dopo dieci anni, dopo venti anni, ecc. o secondo le esigenze dell'Amministrazione/AOO. Ne consegue il PIANO DI CONSERVAZIONE periodica o permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali;
MEMORIZZAZIONE	Processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'articolo 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del decreto legislativo 23 gennaio 2002, n. 10 *(art 1, comma 1, lett. f) Deliberazione CNIPA del 19 febbraio 2004 n.11);*
MISURE MINIME DI SICUREZZA	Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del d. lgs. 30 giugno 2003 n. 196 *(art. 4 comma 3 lett. a) del d. lgs. 30 giugno 2003 n. 196);*
ORIGINALI NON UNICI	I documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o

	documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi *(art. 1, comma 1, lett. v) del d. lgs. 7 marzo 2005, n. 82);*
PAROLA CHIAVE	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica *(art. 4, comma 3, lett. e) del d. lgs. 30 giugno 2003, n. 196);*
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	*Vedi MASSIMARO DI SELEZIONE E SCARTO*
PROFILO DI AUTORIZZAZIONE	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti *(art. 4, comma 3, lett. f) del d. lgs. 30 giugno 2003 n. 196);*
PUBBLICO UFFICIALE	Il notaio, salvo quanto previsto dall'art. 5, comma 4 della Deliberazione CNIPA del 19 febbraio 2004, n. 11 e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 *(art. 1 Deliberazione CNIPA del 19 febbraio 2004, n. 11);*
RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI	La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali *(art. 4, comma 1, lett. g) del d. lgs. 30 giugno 2003 n. 196);*
RESPONSABILE DEL SERVIZIO DI PROTOCOLLO	Il responsabile del servizio per la tenuta del protocollo informatico, per la gestione dei flussi documentali e degli archivi di cui all'articolo 62, comma 2, del DPR 28 dicembre 2000, n. 445;
RESPONSABILI DEI PROCEDIMENTI AMMINISTRATIVI **(RPA**)	È la persona, alla quale è stata affidata la trattazione di un affare amministrativo ivi compresa la gestione/creazione del relativo fascicolo dell'archivio corrente
RIFERIMENTO TEMPORALE	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici *(art 1, comma 1, lett. g) del DPCM 13 gennaio 2004)* o ad un messaggio di posta elettronica certificata *(art. 1, comma 1, lett. i), del DPR 11 febbraio 2005, n. 68);*
RIVERSAMENTO DIRETTO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica *(art. comma 1, lett. l) Deliberazione CNIPA del 19 febbraio 2004, n. 11)*
RIVERSAMENTO SOSTITUTIVO	Processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica *(art. 1, comma 1, lett. o) della Deliberazione CNIPA del 19 febbraio 2004, n. 11)*
SCOPI SCIENTIFICI	Le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore *(art. 4, comma 4, lett. c) del d. lgs. 30 giugno 2003 n. 196);*
SCOPI STATISTICI	Le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici *(art. 4, comma 4, lett. b) del d. lgs. 30 giugno 2003 n. 196);*
SCOPI STORICI	Le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato *(art. 4, comma 4, lett. a) del d. lgs. 30 giugno 2003 n. 196);*
SEGNATURA INFORMATICA	L'insieme delle informazioni archivistiche di protocollo, codificate in formato XML ed incluse in un messaggio protocollato, come previsto dall'articolo 18, comma 1, del DPCM 31 ottobre 2000 *(art. 1 dell'allegato A della circolare AIPA 7 maggio 2001 n. 28);*
SEGNATURA DI PROTOCOLLO	L'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso *(Glossario dell'IPA Indice delle Pubbliche Amministrazioni);*
SISTEMA DI CLASSIFICAZIONE	Lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata *(art. 2, comma 1, lett. h) del DPCM 31 ottobre 2000);*
SISTEMA DI AUTORIZZAZIONE	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente *(art. 4, comma 3, lett. g) del d. lgs. 30 giugno 2003 n. 196);*
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	L'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti *(art. 1, comma 1, lett. r) del DPR 28 dicembre 2000 n. 445);*
STRUMENTI ELETTRONICI	Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento di dati.

Allegato 2 - Normativa di riferimento

1) Legge 7 agosto 1990, n. 241 - Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. del 18 agosto 1990, n. 192)
2) DPR 27 giugno 1992, n. 352 - Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della Legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi. (G.U. 29 luglio 1992, n. 177)
3) DPR 12 febbraio 1993, n. 39 - Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, lettera m), della legge 23 ottobre 1992, n. 421. (G.U. 10 febbraio 1993, n. 42)
4) Legge 15 marzo 1997, n. 59 - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa.
5) DPCM 28 ottobre 1999 - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
6) Decreto legislativo 29 ottobre 1999, n. 490 - Testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'articolo 1 della legge 8 ottobre 1997, n. 352. (G.U. 27 dicembre 1999, n. 302)
7) DPCM 31 ottobre 2000 - Regole tecniche per il protocollo informatico; valido ai sensi dell'art. 78 del DPR 28 dicembre 2000, n. 445. (G.U. n. 272 del 21 novembre 2000)
8) Deliberazione AIPA 23 novembre 2000, n. 51- Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del DPR 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291)
9) DPR 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
10) Circolare del 16 febbraio 2001, n. AIPA/CR/27 – "Art. 17 del DPR 10 novembre 1997, n. 513 - Utilizzo della firma digitale nelle pubbliche amministrazioni".
11) Decreto legislativo 30 marzo 2001, n. 165 - "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".
12) Circolare AIPA 7 maggio 2001, n. AIPA/CR/28 - Articolo 18, comma 2, del DPCM 31 ottobre 2000 recante regole tecniche per il protocollo informatico di cui al DPR 28 dicembre 2000, n. 445 - Standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni e associate ai documenti protocollati. (G.U. 21 novembre 2000, n. 272)
13) Circolare AIPA 21 giugno 2001, n. AIPA/CR/31 (Art. 7, comma 6, del DPCM 31 ottobre 2000 recante "Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili.)
14) Direttiva del Ministro per la funzione pubblica del 13 dicembre 2001 - Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
15) Direttiva 16 gennaio 2002, Dipartimento per l'innovazione e le tecnologie - Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.
16) Decreto legislativo 23 gennaio 2002, n. 10 - Recepimento della direttiva 1999/93/CE sulla firma elettronica.
17) Direttiva del Ministro per l'innovazione e le tecnologie, 9 dicembre 2002 -Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
18) Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002 - Linee guida in materia di digitalizzazione dell'amministrazione.
19) Legge 27 dicembre 2002, n. 289 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
20) DPR 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.
21) Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali.
22) Decreto Ministeriale 14 ottobre 2003 - Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi. (G.U. del 25 ottobre 2003, n. 249)
23) Direttiva del Ministro per l'innovazione e le tecnologie 27 novembre 2003 -Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
24) Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003.
25) Direttiva 18 dicembre 2003 - Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
26) DPCM 13 gennaio 2004 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici. (G.U. 27 aprile 2004, n. 98)

27) Deliberazione CNIPA 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.
28) Decreto legislativo 22 gennaio 2004, n. 42 - Codice dei beni culturali e del paesaggio, ai sensi dell'art. 10 della legge 6 luglio 2002, n. 137. (G.U. 24 febbraio 2004, n. 28).

Allegato 3 – AREE ORGANIZZATIVE OMOGENEE E ORGANIGRAMMA

Dati riguardanti l'Amministrazione:

Nome esteso amministrazione	Comune di San Benedetto del Tronto
Codice Identificativo dell'Amministrazione	125155161201
Indirizzo sede legale amministrazione	Viale Alcide De Gasperi, 124
CAP sede legale amministrazione	63039
Città sede legale amministrazione	San Benedetto del Tronto
Provincia di appartenenza sede legale	AP
Regione di appartenenza sede legale	Marche
Nome responsabile	
Cognome responsabile	
Titolo del Responsabile	Sindaco
Nome referente	
Cognome referente	
Indirizzo e-mail referente	
Telefono Referente	
Dominio di Posta Elettronica Certificata	cert-sbt.it
URL sito istituzionale	www.comunesbt.it

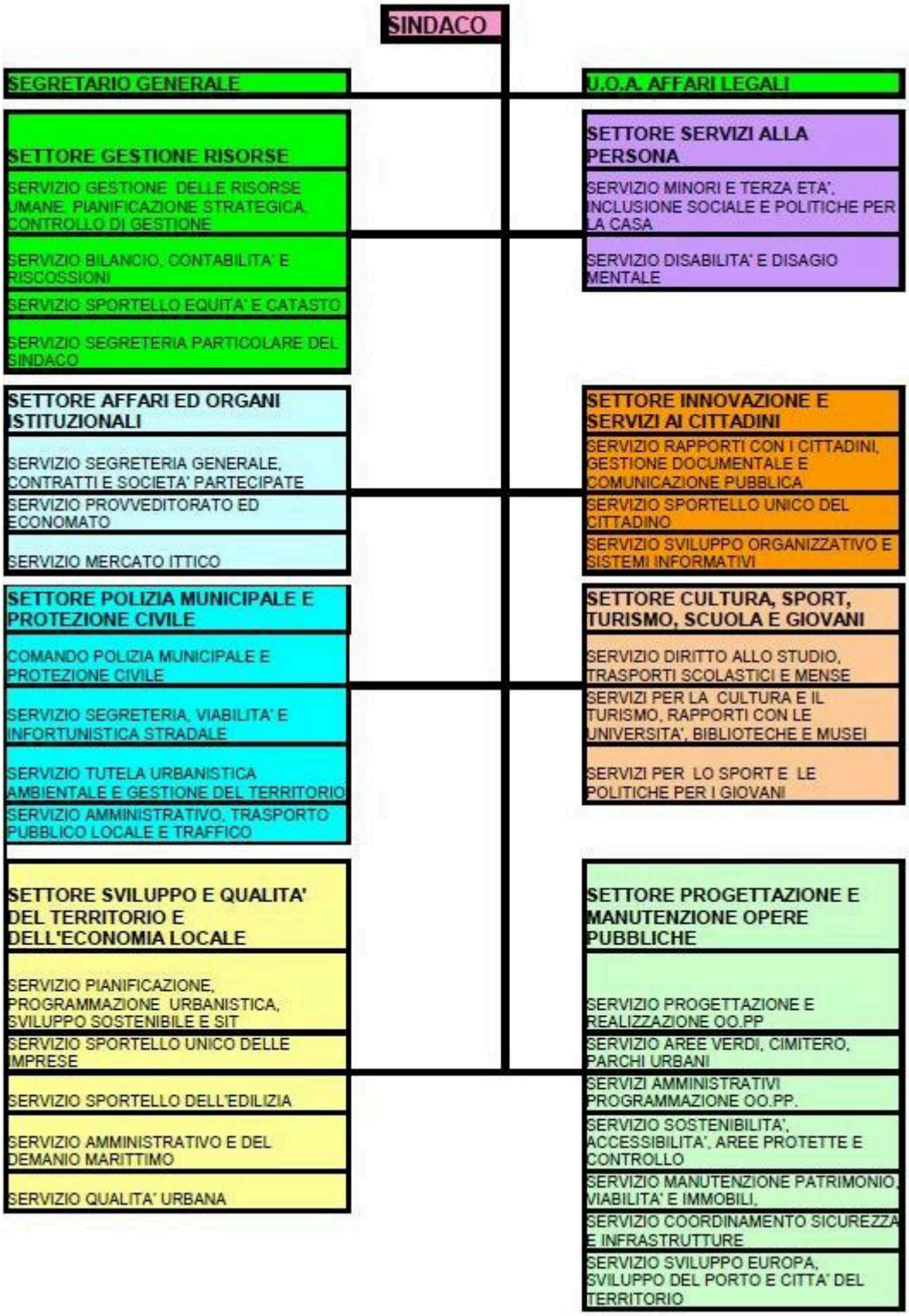
Dati riguardanti la AOO:

Codice AOO	c_h769
Nome AOO	Comune di San Benedetto del Tronto
Indirizzo PEC istituzionale	protocollo@cert-sbt.it
Nome responsabile	
Cognome responsabile	
Data istituzione	05/07/2004
Numero Settori Afferenti	10

Dati riguardanti la UOP

Codice UOP	c_h769-01-10
Nome UOP	Ufficio Gestione documentale e Protocollo Informatico
Codice UO di appartenenza	c_h769-01
Codice AOO di appartenenza	c_h769
Casella di Posta Elettronica Certificata	protocollo@cert-sbt.it
Nome responsabile	
Cognome responsabile	
Nome del vicario	
Cognome del vicario	
Data istituzione	

Organigramma comunale, primo e secondo livello (Allegato "A" alla Delibera G.M. n. 175 del 2011):



Articolazione di ciascuna Unità Organizzativa di registrazione di Protocollo in Uffici Utente

Servizio Rapporti con i cittadini, gestione documentale, comunicazione pubblica	
Denominazione dell'Ufficio Utente	*Ufficio Gestione Documentale e relazioni con soggetti istituzionali*
Nominativo del Responsabile dell'UU	
Ubicazione	*Viale De Gasperi 124, 63039 San Benedetto del Tronto*
Numero di telefono	*0735 794503*
Numero di telefax	*0735 794335*
UOP abilitata allo smistamento	*SI*
UOP abilitata a eseguire la scannerizzazione dei documenti cartacei	*SI*
UOP abilitata all'impiego del Registro di emergenza	*SI*

c_h769 -Comune di San Benedetto del Tronto	
Servizio Aree Verdi, Cimitero e Parchi Urbani	
Denominazione dell'Ufficio Utente	*Area Cimitero*
Nominativo del Responsabile dell'UU	
Ubicazione	*Via Gemito, 1 63039 San Benedetto del Tronto*
Numero di telefono	*0735 794795*
Numero di telefax	
UOP abilitata allo smistamento	*NO*
UOP abilitata a eseguire la scannerizzazione dei documenti cartacei	*NO*
UOP abilitata all'impiego del Registro di emergenza	*NO*
UOP abilitata alla protocollazione in arrivo di:	*solo alla registrazione in arrivo di documenti di propria pertinenza (attività cimiteriale*

c_h769 -Comune di San Benedetto del Tronto	
Settore Polizia Municipale	
Denominazione dell'Ufficio Utente	*Segreteria Comando e Protezione Civile*
Nominativo del Responsabile dell'UU	
Ubicazione	*Piazza Battisti 1 63039 San Benedetto del Tronto*
Numero di telefono	*0735 794212*
Numero di telefax	*0735 794241*
UOP abilitata allo smistamento	*NO*
UOP abilitata a eseguire la scannerizzazione dei documenti cartacei	*NO*
UOP abilitata all'impiego del Registro di emergenza	*NO*
UOP abilitata alla protocollazione in arrivo di:	*solo alla registrazione in arrivo di documenti di propria pertinenza (relativi alla Polizia Municipale)*

c_h769 -Comune di San Benedetto del Tronto	
Servizio Sportello Unico dell'Edilizia	
Denominazione dell'Ufficio Utente	*Sportello dell'edilizia*
Nominativo del Responsabile dell'UU	
Ubicazione	*Viale De Gasperi 124, 63039 San Benedetto del Tronto*
Numero di telefono	*0735 794366*

Numero di telefax	*0735 794376*
UOP abilitata allo smistamento	*NO*
UOP abilitata a eseguire la scannerizzazione dei documenti cartacei	*NO*
UOP abilitata all'impiego del Registro di emergenza	*NO*
UOP abilitata alla protocollazione in arrivo di:	*solo alla registrazione in arrivo di documenti di propria pertinenza (relativi alle pratiche edilizie presentate allo sportello unico dell'Edilizia)*

Allegato 4 - Politiche di sicurezza

Politiche accettabili di uso del sistema informativo

Premessa

L'incarico del Responsabile della Sicurezza (RS), o suo delegato, di pubblicare le politiche accettabili di uso, è quello di stabilire le regole per proteggere l'Amministrazione da azioni illegali o danneggiamenti effettuati da individui in modo consapevole o accidentale senza imporre restrizioni contrarie a quanto stabilito dall'Amministrazione in termini di apertura, fiducia e integrità del sistema informativo.

Sono di proprietà dell'Amministrazione i sistemi di accesso ad Internet, l'Intranet, la Extranet ed i sistemi correlati, includendo in ciò anche i sistemi di elaborazione, la rete e gli apparati di rete, il software applicativo, i sistemi operativi, i sistemi di memorizzazione/archiviazione delle informazioni, il servizio di posta elettronica, i sistemi di accesso e navigazione in Internet, etc. Questi sistemi e/o servizi devono essere usati nel corso delle normali attività di ufficio solo per scopi istituzionali e nell'interesse dell'Amministrazione e in rapporto con possibili interlocutori della medesima.

L'efficacia e l'efficienza della sicurezza è uno sforzo di squadra che coinvolge la partecipazione ed il supporto di tutto il personale (impiegati funzionari e dirigenti) dell'Amministrazione ed i loro interlocutori che vivono con l'informazione del sistema informativo. È responsabilità di tutti gli utilizzatori del sistema informatico conoscere queste linee guida e comportarsi in accordo con le medesime.

Scopo

Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.

Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.

L'uso non appropriato delle risorse strumentali espone l'Amministrazione al rischio di non poter svolgere i compiti istituzionali assegnati, a seguito, ad esempio, di virus, della compromissione di componenti del sistema informatico, ovvero di eventi disastrosi.

Ambito di applicazione

Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati delle ditte fornitrici di software e hardware che per qualsiasi motivo debbano utilizzare il sistema informatico dell'Ente , includendo tutto il personale affiliato con terze parti.

Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

Politiche – Uso generale e proprietà

- Gli utenti del sistema informativo dovrebbero essere consapevoli che i dati da loro creati sui sistemi dell'Amministrazione e comunque trattati, rimangono di proprietà della medesima.
- Gli impiegati sono responsabili dell'uso corretto delle postazioni di lavoro assegnate e dei dati ivi conservati anche perché la gestione della rete (Intranet) non può garantire la confidenzialità dell'informazione memorizzata su ciascun componente "personale" della rete dato che l'amministratore della rete ha solo il compito di fornire prestazioni elevate e un ragionevole livello di confidenzialità e integrità dei dati in transito.
- Per garantire la manutenzione della sicurezza e della rete, soggetti autorizzati dall'Amministrazione (di norma amministratori di rete) possono monitorare gli apparati, i sistemi ed il traffico in rete in ogni momento.
- Per i motivi di cui sopra l'Amministrazione si riserva il diritto di controllare la rete ed i sistemi per un determinato periodo per assicurare la conformità con queste politiche.

Politiche - Sicurezza e proprietà dell'informazione

- Il personale dell'Amministrazione dovrebbe porre particolare attenzione in tutti i momenti in cui ha luogo un trattamento delle informazioni per prevenire accessi non autorizzati alle informazioni.
- Mantenere le credenziali di accesso (normalmente UserID e password) in modo sicuro e non condividerle con nessuno. Gli utenti autorizzati ad utilizzare il sistema informativo sono responsabili dell'uso delle proprie credenziali, componente pubblica (UserID) e privata (password). Le password dovrebbero essere cambiate con il primo accesso al sistema informativo e successivamente, al minimo ogni sei mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
- Tutte le postazioni di lavoro (PC da tavolo e portatili) dovrebbero essere rese inaccessibili a terzi quando non utilizzate dai titolari per un periodo massimo di dieci minuti attraverso l'attivazione automatica del salva schermo protetto da password o la messa in stand-by con un comando specifico.
- Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
- Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
- Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "news group" che utilizzano il sistema di posta elettronica dell'Amministrazione dovrebbero contenere una dichiarazione che affermi che le opinioni sono strettamente personali e non dell'Amministrazione a meno che non si tratti di discussioni inerenti e di interesse dell'Amministrazione eseguite per conto della medesima.
- Tutti i PC, i server ed i sistemi di elaborazione in genere, che sono connessi in rete interna

dell'Amministrazione (Intranet) e/o esterna (Internet/Extranet) di proprietà dell'Amministrazione o del personale, devono essere dotati di un sistema antivirus approvato dal responsabile della sicurezza dell'Amministrazione ed aggiornato.

• Il personale deve usare la massima attenzione nell'apertura dei file allegati alla posta elettronica ricevuta da sconosciuti perché possono contenere virus, bombe logiche e cavalli di Troia.

• Non permettete ai colleghi, né tanto meno ad esterni, di operare sulla vostra postazione di lavoro con le vostre credenziali. Sempre voi risultate autori di qualunque azione.

Politiche - Antivirus

Premessa

I virus informatici costituiscono ancora oggi la causa principale di disservizio e di danno delle Amministrazioni.

I danni causati dai virus all'Amministrazione, di tipo diretto o indiretto, tangibili o intangibili, secondo le ultime statistiche degli incidenti informatici, sono i più alti rispetto ai danni di ogni altra minaccia.

I virus, come noto, riproducendosi autonomamente, possono generare altri messaggi contagiati capaci di infettare, contro la volontà del mittente, altri sistemi con conseguenze negative per il mittente in termini di criminalità informatica e tutela dei dati personali.

Scopo

Stabilire i requisiti che devono essere soddisfatti per collegare le risorse elaborative ad Internet/Intranet/Extranet dell'Amministrazione al fine di assicurare efficaci ed efficienti azioni preventive e consuntive contro i virus informatici.

Ambito di applicazione

Queste politiche riguardano tutte le apparecchiature di rete, di sistema ed utente (PC) collegate ad Internet/Intranet/Extranet. Tutto il personale dell'Amministrazione è tenuto a rispettare le politiche di seguito richiamate.

Politiche per le azioni preventive

• Deve essere sempre attivo su ciascuna postazione di lavoro un prodotto antivirus aggiornabile da un sito disponibile sulla Intranet dell'Amministrazione.

• Su ciascuna postazione deve essere sempre attiva la versione corrente e aggiornata con la più recente versione resa disponibile sul sito centralizzato.

• Non aprire mai file o macro ricevuti con messaggi dal mittente sconosciuto, sospetto, ovvero palesemente non di fiducia. Cancellare immediatamente tali oggetti sia dalla posta che dal cestino.

• Non aprire mai messaggi ricevuti in risposta a messaggi "probabilmente" mai inviati.

• Cancellare immediatamente ogni messaggio che invita a continuare la catena di messaggi, o messaggi spazzatura.

• Non scaricare mai messaggi da siti o sorgenti sospette.

• Evitate lo scambio diretto ed il riuso di supporti rimovibili (floppy disk, CD, DVD, tape, pen drive, etc.) con accesso in lettura e scrittura a meno che non sia espressamente formulato in alcune procedure dell'amministrazione e, anche in questo caso, verificare prima la bontà del supporto con un antivirus.

• Evitare l'uso di software gratuito (freeware o shareware) o documenti di testo prelevati da siti Internet o copiato dai CD/DVD in allegato a riviste.

• Evitare l'utilizzo, non controllato, di uno stesso computer da parte di più persone.

• Evitare collegamenti diretti ad Internet via modem.

• Non utilizzare il proprio supporto di archiviazione rimovibile su di un altro computer se non in condizione di protezione in scrittura.

• Se si utilizza una postazione di lavoro che necessita di un "bootstrap" da supporti di archiviazione rimovibili, usare questo protetto in scrittura.

• Non utilizzare i server di rete come stazioni di lavoro.

• Non aggiungere mai dati o file ai supporti di archiviazione rimovibili contenenti programmi originali.

• Effettuare una scansione della postazione di lavoro con l'antivirus prima di ricollegarla, per qualsiasi motivo (es, riparazione, prestito a colleghi o impiego esterno), alla Intranet dell'Organizzazione.

Di seguito vengono riportati ulteriori criteri da seguire per ridurre al minimo la possibilità di contrarre virus informatici e di prevenirne la diffusione, destinati a tutto il personale dell'Amministrazione ed, eventualmente, all'esterno.

• Tutti gli incaricati del trattamento dei dati devono assicurarsi che i computer di soggetti terzi, esterni, qualora interagiscano con il sistema informatico dell'Amministrazione, siano dotati di adeguate misure di protezione antivirus.

• Il personale delle ditte addette alla manutenzione dei supporti informatici deve usare solo supporti rimovibili preventivamente controllati e certificati singolarmente ogni volta.

• I supporti di archiviazione rimovibili provenienti dall'esterno devono essere sottoposti a verifica da attuare con una postazione di lavoro dedicata, non collegata in rete (macchina da quarantena).

• Il personale deve essere a conoscenza che la creazione e la diffusione, anche accidentale dei virus è punita

dall'Articolo 615 quinquies del Codice penale concernente la "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico … [omissis]… che prevede la reclusione sino a due anni e la multa sino a lire venti milioni".

• Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

• È proibito l'uso di qualsiasi software diverso da quello fornito dall'Amministrazione.

In questo ambito, al fine di minimizzare i rischi di distruzione anche accidentale dei dati a causa dei virus informatici, il Responsabile per la sicurezza informatica stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

Politiche per le azioni consuntive

Nel caso in cui su una o più postazioni di lavoro dovesse verificarsi perdita di informazioni, integrità o confidenzialità delle stesse a causa di infezione o contagio da virus informatici, il titolare della postazione interessata deve immediatamente isolare il sistema e poi notificare l'evento al responsabile della sicurezza, o suo delegato, che deve procedere a:

• verificare se ci sono altri sistemi infettati con lo stesso Virus Informatico;
• verificare se il virus ha diffuso dati;
• identificare il virus;
• attivare l'antivirus adatto ad eliminare il virus rilevato e bonificare il sistema infetto;
• installare l'Antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
• diffondere la notizia dell'evento, all'interno dell'Amministrazione, nelle forme opportune.

Politiche - Uso non accettabile

Le seguenti attività sono in generale proibite. Il personale può essere esentato da queste restrizioni in funzione del ruolo ricoperto all'interno dell'Amministrazione (ad esempio, nessuno può disconnettere e/o disabilitare le risorse ad eccezione degli amministratori di sistema o di rete).

In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.

L'elenco seguente non vuole essere una lista esaustiva, ma un tentativo di fornire una struttura di riferimento per identificare attività illecite o comunque non accettabili.

Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

• Violazioni dei diritti di proprietà intellettuale di persone o società, o diritti analoghi includendo, ma non limitando, l'installazione o la distribuzione di copie pirata o altri software prodotti che non sono espressamente licenziati per essere usati dall'Amministrazione.

• Copie non autorizzate di materiale protetto da copyright (diritto d'autore) includendo, ma non limitando, digitalizzazione e distribuzione di foto e immagini di riviste, libri, musica e ogni altro software tutelato per il quale l'Amministrazione o l'utente finale non ha una licenza attiva.

• È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.

• Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.

• Rivelazione delle credenziali personali ad altri o permettere ad altri l'uso delle credenziali personali, includendo in ciò i familiari o altri membri della famiglia quando il lavoro d'ufficio è fatto da casa o a casa.

• Usare un sistema dell'Amministrazione (PC o server) per acquisire o trasmettere materiale pedo-pornografico o che offende la morale o che è ostile alle leggi e regolamenti locali, nazionali o internazionali.

• Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.

• Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.

• Realizzare brecce nelle difese periferiche della rete del sistema informativo dell'Amministrazione o distruzione della rete medesima, dove per brecce della sicurezza si intendono, in modo riduttivo:

- accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
- attività di "sniffing";
- disturbo della trasmissione;
- spoofing dei pacchetti;
- negazione del servizio;
- modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;
- attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

• Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.

• Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.

• Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.

• Usare o scrivere qualunque programma o comando o messaggio che possa interferire o con i servizi

dell'Amministrazione o disabilitare sessioni di lavoro avviate da altri utenti di Internet/Intranet/Extranet.
- Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.
- Inviare messaggi di posta elettronica non sollecitati, includendo "messaggi spazzatura", o altro materiale di avviso a persone che non hanno specificamente richiesto tale materiale (spamming).
- Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
- Uso non autorizzato delle informazioni della testata delle e-mail,
- Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
- Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
- Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

Linee telefoniche commutate (analogiche e digitali)

Scopo

Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).

Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

Ambito di applicazione

Queste politiche sono relative solo a quelle linee che sono terminate all'interno della/e sede/i dell'Amministrazione. Sono pertanto escluse le eventuali linee collegate con le abitazioni degli impiegati che operano da casa e le linee usate per gestire situazioni di emergenza.

Politiche – Scenari di impatto sull'Amministrazione

Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.

Il *primo* è quello di un attaccante esterno che chiama un gruppo di numeri telefonici nella speranza di accedere alle risorse elaborative che hanno un modem collegato. Se il modem è predisposto per la risposta automatica, allora ci sono buone probabilità di accesso illecito al sistema informativo attraverso un server non monitorato. In questo scenario, al minimo possono essere compromesse solo le informazioni contenute sul server.

Il *secondo* scenario è la minaccia di una persona esterna che può accedere fisicamente alle risorse dell'Amministrazione e utilizza illecitamente un PC da tavolo o portatile corredato di un modem connesso alla rete. In questo caso l'intruso potrebbe essere capace di connettersi, da un lato, alla rete sicura dell'Amministrazione attraverso la rete locale e, dall'altro, simultaneamente di collegarsi con il modem ad un sito esterno sconosciuto (ma precedentemente predisposto). Potenzialmente potrebbe essere possibile trafugare tutte le informazioni dell'Amministrazione, comprese quelle vitali.

Politiche – Telefax

Dovrebbero essere adottate le seguenti regole:
- le linee fax dovrebbero essere approvate solo per uso istituzionale;
- nessuna linea dei telefax dovrebbe essere usata per uso personale;

Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.

Eventuali deroghe a queste politiche possono essere valutate ed eventualmente concesse dal Responsabile della sicurezza caso per caso dopo una attenta valutazione delle necessità dell'Amministrazione rispetto ai livelli di sensitività dei dati.

Politiche – Collegamento di PC alle linee telefoniche analogiche

La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.

Le linee commutate rappresentano una significativa minaccia per l'Amministrazione di attacchi esterni. Le eccezioni alle precedenti politiche dovrebbero essere valutate caso per caso dal responsabile della sicurezza.

Politiche – Richiesta di linee telefoniche analogiche

Una volta approvata la richiesta individuale di linea commutata dal responsabile dell'incaricato all'uso della linea medesima, questa deve essere corredata dalle seguenti informazioni da indirizzare al responsabile della sicurezza di rete:
- una chiara e dettagliata relazione che illustri la necessità di una linea commutata dedicata in alternativa alla disponibilità di rete sicura dell'Amministrazione;
- lo scopo istituzionale per cui si rende necessaria la linea commutata;
- il software e l'hardware che deve essere collegato alla linea e utilizzato dall'incaricato;
- che cosa la connessione esterna richiede per essere acceduta.

Politiche per l'inoltro automatico di messaggi di posta elettronica

Scopo

Lo scopo di queste politiche è prevenire rivelazioni non autorizzare o involontarie di informazioni confidenziali o sensitive dell'Amministrazione

Ambito di applicazione

Queste politiche riguardano l'inoltro automatico di messaggi e quindi la possibile trasmissione involontaria di informazioni confidenziali o sensitive a tutti gli impiegati o soggetti terzi.

Politiche

- Gli impiegati devono esercitare estrema attenzione quando inviano qualsiasi messaggio all'esterno dell'Amministrazione. A meno che non siano espressamente approvati dal Dirigente responsabile i messaggi non devono essere automaticamente inoltrati all'esterno dell'Amministrazione.
- Informazioni confidenziali o sensitive non devono essere trasmesse per posta elettronica a meno che, non siano espressamente ammesse e precedentemente cifrate in accordo con il destinatario.

Politiche per le connessioni in ingresso su rete commutata

Scopo

Proteggere le informazioni elettroniche dell'Amministrazione contro compromissione involontaria da parte di personale autorizzato ad accedere dall'esterno su rete commutata.

Ambito di applicazione

Lo scopo di queste politiche è definire adeguate modalità di accesso da remoto ed il loro uso da parte di personale autorizzato.

Politiche

- Il personale dell'Amministrazione e le persone terze autorizzate (clienti, venditori, altre amministrazioni, cittadini, etc.) possono utilizzare la linea commutata per guadagnare l'ingresso alla Intranet dell'Amministrazione. Tale accesso dovrebbe essere rigidamente controllato usando sistemi di autenticazione forte, quali: password da usare una sola volta (one time password), sistemi di firma digitale o tecniche di challenger/response.
- È responsabilità del personale con i privilegi di accesso dall'esterno alla rete dell'Amministrazione garantire che personale non autorizzato possa accedere illecitamente alla Intranet dell'Amministrazione ed alle sue informazioni. Tutto il personale che può accedere al sistema informativo dell'Amministrazione dall'esterno deve essere consapevole che tale accesso costituisce "realmente" una estensione del sistema informativo che potenzialmente può trasferire informazioni sensitive.
- Il personale e le persone terze devono, di conseguenza, porre in essere tutte le ragionevoli misure di sicurezza in loro possesso per proteggere il patrimonio informativo ed i beni dell'Amministrazione.
- Solo la linea commutata convenzionale può essere utilizzata per realizzare il collegamento. Non sono ammessi cellulari per realizzare collegamenti dati facilmente intercettabili o che consentono un reinstradamento della connessione.

Politiche per l'uso della posta istituzionale dell'amministrazione

Scopo

Evitare l'offuscamento dell'immagine dell'Amministrazione. Quando un messaggio di posta esce dall'Amministrazione il pubblico tenderà a vedere ed interpretare il messaggio come una affermazione ufficiale dell'Amministrazione.

Ambito di applicazione

La politica di seguito descritta intende illustrare l'uso appropriato della posta elettronica istituzionale in uscita che deve essere adottata da tutto il personale e dagli interlocutori dell'Amministrazione stessa.

Politiche – Usi proibiti

- Il sistema di posta dell'Amministrazione non deve essere usato per la creazione o la distribuzione di ogni distruttivo od offensivo messaggio, includendo come offensivi i commenti su razza, genere, capelli, colore, disabilità, età, orientamenti sessuali, pornografia, opinioni e pratiche religiose o nazionalità. Gli impiegati che ricevono messaggi con questi contenuti da colleghi dovrebbero riportare questi eventi ai diretti superiori immediatamente.

Politiche – Uso personale

È considerato accettabile l'uso personale della posta istituzionale dell'Amministrazione a condizione che:

- i messaggi personali siano archiviati in cartelle separate da quelle di lavoro;
- venga utilizzata una ragionevole quantità di risorse pubbliche;
- non si avviino catene di lettere o messaggi scherzosi, di disturbo o di altro genere.
- Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
- L'Amministrazione può però controllare senza preavviso i messaggi che transitano in rete per verificare il rispetto delle politiche concernenti gli "usi proibiti" di cui sopra.

Politiche per le comunicazioni wireless

Scopo

Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
Solo i sistemi wireless che si adattano a queste politiche o hanno la garanzia di sicurezza certificata dal responsabile della sicurezza, possono essere utilizzati per realizzare i collegamenti all'Amministrazione.

Ambito di applicazione

La politica riguarda tutti i dispositivi di comunicazione dati senza fili collegati (PC e cellulari telefonici) alla Intranet dell'Amministrazione, ovvero qualunque dispositivo di comunicazione wireless capace di trasmettere "pacchetti" di dati.
Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

Politiche – Registrazione delle schede di accesso

Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
Questi dispositivi sono soggetti a periodiche "prove di penetrazione" e controlli (auditing). Tutte le schede di PC da tavolo o portatili devono essere parimenti registrate.

Politiche – Approvazione delle tecnologie

Tutti i dispositivi di accesso alle LAN dell'Amministrazione devono utilizzare prodotti di venditori accreditati dal responsabile della sicurezza e configurati in sicurezza.

Allegato 5 - Sottoscrizione dei documenti formati dall'AOO

Documenti da sottoscrivere con firma digitale in ambito comunale

- Delibere
- Liquidazioni
- Ordinanze
- Richiesta pareri tecnici diversi Uffici
- Richiesta pareri per consigli di partecipazione
- Richiesta pareri per piani particolareggiati
- Richiesta pareri Urbanistica – OO.PP.
- Richiesta emissione ordinanza
- Richiesta licenze per manifestazioni
- Richiesta accertamenti per utenti ERP
- Richiesta accertamenti per buono affitto
- Richiesta accertamenti edilizia privata
- Richiesta sopralluoghi SUA
- Richiesta attivazione procedimento SUA
- Richiesta pareri COSAP
- Autorizzazione consultazione fondi archivistici e riproduzione documenti
- Comunicazione abusi edilizi
- Rilascio pareri PM
- Rilevazione abusi edilizi
- Comunicazioni per accertamenti abusi
- Comunicazioni al SUA
- Richieste verifiche edilizia privata
- Rilascio pareri edilizia privata
- Rilascio pareri OO.PP.
- Variazioni anagrafiche
- Richieste accertamenti
- Variazioni stato civile
- Richieste notifiche elettorali
- Richiesta notifica precetti
- Trasmissione documentazioni SUA
- Richiesta procedure autorizzatorie SUA
- Verifiche varie SUA
- Contratti
- Richiesta attestazione per esenzione TARSU
- Richiesta verifiche agibilità immobili

Documenti da sottoscrivere con firma qualificata in ambito comunale

- Proposta variazioni bilancio e PEG
- Richiesta proposta attivazione tirocinio
- Richiesta ferie - permessi - straordinario
- Ordinativi economali
- Buoni economali
- Comunicazione elenchi agevolazione rette scolastiche
- Richiesta verifica percorsi scuolabus
- Richiesta dati anagrafico-statistici
- Richiesta pareri tecnici convenzioni e piani di sviluppo
- Richiesta sopralluoghi musei
- Richiesta servizio d'ordine festa dei parchi
- Verifiche condizioni sociali utenti
- Rilascio nulla osta obiettori
- Aggiornamento carichi di lavoro
- Comunicazioni per ordinativi incassi
- Richieste rimborsi
- Comunicazioni per pagamenti aree PEEP
- Comunicazioni pagamenti per attività estrattive
- Predisposizione schema contratti di locazione

- Comunicazioni aggiornamento canoni di locazione
- Comunicazioni per pagamenti contributi
- Rilascio pareri utilizzo strade
- Rilascio nulla osta per tasse consortili
- Invio assegnazione numeri civici
- Predisposizione schema convenzioni
- Rilevazione presenze commissione edilizia ed ambiente
- Richiesta stanziamenti capitoli di bilancio
- Richiesta pareri applicazione IVA
- Certificazioni anagrafiche
- Comunicazione mensile incassi diritti
- Richiesta pagamento fornitura CI.
- Convocazione CEC
- Nota spese contrattuali
- Buoni d'ordine per forniture
- Comunicazione spese postali
- Comunicazioni varie Gabinetto Sindaco
- Predisposizione tabulati liquidazione stipendi ed assimilati
- Predisposizione bilancio di previsione e rendiconto di gestione
- Completamento delibere lavori e atto liquidazione
- Relazioni P.O. sull'attività gestionale
- Comunicazioni d'incasso
- Comunicazioni rettifiche aggiornamenti
- Richiesta versamento spese gestione c.c.p.
- Report informativi controllo gestione
- Proposte stanziamento bilancio di previsione
- Report SAL PEG CDG STAT SG
- Comunicazioni relative al controllo di gestione S.Q.

Documenti che non necessitano di alcuna firma elettronica

- Report stato avanzamento PEG
- Convocazioni riunioni diversi uffici Richiesta di manutenzioni tecnico/informatiche
- Comunicazioni organizzative
- Informative su legge e circolari
- Verifiche economie di bilancio
- Richiesta riutilizzo economie
- Concessione utilizzo sale pubbliche
- Organizzazione e attività ufficio stampa
- Concessione materiale audiovisivo
- Comunicati stampa attività universitarie
- Corrispondenza gruppo tecnico turismo
- Rilascio elaborazioni statistiche
- Invio dati statistici
- Trasmissione bandi di gara con esiti
- Richiesta e trasmissione informazioni uffici diversi
- Disposizioni di servizio P.M.
- Richieste dati anagrafici
- Assegnazione obiettori
- Autorizzazioni vendite alloggi in aree concesse in diritto di superficie
- Comunicazioni relative ad attestazione ISEE
- Richieste varie utenti ERP e non
- Aggiornamento cartografia
- Invio verbale commissione ambiente
- Richiesta scarto atti Archivio comunale
- Invio atti informativi applicazione contratti e normative fiscali
- Richieste verifiche natura spazi ed aree pubbliche
- Trasmissione tabulati presenze mensa
- Invio prospetto materiale di cancelleria–carta
- Elaborazioni statistiche

Allegato 6 - Regole di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale

La corrispondenza viene quotidianamente raccolta dal servizio postale pubblico dal personale dell'Ufficio Posta della UOP dell'Amministrazione/AOO alle ore 09.00. di ogni giorno;

La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, o quant'altro necessiti di spedizione postale viene consegnata in busta chiusa al servizio postale pubblico alle ore 12.30 di ogni giorno;

Gli Uffici Utente devono far pervenire la posta in partenza all'Ufficio Posta della UOP generale che esegue la spedizione entro e non oltre le ore 12,00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

Allegato 7 - Modulo di consultazione della sezione di deposito e storica dell'archivio

All'Amministrazione Comunale di San Benedetto del Tronto
Servizio archivistico
Sede

Oggetto: Richiesta di consultazione del materiale documentario conservato nella sezione di deposito/storica dell'Archivio generale dell'Amministrazione.

Scopo della Consultazione _____

Durata indicativa della consultazione: _____ mesi

Materiale da consultare:

- **Titolo** _____
- **Classe** _____
- **Sottoclasse** _____
- **Descrizione dei fascicoli:**
  - Oggetto del Fascicolo _____
  - Anno di Repertoriazione _____
  - Dal Numero _____ al numero _____
- **Descrizione dei sottofascicoli:**
  - Oggetto del Fascicolo _____
  - Anno di Repertoriazione _____
  - Dal Numero _____ al numero _____
- **Descrizione degli inserti:**
  - Oggetto del Fascicolo _____
  - Anno di Repertoriazione _____
  - Dal Numero _____ al numero _____

Note: _____

San Benedetto del Tronto, lì ___/_____/ _____

Firma del Richiedente

_____

L'operatore ricevente _____

IL RESPONSABILE DELL'ARCHIVIO: _____

ALLEGATO 8 - Elenco dei documenti esclusi dalla registrazione di protocollo

Sono escluse dalla protocollazione, ai sensi dell'art. 53. c. 5 del DPR n. 445/2000 le seguenti tipologie documentarie:

- Gazzette ufficiali, Bollettini ufficiali PA
- Notiziari PA
- Giornali, Riviste, Libri
- Materiali pubblicitari
- Note di ricezione circolari
- Note di ricezione altre disposizioni
- Materiali statistici
- Atti preparatori interni
- Offerte o preventivi di terzi non richiesti
- Inviti a manifestazioni che non attivino procedimenti amministrativi
- Biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti ecc.)
- Allegati, se non accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)
- Richieste ferie
- Richieste permessi
- Richieste di rimborso spese e missioni
- Verbali e delibere del Consiglio comunitario;
- Verbali e delibere della Giunta esecutiva;
- Determinazioni
- Le ricevute di ritorno delle raccomandate A.R.
- Documenti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa presente o futura
- Gli allegati se accompagnati da lettera di trasmissione, ivi compresi gli elaborati tecnici
- Corsi di aggiornamento
- Certificati di malattia
- Variazione sedi ed anagrafe ditte fornitrici
- Convocazioni ad incontri o riunioni e corsi di formazione interni
- Pubblicità conoscitiva di convegni
- Pubblicità in generale
- Offerte e Listini prezzi
- Solleciti di pagamento (salvo che non costituiscano diffida)
- Comunicazioni da parte di Enti di bandi di concorso, di domande da presentare entro….
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Richieste di copia/visione di atti amministrativi
- Non saranno registrate a protocollo le certificazioni anagrafiche rilasciate direttamente al richiedente, le richieste e/o trasmissioni di certificati e tutta la corrispondenza dell'anagrafe, stato civile e leva diretta agli uffici comunali.
- Richieste di affissione all'albo pretorio e conferma dell'avvenuta pubblicazione
- Comunicazioni di cessione di fabbricato ex L. 191/78
- Assicurazioni d i avvenuta notifica

Allegato 9 - Elenco dei documenti soggetti a registrazione particolare (repertori)

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto all'interno dell'Amministrazione/AOO un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati.
Nel caso di riservatezza temporanea delle informazioni è necessario indicare, contestualmente alla registrazione di protocollo, anche l'anno, il mese ed il giorno nel quale le informazioni temporaneamente riservate divengono soggette all'accesso ordinariamente previsto.

- Documenti relativi a vicende di persone o a fatti privati o particolari;
- Documenti di carattere politico e di indirizzo che, se resi di pubblico dominio, possono ostacolare il raggiungimento degli obbiettivi prefissati;
- Documenti dalla cui contestuale pubblicità possa derivare pregiudizio a terzi o al buon andamento dell'attività amministrativa;
- I documenti anonimi individuati ai sensi dell'art. 8, comma 4, e 141 del codice di procedura penale;
- corrispondenza legata a vicende di persone o a fatti privati o particolari;
- le tipologie di documenti individuati dall'art. 24 della legge 7 agosto 1990 n. 241; dall'art. 8 del DPR 27 giugno 1992 n. 352, nonché dalla legge 675/96 (e successive modifiche ed integrazioni) e norme collegate.
- Atti rogati o autenticati dal segretario comunale (registrazione informatica e cartacea);
- Contratti e convenzioni (registrazione informatica e cartacea);
- Verbali delle adunanze del Consiglio comunale (registrazione informatica);
- Verbali delle adunanze della Giunta comunale (registrazione informatica);
- Verbali degli organi collegiali del Comune (registrazione informatica);
- Autorizzazioni commerciali (registrazione cartacea);
- Autorizzazioni artigiane (registrazione cartacea);
- Autorizzazioni turistiche (registrazione cartacea);
- Autorizzazioni di pubblica sicurezza (registrazione cartacea);
- Autorizzazioni di polizia mortuaria (registrazione informatica);
- Autorizzazioni igienico-sanitaria e veterinaria (registrazione cartacea);
- Licenze di pesca (registrazione cartacea);
- Certificati di iscrizione all'anagrafe canina;
- Atti di stato civile (registrazione informatica);
- Pubblicazioni di matrimonio (registrazione informatica);
- Carte d'identità (registrazione informatica);
- Certificati anagrafici;
- Tessere elettorali (registrazione informatica);
- Rapporti incidenti (registrazione informatica);
- Verbali oggetti smarriti;
- Verbali CdS (registrazione informatica);
- Richieste permessi transito ZTL.
- Fatture attive (registrazione informatica);
- Liquidazioni (registrazione informatica);
- Mandati di pagamento (registrazione informatica);
- Reversali (registrazione informatica);
- Dichiarazioni ICI (registrazione informatica).
- Registro verbali di violazione regolamenti e leggi varie;
- Fatture emesse registri IVA;
- Autorizzazioni sanitarie registro autorizzazioni sanitarie; Autorizzazioni commerciali registro autorizzazioni commerciali;
- Autorizzazioni di pubblico esercizio registro autorizzazioni di pubblico;
- I verbali di violazione del Codice della strada ed i verbali di violazioni amministrative.
- Dichiarazioni per la certificazione ISEE – Riccometro (registrazione cartacea)
- Deliberazioni di Consiglio comunale registro delle deliberazioni del consiglio comunale;
- Deliberazioni di Giunta comunale registro delle deliberazioni della giunta comunale;
- Determinazioni dei responsabili dei servizi registro delle determinazioni;
- Decreti protocollati al protocollo generale;
- Ordinanze registro delle ordinanze;
- Contratti in forma pubblica;
- Repertorio dei contratti;
- Documenti anonimi o non firmati non soggetti ad alcuna registrazione;

- Documenti totalmente illeggibili nel testo non soggetti ad alcuna registrazione;
- Documenti con mittente non riconoscibile non soggetti ad alcuna registrazione;
- Fatture senza lettera di trasmissione registrazione a cura dell'ufficio ragioneria;
- Permessi di costruire registro dei permessi di costruire;
- Verbali di violazione Codice della strada registro dei verbali di violazione Codice della strada;
- Atti pubblicati all'Albo pretorio registro pubblicazioni Albo pretorio;
- Atti depositati nella casa comunale registro deposito atti alla casa comunale;
- Notifiche registro notifiche;
- Verbali di violazione regolamenti comunali e leggi varie (escluso il CdS);
- Le denunce di variazioni ai fini ICI;
- La TARSU;
- L'occupazione di suolo pubblico ed altri tributi ed entrate dell'Amministrazione.

Titolo I. Amministrazione generale

- Registro di protocollo
- Repertorio dei fascicoli
- Registro dell'Albo pretorio
- Registro delle notifiche
- Ordinanze emanate dal Sindaco: serie con repertorio
- Decreti del Sindaco: serie con repertorio
- Ordinanze emanate dai dirigenti
- Determinazioni dei dirigenti
- Deliberazioni del Consiglio comunale
- Deliberazioni della Giunta comunale
- Verbali delle adunanze del Consiglio comunale
- Verbali delle adunanze della Giunta comunale
- Verbali degli organi collegiali del Comune
- Contratti e convenzioni
- Albo dell'associazionismo: elenco delle associazioni accreditate
- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

- Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive

Titolo III. Risorse umane

- Registro infortuni
- Elenco degli incarichi conferiti
- Verbali dei rappresentanti dei lavoratori per la sicurezza

Titolo IV. Risorse finanziarie e patrimoniali

- Mandati
- Reversali
- Concessioni di occupazione suolo pubblico
- Concessioni di beni del demanio statale
- Elenco dei fornitori (facoltativo)

Titolo VI. Pianificazione e gestione del territorio

- Concessioni edilizie

Titolo VII. Servizi alla persona

- Verbali degli organi di gestione degli Istituti culturali

Titolo VIII. Attività economiche

- Repertorio delle autorizzazioni artigiane
- Repertorio delle autorizzazioni commerciali
- Repertorio delle autorizzazioni turistiche

Titolo IX. Polizia locale e sicurezza pubblica

- Autorizzazioni di pubblica sicurezza
- Verbali degli accertamenti

Titolo X. Tutela della salute

- Repertorio delle autorizzazioni sanitarie
- Repertorio delle concessioni di agibilità

Titolo XI. Servizi demografici

- Registro dei nati
- Registro dei morti
- Registro dei matrimoni
- Registro di cittadinanza
- Registro della popolazione
- Registri di seppellimento
- Registri di tumulazione
- Registri di esumazione
- Registri di estumulazione
- Registri di cremazione
- Registri della distribuzione topografica delle tombe con annesse schede onomastiche

Titolo XII. Elezioni e iniziative popolari

- Verbali della commissione elettorale comunale
- Verbali dei presidenti di seggio

Allegato 10 - Piano di conservazione

Il massimario è soggetto a revisione ed aggiornamento per adeguarsi alla documentazione che può essere prodotta dall'Amministrazione.

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.

Indice dei titoli

Titolo I. Amministrazione generale

Classi	Tipologie documentarie	Conservazione	Note
1. Legislazione e circolari esplicative			
	Pareri chiesti dal Comune su leggi specifiche	Permanente	
	Circolari pervenute: repertorio annuale	Permanente	
	Circolari emanate dal Comune: repertorio annuale	Permanente	
2. Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica			
	Denominazione del Comune	Permanente	
	Attribuzione del titolo di città	Permanente	
	Confini del Comune	Permanente	
	Costituzione delle circoscrizioni	Permanente	
	Verbali e deliberazioni della Commissione comunale per la toponomastica: repertorio annuale	Permanente	
3. Statuto			
	Redazione, modifiche e interpretazioni dello statuto	Permanente, dopo sfoltimento del materiale informativo relativo ad altri Comuni	
4. Regolamenti			
	Regolamenti emessi dal Comune: repertorio annuale	Permanente	
	Redazione dei regolamenti: un fasc. per ciascun affare	Permanente, previo sfoltimento dei documenti di carattere transitorio	Tenere un solo esemplare, scartare gli altri
5. Stemma, gonfalone, sigillo			
	Definizione, modifica, riconoscimento dello stemma	Permanente	
	Definizione, modifica, riconoscimento del gonfalone	Permanente	
	Definizione, modifica, riconoscimento del sigillo	Permanente	
	Concessione del patrocinio gratuito e del connesso uso dello stemma del Comune: fasc. annuale per attività	Permanente	Perché documenta attività che si svolgono nel territorio
6. Archivio generale			
	Registro di protocollo	Permanente	
	Repertorio dei fascicoli	Permanente	

	Organizzazione del servizio e dell'attività ordinaria (aggiornamento del manuale di gestione con titolario e piano di conservazione, selezione periodica, riordino, inventariazione, spostamenti e versamenti di materiale, depositi e comodati):	Permanente	
	Interventi straordinari (ad esempio, traslochi, restauri, gestione servizi esterni, scelta del software di gestione)	Permanente	
	Richieste di accesso per fini amministrativi	1 anno dalla ricollocazione del materiale	
	Richieste di informazioni archivistiche e richieste per motivi di studio	Permanente	
	Richieste di pubblicazione all'albo pretorio	1 anno	
	Registro dell'Albo pretorio	20 anni	
	Richieste di notifica presso la casa comunale (con allegati)	2 anni	
	Registro delle notifiche	20 anni	
	Registri delle spedizioni e delle spese postali	1 anno	
	Ordinanze del Sindaco: repertorio	Permanente	
	Decreti del Sindaco: repertorio	Permanente	
	Ordinanze dei dirigenti: repertorio	Permanente	
	Determinazioni dei dirigenti: repertorio	Permanente	
	Deliberazioni del Consiglio comunale: repertorio	Permanente	
	Deliberazioni della Giunta comunale: repertorio	Permanente	
	Verbali delle adunanze del Consiglio comunale: repertorio	Permanente	
	Verbali delle adunanze della Giunta comunale: repertorio	Permanente	
	Verbali degli altri organi collegiali del Comune: repertorio	Permanente	
	Verbali delle adunanze dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni dei Consigli circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Verbali delle adunanze degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Deliberazioni degli Esecutivi circoscrizionali: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Verbali degli organi collegiali delle circoscrizioni: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Registro dell'Albo della circoscrizione: un repertorio annuale per ciascuna circoscrizione	Permanente	
	Contratti e convenzioni: repertorio	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Contratti e convenzioni delle circoscrizioni: un repertorio per ciascuna circoscrizione	Permanente	20 anni per un'eventuale serie separata di contratti di scarsa rilevanza
	Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa)	Permanente	
7. Sistema informativo			
	Organizzazione del sistema	Permanente	
	Statistiche	Permanente, dopo l'eliminazione dei materiali preparatori	
8. Informazioni e relazioni con il pubblico			
	Iniziative specifiche dell'URP: un fasc. per ciascun affare	Permanente, dopo sfoltimento del carteggio di carattere transitorio e strumentale	
	Reclami dei cittadini (comunque pervenuti)	Permanente	
	Atti del Difensore civico	Permanente	
	Bandi e avvisi a stampa	Permanente	
	Materiali preparatori per il sito Web	Permanente	
9. Politica del personale; ordinamento degli uffici e dei servizi			
	Attribuzione di competenze agli uffici	Permanente	

	Organigramma: un fasc. per ciascuna definizione dell'organigramma	Permanente	
	Organizzazione degli uffici: un fasc. per ciascun affare	Permanente	
	Orari di apertura degli uffici comunali e degli altri uffici e attività insistenti sul territorio comunale	Permanente	
	Materiale preparatorio per le deliberazioni in materia di politica del personale	10 anni	
10. Relazioni con le organizzazioni sindacali e di rappresentanza del personale			
	Rapporti di carattere generale	Permanente	
	Costituzione delle rappresentanze del personale	Permanente	
	Verbali della Delegazione trattante per la contrattazione integrativa decentrata	Permanente	
11. Controlli esterni			
	Controlli	Permanente	
12. Editoria e attività informativo-promozionale interna ed esterna			
	Pubblicazioni istituzionali del Comune (libri, riviste, inserzioni o altro)	Permanente	
	Pubblicazioni istituzionali del Comune (materiali preparatori)	2 anni	
	Comunicati stampa	Permanente	
13. Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti			
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente	
	Onorificenze (concesse e ricevute): un fasc. per ciascun evento	Permanente	
	Concessione dell'uso del sigillo: un fasc. annuale	Permanente	
14. Interventi di carattere politico e umanitario; rapporti istituzionali			
	Iniziative specifiche (ad esempio, adesione a movimenti di opinione): un fasc. per ciascun affare	Permanente	
	Gemellaggi	Permanente	
	Promozione di comitati: un fasc. per ciascun affare	Permanente	
15. Forme associative e partecipative per l'esercizio di funzioni e servizi e adesione del Comune ad Associazioni			
	Costituzione di enti controllati dal Comune (comprensivo della nomina dei rappresentanti e dei verbali inviati per approvazione)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
	Partecipazione del Comune a enti e associazioni (comprensivo della nomina dei rappresentanti)	Permanente, previo sfoltimento del carteggio di carattere transitorio	
16. Area e città metropolitana			
	Costituzione e rapporti istituzionali	Permanente	
17. Associazionismo e partecipazione			
	Politica di incoraggiamento e appoggio alle associazioni	Permanente	
	Albo dell'associazionismo: elenco delle associazioni accreditate	Permanente	
	Fascicoli delle associazioni che chiedono l'iscrizione all'albo	Permanente	

Titolo II. Organi di governo, gestione, controllo, consulenza e garanzia

Classi	Tipologie documentarie	Conservazione	Note
1. Sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
2. Vice-sindaco			
	Fasc. personale che dura quanto il mandato	Permanente	
3. Consiglio			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	

	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni e mozioni consiliari	Permanente	dopo sfoltimento
	Bollettino della situazione patrimoniale dei titolari di cariche elettive e di cariche direttive	Permanente	
4. Presidente del Consiglio			
	Fasc. personale che dura quanto il mandato	Permanente	
5. Conferenza dei capigruppo e Commissioni del Consiglio			
	Verbali della Conferenza	Permanente	
	Verbali delle Commissioni	Permanente	
6. Gruppi consiliari			
	Accreditamento presso il Consiglio	Permanente	Scartare i materiali prodotti o raccolti dai Gruppi
7. Giunta			
	Nomine, revoche e dimissioni degli assessori	Permanente	
	Convocazioni della Giunta e OdG	1 anno	Purché riportati nei verbali
8. Commissario prefettizio e straordinario			
	Fasc. personale	Permanente	
9. Segretario e Vice-segretario			
	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
10. Direttore generale e dirigenza			
	Fasc. personale	Permanente	
11. Revisori dei conti			
	Fasc. personale	Permanente	
12. Difensore civico			
	Fasc. personale	Permanente	
13. Commissario *ad acta*			
	Fasc. personale	Permanente	
14. Organi di controllo interni			
	Un fasc. per ogni organo	Permanente	
15. Organi consultivi			
	Un fasc. per ogni organo	Permanente	
16. Consigli circoscrizionali			
	Fasc. personali: un fasc. per ogni consigliere che dura quanto dura il mandato	Permanente	
	Convocazioni del Consiglio e OdG	1 anno	Purché riportati nei verbali
	Interrogazioni consiliari	Permanente	
17. Presidenti dei Consigli circoscrizionali			
	Fasc. personale che dura quanto il mandato	Permanente	
18. Organi esecutivi circoscrizionali			
	Nomine e dimissioni dei componenti	Permanente	
	Convocazioni e OdG delle riunioni	1 anno	Purché riportati nei verbali
19. Commissioni dei Consigli circoscrizionali			
	Un fasc. per ogni commissione	Permanente	
20. Segretari delle circoscrizioni			
	Fasc. personale (nomina, etc.) per la durata dell'incarico	Permanente	
21. Commissario *ad acta* delle circoscrizioni			
	Fasc. personale	Permanente	
22. Conferenza dei Presidenti di quartiere			
	Verbali della Conferenza	Permanente	

Titolo III. Risorse umane

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli personali dei dipendenti e assimilati (quindi anche collaboratori a contratto o a progetto)	Permanente previo sfolti-mento da eseguire seguendo la	

		tempistica prevista per le singole classi	
1. Concorsi, selezioni, colloqui			
	Criteri generali e normativa per il reclutamento del personale: un fasc. con eventuali sottofascicoli	Permanente	
	Procedimenti per il reclutamento del personale: un fasc. per ciascun procedimento (fasc. per affare), con i seguenti sottofascicoli: -Bando e manifesto - Domande - Allegati alle domande (ove previsti dal bando) - Verbali - Prove d'esame - Copie bando restituite al Comune	Permanente 1 anno dopo la scadenza dei termini per i ricorsi da restituire dopo la scadenza dei termini per i ricorsi permanente 1 anno dopo la scadenza dei termini per i ricorsi 1 anno dopo la scadenza dei termini per i ricorsi	Agli interessati
	Curricula inviati per richieste di assunzione	2 anni	
	Domande di assunzione pervenute senza indizione di concorso o selezione	1 anno	
2 Assunzioni e cessazioni			
	Criteri generali e normativa per le assunzioni e cessazioni	Permanente	
	Determinazioni di assunzione e cessazione dei singoli inserite nei singoli fascicoli personali	Permanente	
3. Comandi e distacchi; mobilità			
	Criteri generali e normativa per comandi, distacchi, mobilità	Permanente	
	Determinazioni di comandi, distacchi e mobilità inserite nei singoli fascicoli personali	Permanente	
4. Attribuzione di funzioni, ordini di servizio e missioni			
	Criteri generali e normativa per le attribuzioni di funzioni, ordini di servizio e missioni	Permanente	
	Determinazioni di attribuzione di funzioni inserite nei singoli fascicoli personali	Permanente	
	Determinazioni di missioni inserite nei singoli fascicoli personali	10 anni	
	Determinazioni di ordini di servizio inserite nei singoli fascicoli personali	Permanente	
	Ordini di servizio collettivi	Permanente	
	Autorizzazione allo svolgimento di incarichi esterni	2 anni	
5. Inquadramenti e applicazione contratti collettivi di lavoro			
	Criteri generali e normativa per gli inquadramenti e le applicazione dei contratti collettivi di lavoro	Permanente	
	Determinazione dei ruoli e contratti collettivi	Permanente	NB i contratti con il singolo confluiscono nel fasc. personale
	Determinazioni relative ai singoli	Permanente	
6. Retribuzioni e compensi			
	Criteri generali e normativa per le retribuzioni e compensi	Permanente	
	Anagrafe delle prestazioni: schede	5 anni	
	Determinazioni inserite nei singoli fascicoli personali	5 anni dalla cessazione dal servizio	
	Ruoli degli stipendi: base di dati/ tabulati	Permanente	
	Provvedimenti giudiziari di requisizione dello stipendio	5 anni	
7 Trattamento fiscale, contributivo e assicurativo			
	Criteri generali e normativa per gli adempimenti fiscali, contributivi e assicurativi	Permanente	
	Trattamento assicurativo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento contributivo inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
	Trattamento fiscale inserito nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	

	Assicurazione obbligatoria inserita nei singoli fascicoli personali	5 anni dalla chiusura del fascicolo	
8 Tutela della salute e sicurezza sul luogo di lavoro			
	Criteri generali e normativa per la tutela della salute e sicurezza sul luogo di lavoro	Permanente	
	Rilevazione dei rischi, ai sensi della 626/94: un fasc. per sede	Tenere l'ultima e scartare la precedente	
	Prevenzione infortuni	Permanente	
	Registro infortuni	Permanente	Per L. 626/94
	Verbali delle rappresentanze dei lavoratori per la sicurezza	Permanente	
	Denuncia di infortunio e pratica relativa, con referti, inserita nei singoli fascicoli personali	Permanente	
	Fascicoli relativi alle visite mediche ordinarie (medicina del lavoro)	10 anni	
9. Dichiarazioni di infermità ed equo indennizzo			
	Criteri generali e normativa per le dichiarazioni di infermità	Permanente	
	Dichiarazioni di infermità e calcolo dell'indennizzo inserite nel singolo fascicolo personale	Permanente	
10 Indennità premio di servizio e trattamento di fine rapporto, quiescenza			
	Criteri generali e normativa per il trattamento di fine rapporto	Permanente	
	Trattamento pensionistico e di fine rapporto inserito nel singolo fascicolo personale	Permanente	
11. Servizi al personale su richiesta			
	Criteri generali e normativa per i servizi su richiesta	Permanente	
	Domande di servizi su richiesta (mensa, asili nido, colonie estive, soggiorni climatici, etc.)	2 anni	
12. Orario di lavoro, presenze e assenze			
	Criteri generali e normativa per le assenze	Permanente	
	Domande e dichiarazioni dei dipendenti sul'orario inserite nel singolo fascicolo personale: -150 ore - permessi d'uscita per motivi personali - permessi per allattamento - permessi per donazione sangue - permessi per motivi sindacali - opzione per orario particolare e part-time	 2 anni 2 anni 2 anni 2 anni 2 anni Permanente	
	Domande e dichiarazioni dei dipendenti sulle assenze (con allegati) inserite nel singolo fascicolo personale: - congedo ordinario - congedo straordinario per motivi di salute - congedo straordinario per motivi personali e familiari - aspettativa per infermità - aspettativa per mandato parlamentare o altre cariche elettive - aspettativa obbligatoria per maternità e puerperio - aspettativa facoltativa per maternità e puerperio - aspettativa per motivi di famiglia - aspettativa sindacale - certificati medici	 2 anni 2 anni Alla cessazione dal servizio Permanente Permanente Permanente Permanente Permanente Permanente Alla cessazione dal servizio	
	Referti delle visite di controllo inseriti nel singolo fascicolo personale	Alla cessazione dal servizio	
	Fogli firma; cartellini marcatempo; tabulati elettronici di rilevazione presenze	2 anni	In assenza di pendenze disciplinari o giudiziarie
	Rilevazioni delle assenze per sciopero: - singole schede - prospetti riassuntivi	 1 anno dopo la redazione dei prospetti riassuntivi Permanente	
13. Giudizi, responsabilità e provvedimenti disciplinari			
	Criteri generali e normativa per i provvedimenti disciplinari	Permanente	

	Provvedimenti disciplinari inseriti nel singolo fascicolo personale	Permanente	
14. Formazione e aggiornamento professionale			
	Criteri generali e normativa per la formazione e l'aggiornamento professionale	Permanente	
	Organizzazione di corsi di formazione e aggiornamento: un fasc. per ciascun corso	Permanente previo sfoltimento dopo 5 anni	
	Domande/Invio dei dipendenti a corsi inseriti nel singolo fascicolo personale	Permanente previo sfoltimento dopo 5 anni	
15. Collaboratori esterni			
	Criteri generali e normativa per il trattamento dei collaboratori esterni	Permanente	
	Elenco degli incarichi conferiti: repertorio	Permanente	

Titolo IV. Risorse finanziarie e patrimoniali

Classi	Tipologie documentarie	Conservazione	Note
1.Bilancio preventivo e Piano esecutivo di gestione (PEG)			
	Bilancio preventivo e allegati, tra cui Relazione previsionale e programmatica	Permanente	
	PEG: articolato in fascicoli: un fasc. per ogni obiettivo	Permanente, previo sfoltimento	
	Carteggio prodotto dai differenti uffici del Comune per questioni afferenti alla formazione del bilancio e del PEG	10 anni	
2. Gestione del bilancio e del PEG (con eventuali variazioni)			
	Gestione del bilancio: un fasc. per ciascuna variazione	Permanente, previo sfoltimento	
3. Gestione delle entrate: accertamen-to, riscossione, versamento			
	Fascicoli personali dei contribuenti comunali: un fasc. per ciascun contribuente per ciascun tipo di imposte (ICI, TARSU, TOSAP, etc.), con eventuali sottofascicoli (variazioni, ricorsi, etc.)	10 dopo la cancellazione del contribuente dai ruoli	
	Ruolo ICI: base di dati/ stampe	10 anni	Prevedere una stampa periodica
	Ruolo imposta comunale sulla pubblicità: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo diritti sulle pubbliche affissioni: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo TARSU: base di dati	10 anni	Prevedere una stampa periodica
	Ruolo COSAP: base di dati	10 anni	Prevedere una stampa periodica
	Contratti di mutuo: un fasc. per ciascun mutuo	5 anni dall'estinzione del mutuo	
	Proventi da affitti e locazioni: un fasc. annuale per ciascun immobile locato	5 anni dal termine del contratto	
	Diritti di segreteria: registrini annuali o pagamenti virtuali	5 anni	
	Matrici dei bollettari delle entrate: registri annuali	5 anni	
	Ricevute dei versamenti in banca delle somme riscosse nelle differenti UOR per diritti di segreteria	5 anni	
	Fatture emesse: repertorio annuale	10 anni	
	Reversali	5 anni	
	Bollettari vari	5 anni	
	Ricevute di pagamenti vari	5 anni	
4 Gestione della spesa: impegno, liqui-dazione, ordinazione e pagamento			
	Impegni di spesa (determinazioni dei dirigenti delle UOR): copie inviate dalle UOR alla Ragioneria: repertorio annuale	2 anni	
	Fatture ricevute: repertorio annuale	10 anni	
	Atti di liquidazione con allegati trasmessi da ciascuna	2 anni	

	UOR: repertorio annuale		
	Mandati di pagamento con allegati emessi dalla Ragioneria e inviati alla Tesoreria: repertorio annuale	10 anni dall'approvazione del bilancio	Purché registrati in scritture contabili di sintesi
	Eventuali copie di mandati	2 anni	
5. Partecipazioni finanziarie			
	Gestione delle partecipazioni finanziarie: un fasc. per ciascuna partecipazione	Permanente, previo sfoltimento	
6. Rendiconto della gestione; adempimenti e verifiche contabili			
	Rendiconto della gestione, articolato in Conto del bilancio, Conto del patrimonio e Conto economico	Permanente	
7. Adempimenti fiscali, contributivi e assicurativi			
	Mod. 770	10 anni	Più se si ritiene opportuno
	Ricevute dei versamenti (IVA, IRPEF, etc.)	10 anni	
	Pagamento dei premi dei contratti assicurativi	5 anni dall'estinzione del contratto	
8. Beni immobili			
	Inventario dei beni immobili: registro o base di dati perenne	Permanente	
	Fascicoli dei beni immobili: un fasc. per ciascun bene immobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: -acquisizione - manutenzione ordinaria -gestione -uso - alienazione e dismissione	 Permanente 20 anni 5 anni 5 anni Permanente	
	Concessioni di occupazione di spazi e aree pubbliche: repertorio	Permanente	
	Concessioni di beni del demanio statale: repertorio	Permanente	
	Concessioni cimiteriali: repertorio	Permanente	
	Fascicoli personali dei concessionari: un fasc. per ciascun concessionario	5 anni dalla cessazione del rapporto	
9. Beni mobili			
	Inventari dei beni mobili: uno per consegnatario	Permanente	
	Fascicoli dei beni mobili: un fasc. per ciascun bene mobile, articolato nei seguenti sottofascicoli, relativi ad attività specifiche, che possono anche essere di competenza di UOR diverse: - acquisizione - manutenzione - concessione in uso - alienazione e altre forme di dismissione	 5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione 5 anni dalla dismissione	
10. Economato			
	Acquisizione di beni e servizi: un fasc. per ciascun acquisto	5 anni dalla dismissione del bene	
	Elenco dei fornitori: repertorio (in forma di base di dati)	Permanente	
11. Oggetti smarriti e recuperati			
	Verbali di rinvenimento: serie annuale repertoriata	2 anni	
	Ricevute di riconsegna ai proprietari: serie annuale repertoriata	2 anni	
	Vendita o devoluzione: un fasc. periodico (per attività)	2 anni	
12. Tesoreria			
	Giornale di cassa	Permanente	
	Mandati quietanzati, che vengono inviati in Ragioneria: repertorio periodico (mese/anno)	10 anni	
13 Concessionari ed altri incaricati della riscossione delle entrate			
	Concessionari: un fasc. per ciascuno dei concessionari	10 anni dalla cessazione del rapporto	
14. Pubblicità e pubbliche affissioni			
	Autorizzazioni alla pubblicità stabile: repertorio an-	5 anni dalla scadenza dell'au-	Salvo non si rilevi qualche neces-

	nuale	torizzazione	sità particolare di conservazione a campione
	Autorizzazioni alla pubblicità circoscritta: repertorio annuale	5 anni dalla scadenza dell'autorizzazione	
	Richieste di affissione (con allegati da affiggere): un fasc. per richiesta	5 anni dalla scadenza dell'autorizzazione	

Titolo V. Affari legali

Classi	Tipologie documentarie	Conservazione	Note
1. Contenzioso			
	Fascicoli di causa	Permanente	Concentrare quelli presso gli studi professionali esterni
2. Responsabilità civile e patrimoniale verso terzi; assicurazioni			
	Contratti assicurativi	2 anni dalla scadenza	
	Richieste e pratiche di risarcimento	10 anni	
3. Pareri e consulenze			
	Pareri e consulenze	Permanente	

Titolo VI. Pianificazione e gestione del territorio

Classi	Tipologie documentarie	Conservazione	Note
1. Urbanistica: piano regolatore generale e varianti			
	PGR	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Pareri su piani sovracomunali	Permanente	Dopo sfoltimento
	Certificati di destinazione urbanistica	1 anno dopo la scadenza	
	Varianti al PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
2. Urbanistica: strumenti di attuazione del piano regolatore generale			
	Piani particolareggiati del PRG	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di lottizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piani di edilizia economica e popolare – PEEP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano particolareggiato infrastrutture stradali - PPIS	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano di riqualificazione urbana – PRU	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Piano insediamenti produttivi - PIP	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Programma integrato di riqualificazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	programma di riqualificazione urbana e di sviluppo so-	Permanente	Possono essere eliminate le copie

	stenibile del territorio		degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
3. Edilizia privata			
	Autorizzazioni edilizie: repertorio	Permanente	
	Fascicoli dei richiedenti le autorizzazioni: un fasc. per ciascuna autorizzazione	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Accertamento e repressione degli abusi	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Denunce e relazioni finali delle opere in cemento armato	Fino a quando esiste l'edificio	
4. Edilizia pubblica			
	Costruzione di edilizia popolare	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
5. Opere pubbliche			
	Realizzazione di opere pubbliche	Permanente	Possono essere eliminate le copie degli elaborati non più occorrenti agli uffici ed il carteggio transitorio
	Manutenzione ordinaria	5 anni	Salvo necessità particolari
	Manutenzione straordinaria	20 anni	Salvo necessità particolari
6. Catasto			
	Catasto terreni: mappe	Permanente	
	Catasto terreni: registri	Permanente	
	Catasto terreni: indice alfabetico dei possessori	Permanente	
	Catasto terreni: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (volture)	Permanente	
	Catasto fabbricati: mappe	Permanente	
	Catasto fabbricati: registri	Permanente	
	Catasto fabbricati: indice alfabetico dei possessori	Permanente	
	Catasto fabbricati: estratti catastali	Permanente	
	Catasto terreni: denunce di variazione (volture)	Permanente	
	Richieste di visure e certificazioni	1 anno	
7. Viabilità			
	Piano Urbano del Traffico:un fasc. per ciascun affare	Permanente con sfoltimento	
	Piano Urbano della Mobilità: un fasc. per ciascun affare	Permanente con sfoltimento	
	Autorizzazioni in deroga: serie annuale repertoriata	2 anni	
8. Servizio idrico integrato, luce, gas, trasporti pubblici, gestione dei rifiuti e altri servizi			
	Approvvigionamento idrico (organizzazione e funzionamento)	Permanente con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative a favore dell'ambiente	Permanente con sfoltimento	
	Distribuzione dell'acqua: contratti con gli utenti	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Produzione di energia elettrica o altre fonti energetiche (organizzazione e funzionamento)	Permanente con sfoltimento	
	Distribuzione di energia elettrica o altre fonti energetiche: contratti con gli utenti:	2 anni dalla cessazione del rapporto	Purché in assenza di contenzioso
	Trasporti pubblici (gestione)	Permanente con sfoltimento	
	Vigilanza sui gestori dei servizi: un fasc. annuale per attività	Permanente con sfoltimento	
	Fascicoli relativi alle irregolarità	10 anni	
	Iniziative di sensibilizzazione degli utenti per consumi razionali: un fasc. per ciascuna iniziativa	Permanente con sfoltimento	
	Dichiarazioni di conformità degli impianti: repertorio	1 anno	

	annuale		
9. Ambiente: autorizzazioni, monitoraggio e controllo			
	Valutazioni e pareri di impatto ambientale: un fasc. per ciascun parere	Permanente	
	Monitoraggi della qualità delle acque: fasc. annuale per attività	10 anni	
	Monitoraggi della qualità dell'aria: fasc. annuale per attività	10 anni	
	Monitoraggi della qualità dell'etere: un fasc. annuale per attività	10 anni	
	Altri eventuali monitoraggi: fasc. annuale per attività	10 anni	
	Fascicoli relativi alle irregolarità	10 anni	
	Controlli a campione sugli impianti termici dei privati: fasc. annuale per attività	2 anni	
	Fascicoli relativi alle irregolarità	10 anni	
10. Protezione civile ed emergenze			
	Segnalazioni preventive di condizioni meteorologiche avverse: un fasc. annuale	2 anni	
	Addestramento ed esercitazioni per la protezione civile: un fasc. annuale	5 anni	
	Interventi per emergenze: un fasc. per ciascuna emergenza	Permanente con sfoltimento	

Titolo VII. Servizi alla persona

Osservazioni generali	*L'autonomia dei Comuni si può esplicare in forme svariate soprattutto in questo titolo: perciò l'indicazione generica di evento o attività verrà riempita di contenuti concreti dalla singola amministrazione.*

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli per persona	Permanente, previo sfoltimento del carteggio tempo-raneo e strumentale dopo 5 anni	
1. Diritto allo studio e servizi			
	Concessione di borse di studio: - bando - domande - graduatorie - assegnazioni	 permanente 5 anni permanente 5 anni	
	Distribuzione buoni libro: un fasc. per scuola	2 anni	
	Gestione buoni pasto degli iscritti alle scuole: un fasc. per periodo	2 anni	
	Verbali del comitato genitori per la mensa	3 anni	
	Azioni di promozione e sostegno del diritto allo studio: un fasc. per intervento	5 anni	
	Gestione mense scolastiche: un fasc. per mensa scolastica e per periodo	10 anni	
	Integrazione di neo-immigrati e nomadi: un fasc. per intervento	10 anni	
	Gestione trasporto scolastico: un fasc. per periodo e per tratta	2 anni	
2. Asili nido e scuola materna	Domande di ammissione agli asili nido e alle scuole materne: un fasc. per asilo/scuola	2 anni	
	Graduatorie di ammissione	2 anni	
	Funzionamento. degli asili e delle scuole materne: un fasc. per struttura	10 anni	
3. Promozione e sostegno delle istituzioni di istruzione e della loro attività			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
	Registri scolastici (del professore e della classe) prodotti dalle Scuole civiche (ove presenti)	Permanenti	

4. Orientamento professionale; educazione degli adulti; media-zione culturale			
	Iniziative specifiche: un fasc. per iniziativa	10 anni	
5. Istituti culturali			
	Funzionamento delle diverse istituzioni culturali: un fasc. per istituto	Permanente	
	Verbali degli organi di gestione degli Istituti culturali	Permanente	
6. Attività ed eventi culturali			
	Attività ordinarie annuali: un fasc. per attività e per periodo)	10 anni	
	Eventi culturali: un fasc. per evento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Feste civili e/o religiose: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative culturali. un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Prestiti di beni culturali: un fasc. per affare	Permanente	
7. Attività ed eventi sportivi			
	Eventi e attività sportive: un fasc. per evento/attività	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
8. Pianificazione e accordi strate-gici con enti pubblici e privati e con il volontariato sociale			
	Piano sociale: un fasc. annuale eventualmente organizzato in sottofasc.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Programmazione per settori: un fasc. per ciascun settore	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Accordi con i differenti soggetti: un fasc. per ciascun soggetto	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
9. Prevenzione, recupero e reintegrazione dei soggetti a rischio			
	Campagne di prevenzione: un fasc. per campagna	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Interventi di recupero e reintegrazione dei soggetti a rischio: un fasc. per intervento	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Ricognizione dei rischi: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
10. Informazione, consulenza ed educazione civica			
	Funzionamento e attività delle strutture (consultori, informagiovani, etc.): un fasc. per struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative di vario tipo: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
11. Tutela e curatela di incapaci			
	Interventi per le persone sottoposte a tutela e curatela: un fasc. per intervento.	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
12. Assistenza diretta e indiretta, benefici economici			
	Funzionamento e attività delle strutture: un fasc. annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e	

		strumentale dopo 10 anni	
13. Attività ricreativa e di socia-lizzazione			
	Funzionamento e attività delle strutture (colonie, centri ricreativi, etc.): un fasc. annuale per ciascuna struttura	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
	Iniziative specifiche: un fasc. per ciascuna iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	
14. Politiche per la casa			
	Assegnazione degli alloggi: un fasc. per bando, organizzato in sottofascicoli: - bando - domande - graduatoria - assegnazione	 permanente 5 anni permanente 5 anni	
	Fasc. degli assegnatari : un fasc. per assegnatario	5 anni dopo la scadenza del contratto	In assenza di contenzioso
15. Politiche per il sociale			
	Iniziative specifiche: un fasc. per iniziativa	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 10 anni	

Titolo VIII. Attività economiche

Classi	Tipologie documentarie	Conservazione	Note
	Fascicoli individuali degli esercenti attività economiche: un fasc. per persona	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
1. Agricoltura e pesca			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Dichiarazioni raccolta e produzione: un fasc. per periodo	5 anni	
2. Artigianato			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni artigiane: repertorio	Permanente	
3. Industria			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
4. Commercio			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Comunicazioni dovute: un fasc. per periodo	1 anno	
	Autorizzazioni commerciali: repertorio	Permanente	
5. Fiere e mercati			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
6. Esercizi turistici e strutture ricettive			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	
	Autorizzazioni turistiche: repertorio	Permanente	
7. Promozione e servizi			
	Iniziative specifiche: un fasc. per affare	Permanente, previo sfoltimento del carteggio temporaneo e strumentale dopo 5 anni	

Titolo IX. Polizia locale e sicurezza pubblica

Classi	Tipologie documentarie	Conservazione	Note
1.Prevenzione ed educazione stradale			
	Iniziative specifiche di prevenzione: un fasc. per iniziativa	5 anni	
	Corsi di educazione stradale nelle scuole: un fasc. per corso	5 anni	
2. Polizia stradale			
	Direttive e disposizioni: un fasc. annuale	Permanente	
	Organizzazione del servizio di pattugliamento: un fasc. annuale	3 anni	
	Verbali di accertamento di violazioni al Codice della strada: repertorio annuale	10 anni	
	Accertamento di violazioni al Codice della strada e conseguente erogazione di sanzioni: un fasc. per accertamento	5 anni	
	Verbali di rilevazione incidenti: repertorio annuale	20 anni	In assenza di contenzioso (ai sensi dell'art. 157 del Codice penale)
	Statistiche delle violazioni e degli incidenti: un fasc. annuale	Permanente	
	Gestione veicoli rimossi: un fasc. per ciascun veicolo	2 anni	
3. Informative			
	Informative su persone residenti nel Comune: un fasc. per ciascuna persona	5 anni	
4. Sicurezza e ordine pubblico			
	Direttive e disposizioni generali: un fasc. annuale	Permanente	
	Servizio ordinario di pubblica sicurezza: un fasc. annuale	5 anni	
	Servizio straordinario di pubblica sicurezza, in caso di eventi particolari (manifestazioni, concerti, etc.): un fasc. per evento	5 anni	
	Autorizzazioni di pubblica sicurezza: repertorio annuale, organizzata in sottoserie	Permanente	
	Fascicoli dei richiedenti l'autorizzazione di pubblica sicurezza: un fasc. per richiedente	5 anni	
	Verbali degli accertamenti nei diversi settori (edilizio, sanitario, commerciale, anagrafico, sociale, etc.): un repertorio annuale per ciascun settore di accertamento	Permanente	

Titolo X. Tutela della salute

Classi	Tipologie documentarie	conservazione	Note
1. Salute e igiene pubblica			
	Emergenze sanitarie: un fasc. per ciascun evento	Permanente	
	Misure di igiene pubblica: un fasc. per ciascun affare	Permanente	
	Interventi di derattizzazione, dezanzarizzazione etc.: un fasc. per ciascun intervento	1 anno	
	Trattamenti fitosanitari e di disinfestazione: un fasc. per ciascun intervento	1 anno	
	Autorizzazioni sanitarie: repertorio annuale	Permanente	
	Fascicoli dei richiedenti autorizzazioni sanitarie: un fasc. per ciascuna persona/ditta	5 anni dalla cessazione dell'attività	
	Concessioni di agibilità: repertorio annuale	Permanente	
	Fascicoli dei richiedenti l'agibilità: un fasc. per ciascun richiedente	Permanente	
2. Trattamenti Sanitari Obbligatori			
	TSO: un fasc. per ciascun procedimento	Permanente	
	ASO: un fasc. per ciascun procedimento	Permanente	
	Fascicoli personali dei soggetti a trattamenti: un fasc. per ciascuna persona	Permanente	
3. Farmacie			

	Istituzione di farmacie: un fasc. per ciascuna farmacia	Permanente	
	Funzionamento delle farmacie: un fasc. per ciascun periodo (anno o mese)	2 anni	
4. Zooprofilassi veterinaria			
	Fasc. relativi a epizoozie (epidemie animali): un fasc. per ciascun evento	Permanente	
5. Randagismo animale e ricoveri			
	Gestione dei ricoveri e degli eventi connessi: un fasc. per ciascun procedimento	3 anni	

Titolo XI. Servizi demografici

Classi	Tipologie documentarie	Conservazione	Note
1. Stato civile			
	Registro dei nati: repertorio annuale	Permanente	
	Registro dei morti: repertorio annuale	Permanente	
	Registro dei matrimoni: repertorio annuale	Permanente	
	Registro di cittadinanza: repertorio annuale	Permanente, se recanti registrazioni	
	Atti allegati per registrazioni	=	Trasmessi annualmente all'ufficio del governo competente per territorio
	Atti per annotazioni sui registri di stato civile: un fasc. per ciascun procedimento	10 anni	
	Comunicazione dei nati all'Agenzia per le entrate: un fasc. per ciascun periodo	1 anno	
2. Anagrafe e certificazioni			
	APR 4: iscrizioni anagrafiche: un fasc. per ciascuna persona	Permanente	
	AIRE: un fasc. per ciascuna persona	Permanente	
	Richieste certificati: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Corrispondenza con altre amministrazioni per rilascio e trasmissione documenti: un fasc. per ciascun periodo (mese o anno)	1 anno	
	Cartellini per carte d'identità: uno per ciascuna persona	1 anno	Mediante incenerimento o triturazione
	Carte d'identità scadute e riconsegnate: un fasc. per ciascuna persona	5 anni	Mediante incenerimento o triturazione Circ. Min. interno – Direz. gen. PS 23 ott. 1950, n. 10-13070-12982-7-1
	Cambi di abitazione e residenza: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Cancellazioni: un fasc. per ciascuna persona	10 anni	Salvo esigenze particolari
	Carteggio con la Corte d'appello per la formazione degli Albi dei giudici popolari: un fasc. per ciascun periodo	3 anni dall'ultima revisione	
	Registro della popolazione: su base di dati	Permanente	Salvataggi periodici per storicizzare la banca dati
3. Censimenti			
	Schedoni statistici del censimento	Si conservano quelli dell'ultimo censimento; quelli del precedente si scartano dopo 1 anno dall'ultimo	
	Atti preparatori e organizzativi	3 anni	
4. Polizia mortuaria e cimiteri			
	Registri di seppellimento	Permanente	
	Registri di tumulazione	Permanente	
	Registri di esumazione	Permanente	
	Registri di estumulazione	Permanente	
	Registri di cremazione	Permanente	
	Registri della distribuzione topografica delle tombe	Permanente	

	con annesse schede onomastiche		
	Trasferimento delle salme: un fasc. per ciascun trasporto	50 anni	

Titolo XII. Elezioni e iniziative popolari

Osservazioni	Ci si riferisca per i particolari a Ministero dell'interno-Direz. gen. dell'amministrazione civile –Direz centrale per i servizi elettorali, Massimario per lo scarto degli atti elettorali, Roma 1984

Classi	Tipologie documentarie	Conservazione	Note
1. Albi elettorali			
	Albo dei presidenti di seggio: un elenco per ciascuna elezione	5 anni	
	Albo degli scrutatori: un elenco per ciascuna elezione	5 anni	
2. Liste elettorali			
	Liste generali	1 anno dopo la redazione della successiva	
	Liste sezionali	1 anno dopo la redazione della successiva	
	Verbali della commissione elettorale comunale	Permanente	
	Copia dei verbali della Commissione elettorale mandamentale in ordine alle operazioni e deliberazioni adottate dalla Commissione elettorale comunale	5 anni	
	Schede dello schedario generale	5 anni dopo la redazione della successiva	
	Schede degli schedari sezionali	5 anni dopo la redazione della successiva	
	Fasc. personali degli elettori: un fasc. per ciascun elettore	5 anni dopo la cancellazione dalla lista	
	Elenchi recanti le proposte di variazione delle liste elettorali	5 anni dopo la redazione della lista successiva	
	Carteggio concernente la tenuta e la revisione delle liste elettorali	5 anni dopo la redazione della lista successiva	
3. Elezioni			
	Convocazione dei comizi elettorali: un fasc. per ciascuna elezione	Permanente	
	Presentazione delle liste: manifesto	Permanente	
	Presentazione delle liste: carteggio	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	
	Verbali dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno
	Pacchi scorta elezioni	2 anni	
	Certificati elettorali non ritirati	2 anni	
	Istruzioni elettorali a stampa	2 anni	
4. Referendum			
	Atti preparatori	5 anni	
	Atti relativi alla costituzione e arredamento dei seggi	5 anni	
	Verbali dei presidenti di seggio	=	Trasmessi al Min dell'interno
	Schede	=	Trasmesse al Min dell'interno
5. Istanze, petizioni e iniziative popolari			
	Raccolta di firme per referendum previsti dallo statuto: un fasc. per ciascuna iniziativa	5 anni dopo il referendum	

Titolo XIII. Affari militari

Classi	Tipologie documentarie	Conservazione	Note
1. Leva e servizio civile sostitutivo			
	Liste di leva: una per anno	Permanente	
	Lista degli eliminati/esentati: una per anno	Permanente	
2. Ruoli matricolari			
	Uno per anno	Permanente	
3. Caserme, alloggi e servitù militari			

	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	
4. Requisizioni per utilità militari			
	Procedimenti specifici: un fasc. per ciascun procedimento	Permanente	

Allegato 11 - Titolario di classificazione

In uso

Titolo I. Amministrazione generale				
	1.	Legislazione e circolari esplicative		
	2.	Denominazione, territorio e confini, circoscrizioni di decentramento, toponomastica		
			1.	Toponomastica e denominazione aree di circolazione
			2.	Assegnazione numerazione civica
	3.	Statuto		
	4.	Regolamenti		
			1.	Aggiornamento e tenuta regolamenti
	5.	Stemma, gonfalone, sigillo		
	6.	Archivio generale		
			1.	Notifiche
			2.	Albo Pretorio
			3.	Accesso agli atti
	7.	Sistema informativo		
			1.	Acquisti
			2.	Manutenzioni
			3.	Incarichi
			4.	Formazione
			5.	Progetti
	8.	Informazioni e relazioni con il pubblico		
			1.	Sportello Informativo
	9.	Politica del personale; ordinamento degli uffici e dei servizi		
	10.	Relazioni con le organizzazioni sindacali e di rappresentanza del personale		
	11.	Controlli esterni		
	12.	Editoria e attività informativo-promozionale interna ed esterna		
			1.	Stampa
			2.	Immagine
	13.	Cerimoniale, attività di rappresentanza; onorificenze e riconoscimenti		
	14.	Interventi di carattere politico e umanitario; rapporti istituzionali		
	15.	Forme associative per l’esercizio di funzioni e servizi		
			1.	Servizi pubblici locali
			2.	Affidamenti di servizi a terzi
			3.	*Accordi di programma*
	16.	Associazionismo e partecipazione		
			1.	Organismo di partecipazione
			2.	Comitati di Quartiere
			3.	Consulta comunale per l'immigrazione
			4.	Consulta per lo sport

Titolo 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.	Nucleo di valutazione (	
		1.	Corrispondenza nucleo valutazione
	17 . Conferenza dei Presidenti di quartiere		
Titolo 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.	Adempimenti fiscali, contributivi e assicurativi	
	8.	Tutela della salute e sicurezza sul luogo di lavoro	
		1.	Procedimenti di verifica della idoneità dei luoghi 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	
		1.	Personale Polizia Municipale
	13.	Giudizi, responsabilità e provvedimenti disciplinari	
	14.	Formazione e aggiornamento professionale	
	15.	Collaboratori esterni	
		1.	Collaborazioni e consulenze
Titolo IV. Risorse finanziarie e patrimoniali			
	-1.-Bilancio preventivo e Piano esecutivo di gestione (PEG		
	1.	Entrate non tributarie	
		1.	Rendiconti concessionari di riscossione
		2.	Comunicazioni intersettoriali
		3.	Recupero crediti

		4. Finanziamenti
		5. Contributi di costruzione
	-2.-Gestione del bilancio e del PEG (con eventuali variazioni)	
	2. Entrate tributarie	
		1. Corrispondenza concessionari riscossione
		2. I.C.I.
		3. T.A.R.S.U.
		4. T.O.S.AP.
		5. Imposta pubblicità Diritti Pubbliche affissioni
	-3-Gestione delle entrate: accertamento, riscossione, versamento	
	3. Uscite	
		1. Impegni
		2. Contabilità IVA
		3. Fatture
		4. Mandati e liquidazioni
	-4-Gestione della spesa: impegno, liquidazione, ordinazione e pagamento	
	4. Partecipazioni finanziarie)	
		1. Acquisti e alienazioni
		2. Corrispondenza società
	5. Bilancio preventivo, variazioni di bilancio, verifiche contabili	
		1. PEG
		2. Comunicazioni intersettoriali
		3. Patto di stabilità
	6. Rendiconto della gestione	
		1.Contabilità economico - patrimoniale
		2.Controllo di gestione
		3. Agenti contabili
		4.Corte dei Conti
	7. Adempimenti fiscali	
	8. Inventari e consegnatari dei beni	
		1. Inventari
	9. Beni immobili	
		1. Manutenzione beni immobili
		2. Concessioni ed autorizzazioni in uso aree comunali
		3. Corrispondenza proprietà comunali ed aggiornamento inventario
		4. Richieste pagamento canoni concessioni demaniali marittime
		5. Richieste pagamento canoni concessioni aree dello Stato
		6. Utenze
		7. Alienazioni immobili
	10. Beni mobili	
		1. Inventari e consegnatari dei beni
		2. automezzi

		3.	Assicurazioni
	11. Economato		
		1.	Provveditorato
		2.	Mense Scolastiche
		3.	Incassi Economali
		4.	Anticipazioni economali
	12. Oggetti smarriti e recuperati		
	13. Tesoreria		
		1.	Corrispondenza
		2.	Gare d'appalto
	14. Concessionari ed altri incaricati della riscossione delle entrate		
	15. Pubblicità e pubbliche affissioni		
		1.	Controlli e accertamenti
Titolo V. Affari legali			
	1. Contenzioso		
		1.	Codice della Strada
		2.	Commercio e PE
		3.	Edilizia
		4.	Ambiente
		5.	Polizia Urbana
		6.	Altre materie
	2. Responsabilità civile e patrimoniale verso terzi; assicurazioni		
	3. Pareri e consulenze		
Titolo VI. Pianificazione e gestione del territorio			
	1. Urbanistica: piano regolatore generale e varianti		
		1.	PRG e Varianti
		2.	Certificazione di Destinazione Urbanistica
		3.	Atti Compravendita
		4.	Visti di Frazionamento
	2. Urbanistica: strumenti di attuazione del Piano regolatore generale		
		1.	Piani Particolareggiati
		2.	Piani Attuativi
	3. Edilizia privata		
		1.	Permessi di Costruire
		2.	Proroghe e volture
		3.	DIA
		4.	Agibilità/Abitabilità
		5.	Condono
		6.	Controllo urbanistico
		7.	Controllo Sicurezza cantieri
		8.	Mezzi Pubblicitari
		9.	Esposti per abusi
		10.	Autorizzazioni Paesaggistiche
		11.	Servizio decentrato OO.PP. e difesa del suolo

	4.	Edilizia pubblica	
		1.	Costruzione case popolari
		2.	Edilizia scolastica
		3.	Impianti sportivi
		4.	Edilizia pubblica
		5.	Sedi Comunali
	5.	Opere pubbliche	
		1.	Strade e Arredo Urbano
		2.	Fognature e Depurazione
		3.	Pubblica Illuminazione
		4.	Verde Pubblico
		5.	Edilizia Cimiteriale
		6.	Attrezzature Portuali
		7.	Interventi Ambientali
	6.	Catasto	
	7.	Viabilità	
		1.	Piano Urbano Del Traffico
		2.	Piano Della Sosta
		3.	Piano Della Mobilità
		4.	Autorizzazione (ZTL, Zone BLU, Passi Carrabili e Permessi Invalidi- Transiti Eccezionali)
	8.	Servizio Idrico Integrato, Luce, Gas, Trasporti Pubblici, Gestione Dei Rifiuti E Altri Servizi	
		1.	Autorizzazioni Allacci
		2.	Autorizzazioni Scarichi
		3.	Gestione Rete Gas
		4.	Gestione Rifiuti
	9.	Ambiente: Autorizzazioni, Monitoraggio E Controllo	
		1.	Politiche ed Iniziative Ambientali (Bandiera Blu, Ecc.)
		2.	Sviluppo Sostenibile
		3.	Controlli Ambientali
		4.	Controlli Ambientale Attività Produttive e Industriali
		5.	Controllo Degli Scarichi
		6.	Controllo Degli Impianti Termici
		7.	Esposti
	10.	Protezione Civile Ed Emergenze	
		1.	Eventi Sul Territorio
		2.	Eventi Ambientali
	11.	Demanio	
		1.	Concessioni Demaniali
		2.	Autorizzazioni
Titolo VII. Servizi Alla Persona			
	1.	Diritto Allo Studio e Servizi	
	2.	Asili Nido E Scuola Materna	
		1.	Asili Nido
		2.	Cuoche

3.	Promozione E Sostegno Delle Istituzioni Di Istruzione E Della Loro Attività	
4.	Orientamento Professionale; Educazione Degli Adulti; Mediazione Culturale	
	1.	Stage
	2.	Tirocini Di Formazione E Orientamento
	3.	Servizio Immigrati
5.	Istituti Culturali (Musei, Biblioteche, Teatri, Scuola Comunale Di Musica, Etc.)	
	1.	Biblioteca Comunale
	2.	Sala Auditorium
	3.	Musei
	4.	Attività Espositive
	5.	Archivio Storico
	6.	Palacongressi
	7.	Istituto Musicale Vivaldi
	8.	Altri Istituti
6.	Impianti Sportivi	
	1.	Palazzetto Dello Sport
	2.	Piscina Comunale
	3.	Stadio Comunale
	4.	Campo Di Atletica
	5.	Altre Strutture Sportive
7.	Attività Ed Eventi Culturali	
	1.	Teatro
	2.	Arte E Mostre
	3.	Musica E Concerti
	4.	Cinema
	5.	Eventi Culturali
	6.	Rapporti Con Le Università
	7.	Patrocinio e/o contributo in favore delle manifestazioni culturali
8.	Attività Ed Eventi Sportivi	
	1.	Convenzioni con Società Sportive
	2.	Programmazione
9.	Pianificazione e Accordi Strategici Con Enti Pubblici e Privati e Con il Volontariato Sociale	
	1.	Pianificazione e Accordi Strategici
	2.	Convenzioni con Enti e Associazioni Culturali
10.	Prevenzione, Recupero E Reintegrazione Dei Soggetti A Rischio	
	1.	Borse Lavoro Tossicodipendenza, Disabili e Disagio Mentale
	2.	Risposte Alcologiche
	3.	Unità Di Strada
	4.	Servizi Pluridipendenze
11.	Informazione, Consulenza Ed Educazione Civica	
	1.	Informagiovani
12.	Tutela E Curatela Di Incapaci (Minori)	
	1.	Affidamento Minori Abbandonati a Strutture Convenzionate
	2.	Affidi Familiari

		3.	Affidi in Istituti
		4.	Servizi Prevenzione
		5.	Tribunale Dei Minori
		6.	Ospiti in Istituto
		7.	Disabili e Malati Gravi
	13. Assistenza Diretta E Indiretta, Benefici Economici		
		1.	Prestito sull'onore
		2.	Assegno 2° Figlio/INPS (Demografici)/Maternità
		3.	Interventi a Favore della Famiglia
		4.	Assistenza Domiciliare a Minori
		5.	Assistenza Domiciliare ad Anziani
		6.	Assistenza Domiciliare ai Portatori di Handicap e Disturbo Mentale
		7.	Casa di Riposo Centro Primavera
		8.	Cediser
		9.	Biancoazzuro - Centro Diurno
		10.	Casa Famiglia per Problemi Psichici
	14. Attività Ricreativa E Di Socializzazione		
		1.	Centri Ricreativi Estivi
		2.	Centro per le Famiglie
		3.	Centro Giovani e Politiche Giovanili
	15. Politiche Per La Casa		
		1.	Commissione Assegnazione Alloggi Asl 12
		2.	Assegnazione Alloggi Popolari
		3.	Gestione Alloggi Parcheggio
		4.	L.431/98 Contributo affitto
		5.	Contributi Comunali Acquisto Prima Casa
		6.	Attestazioni subentri mutui agevolati Regione Marche
Titolo VIII. Attività economiche			
	1. Agricoltura		
		1.	Autorizzazioni
		2.	Certificazioni
	2. Artigianato		
		1.	DIA
		2.	Certificazioni
		3.	Barbiere/Parrucchiere/Estetista/Centri Abbronzatura
	3. Industria		
		1.	SPUN
	4. Commercio		
		1.	DIA vicinato
		2.	Autorizzazioni Medie e Grandi Strutture
		3.	Autorizzazione Somministrazione Alimenti e Bevande
		4.	Giornali e riviste
		5.	Autonoleggio con conducente

		6.	Autonoleggio senza conducente
		7.	Taxi
		8.	Agenzie di Viaggio
		9.	Accertamenti
	5. Fiere e mercati		
		1.	Autorizzazioni
		2.	Revoche
		3.	Mercato settimanale SBT
		4.	Mercato settimanale PdA
		5.	Fiere
		6.	Mercatini stagionali o occasionali
	6. Esercizi turistici e strutture ricettive		
		1.	Autorizzazioni
		2.	Rilevamento prezzi
		3.	Accertamenti
	7. Promozione e servizi		
	8. Pesca e Mercato Ittico		
		1.	Asta - Produttori e Acquirenti
		2.	Affitti - Utenze - Condominio
		3.	Acquisti Vari e Manutenzioni Ordinarie
	9. Autorizzazione PS		
		1.	Rilascio autorizzazioni
		2.	Revoche
	10. Promozione e servizi turistici		
		1.	patrocinio e/o contributo in favore delle manifestazioni turistiche
		2.	animazione turistica
		3.	Convegni
		4.	Convenzioni
		5.	Mostra evento nazionale
		6.	Manifestazione evento nazionale
		7.	Rapporti con soggetti o organismi esterni, pubblici o privati
Titolo IX. Polizia locale e sicurezza pubblica			
	1. Prevenzione ed educazione stradale		
		1.	Statistiche
		2.	Educazione stradale nelle scuole
	2. Polizia stradale		
		1.	Accertamenti
		2.	Proventi da Sanzioni Amministrative
		3.	Incidenti stradali
		4.	Beni Strumentali (PM)
	3. Informative		
		1.	Per altri settori comunali
		2.	Per Altri Enti
	4. Sicurezza e ordine pubblico		

Titolo X. Tutela della salute			
	1.	Salute e igiene pubblica	
		1.	Autorizzazioni sanitarie di Commercio
		2.	Autorizzazioni sanitarie mense scolastiche
		3.	Autorizzazioni sanitarie mezzi comunali
		4.	Autorizzazioni Ambientali
		5.	Autorizzazione Studi Medici e Struttura Sanitarie
		6.	Interventi a tutela della salute pubblica
	2.	Trattamento Sanitario Obbligatorio	
	3.	Farmacie	
	4.	Zooprofilassi veterinaria	
	5.	Randagismo animale e ricoveri	
		1.	Canile Comprensoriale
		2.	Informative su animali molesti
		3.	Attivazione Servizio Veterinario per cani randagi
Titolo XI. Servizi demografici			
	1.	Stato civile	
		1.	Nascita
		2.	Morte
		3.	Pubblicazioni
		4.	Matrimoni/divorzi
		5.	Cittadinanza
	2.	Anagrafe e certificazioni	
		1.	AIRE
		2.	Immigrazioni/Iscrizioni
		3.	Emigrazioni/Cancellazioni
		4.	Cambio Indirizzo
		5.	Corrispondenza/certificazioni
		6.	Carte di Identità
		7.	Pensioni
		8.	Progetti e Collegamenti con altri Enti
	3.	Censimenti	
		1.	Generale della Popolazione/Abitazioni
		2.	Generale dell'Agricoltura
		3.	Generale Attività economiche/professioni
		4.	Indagini campionarie ISTAT
	4.	Polizia mortuaria e cimiteri	
		1.	Permessi di seppellimento
		2.	Tumulazioni/esumazioni/traslazioni/riduzioni/trasferimenti
		3.	Contratti
		4.	Cremazioni
		5.	Contabilità
		6.	Carteggi
Titolo XII. Elezioni e iniziative popolari			

	1.	Albi elettorali	
		1.	Albo Scrutatori
		2.	Albo Presidenti di Seggio
		3.	Giudici Popolari
	2.	Liste elettorali	
		1.	Normali
		2.	Aggiuntive/Speciali
	3.	Elezioni	
		1.	Comunali
		2.	Provinciali
		3.	Regionali
		4.	Politiche
		5.	Europee
	4.	Referendum	
		1.	Abrogativi
		2.	Propositivi
	5.	Istanze, petizioni e iniziative popolari	
		1.	Consultazioni popolari
		2.	Istanze e petizioni
Titolo XIII. Leva militare			
	1.	Leva e servizio civile sostitutivo	
		1.	Iscrizioni
		2.	Precetti
		3.	Pratiche esoneri
		4.	Corrispondenza e Informazioni (congedi)
	2.	Ruoli matricolari	
	3.	Caserme, alloggi e servitù militari	
	4.	Requisizioni per utilità militari	
Titolo XIV. Oggetti diversi			

Allegato 12 - Repertori generali

Repertori di documenti in doppio esemplare

- Ordinanze emanate dal Sindaco;
- Decreti del Sindaco;
- Ordinanze emanate dai dirigenti (un unico repertorio);
- Determinazioni dei dirigenti;
- Deliberazioni del Consiglio comunale;
- Deliberazioni della Giunta comunale;
- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma pubblica amministrativa);
- Circolari;
- Deliberazioni dei Consigli circoscrizionali (uno per quartiere);
- Deliberazioni degli Esecutivi circoscrizionali (uno per quartiere).

Repertori di documenti in esemplare unico

- Verbali delle adunanze del Consiglio comunale;
- Verbali delle adunanze della Giunta comunale;
- Verbali degli organi collegiali del Comune;
- Contratti e convenzioni;
- Verbali delle adunanze dei Consigli circoscrizionali (uno per quartiere);
- Verbali delle adunanze degli Esecutivi circoscrizionali (uno per quartiere);
- Verbali degli organi collegiali delle circoscrizioni (uno per organo e per quartiere); Registro dell'Albo della circoscrizione (uno per quartiere);
- Contratti e convenzioni delle circoscrizioni (uno per quartiere).

Allegato 13 - Descrizione funzionale ed operativa del Prodotto di Protocollo (PdP) informatico in uso presso l'area organizzativa omogenea

Prodotto software in uso

La soluzione di PdP utilizzata dal Comune di San Benedetto del Tronto è il prodotto IRIDE della ditta CEDAF Srl con sede in Forlì, che si configura non solo come un prodotto per il protocollo, ma più in generale come una suite per la completa gestione documentale.

Di seguito si riportano le caratteristiche operative del prodotto

Protocollo Informatico

Il modulo **PdP**-Protocollo si configura come un sistema che oltre a svolgere le funzioni "istituzionali" del protocollo (dare validità formale ad un documento), permette anche lo svolgimento di compiti gestionali attraverso il monitoraggio del flusso del documento ed il suo legame con altri documenti.

In particolare **PdP**-Protocollo, così come indicato dalla normativa, non si propone semplicemente come sistema di Protocollo Informatizzato (nel quale è l'operazione di registrazione ad essere trattata con strumenti informatici), ma anche come sistema di gestione del Protocollo Informatico attraverso il quale viene gestito il documento informatico.

Nel rispetto di quanto indicato dal Testo Unico sulla documentazione amministrativa (DPR 445/00) dove per "area organizzativa omogenea" (AOO) si intende "gli uffici da considerare ai fini della gestione unica o coordinata dei documenti" dove vengono assicurati "criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le stesse aree", il modulo **PdP**-Protocollo è strutturato in modo tale da poter essere logicamente accentrato ma fisicamente distribuito.

Quindi, senza prescindere dalla possibilità/necessità di mantenere un protocollo logicamente accentrato, e quindi con un'unica numerazione, l'architettura del sistema ne permette la diffusione delle funzionalità non soltanto in senso fisico ma anche con la distribuzione logica delle funzioni all'interno dell'organizzazione dell'Ente consentendo la cosiddetta protocollazione diffusa/ decentrata.

Interoperabilità di protocollo

PdP è conforme alla normativa sulla interoperabilità dei protocolli informatici, secondo i criteri specificati nella Circolare AIPA n. 28 del 07/05/2001.

Alle informazioni inserite in fase di protocollazione è possibile associare il documento informatico ed autenticarlo attraverso l'apposizione della firma digitale sul documento stesso; in tale contesto il sistema utilizza le funzionalità messe a disposizione da parte del modulo di Firma Digitale della suite **PdP**.

Prima dell'invio è possibile effettuare la generazione della segnatura informatica in formato XML secondo il DTD definito dall'AIPA. Oltre alle informazioni minime previste da tale DTD **PdP** estende le informazioni minime richieste, includendo ad esempio una serie di informazioni utili alla costituzione del fascicolo elettronico.

Una volta ottenuta la segnatura XML, sarà possibile inviare il messaggio di posta contenente tutte le informazioni previste attraverso il modulo di integrazione con i sistemi di posta elettronica certificata sarà possibile inviare il documento al destinatario.

Per la gestione degli indirizzi delle caselle di posta elettronica istituzionale, il sistema **PdP** prevede l'integrazione con l'IPA (Indice delle Pubbliche Amministrazioni).

Nell'ambito della gestione dell'interoperabilità, il sistema **PdP** consente la gestione di tutti i messaggi generati nell'ambito dei meccanismi relativi all'interoperabilità e dell'integrazione con la posta certificata (messaggi di notifica eccezione, messaggi di conferma recapito, etc.).

Flussi documentali

Tutti i passaggi inter-settoriali che un documento subisce trovano copertura nella gestione del flusso documentale del sistema **PdP**, con il quale viene registrato ogni passaggio del documento da una struttura ad un'altra (quindi in particolare da un settore ad un altro) consentendo di conoscere in ogni momento la collocazione di un documento all'interno dell'Ente. Pertanto, con l'attivazione delle funzionalità di gestione del protocollo informatico e dei flussi documentali previsti dal sistema, non sarà più necessaria l'attribuzione di protocolli interni intesi come sistemi di registrazione alternativi.

In tale contesto, l'attivazione del sistema di gestione dei documenti con inclusa la gestione del flusso documentale dei documenti si pone l'obiettivo di ottenere le informazioni relative a:

- dove si trova il documento;
- quali unità organizzative dell'ente sono state coinvolte nel flusso del documento.

Procedimenti amministrativi (workflow management)

Un workflow è un sistema che definisce, crea e gestisce l'esecuzione di flussi di lavoro pianificati tramite un software in grado di interpretare la metodologia con la quale i processi sono stati organizzati, che interagisce con gli attori e le risorse coinvolte nel processo e che è in grado, se e quando richiesto, di invocare, utilizzare e interagire con tools, applicazioni e più in generale con sistemi esterni.

Il Workflow (WFM) di **PdP** si interfaccia con le componenti applicative, ed in particolare con la componete di

protocollo e quella di gestione dei procedimenti amministrativi per fornire i servizi necessari all'esecuzione dei processi pianificati. Il WFM di **PdP** inoltre, permette di pianificare i processi secondo una metodologia che è implementata come modulo del prodotto stesso. Attraverso un strumento, grafico permette il disegno dello sviluppo temporale (iter del processo) delle singole attività elementari in cui il processo viene scomposto.

Il WFM non gestisce di per sé data base verticali che contengono dati specifici. Oltre ad implementare e gestire le regole che permettono lo svolgimento delle istanze, registra i dati, gli stessi per tutti i processi, trasversali rispetto alla specificità dei singoli processi.

Ad ogni "passo", cioè ogni punto in cui termina un'attività e ne inizia un'altra, è possibile inserire degli eventi che consentono il passaggio da un'attività alla successiva, e questi ultimi possono essere eseguiti sia in modalità automatica da parte del sistema, sia in modalità manuale in base alla decisione dell'operatore.

I processi, per poter essere gestiti dal WFM, devono essere decomposti nelle loro attività elementari, quindi le attività individuate devono essere riconcatenate secondo uno schema logico che segue lo sviluppo temporale. Le informazioni confrontate con i dati impostati nella fase di pianificazione del processo danno lo scostamento tra l'andamento teorico previsto per un dato processo e quello reale.

I dati di monitoraggio relativi alla singola istanza di un procedimento possono essere utilizzati anche per fornire informazioni all'esterno dell'Ente, al soggetto che ha innescato l'istanza del processo. Mentre quelli relativi all'andamento del processo possono essere utilizzati per il controllo di gestione e per effettuare verifiche circa il funzionamento del modello teorico del processo.

Una volta disegnato il processo in termini di flusso e messo in funzione, il WFM inizia a collezionare istanze relative ai vari processi messi in produzione.

L'iter di un ipotetico processo, può essere così descritto:

- la pratica relativa ad uno specifico processo viene attivata, ad esempio a seguito di una richiesta che arriva dall'esterno;
- la richiesta viene presa in carico da un addetto della struttura dell'Ente responsabile del processo che ne controlla la completezza in termini di dati e documenti;
- la richiesta viene protocollata (protocollazione e fascicolazione) ed eventualmente trasferita ad un altro addetto;
- se la richiesta è stata trovata mancante di dati e documenti obbligatori viene inviata una richiesta di integrazione delle parti mancanti;
- a seguito della richiesta di integrare le parti mancanti può essere attivata una sospensione nel conteggio dei termini (teorici) del processo;
- a questo punto inizia la fase istruttoria, più o meno complessa, in cui l'istanza viene trattata. In questa parte dell'iter potrebbe essere richiesto l'intervento di altri Enti, la convocazione di commissioni, la presentazione di altri documenti, etc.;
- durante il percorso attraverso le attività elementari in cui il processo è stato scomposto, la pratica viene messa in carico a diversi addetti ognuno dei quali la arricchisce di documenti.

Tutto questo è governato e gestito dal motore del WFM che non fa altro che proporre l'esecuzione passo per passo dell'articolato di attività elementari secondo la logica implementata tramite il modulo di disegno dell'iter del processo.

Gestione Documentale

Tale componente offre tutte i servizi necessari per fornire le funzionalità tipiche di gestione documentale, tra cui si ricordano:

- **Attach** (acquisizione documenti) dei documenti informatici di qualsiasi formato di file;
- **ACL** (Access Control Listi) per la definizione degli accessi ai documenti (dati strutturati e file);
- **Versioning** per la gestione delle versioni dei documenti e conseguente tracciatura e storicizzazione delle diverse versioni succedute nel tempo;
- **Check-in/Check-out per gestire i meccanismi di accesso ai documenti in modifica da parte di più utenti.**

La componente di Gestione Documentale si occupa inoltre di interfacciarsi con il repository documentale per l'archiviazione fisica dei documenti. In tale ambito **PdP** prevede le seguenti tipologie di repository documentale:

- RDBMS prescelto per l'attivazione dell'applicazione;
- Utilizzo di file system;
- Integrazione con una piattaforma di EDMS (es.: Documentum, Hummingbird, Alfresco ecc.).

Gestione Immagini

Il modulo di acquisizione immagini permette la scansione dei documenti cartacei e la conseguente associazione delle immagini alle relative registrazioni dei documenti sul sistema **PdP**.

La scansione dei documenti può avvenire sia attraverso scansioni interattive che attraverso funzionalità di acquisizione massiva. Per quest'ultima opzione, il sistema **PdP** si integra con piattaforme di acquisizione documenti consolidate sul mercato della GED (Gestione Elettronica dei documenti).

Firma Digitale

Il sistema **PdP** è interfacciabile verso i sistemi di Firma Digitale delle Certification Autority iscritte al CNIPA, per

consentire di applicare e gestire, attraverso opportune funzionalità offerte dal sistema, la firma digitale sui documenti trattati dal sistema.
In particolare il sistema il sistema **PdP** effettua il disaccoppiamento della componente di integrazione con i dispositivi, dalle funzionalità offerte nel sistema, a garanzia di trasparenza funzionale da parte degli operatori, indipendentemente dai sistemi di firma utilizzati.
Dal punto di vista architetturale, la componente di integrazione consente l'interfacciamento con i sistemi di firma di qualsiasi dei fornitori di sistemi di firma iscritti all'albo delle Certification Autorità del CNIPA. Nelle attivazioni del sistema **PdP** , sono state effettuate le integrazioni con i seguenti certificatori:

- Actalis S.p.A.;
- Infocamere S.p.A;
- Postecom S.p.A.;
- I.T. Telecom S.r.l.;
- Trust Italia S.p.A.

Atti Formali (determine e delibere)
La componente applicativa della Suite PdP per la gestione degli Atti Formali effettua la gestione completa delle Deliberazioni, delle Determinazioni, e più in generale degli Atti Formali, estendendo quindi le funzionalità ai Decreti e delle Ordinanze. Questi atti formali sono assimilati ad un Procedimento Amministrativo supportato durante tutto il suo intero ciclo: la fase propositiva, l'istruttoria di Ragioneria, l'istruttoria della Segreteria, l'assunzione della decisione, la redazione degli atti e la loro esecuzione.
Il sottosistema segue tutto l'iter dell' atto formale (delibera, determina, decreto, ecc.) dalla fase propositiva a quelle relative all'esecutività ed alla pubblicazione mediante automatismi che consentono il passaggio del Provvedimento nei vari uffici dell'Ente coinvolti.
Tutti i passaggi effettuati dal provvedimento sono memorizzati nel sistema e questi permette di gestire e controllare per via informatica e telematica tutto il flusso di informazioni connesse con la produzione degli atti amministrativi. Infatti ogni azione intrapresa da un qualsiasi operatore, avente diritto di intervento lascia una traccia memorizzata relativa all'azione intrapresa (l'operatore, il giorno, l'ora dell'avvenuta azione, etc.).
Il sistema permette di individuare i tempi di giacenza nei vari uffici e di esercitare stretti controlli sull'iter, in modo da fornire informazioni statistiche o dettagli sullo stato di ogni Atto. Inoltre consente di mantenere il segreto di ufficio su alcuni atti o documenti riservati, anche in modo differenziato, a seconda della provenienza delle richieste, in ottemperanza a quanto contenuto nel DPR n. 352 del 27.06.92, sulla regolazione dell'accesso alle informazioni (Gestione delle Access Control List).
Il sistema consente l'inserimento dei testi delle delibere e delle determine che vengono raccolti in un unico archivio logico, che costituisce l'archivio ufficiale degli Atti dell'Amministrazione a cui si potrà far riferimento per ogni tipo di ricerca necessaria, secondo criteri e modalità tali da soddisfare ogni tipo di esigenza degli Uffici e l'ottemperanza delle vigenti leggi in materia, riguardanti le Amministrazioni Pubbliche. Ogni Settore dell'Amministrazione viene messo in grado di produrre le proprie proposte, in modo indipendente, senza vincolo o condivisione alcuna da parte degli altri Settori dell'Amministrazione, o da parte di altre apparecchiature, se non quelle in dotazione al Settore.
Gli Uffici proponenti dei vari Settori sono messi in grado di predisporre schemi standard, atti a coprire tutte le necessità del Settore, in modo da accelerare i tempi di preparazione delle proposte.
Il modulo applicativo di gestione degli Atti Formali, anche attraverso l'integrazione con gli altri moduli applicativi della suite **PdP**, consente:

- l'aggregazione di più documenti in pratiche, a cui far riferimento in fase di ricerca o controllo;
- la ricerca ogni tipo di documento mediante i dati strutturati che sono associati a ciascuno di essi o mediante metodi di "information retrieval" (tramite modulo di Document Management) partendo da parole contenute nel testo, con visualizzazione dei dati strutturati associati e del contenuto (testo o immagine) del documento;
- statistiche per ogni documento per ufficio proponente, per Unità Operativa, per Servizio, per Settore (per vari tipi di indicatore, ad. es. i tempi di giacenza, i ritardi, i ritorni per correzioni, etc.);
- il controllo di tutte le proposte ritornate all'ufficio proponente per chiarimenti;
- l'inserimento, per ogni tipo di documento inserito nell'iter, dei tempi minimi di giacenza in ciascun ufficio, e attivazione di un automatismo che ne segnali, in modo asincrono, il mancato rispetto
- la preparazione degli ordini del giorno degli organi (Giunta, Consiglio, etc.), a cui saranno inviate le proposte/delibere, mediante selezioni di singole proposte o di gruppi formati sulla base dei criteri espressi dalla Segreteria Generale, dei tipi di proposta, dei relatori, degli uffici proponenti
- la preparazione di tutti i verbali delle riunioni degli organi (Giunta, Consiglio. etc.) in modo automatico, seguendo regole di ordinamento, che si basano sul tipo di provvedimento, relatore, numero di Segreteria Generale (la funzione prevede di spostare alcuni punti all'interno dell'Odg e non rispettare l'ordine scelto dall'automatismo)
- la preparazione di tutti gli elenchi di pubblicazione per i vari organi di controllo e la gestione dei relativi invii e dei ricevimenti
- la possibilità di numerare le delibere, dopo l'approvazione da parte degli organi, in modo automatico, mediante

individuazione di gruppi logici sulla base di numeri di Odg consecutivi

• la definizione della modulistica personalizzata per tutti gli elaborati relativi alle sedute

• integra i dispositivi di Firma Digitale di tutte le Certification Authority nel pieno rispetto dei principi di autenticazione, integrità, riservatezza e non ripudiabilità.

• Il sistema supporta la reingegnerizzazione ed informatizzazione dei processi relativi ai flussi documentali nelle diverse tipologie ed il monitoraggio dei tempi e delle scadenza. Viene rappresentato l'intero ciclo di vita del Procedimento, del Fascicolo Elettronico e dei documenti che lo formano ovvero di tutte le informazioni che concorrono alla definizione dei procedimenti.

• è fortemente integrato con i sistemi di produttività individuale in modo particolare con la suite Microsoft Office ed anche con la suite Open Office. Tale integrazione permette la creazione, anche automatica, e la gestione di modelli predefiniti, personalizzati e standardizzati.

La componente di gestione degli atti formali, tramite apposito modulo, si può integrare con programmi di Contabilità Finanziaria (attraverso Web services) e quindi permettere di innescare automatismi di interazione con altre applicazioni, sia per il controllo della disponibilità dei capitoli di bilancio, in fase di proposta, sia per la conferma dell'impegno, in fase di approvazione ed esecutività dell'atto (tramite componenti opzionale).

Elenco delle specifiche funzionali

Nucleo minimo di protocollo

Gestione del titolario di classificazione

PdP prevede la gestione completa del titolario di classificazione, mediante l'utilizzo di apposite funzionalità rese disponibili con l'applicativo.

Strutturazione del titolario

La gestione del titolario d'archivio è parametrica, e di conseguenza è lasciata ampia scelta all'Ente di dotarsi di un tipo di classificazione piuttosto che un altro (ad esempio, classificazione per "materia" piuttosto che per "funzione"). Nella maschera di inserimento dei dati del titolario è possibile indicare le voci relative a titolo, categoria, classe ed eventuale sottoclasse mediante la compilazione del campo denominato "codice".

Navigazione del titolario

E' possibile effettuare le ricerche sul titolario in vigore oppure sui titolari storici inseriti nel sistema. Per cercare tutti i documenti (o fascicoli) che fanno riferimento ad un titolario, occorre eseguire le funzioni di ricerca standard. Dalla maschera delle ricerche è possibile filtrare la tipologia di dato da estrapolare (documenti, fascicoli) agendo opportunamente sui campi resi disponibili dalla maschera di ricerca.

La ricerca restituisce l'elenco di documenti oppure di fascicoli in base alle selezioni effettuate; dall'elenco è possibile:

- Accedere in visualizzazione ai dati dei documenti/fascicoli
- Stampare il report contenente l'elenco di file selezionati.

In fase di protocollazione oppure di gestione del documento è possibile navigare all'interno del titolario per scegliere la voce di classifica corrispondente, il sistema **PdP** offre la modalità di rappresentazione ad albero del titolario di classificazione, che permette di visualizzare e poter selezionare le voci:

PdP mette a disposizione anche un'altra rappresentazione grafica del titolario di archivio, con uno stile differente che consente di effettuare le seguenti operazioni:

- Ordinamenti sulle colonne
- Ricerche sulle singole voci
- Multi selezione di voci

E' anche possibile impostare delle funzioni parametriche che consentono la personalizzazione della visualizzazione del titolario per alcuni utenti del sistema. Modificando un opportuno cursore di visualizzazione è infatti possibile inibire la visualizzazione di porzioni di titolario per alcuni utenti oppure mostrando informazioni aggiuntive.

Storicizzazione di una voce del titolario

Per ogni voce del titolario è possibile definire una data di inizio e di fine validità, in questo modo è possibile inserire voci di titolario nuove ovvero che entrano in vigore dopo una certa data.

Analogamente, compilando la data di fine validità è possibile inibire la visualizzazione e assegnazione di voci di titolario che non sono più in vigore.

Mediante il meccanismo appena descritto è possibile effettuare modifiche al titolario che vengono opportunamente storicizzate nel sistema.

Storicizzazione del titolario

PdP consente di inserire nel sistema più di un titolario e di rendere effettivo e utilizzabile dagli utenti uno dei titolari inseriti. In questo modo viene garantita la storicizzazione del titolario e di tutti i collegamenti alle registrazioni di protocollo effettuate infatti saranno disponibili ai protocollatori solo le voci del nuovo titolario per le nuove registrazioni, mentre per le registrazioni già effettuate è garantita la conservazione dell'indicazione della voce storica di titolario.

Questo meccanismo inibisce all'utente l'apertura di nuovi fascicoli nel titolario non più in vigore.

Massimario di selezione

Le operazioni di parametrizzazione per lo scarto di Archivio in **PdP** vengono effettuate secondo una parametrizzazione del sistema sulle tabelle del titolario d'archivio e tipo documento:

- ad ogni classifica di titolario può essere associato un valore che indichi il numero di anni dopo il quale un fascicolo con tale classificazione può essere soggetto a scarto, secondo quanto previsto dell'art. 35 del DPR 30 settembre 1963, n. 1409;
- allo stesso modo, ad ogni tipo documento (es. certificato medico, istanza di ferie, verbale di gara, ecc.) può essere associato un valore che indichi che tale tipologia è scartabile.

PdP mette a disposizione apposite funzioni che consentono di estrapolare una lista di documenti e fascicoli proposti per lo scarto.

Scarto archivistico

Le operazioni di scarto vengono effettuate sui fascicoli chiusi.

Per effettuare lo scarto d'archivio è necessario individuare inizialmente i fascicoli che possono essere sottoposti all'operazione di scarto (sia per contenuti che per tempo), e successivamente i documenti all'interno del fascicolo che possono essere "scartati".

In riferimento alle operazioni di scarto, la situazione dei fascicoli (pratiche) potrà essere la seguente:

a. *Pratiche totalmente scartate:* rappresentano fascicoli che possono essere completamente scartate nel loro contenuto documentale;
b. *Pratiche parzialmente scartate:* rappresentano fascicoli che contengono documenti che possono essere scartati, ma anche documenti che invece non lo possono essere.
c. *Pratiche totalmente scartabili:* rappresentano fascicoli che contengono tutti documenti "scartabili", ma non è ancora trascorso il tempo necessario per procedere con l'operazione di scarto.
d. *Pratiche parzialmente scartabili:* rappresentano fascicoli che contengono alcuni documenti scartabili ed altri non, ma non è ancora trascorso il tempo necessario per procedere con l'operazione di scarto definito nel titolario di classificazione.

Tramite un'apposita funzione è possibile visionare l'elenco dei documenti e pratiche scartati o da scartare.

Registrazione di Protocollo

L'obiettivo del modulo Protocollo della Suite **PdP** è recepire ed implementare le indicazioni presenti nel nuovo Testo Unico delle Disposizioni legislative e regolamentari in materia di documentazione amministrative (DPR 445/00) dove vengono ripresi e ampliati i concetti già contenuti nel Regolamento recante norme sul Protocollo Informatico nelle PP.AA. (DPR 428/98).

Registrazione documenti A/P/I

Tramite la procedura **PdP** è possibile protocollare documenti in entrata e in uscita, compresi i documenti interni scambiati tra le unità operative dell'Ente.

Tramite opportune parametrizzazioni è possibile abilitare a particolari ruoli solo una determinata tipologia di protocollazione. Ad esempio il ruolo Ufficio tecnico potrebbe essere abilitato alla sola protocollazione interna e in partenza, a differenza del ruolo Ufficio Protocollo che sarà abilitato a tutte le tipologie di protocollo.

PdP prevede anche la memorizzazione di documenti generici, senza cioè numero di protocollo. Tali documenti vengono definiti Documenti non Protocollati.

I protocolli interni e in partenza possono essere inviati tramite la casella di Posta elettronica istituzionale.

Registrazione dei dati minimi di protocollo

Materialmente, per "registrazione di protocollo" si intende l'operazione che desume da un documento alcune informazioni di sintesi atte ad identificarlo e le memorizza in un sistema informatico.

Le informazioni minime che il sistema richiede e/o memorizza all'atto della registrazione di un documento, in linea con quanto indicato all'art. 53 del D.P.R. 445/00, sono:

- **Numero di protocollo** inteso come progressivo unico di registrazione nell'anno solare generato automaticamente dal sistema;
- **Data di protocollazione** intesa come data di registrazione del protocollo assegnata automaticamente dal sistema;
- **Mittente per i documenti ricevuti** o, in alternativa, il destinatario o i destinatari per i documenti spediti.
- **Oggetto del documento**
- **Data e protocollo del documento ricevuto**, se disponibili

Le informazioni indicate all'atto della registrazione di protocollo verranno utilizzate e riportate sul registro di protocollo che il sistema è in grado di produrre.

Registrazione di ulteriori elementi

Oltre alle informazioni minime sopra indicate, **PdP** permette anche la memorizzazione di ulteriori informazioni che possono essere utili nella normale gestione dei documenti

In particolare:

- **Numero e Data del Documento:**indicazione di un eventuale numero e una data associati al documento

- **La Data di Evidenza:** E' una data che il documento richiama evidenziata nel documento stesso.
- **Data Protocollo e Numero protocollo**: indicazione della data del protocollo attribuita dal mittente e il relativo numero
- **Mezzo:** indicazione del mezzo di ricevimento.
- **Data di ricevimento**: indicazione della data in cui il documento è stato ricevuto
- **Tipologia di Soggetto :** nel caso compaiano più soggetti è possibile specificare chi è il soggetto principale.
- **Estremi di Fascicolazione**

All'interno del sistema sono previste funzionalità atte a facilitare le modalità operative di protocollazione dei documenti. In particolare si segnalano le seguenti:

- **Default informazioni di protocollo:** questa funzionalità consente a particolari utenti che abitualmente protocollano documenti che presentano caratteristiche similari che dipendono strettamente dall'utente in questione, di avere le informazioni del documento già preimpostate dal sistema, così che l'utente debba inserire solo le informazioni pertinenti al documento in esame e procedere direttamente con la registrazione di protocollo.
- **Duplicazione informazioni protocollo:** questa funzione risulta particolarmente utile nel caso in cui sia necessaria la protocollazione di una serie di documenti con caratteristiche simili (es. richiesta di partecipazione ad una gara); in questo caso le informazioni di protocollo non dovranno essere ridigitate per ogni documento, ma sarà possibile duplicare le informazioni del protocollo precedente e inserire/modificare le informazioni che si ritengono opportune procedendo quindi alla registrazione di protocollo.
- **Oggetti Standard**: il sistema prevede che possa essere creato un elenco di oggetti di protocollo utilizzato frequentemente; in fase di protocollazione l'operatore potrà eventualmente richiamare l'oggetto da quelli predefiniti ed eventualmente completarlo, senza doverlo digitare completamente.
- **Classificazioni anagrafiche**: PdP prevede la creazione di gruppi di anagrafiche a cui poter associare più soggetti mittenti/destinatari per poterli associare contestualmente in uno stesso protocollo in maniera automatica**.**

A inserimento effettuato di tutti i documenti, sia protocollati che non, **PdP** memorizza, oltre a tutte le informazioni relative ai dati del documento, tutte le informazioni di inserimento: utente, ruolo, data sia di inserimento che di aggiornamento.

Modifica della registrazione di protocollo

La modifica di un protocollo risulta possibile per gli utenti che ne vengono abilitati all'interno del sistema. E' possibile modificare solamente i dati non sostanziali (numero e data di protocollo).

Le operazioni di modifica e inserimento relative ai dati di protocollo vengono sempre memorizzate all'interno di una tabella del database denominata LOG_**PdP**. In tale tabella vengono memorizzati i seguenti dati:

- Nome della tabella del database interessata alla modifica;
- Nome del campo interessato alla modifica;
- Identificativo del documento su cui è stata apportata la modifica;
- Codice operazione (D= delete, I= insert, U= update);
- Data in cui è stata fatta la modifica;
- Valore prima della modifica;
- Valore dopo la modifica;
- Utente che ha effettuato l'operazione di modifica.

Da procedura è possibile stampare un report contenente il dettaglio della tabella impostando come parametri di stampa l'utente e il range di data delle modifiche.

Assegnazione protocollo

Nel contesto del sistema del Protocollo viene gestito il flusso documentale dei documenti con l'obiettivo di ottenere le informazioni relative a:

- dove si trova il documento;
- quali unità organizzative dell'Ente sono state coinvolte nel flusso del documento.

Per la gestione dei flussi documentali attraverso il sistema di Protocollo è opportuno evidenziare le seguenti funzionalità:

- **smistamento di documenti:** con questa funzione un operatore può registrare il passaggio di un documento o di un intero fascicolo dalla propria unità operativa ad un'altra.
- **consultazione documenti ricevuti:** con questa funzione un operatore può verificare quali documenti gli sono stati inviati; una volta consultato il documento l'operatore potrà decidere se trattenerlo, oppure smistarlo ad un'altra unità operativa oppure restituirlo all'unità operativa mittente a causa di una errata assegnazione.

- **copie di documenti:** nel caso in cui un documento debba essere smistato a più di una unità operativa, risulta possibile effettuare una o più copie del documento protocollato (alla stessa stregua di ciò che avviene con il documento cartaceo) ed essere inviate alle Unità operative di competenza.

Oltre a quanto specificato sopra, tramite opportune parametrizzazioni di iter è possibile definire il percorso del documento all'interno dell'Ente, tempi e responsabili delle varie fasi.

Annullamento della registrazione di protocollo

PdP prevede la funzione di annullamento di una registrazione di protocollo secondo le indicazioni dettate dalla norma (Art. 54 DPR 445/2000). Tale operazione viene gestita dal sistema in modo puramente logico, infatti, pur mantenendo memorizzate e consultabili tutte le informazioni relative alla registrazione di protocollo viene aggiunta l'informazione indicante l'annullamento del protocollo e la motivazione corrispondente.

Impronta informatica

Il sistema fornisce la possibilità di apporre al documento informatico una impronta non modificabile che viene generata utilizzando la funzione di hash, definita nella norma ISO/IEC 10118-3:1998, Dedicated Hash-Function 3, corrispondente alla funzione SHA-1. Con l'impronta così calcolata è possibile utilizzare le funzionalità di controllo della impronta per verificare l'integrità del documento

Segnatura di protocollo

PdP gestisce la segnatura di protocollo e la possibilità di effettuarne la stampa su supporto in forma permanente e non modificabile. I dati contenuti nella segnatura di protocollo sono, come previsto dalla normativa il Nome dell'Ente o codice AOO, il numero e la data di protocollo. **PdP** fornisce la possibilità di aggiungere altri dati alle informazioni sopra descritte mediante opportune parametrizzazioni del sistema.

Registro di protocollo (stampa)

Il sistema **PdP** permette la produzione del registro di protocollo secondo i parametri e le regole previsti dalla normativa vigente; in particolare la stampa del registro di protocollo viene effettuata in formato PDF e può essere salvata in tale formato per la rispondenza a quanto richiesto dalla normativa.

Registro di emergenza

Nel caso di impossibilità di effettuare la registrazione informatica dei protocolli, così come previsto dalla norma, l'Ente potrà ricorrere alla registrazione dei protocolli sul registro di emergenza (in forma cartacea). Al ripristino delle funzionalità del sistema è prevista una funzionalità che consente il recupero dei protocolli registrati sul registro di emergenza; tale funzionalità permette di proseguire la protocollazione con attribuzione del numero di protocollo immediatamente successivo a quello registrato sul registro di emergenza, consentendo inoltre l'inserimento dei protocolli registrati manualmente specificando numero e data con cui sono stati effettivamente registrati.

Classificazione del documento

Per i documenti protocollati è previsto l'attribuzione di una classificazione attinente ad un titolario di archivio. La gestione del titolario di archivio è parametrica, e di conseguenza è lasciata ampia scelta all'Ente di dotarsi di un tipo di classificazione piuttosto che un altro (ad esempio, classificazione per "materia" piuttosto che per "funzione"). Durante la fase di protocollazione viene proposta una maschera di aiuto che consente di navigare nel titolario e ricercare la voce corrispondente, come viene mostrato anche dalla maschera seguente:

Ricevuta di protocollo

PdP consente di effettuare la stampa della ricevuta di protocollo, In fase di parametrizzazione del sistema è possibile impostare più di un modello di stampa e **PdP**, in fase di stampa proporrà all'utente la scelta del modello da stampare. I report sono costruiti mediante il software standard di reportistica denominato Crystal Report, che fornisce la possibilità all'Ente di poter anche modificare in autonomia il layout delle stampe.

Fascicolazione

Apertura di un fascicolo

Un fascicolo è una aggregazione logica di documenti avente una numerazione in base annua basata sul titolario di classificazione.

Fascicolo- Contenitore di documenti al primo livello (radice dell'albero del faldone)

SottoFascicolo – Contenitore di documenti figlio di un fascicolo oppure di un altro sottofascicolo.

Faldone – Insieme di Fascicoli Sottofascicoli e dei Documenti (non è una entità informatica)

Nomenclatura del Numero dei Fascicoli e Sottofascicoli.

Le operazioni di apertura di un fascicolo avvengono mediante una funzionalità resa disponibile dal sistema che richiede i seguenti dati obbligatori

- Anno del fascicolo
- Data di apertura del fascicolo (viene proposta la data del giorno)
- Oggetto del fascicolo
- Voce del titolario di classificazione

La numerazione del fascicolo e' automatica e progressiva all'interno dell'anno e della classificazione del titolario.

Il sistema memorizza anche il ruolo che ha effettuato l'apertura del fascicolo.

Fascicolazione di un documento

Mediante il sistema **PdP** è possibile collocare in fascicoli o sottofascicoli sia documenti protocollati che documenti non protocollati. A tal scopo viene resa disponibile una funzionalità relativa alla fascicolazione che può essere attivata:

- durante la fase di inserimento di un documento nel sistema (protocollazione o inserimento di un documento non protocollato)
- in fase di gestione del documento stesso.

Una volta selezionato il documento da fascicolare è possibile ricercare nel sistema l'elenco di fascicoli già creati precedentemente e includere il documento nel fascicolo prescelto.

In alternativa è possibile anche aprire un nuovo fascicolo per l'inserimento del documento.

Sono disponibili anche le funzionalità relative a:

- creazione e spostamento in sottofascicoli
- collegamento con altri fascicoli
- annullamento pratica
- chiusura apertura pratica
- assegnazione livelli di visibilità
- attivazione iter

Chiusura di un fascicolo

E' possibile chiudere o riaprire un fascicolo mediante la valorizzazione della data di chiusura.

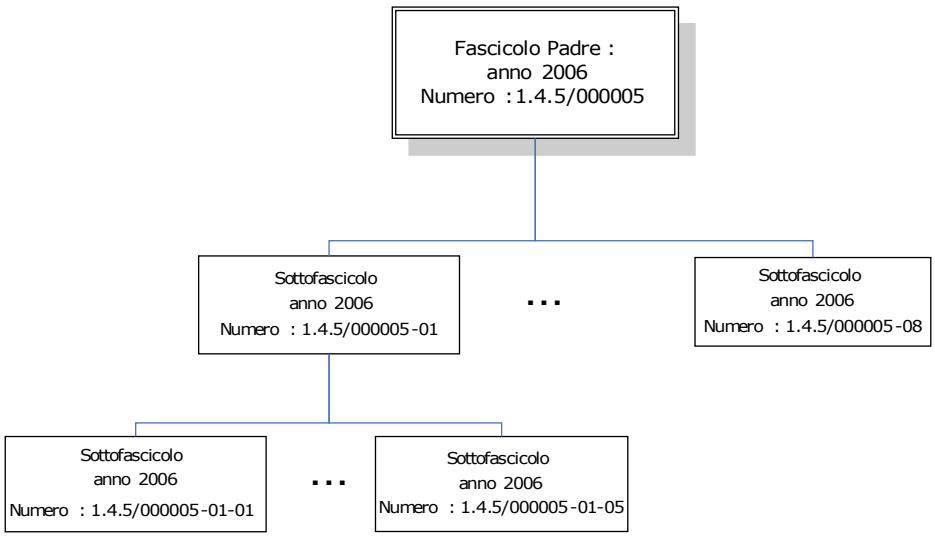
La chiusura di un fascicolo è consentita solo se tutti i suoi sottofascicoli sono chiusi.

Gestione dei sottofascicoli

Un fascicolo può contenere al suo interno fino a 99 sottofascicoli ognuno con gli stessi dati di profilazione del fascicolo padre e che vengono ereditati in fase di creazione, fa eccezione il numero di sottofascicolo che viene assegnato automaticamente in modo progressivo all'interno del fascicolo padre.

Un sottofascicolo può a sua volta contenere ulteriori sottofascicoli (inserti) creando così una struttura ad albero che a partire dal fascicolo padre può estendersi fino ad un massimo teorico di 15 livelli ognuno contenente fino a 99 sottofascicoli.

Di seguito viene mostrato un esempio di strutturazione in sottofascicoli:



La creazione del sottofascicolo avviene mediante l'utilizzo della funzionalità della gestione dei fascicoli ed eredita dal fascicolo padre alcuni dati principali, come ad esempio la classifica e l'oggetto, ognuno di questi dati poi può essere modificato dall'operatore.

La maschera di gestione dei sottofascicoli consente di attivare la visualizzazione di tutti i dati di tutti i documenti contenuti nei vari sottofascicoli del fascicolo padre, come viene mostrato nella maschera seguente.

Collegamenti tra fascicoli

I fascicoli possono essere collegati tra loro in serie così da formare aggregazioni specifiche. Un fascicolo può essere inserito anche in serie differenti. Ogni serie ha la strutturazione ad albero.

Mediante le maschere relative alla gestione del fascicolo è possibile effettuare il collegamento di uno o più fascicoli ed esprimere le specifiche relative a:

- tipo di collegamento dei fascicoli

- cronologia del fascicolo: indicazione del fascicolo precedente e successivo

Per effettuare il collegamento di fascicoli è necessario ricercare i fascicoli che si intendono selezionare. **PdP** mette a disposizione le funzioni di ricerca che possono essere attivate sfruttando con gli stessi meccanismi standard utilizzati in tutta la suite **PdP**.

In particolare per quel che riguarda i fascicoli, i campi sui quali poter effettuare la ricerca sono i seguenti:

- Anno
- Numero
- Classifica
- Id
- Data
- Oggetto
- Livello di visibilità
- Ruolo di inserimento
- Utente di inserimento
- Data Chiusura Fascicolo
- Visualizzazione dei soli fascicoli aperti

Una volta individuati i fascicoli ed effettuato il collegamento il sistema offre alcune funzionalità che consentono di:

- spostare uno o più documenti fra un fascicolo e l'altro.
- visualizzare tutti i collegamenti effettuati sul fascicolo selezionato
- visualizzazione di tutte le informazioni riguardanti i documenti inseriti nei vari fascicoli.

Visibilità sui fascicoli

Fascicoli e sottofascicoli sono soggetti a meccanismi di riservatezza definiti dalle ACL a loro assegnati.

I meccanismi utilizzati per l'assegnazione e la modifica delle ACL sono gli stessi utilizzati per i documenti e i protocolli. Attraverso questi meccanismi i livelli di visibilità vengono "ereditati" in modo automatico da un fascicolo al sottofascicolo creato ed è possibile abilitare oppure disabilitare altre unità operative alla visualizzazione.

Funzionalità di Reportistica

Configurazione della reportistica

PdP gestisce le stampe mediante uno strumento standard di mercato denominato Crystal Report (Business Object) del quale viene fornito il runtime per l'esecuzione dei report messi a disposizione della procedura.

Lo strumento Crystal Report è di semplice utilizzo e consente all'Ente di effettuare le modifiche ai report già esistenti oppure di creare in autonomia nuovi report.

La configurazione in **PdP** dei report è di semplice attuazione poiché basta collegare, mediante una funzione di configurazione il report disegnato alla pagina corrispondente del sistema, ed è possibile anche vincolare la possibilità di lanciare un report solo ad alcuni utenti del sistema.

I report ottenuti sono per default in formato pdf e sono visualizzabili utilizzando il browser . Sfruttando le funzionalità rese disponibili dal browser è possibile:

- Inviare via mail;
- Salvare su disco;
- Stampare il report prodotto.

Come ulteriore formato dei report e' utilizzabile il Crystal Report Viewer da cui e' possibile esportare il report in formato Word (rtf) ,EXCEL,PDF,RTF.

Registro modifiche

PdP memorizza in una tabella tutte le modifiche effettuate sui dati protocollati, così come previsto dalla normativa. Tutte le modifiche di protocollo (cambio oggetto,cambio pratica, cambio destinatari e mittenti, etc,) vengono registrate ed è possibile stamparle mediante il report di stampa delle modifiche di protocollo, che richiede in input l'intervallo di date e l'utente di riferimento.

Lista documenti ricercati

PdP consente di effettuare una stampa degli elenchi prodotti dalle funzioni di ricerca; infatti esiste un report che propone i documenti risultato delle ricerche e permette di scegliere quelli da stampare.

Distinta protocollo

Il report di distinta di protocollo rappresenta l'elenco di tutti i documenti che sono stati protocollati in un giorno da un determinato ufficio e suddiviso per scrivanie di destinazione:

Repertori e serie

Per repertorio si intende la numerazione interna ad un registro dell'Ente quale ad esempio il registro delle ordinanze.

Inserimento di un repertorio

Il numero di repertorio, o registro, è un numero che può essere attribuito sia a documenti protocollati che non protocollato.

I registri vengono numerati progressivamente per tipo registro e per anno. La numerazione può avvenire manualmente o può essere assegnata automaticamente dal sistema. Nel primo caso è l'utente che dopo l'inserimento del documento assegna un numero di repertorio tramite la funzione di numerazione, nel secondo caso l'attribuzione del numero di registro avviene in maniera automatica contestualmente alla memorizzazione del documento.

Configurazione dei repertori

In **PdP** è possibile gestire la numerazione dei documenti in registri definiti a priori dall'amministratore del sistema.
La numerazione dei repertori può essere impostata in base al tipo dì documento o per tutti i tipi documenti indistintamente (ad esempio il numero di repertorio delle Ordinanze può essere attribuito solo a documenti di tipo Ordinanza oppure a tutti) , e può essere manuale,quindi tramite una particolare funzione, oppure automatica, quindi attribuita automaticamente all'atto della memorizzazione del documento.

Ricerche

PdP permette di effettuare le ricerche delle informazioni relative a documenti, fascicoli e documenti contenuti all'interno di fascicoli tramite l'impostazione di filtri. E' possibile indicare in una singola ricerca più parametri (esempio, oggetto, classificazione, data, etc.) ed utilizzare nelle ricerche per intervalli (utilizzando i caratteri > = < come operatori di confronto), attraverso i connettori logici "AND" e "OR" e mediante l'utilizzo di caratteri jolly.
I campi di ricerca utilizzabili sono molteplici; inoltre esistono già impostate delle macro-aree di ricerca per tipologia di atto:

- dalla sezione DOCUMENTI possono essere ricercati tutti i documenti inseriti nel DB PdP indipendentemente dalla tipologia (protocolli, documenti non protocollati, atti, etc..); in particolare è prevista la selezione per i campi richiesti dall'Ente e la possibilità di ricercare in base alle varie unità operative che hanno trattato il documento ricercato;
- dalla sezione PROPOSTE è possibile restringere la ricerca ai soli documenti di tipo proposta (Proposte di Delibera, Emendamenti, etc…);
- dalla sezione DELIBERE è possibile restringere la ricerca alle deliberazioni;
- dalla sezione DETERMINE è possibile restringere la ricerca alle determinazioni dirigenziali;
- dalla sezione ALTRE RICERCHE e possibile effettuare delle ricerche con dei criteri non contemplati nelle precedenti sezioni;
- dalla sezione FULL-TEXT è possibile effettuare delle ricerche full text nel caso in cui si utilizzi una gestione documentale su file system oppure una piattaforma di gestione documentale (Hummingbird o Documentum);
- nella sezione QUERY vengono visualizzate tutte le ricerche di uso comune che un utente decide di salvare avendo quindi la possibilità di rieseguire la medesima ricerca senza impostarne nuovamente i criteri.

Il risultato della ricerca riporta tutte le informazioni relative i dati strutturati di ogni singolo documento/fascicolo con indicazione della tracciatura subita all'interno dell'Ente.
Tramite le ricerche è sempre possibile, ai fini statistici, visualizzare il totale dei documenti trovati in base ai parametri di ricerca impostati.
A proposito di statistiche **PdP** fornisce report standard per il monitoraggio statistico della documentazione dell'Ente:

- Statistiche protocolli in carico per ufficio: viene prodotto un report contenente il totale documenti assegnati e suddivisi per scrivania
- Statistiche per Scrivania: viene prodotto un report contenente il totale dei documenti in scrivania suddivisi per sezione di arrivo e carico
- Statistiche protocolli inseriti per ruolo: viene prodotto un report contenente i totali dei documenti inseriti per ruolo
- Statistica documenti per Mittente/Destinatario: viene prodotto un report contenente il totale dei documenti per mittenti e/o destinatari esterni.

Ricerche documenti per chiavi

Nella procedura **PdP** è possibile effettuare ricerche utilizzando molteplici chiavi e regole.
Le regole per la costruzione di una ricerca sono le seguenti:

=	uguale ad un valore
>	maggiore di un valore
>=	maggiore uguale ad un valore
<	minore di un valore
<=	minore uguale di un valore
*	tutti i valori (solo per campi carattere)
|	un valore oppure un altro (OR logico)
&	un valore e un altro (AND logico)

Ad esempio se si volessero ricercare:

- tutti i protocolli del 01/02/2007 occorre impostare il campo “Data protocollo”: 01/02/2007;
- Tutti i protocolli del mese di dicembre 2006 occorre impostare il campo “Data protocollo”: >= 01/12/2006 & <= 31/12/2006;
- Tutti i protocolli del 2006 con numero che va da 1569 al 1598 occorre impostare il campo “Anno protocollo” : 2006 e il campo “Numero protocollo” >= 1569 & <= 1598;
- Tutti i documenti che hanno nell'oggetto la parola "richiesta" occorre impostare il campo “Oggetto”: richiesta;
- Tutti i documenti che hanno nell'oggetto la parola "richiesta" o la parola "domanda" occorre impostare il campo “Oggetto” : richiesta | domanda;
- Tutti i documenti che hanno nell’oggetto una parola che inizia per “richiest” occorre impostare il campo “Oggetto” : richiest*

Ricerche full-text

Il sistema **PdP** è fornito di un sistema di ricerca full-text basato sulla indicizzazione dei documenti informatici che vengono inseriti nel sistema . In particolare è possibile utilizzare gli operatori logici per selezionare in modo opportuno i dati da estrapolare, nella tabella seguente viene fornito un esempio di impostazioni:

Operatore	Risultato
AND	Documenti che contengono le parole indicate
OR	Documenti che contengono la prima oppure la seconda parola
NOT	Documenti che contengono una parola ma non un’altra
NEAR	Documenti contenenti due parole vicine
EQUALS	Documenti contenenti esattamante le parole inserite
JOLLY	Documenti che contengono la parola indicata

Ricerche per fascicolo

E’ possibile effettuare le ricerche utilizzando come criteri di estrazione i dati del fascicolo e delle pratiche andando a compilare i campi corrispondenti della maschera delle ricerche mostrata in questo capitolo, **PdP** mostrerà come risultato della ricerca l’elenco dei documenti che soddisfano i criteri indicati.

In particolare nella maschera seguente viene mostrata la maschera che consente di effettuare le ricerche sui fascicoli e che si basa sui seguenti criteri di selezione del fascicolo:

Anno: Anno
Numero: Numero
Classifica: Classifica assegnata al fascicolo
ID: identificativo
Data: data di creazione
Oggetto:Oggetto inserito in fase di creazione di un nuovo fascicolo
Liv.Sic.: livelloo di sicurezza e visibilità assegnato
Ruolo ins:Ruolo dell’utente di inserimento del fascicolo
Utente di ins.:Utente di inserimento del fascicolo
Data chiusura fascicolo: data chiusura fascicolo
Solo fascicoli aperti: estrae solo i fascicoli aperti

In aggiunta a questa funzionalità viene messa a disposizione degli utenti del sistema anche una tipologia di ricerca che agisce sui dati specifici del fascicolo e permette di estrapolare i dati con la stessa metodologia indicata in questo capitolo per le ricerche di documenti.

Il risultato prodotto dalla ricerca è un elenco di fascicoli che rispondono ai parametri di ricerca impostati, è possibile accedere ad ogni singolo fascicolo e visionare i documenti in esso inseriti.

E’ possibile attivare questo criterio di ricerca sia in fase di ricerca generalizzata dei dati di un fascicolo sia in fase di inserimento di un documento protocollato o non protocollato all’interno di un fascicolo esistente.

Interoperabilità

Registrazione e trasmissione di documenti informatici

PdP gestisce per ogni Ente una o più caselle di posta elettronica istituzionali che vengono collegate agli utenti del sistema autorizzati ad accedere ed utilizzare la casella di posta istituzionale.

La prima fase prevista per l’invio ad un altro Ente di un documento informatico attraverso le funzioni di interoperabilità tra protocolli informatici, consiste nell’effettuare la protocollazione del documento da inviare.

Questa fase viene svolta dall’operatore utilizzando la maschera di protocollazione, nella quale viene richiesto di completare tutte le informazioni minime richieste per effettuare la protocollazione a norma (oggetto, destinatario, ecc.). Oltre a tali informazioni sarà possibile per l’operatore aggiungere ulteriori informazioni gestite dal sistema **PdP** utili per l’Ente nella gestione documentale interna.

Apposizione della Firma Digitale al documento Protocollato

Alle informazioni inserite in fase di protocollazione è possibile associare il documento informatico ed eventuali allegati ed effettuare l’autenticazione attraverso l’apposizione della firma digitale. Per compiere tale operazione

all'operatore verrà richiesto di inserire nel lettore collegato al proprio Personal computer la smart-card contenente il proprio certificato di firma e digitare il proprio codice di identificazione rilasciato insieme al certificato di firma.

Evidenza del documento e della relativa Firma Digitale apposta

Al termine della fase di firma, nel sistema **PdP** saranno presenti i dati strutturati associati al protocollo, il documento sottoscritto ed autentificato tramite un certificato di firma.

Segnatura informatica

Sul documento in partenza viene automaticamente generata dal sistema la segnatura informatica in formato XML secondo le modalità indicate dal DTD definito dall'AIPA. Oltre alle informazioni minime previste **PdP** estende le informazioni minime richieste, includendo ad esempio una serie di informazioni utili alla costituzione del fascicolo elettronico.

Inoltro del documento all'Ente destinatario con inclusa la Segnatura tramite il sistema di interoperabilità fra Protocolli Informatici presente in PdP

Attraverso un'apposita funzione viene generato automaticamente un messaggio di posta elettronica nei formati previsti dalla circolare AIPA n° 28/2001 che consente di inviare all'Ente destinatario il documento protocollato in partenza. Il sistema, attraverso le informazioni riguardanti il destinatario del protocollo sarà in grado di individuare l'indirizzo di posta elettronica della casella di posta istituzionale dell'Ente destinatario a cui inviare il messaggio. Il messaggio conterrà naturalmente sia il documento informatico sottoscritto tramite firma digitale che il file di segnatura in formato XML per consentire al sistema di protocollo ricevente di protocollare automaticamente il documento.

Ricezione dei documenti informatici

Per quanto attiene alla funzione di acquisizione di documento in arrivo da Altri Enti, **PdP** mette a disposizione una funzionalità che attraverso la scrivania virtuale dei documenti consente di accedere alla casella di posta elettronica istituzionale su cui saranno visibili i documenti in arrivo che potranno essere protocollati.

Acquisizione del documento Informatico dalla casella di Posta Elettronica Istituzionale (della AOO) da parte dell'Ente destinatario

Dalla casella di posta elettronica della AOO è possibile acquisire il messaggio in arrivo dall'Ente mittente per poterlo protocollare; il messaggio in arrivo, se opportunamente costruito dal sistema di protocollo dell'Ente mittente, conterrà il documento informatico opportunamente sottoscritto e la segnatura informatica con le informazioni minime necessarie per la protocollazione del documento stesso. Il sistema **PdP** in fase di protocollazione fornisce la possibilità di effettuare la verifica della firma.

Protocollazione del documento da parte dell'Ente destinatario ed inoltro della conferma di avvenuta ricezione all'Ente emittente

Il messaggio acquisito dalla casella di posta elettronica istituzionale viene automaticamente protocollato attraverso le informazioni contenute nella segnatura e diventa parte integrante del sistema alla stregua degli altri documenti protocollati. Pertanto viene gestito attraverso le funzioni di gestione documentale e Workflow presenti nel sistema **PdP**.
Nel caso in cui nella segnatura informatica dell'Ente mittente fosse stata richiesta una conferma di ricezione, il sistema **PdP** genera in automatico una conferma di ricezione che viene inviata alla casella di posta elettronica dell'Ente mittente.

Gestioni dei messaggi di ritorno

Nel caso in cui nella casella di posta elettronica dell'Ente sia presente una conferma di ricezione proveniente dall'ente destinatario, il sistema **PdP** è in grado di acquisire tale documento e attraverso le informazioni contenute nel file XML è in grado di effettuare l'abbinamento con il numero di protocollo originale.

Funzioni per IPA (Indice delle Pubbliche Amministrazioni)

Mediante le maschere che consentono l'accesso alle funzionalità sopra descritte è possibile eseguire l'accesso all'indice delle pubbliche amministrazioni (IPA) al fine di consultare le informazioni che vi sono iscritte e di utilizzarle per inviare mail da **PdP**.
Mediante la funzionalità di ricerca è possibile individuare velocemente l'ente che si desidera consultare.
E' possibile ricercare le amministrazioni accreditate filtrandole sulla base di:

- codice amministrazione:
- tipologia di Ente:
- Regione di appartenenza:

ed altri (Provincia, etc.).

Nel caso in cui i criteri di ricerca resi disponibili non vengano considerati sufficienti dall'utente è disponibile un link al sito dell'IPA in modo che si possa accedere all'elenco completo e alle funzionalità di ricerca estese che il sito stesso rende disponibili.
L'esecuzione della ricerca produce una visualizzazione che elenca le PA che soddisfano le condizioni di filtro.
La tabella delle AOO permette di selezionare una riga e attraverso l'uso del bottone conferma permette di utilizzare l'indirizzo di posta ad esso associata come destinatario dell'mail che si stava componendo all'atto dell'apertura della pagina che consulta l'IPA.

Workflow documentale

Un work flow è un sistema che definisce, crea e gestisce l'esecuzione di flussi di lavoro pianificati tramite un software in grado di interpretare la metodologia con la quale i processi sono stati organizzati; che interagisce con gli attori e le risorse coinvolte nel processo. che è in grado, se e quando richiesto, di invocare, utilizzare e interagire con tool, applicazioni e più in generale con sistemi esterni.

Di seguito il sistema di work flow di **PdP** verrà chiamato WFM.

Il WFM di **PdP** si interfaccia con l'applicativo per fornire i servizi necessari all'esecuzione dei processi pianificati. Il WFM di **PdP** inoltre, permette di pianificare i processi secondo una metodologia che è implementata come modulo del prodotto stesso. Attraverso un strumento, grafico permette il disegno dello sviluppo temporale (iter del processo) delle singole attività elementari in cui il processo viene scomposto.

Il WFM non gestisce di per sé data base verticali che contengono dati specifici. Oltre ad implementare e gestire le regole che permettono lo svolgimento delle istanze, registra i dati, gli stessi per tutti i processi, trasversali rispetto alla specificità dei singoli processi.

Ad ogni "passo", cioè ogni punto in cui termina un'attività e ne inizia un'altra, è possibile inserire degli eventi che consentono il passaggio da un'attività alla successiva, e questi ultimi possono essere eseguiti sia in modalità automatica da parte del sistema, sia in modalità manuale in base alla decisione dell'operatore.

I processi, per poter essere gestiti dal WFM, devono essere decomposti nelle loro attività elementari, quindi le attività individuate devono essere riconcatenate secondo uno schema logico che segue lo sviluppo temporale. Le informazioni confrontate con i dati impostati nella fase di pianificazione del processo danno lo scostamento tra l'andamento teorico previsto per un dato processo e quello reale.

I dati di monitoraggio relativi alla singola istanza di un procedimento possono essere utilizzati anche per fornire informazioni all'esterno dell'Ente, al soggetto che ha innescato l'istanza del processo. Mentre quelli relativi all'andamento del processo possono essere utilizzati per il controllo di gestione e per effettuare verifiche circa il funzionamento del modello teorico del processo.

Una volta disegnato il processo in termini di flusso e messo in funzione, il WFM inizia a collezionare istanze relative ai vari processi messi in produzione.

Iter di un processo teorico:

- la pratica relativa ad uno specifico processo viene attivata, ad esempio a seguito di una richiesta che arriva dall'esterno,
- la richiesta viene presa in carico da un addetto della struttura dell'Ente responsabile del processo che ne controlla la completezza in termini di dati e documenti,
- la richiesta viene protocollata (protocollazione e fascicolazione) ed eventualmente trasferita ad un altro addetto,
- se la richiesta è stata trovata mancante di dati e documenti obbligatori viene inviata una richiesta di integrazione delle parti mancanti
- a seguito della richiesta di integrare le parti mancanti può essere attivata una sospensione nel conteggio dei termini (teorici) del processo
- a questo punto inizia la fase istruttoria, più o meno complessa, in cui l'istanza viene trattata. In questa parte dell'iter potrebbe essere richiesto l'intervento di altri Enti, la convocazione di commissioni, la presentazione di altri documenti, etc
- durante il percorso attraverso le attività elementari in cui il processo è stato scomposto, la pratica viene messa in carico a diversi addetti ognuno dei quali la arricchisce di documenti.

Tutto questo è governato e gestito dal motore del WFM che non fa altro che proporre l'esecuzione passo per passo dell'articolato di attività elementari secondo la logica implementata tramite il modulo di disegno dell'iter del processo.

Scrivania: applicazione al WFM

L'interfaccia del motore di workflow viene definita "scrivania virtuale" in quanto, per similitudine con le scrivanie reali, rappresenta il luogo dove i documenti transitano. Una scrivania virtuale può essere associata ad una persona fisica (attore, utente della procedura) oppure ad una struttura (ufficio, servizio). In questo secondo caso più attori potranno contemporaneamente accedere alla scrivania virtuale.

Implicitamente la scrivania virtuale implementa un efficace modello di sicurezza in quanto l'accesso e le azioni nella procedura possono essere effettuate sui documenti solo dall'attore (utente) associato alla scrivania medesima.

Disegno di un iter

Il modulo software per disegnare il flow del processo (ITER DESIGNER) consente attraverso un'interfaccia grafica semplice ed intuitiva la costruzione del diagramma dei procedimenti e la definizione, ad ogni punto di passaggio da una fase a quella successiva, le regole secondo le quali i vari step del processo devono essere eseguiti. I procedimenti documentali per essere disegnati vengono prima analizzati attraverso metodologie di BPR (Business Process management) in funzione delle caratteristiche specifiche della struttura organizzativa dell'ente.

Iter

L'entità rappresenta logicamente tutto il procedimento in termini d responsabilità e durata.

L'entità non rappresenta una azione eseguibile vera e propria ma solamente il punto logico di partenza di un procedimento.
L'entità ITER contiene le entità FASI- PASSI – ESITI.

Fase

L'entità rappresenta l'insieme dei passi omogenei che realizzano una macro-azione. Ha rilevanza soprattutto in funzione dell'assegnazione della responsabilità e della durata di un sottoprocesso. La proprietà 'scrivania' indica il punto di spostamento all'interno della struttura.
Le FASI si devono susseguire in modo sequenziale, è però permesso tornare ad una fase precedente.
Il cambio di FASE avviene (visivamente) quando la linea di un ESITO incrocia la linea di una FASE
Il motore di ITER invece modica la FASE quando un ESITO porta il motore in un PASSO appartenente ad una FASE differente.
La proprietà SCRIVANIA indica il punto della struttura che eseguirà tutti i PASSI contenti in una FASE.
Una particolare scrivania è indicata con 'Me' sinonimo di scrivania attuale.
Non esiste limite al numero di fasi inseribili in un ITER e al numero di PASSI assegnati ad una FASE.
L'entità FASE contiene le entità PASSI e ESITI

Passo

L'entità rappresenta l'unità minima elaborabile dall'esecutore. I PASSI sono tipizzati a seconda della funzione che svolgono. La proprietà 'parametri' stabilisce il comportamento del passo.
I passi sono collegati tra di loro dagli ESITI
Non è ammesso collegare o inserire un passo non collegato a nessun altro passo.
Un PASSO deve essere sempre contenuto in una e una sola FASE.
Il passo viene eseguito dalla scrivania indicata nella proprietà della FASE in cui è contenuto.
Un passo può essere collegato a se stesso attra verso un particolare esito detto AUTOCOLLEGAMENTO
I tipi di PASSO eseguibili sono:

 **FORM o PAGINA WEB** Esecuzione di pagina WEB

 **FUNZIONE** esecuzione di una funzione di libreria senza interfaccia utente.

 **MESSAGGIO** attivazione di un messaggio o MAIL o SMS

 **ODG** sospensione dell'ITER per gestione di una seduta.

 **PROGRAMMA** esecuzione di un programma esterno

 **SOSTA** sosta generica con possibilità di sblocco manuale

 **EVIDENZA** sosta con impossibilità di sblocco manuale

 **TERMINE ITER** chiusura di un iter

 **NUOVO ITER** avvio di un nuovo iter sullo stesso documento o su altro

 **WS** esecuzione di un Web-Services

 **SOSPENSIONE** sospensione di un ITER

 **SUB ITER** avvio di un sub-iter (l'iter principale è sospeso e verrà riattivato alla conclusione del sub iter)

 **ITER PARALLELO** avvio di un iter parallelo

 **SINCRONIA ITER** sincronia tra iter principale e iter parallelo (il primo non procede se il secondo non è terminato)

 **SCRIPT** Esecuzione Script (linguaggio VBA)

L'entità PASSO contiene l'entità ESITI

Esito

L'entità rappresenta il collegamento tra i PASSI e quindi determina la successione temporale degli stessi.
le regole di visibilità degli ESITO sono:

- Un esito può essere dichiarato visibile o non visibile:
- Se per un passo esiste più di un esito tutti gli esiti sono automaticamente visibili.
- Gli esiti possono essere sottoposti a condizione.

- Quando run-time le condizioni sono state risolte si applica la regola 2

Esecuzione di un iter

PdP PAW è la componente applicativa di gestione documentale della Suite **PdP** per la gestione dei procedimenti amministrativi. In particolare è il motore di workflow (**PdP** WorkFlow management) che gestisce i processi documentali degli Enti. Si presenta come un sistema modulare che permette la creazione, la configurazione, la gestione, il tracciamento e l'esecuzione automatica dei flussi di lavoro (Work-Flow) della Gestione Documentale dell'ente. Inoltre è integrato con un'ampia gamma di moduli applicativi opzionali immediatamente fruibili a supporto dei procedimenti amministrativi degli enti.

In **PdP** PAW le informazioni trattate rispondono ad una logica molto intuitiva di tipo *multimediale*, sono convalidabili con l'apposizione della *Firma Digitale* e sono rigorosamente protette da accessi non previsti.

PdP PAW è un sistema che definisce, crea e gestisce l'esecuzione di flussi di lavoro pianificati, tramite un software in grado di interpretare la metodologia con la quale i processi sono stati organizzati e che interagisce con gli attori e le risorse coinvolte nel processo.

Quindi è in grado, se e quando richiesto, di invocare, utilizzare e interagire con tool, applicazioni e più in generale con sistemi esterni.

PdP PAW permette di classificare e rappresentare i processi dei procedimenti amministrativi di ogni Ente attraverso un modulo interno.

Questo è uno strumento grafico che permette il disegno dello sviluppo temporale (iter del processo) delle singole attività elementari in cui il processo viene scomposto.

I processi, per poter essere gestiti da **PdP** PAW, devono essere decomposti nelle loro attività elementari, quindi, le attività individuate devono essere concatenate secondo uno schema logico che segue lo sviluppo temporale: si parte dall'attività che innesca il processo, per passare alla/alle attività intermedie di verifica dei dati di produzione o di richiesta per arrivare all'attività conclusiva del processo.

I processi vengono disegnati comprendendo nello sviluppo temporale le attività standard, quelle condizionate, quelle eventuali attinenti a percorsi alternativi (endo e/o sub procedimentali).

Ad ogni "passo" dell'iter, cioè in ogni punto in cui termina un'attività e ne inizia un'altra, è possibile predefinire degli eventi che consentono il passaggio all'attività successiva o attraverso attività eseguite in modalità automatica da parte del sistema oppure attraverso modalità manuali.

PdP PAW propone all'utilizzatore il procedimento come una successione di "cose da fare" (task list), permettendogli di seguire in modo intuitivo la sequenza corretta tutte le attività.

PdP PAW permette il monitoraggio, il controllo ed il tracciamento, anche con visualizzazione grafica, di tutte le attività di tutti i procedimenti dell'ente registrandone una serie di informazioni consultabili in tempo reale anche attraverso elaborazioni statistiche.

La visualizzazione grafica permette di conoscere in tempo reale lo stato di ogni singolo processo dell'ente.

PdP PAW è in grado di gestire privacy e sicurezza in quanto ogni attività dei processi può essere assegnata ad attori specifici. Le assegnazioni agli attori abilitati possono essere fatte automaticamente dal sistema o manualmente dall'operatore ma sempre eseguendo una scelta fatta sulla base di quanto impostato, in fase di analisi, nel modello del processo.

Flussi documentali

Scrivania (lista attività)

La soluzione applicativa proposta dispone di una area di lavoro per utente definita "Scrivania Virtuale".

La "scrivania virtuale" vuole emulare e rendere quanto più possibile simile il lavoro di un operatore su una scrivania reale . Pertanto vengono ripresi i concetti di "pila di documenti" e di "strumento di scrivania", inteso come strumento che opera sulla pila dei documenti. La scrivania virtuale si può definire come il luogo informatico dove i documenti transitano. La definizione delle scrivanie virtuale è data dall'amministratore del sistema in base alla struttura dell'ente cioè dell'organigramma in modo che un utente (così come succede nella realtà) possa sedersi a più scrivanie oppure una scrivania possa essere condivisa da più utenti nel lavoro quotidiano.

Normalmente e nei casi più comuni si è soliti assegnare una scrivania ad ogni ufficio, le persone dell'ufficio che condividono lo stesso lavoro e quindi anche stessa scrivania. La scrivania virtuale è anche un paradigma per assegnare le azioni che un utente può compiere; l'utente infatti, può interagire con i documenti solamente attraverso gli strumenti di scrivania e questi sono assegnati parametricamente dall'amministratore della procedura.

La scrivania virtuale è composta di sezioni denominate "pile" (corrispondenti a folder informatici) di seguito descritte:

Sezione Arrivi: Qui compaiono i documenti assegnati o trasmessi da un'altra scrivania. In questa sezione normalmente, non viene permessa la modifica di dati dei documenti, ma solamente la presa in carico, quindi lo spostamento manuale tramite selezione dei documenti nella sezione "carico" .

Sezione Carico: Questa è la sezione principale della procedura in quanto permette una interazione forte con il documento stesso attraverso gli strumenti di scrivania. Gli strumenti di scrivania vengono assegnati dall'amministratore scegliendoli tra tutti quelli messi a disposizione dalla soluzione proposta. L'amministratore ha altresì facoltà di assegnare uno strumento a tutti indicandone nella sua abilitazione "Ogni Ruolo". Uno strumento può essere sviluppato

anche in momenti successivi l'installazione e a seguito del mutare delle esigenze informatiche. Questo paradigma di fatto garantisce che esigenze future possano trovare una facile soluzione nella creazione di strumenti "ad hoc". Nella sezione carico è poi possibile inoltrare il documento ad altre scrivanie così come rifiutarlo. La presa in carico di un documento pone il documento stesso in uno stato di "già letto".
Sezione Trasmessi: La sezione trasmessi contiene i documenti trasmessi dalla scrivania attuale ad altra scrivania. Un documento compare nella sezione trasmessi dopo che è stato trasmesso/assegnato.
Sezione Archivio: Questa sezione è di fatto come la sezione "Carico" serve come utilità all'utente per parcheggiarvi documenti che non saranno lavorati a breve. **Sezione**
Sezione e-mail: Questa sezione è di fatto un piccolo client di posta associato alla scrivania avente le funzionalità di lettura e invio di e-mail. Alla scrivania normalmente viene associata una casella di posta istituzionale (PEC o "normale") oppure di configurare la scrivania sulla casella di posta propria dell'utente. Esiste anche la possibilità di avere ambedue le scelte cioè una casella istituzionale (edilizia_nomemiocomune@ postacert. it) e una normale (nome.cognome@nomemiocomune.fc.it) .
Una funzione presente in questa sezione permette di trasformare un e-mail in un documento della soluzione applicativa. Tale documento una volta creato comparià direttamente nella sezione "carico" per essere "lavorato". Si notino le similitudini tra la scrivania virtuale e i programmi client di posta elettronica come "MS-Outlook". Questa similitudine aiuta gli utenti nell'apprendere le modalità di utilizzo in quanto molto simili a quelle utilizzate con i client di posta.
La Scrivania virtuale è dotata di due serie di tasti così definiti.
Bottoni di scrivania: Nella parte inferiore della "scrivania virtuale" compaiono una serie di tasti dipendenti dalla sezione prescelta questi tasti svolgono funzioni di servizio sempre disponibili ad esempio "rifiuto" "Nuovo E-mail" "Report" "Ricerca su scrivania"
Strumenti di scrivania: Nella parte sinistra della "scrivania virtuale" compaiono una serie di tasti dipendenti dalle abilitazioni assegnate alla scrivania dall'amministratore. Questi tasti permettono di svolgere operazioni sui documenti come ad esempio "classifica" Gli strumenti sono assegnabili per sezione a seconda del loro significato , ad esempio lo strumento "Ricerca" che permette la ricerca in tutto l'archivio può essere assegnato a tutte le sezioni, lo strumento classifica è opportuno sia assegnato alla sola sezione carico.
La definizione di uno strumento comporta anche l'indicazione se lo strumento possa applicarsi ad un documento, a più di un documento oppure non debba applicarsi a nessun documento. L'interfaccia controlla che nei tre casi sia state fatte le scelte opportune dall'operatore prima di lanciare lo strumento vero e proprio.
Presa in carico di un documento
I documenti inviati da altre unità operative confluiscono tutti nella sezione di Arrivo. Per poter lavorare i documenti è necessario però effettuare la presa in carico, ovvero spostare i documenti dalla sezione di arrivo alla sezione di carico.
Tale operazione è considerata come la lettura del documento e viene memorizzata nel sistema. In qualsiasi momento accedendo alle informazioni del documento si ha l'informazione di quando un'unità operativa ha effettuato la presa in carico.
Una volta nella sezione di carico il documento può essere gestito e portato avanti nell'iter previsto.
Check-in check-out
Se un documento è aperto da un utente della scrivania chiunque tenti di accedere allo stesso ottiene una segnalazione che gli rende evidente che l'oggetto stesso non può essere modificato poiché in possesso di un altro utente.
Gli oggetti su cui è presente la gestione di checkin/checkout sono:

- Il profilo di una registrazione.
- I dati utente di una registrazione,
- Gli allegati ad una registrazione
- I partecipati di una registrazione
- L'anagrafica dei soggetti
- L'anagrafica dei fascicoli

Inoltro dei documenti
Una volta in carico il documento può essere inoltrato ad altre scrivanie. Lo smistamento può avvenire in maniera manuale, scegliendo quindi tra tutte le scrivanie presenti nella procedura, o i maniera automatica, impostando un particolare iter e prevedendo l'invio ad una determinata scrivania.
Il documento una volta inoltrato, non si troverà più sulla scrivania nella sezione Carico, ma ci sarà l'informazione dell'avvenuto spostamento nella sezione Inviati Terminati.
Tracciamento della movimentazione
In qualsiasi momento, tramite le ricerche, è possibile visualizzare tutte le informazioni relative alla movimentazione dei documenti tra le scrivanie.
Gestione dei documenti/fascicoli
Dalla scrivania è possibile gestire l'iter sia di singoli documenti che di interi fascicoli. E' possibile ad esempio smistare sia un singolo documento, che tutti i documenti contenuti in un fascicolo.
E' possibile altresì dalla sezione di carico, movimentare i documenti da una pratica ad un'altra o creare fascicoli nuovi.

Gestione Tempistica

Mediante l'utilizzo del sistema di workflow è possibile associare ad ogni singola fase dell'iter procedurale, e all'iter nel suo complesso la tempistica di riferimento. In fase di esecuzione dell'iter documentale viene visualizzato un simbolo grafico che mostra l'andamento dei tempi di esecuzione.

Per ogni pratica compaiono degli indicatori che mostrano lo stato della pratica mediante una colorazione che esprime la tempistica.

Ad esempio:

 pratica nei termini

 pratica in prossimità di scadenza termini

 pratica fuori termine

PdP gestisce anche lo scadenziario dei documenti presenti nel sistema, che consente di estrapolare dal sistema i documenti in scadenza.

Acquisizione immagini

Nel sistema **PdP** è previsto un modulo funzionale a cui viene demandato il compito di curare la fase di acquisizione dei documenti da scanner e della gestione degli stessi garantendo la completa integrazione del documento acquisito all'interno del sistema **PdP**.

Le soluzioni funzionali messe a disposizione dal modulo di acquisizione ottica dei documenti sono di due tipologie fondamentali che vengono descritte nel seguito.

Entrambe le soluzioni consentono che la funzione di scansione possa avvenire in un momento successivo a quello di registrazione e segnatura del documento con Barcode realizzando il collegamento automatico fra immagine e documento solo al momento della lettura del barcode.

Funzioni di acquisizione sincrona

La soluzione prevede che l'utilizzo di uno scanner e di stampante per la stampa di timbro di protocollo. Il flusso procedurale previsto da questa soluzione risulta essere:

- I documenti vengono protocollati in **PdP** e contestualmente viene stampato sul documento la segnatura di protocollo (segnatura), od in alternativa viene stampata un'etichetta autoadesiva riportante la segnatura di protocollo (l'operazione può essere svolta su più postazioni di lavoro, dotate di una stampante di codici a barre). La protocollazione in questa fase può consistere esclusivamente nell'acquisizione del numero di protocollo e nella stampa dell'etichetta con la segnatura e il codice a barre.
- Contestualmente può essere effettuata la scansione ed acquisizione ottica dell'immagine del documento, oppure in un momento successivo il protocollo viene completato con l'immagine attraverso il sistema **PdP**, associando automaticamente l'immagine del documento alla registrazione di protocollo.
- Contestualmente avviene la fase di controllo e validazione delle immagini scansite poiché viene visualizzata a video la scansione del documento inserito nello scanner. In caso di errata scansione è possibile effettuare nuovamente l'operazione di lettura digitale del documento.

Le apparecchiature necessarie per questa soluzione sono le seguenti:

- scanner: qualunque scanner di mercato (standard twain);
- stampante per segnatura di protocollo (a impatto o trasferimento termico per etichette);
- eventualmente lettore portatile di codici a barre, qualora si utilizzino etichette con codice a barre incluso nella segnatura di protocollo.

Funzioni di acquisizione batch

La soluzione prevede l'utilizzo di uno scanner in grado di riconoscere codici a barre e l'utilizzo di stampanti in grado di produrre etichette con codice a barre. Il flusso procedurale previsto da questa seconda soluzione risulta essere:

- I documenti vengono protocollati in PdP e contestualmente viene stampata l'etichetta autoadesiva con la segnatura e il barcode da applicare al documento cartaceo (l'operazione può essere svolta su più postazioni di lavoro, dotate di una stampante di codici a barre).
- I documenti così etichettati vengono raggruppati e posizionati sul caricatore dello scanner.
- Un apposito programma batch acquisisce le immagini riconoscendo otticamente il barcode e quindi effettuando l'associazione tra immagine e protocollo. Durante questa fase viene effettuato anche il controllo delle immagini scansionate e, nel caso non fosse andata a buon fine, è possibile ripetere l' operazione.

Le apparecchiature necessarie per questa soluzione sono le seguenti:

- scanner con ADF, che preveda la gestione con codice a barre ;
- Software di riconoscimento del codice a barre (incluso nell'offerta);
- stampante di etichette per segnatura e codice a barre (trasferimento termico per etichette).

Firma digitale

Il sistema **PdP** è interfacciabile verso i sistemi di Firma Digitale delle Certification Autority iscritte al CNIPA, per consentire di applicare la firma digitale sui documenti trattati dal sistema.

Attraverso questa integrazione, **PdP** consente di avere la stessa interfaccia utente indipendentemente dal certificato di firma utilizzato.

Firma di un documento

PdP consente di accedere alle funzionalità di firma di un documento direttamente dalla maschera di gestione del documento stesso mettendo a disposizioni funzioni di firma integrate con le funzionalità di **PdP**. Infatti per ogni documento inserito nel sistema è possibile attivare le funzioni di firma e verifica della firma digitale apposta sui documenti.

Multi-firma di un documento

PdP gestisce la possibilità di apporre le firme di più persone su un unico documento informatico presente nel sistema. In questo caso la funzionalità di firma multipla è attivabile ripetendo il processo di firma mediante il bottone corrispondente.

Firma di un lotto di documenti

PdP consente di apporre la firma digitale su un lotto di documenti selezionati. Mediante la scrivania virtuale di **PdP** viene mostrata una maschera a video che contiene una lista di documenti corrispondenti ai parametri di sistema, è possibile selezionare il set di documenti da firmare e cliccare sul bottone "Firma" per effettuare la firma del lotto selezionato.

Verifica della firma

E' possibile verificare le firme applicate sui documenti mediante un bottone in corrispondenza del documento di testo firmato. I dati di verifica di firma che vengono evidenziati sono quelli del certificato, ovvero: soggetto (cognome, nome, codice fiscale), Authority, serial number del certificato,data di validità (inizio e fine) del certificato. Se il documento è stato firmato più volte, vengono visualizzate tutte le firme applicate.

Cancellazione di una firma

È possibile cancellare la firma su un documento solo se è l'unica firma apposta sul documento stesso.

Funzioni infrastrutturali

Struttura organizzativa

Gli Enti e le AOO formano all'interno del sistema una "Anagrafica Ente" dove le AOO sono in relazione 1-n con gli Enti e dove non può esistere una AOO senza un Ente di riferimento. Particolari funzioni per l'amministratore del sistema permettono la gestione di Enti e AOO direttamente da browser.

I dati descritti possono essere modificati ad eccezione del codice AOO e codice Ente.

La cancellazione fisica di una AOO è permessa solo all'amministratore del sistema con opportuni script dedicato solo a questa attività e dopo gli opportuni controlli (non deve esistere nessun documento appartenente alla AOO sia esso inserito o meno in un registro o repertorio,non deve esistere nessun utente appartenente alla AOO).

La disattivazione di una AOO, corrisponde all'inserimento della data di fine validità e inibisce qualsiasi funzione di inserimento e aggiornamento. Rimangono invece attive tutte le altre funzionalità che non coinvolgano nuovi inserimenti o aggiornamenti di dati presenti.

L'organigramma è definito nella soluzione applicativa come "Struttura"; tale struttura è un albero a partire dalla radice "AOOx" con profondità teoricamente illimitata. In ogni ramo può essere definito un nodo con caratteristiche funzionali di "ufficio,settore,servizio etc. ". Le foglie dell'albero sono (di norma) i dipendenti della AOO. Non è posto nessun vincolo circa la collocazione dei dipendenti, unico vincolo è che non possono avere rami figli nella struttura.

La "struttura" è rappresentata graficamente all'interno delle pagine web come albero con i nodi collassabili il che ne permette una migliore navigazione e permette di (come avviene nel file system di Windows) "espandere" o "comprimere" i nodi in modo da passare agevolmente da un livello all'altro. Sono permesse sulle UO tutte le operazione descritte in questo punto ad eccezione della cancellazione che è permessa solo se non sono correlati documenti all'unità operativa che si vuole cancellare.

Tutti i campi descritti fanno parte della "struttura" definita nella soluzione applicativa . IL campo responsabile di una UO (o nodo) è a sua volta una foglia della "struttura".

Essendo l'organigramma una struttura ad albero viene impedita la cancellazione di un qualsiasi nodo che abbia figli siano questi utenti o altre UO.

Gestione ruoli/utenti

Nella soluzione applicativa proposta gli utenti sono caratterizzati da un'anagrafica (al pari di un corrispondente) e di un attributo che li identifica come "utente di login" . Un dipendente infatti può essere definito nella struttura (organigramma) ma non essere definito come utente di login, cioè come un utente che può collegarsi alla procedura applicativa attraverso una login al sistema.

Un utente di login deve avere almeno un ruolo associato. Il ruolo rappresenta la modalità operativa in termini di operazione e risorse disponibili e/o abilitabili comprese le credenziali di accesso ai documenti. Quindi tutte le abitazioni passano attraverso la definizioni di particolari per il ruolo in oggetto. Un particolare ruolo sempre presente è "Ogni Ruolo" con in significato di abilitare a tutti i ruoli e quindi a tutti gli utenti una particolare risorsa. Facendo

corrispondere ad ogni utente di login un ruolo sempre diverso si ottiene la massima granularità di abilitazione alle risorse.
Un utente è associato ad una sola UO corrispondente al punto dell'organigramma in cui è stato collocato. Dato però che un utente può assumere ruoli diversi (al limite anche tutti quelli definiti) in modo indiretto un utente è associabile a più UO. L'associazione tra gli utente e i ruoli abilitabili o abilitati viene fatta direttamente dalla struttura grafica dell'organigramma.
La modifica di un utente non coinvolge mai i dati di sua univocità.
La cancellazione di un utente non è funzionalmente possibile, la cancellazione avviene logicamente valorizzando "data di fine validità" dell'utente e mantenendo quindi la storicità dell'utente.
Nella soluzione applicativa, il ruolo ha un elemento fondamentale in quanto ad esso afferiscono gran parte delle abilitazioni e delle profilazione della procedura. Il ruolo rappresenta quindi "ciò che un utente è abilitato a fare e quali risorse è abilitato ad usare", naturalmente un utente può ricoprire più ruoli e spostarsi da un ruolo ad un altro senza effettuare un nuovo login ma semplicemente attivando la funzione "cambio ruolo". Per quanto riguarda le abilitazioni alla visualizzazione di un documento esse sono date dalla somma di tutte le abilitazioni dei ruoli che l'utente può ricoprire senza necessità quindi di modificare il ruolo attuale dell'utente.

Storicizzazione della struttura

In **PdP** è possibile effettuare la storicizzazione di un organigramma dovuto, ad esempio, al riassetto della struttura dell'Ente. A questo proposito è possibile inserire una data di fine validità ad una determinata radice ed attivarne una nuova con data di validità superiore alla vecchia.
Tutte le unità operative presenti nella vecchia struttura verranno visualizzate e quindi utilizzate solo per le ricerche, per gli inserimenti verrà invece utilizzata solo la nuova struttura con data di validità più recente.
E' possibile inoltre storicizzare solo le singole UO, inserendo nel relativo dettaglio la data di fine validità.

Abilitazioni

Nella soluzione applicativa proposta i profili funzionali coincidono con le abilitazioni funzionali assegnante ai ruoli. Le abilitazioni funzionali hanno diversa granularità ed esattamente:

- Abilitazione di menu
- Abilitazione di funzione (all'interno del menu)
- Abilitazione di folder (all'interno della funzione)
- Abilitazione di bottone (all'interno del folder)
- Abilitazione di report (all'interno della funzione)

Le funzioni di abilitazione dei profili sono a carico dell'amministratore del sistema**.**
Tramite determinate funzioni di amministrazione è possibile visualizzare, dato un determinato utente, il ruolo, il livello gerarchico, il profilo funzionale, l'elenco dei registri/repertori e delle funzioni cui l'utente è abilitato.

Soggetti

Inserimento soggetti

La procedura **PdP** memorizza le informazioni delle anagrafiche relative ai mittenti e destinatari in una tabella della banca dati a cui vengono collegati i documenti di riferimento (sia protocollati che non protocollati). La memorizzazione di un'anagrafica può essere fatta sia contestualmente all'operazione di protocollazione che in qualsiasi altro momento.
La pagina dei soggetti e' stata progettata per gestire i soggetti ed i loro indirizzi in maniera completa e dettagliata, infatti oltre ai dati identificativi di base è possibile gestire in modo dettagliato anche la residenza e i domicili.
Ad ogni soggetto e' associata una e una sola residenza valida, quando il soggetto cambia residenza, la residenza precedente viene storicizzata e ne viene inserita una nuova.
Ad un soggetto possono altresì essere associati altri indirizzi (domicili) tutti validi allo stesso tempo.
Nella maschera seguente viene mostrato un esempio di visualizzazione di un soggetto e, come si nota dall'immagine è possibile accedere a diversi folder contenenti i dati di dettaglio del soggetto prescelto:
In particolare:

Soggetto:

si possono leggere le informazioni relative al soggetto corrente. In particolare in questo folder sono presenti le informazioni relative a nome e cognome (o ragione sociale), estremi di nascita e di residenza, chiavi di identificazione.

Recapiti:

All'interno di questo folder sono disponibili i differenti tipi di recapiti associabili ad un soggetto di cui si vuole tenere traccia.

Altri Indirizzi:

Consultazione e annotazione dei nuovi indirizzi associabili ad un soggetto.

Riepilogo Indirizzi:

Compaiono distintamente le residenze cambiate dal soggetto e quella attualmente valida e gli indirizzi associati ad esso.

Ricerca e Lista:

Funzioni di ricerca mediante l'impostazione di filtri e visualizzazione dei risultati della ricerca effettuata. I meccanismi di impostazione di filtri con i relativi criteri di ricerca sono gli stessi utilizzati per tutti gli altri tipi di ricerche. Le funzioni di ricerca possono essere attivate sia dalla maschera della protocollazione sia dalla funzione specifica di gestione dei soggetti

Variazione soggetti

Una volta inserita, l'anagrafica può anche essere modificata. Vi è però la possibilità di impostare una regola per cui le modifiche sulle anagrafiche viene concessa solo all'utente di inserimento.

E' possibile impostare su ogni singola anagrafica una data di fine validità, utile nel caso di variazioni di indirizzo di cui si ritiene necessario mantenere profondità storica.

Classificazione soggetti

Il sistema **PdP** prevede la creazione di gruppi di anagrafiche ai quali collegare più soggetti mittenti/destinatari.

Occorre prima di tutto individuare i gruppi e successivamente associarvi le anagrafiche:

Tale funzionalità è molto utile nel caso nella protocollazione in partenza ci gruppi di soggetti ricorrenti; anziché inserire un'anagrafica per volta è possibile selezionarle tutte o alcune dalla maschera del raggruppamento.

Visibilità documenti/fascicoli

Gestione ACL

Il sistema gestisce i livelli di sicurezza sia sui documenti che sulle pratiche, attraverso meccanismi di ACL (Access Control List).

Un utente, attraverso il ruolo associatogli nel sistema, potrà avere visibilità totale, parziale o nessuna su di un documento o su di una pratica.

Le chiavi che consentono l'accesso/visibilità di un documento sono distinte in due categorie:

- chiavi implicite;
- chiavi esplicite.

Chiavi Implicite:

Le chiavi implicite per l'accesso/visibilità di un documento/pratica vengono associate automaticamente dal sistema nei seguenti casi:

- Utenti con lo stesso ruolo dell'utente che ha protocollato il documento;
- Utenti con ruolo di assegnazione di carico del documento;
- Utenti con ruolo di assegnazione di copia del documento;
- Utenti con ruolo di assegnazione di presa visione (uffici partecipati) del documento;
- Utenti con ruolo abilitato alla visibilità del livello di sicurezza assegnato al documento;

Chiavi Esplicite:

All'inserimento di un documento/pratica nel sistema si ha la possibilità di attivare un livello di sicurezza sul documento stesso definendo anche la lista degli utenti che saranno abilitati alla visibilità del documento stesso.

Assegnazione ACL

La gestione delle ACL in **PdP** può avvenire in 3 modi:

- Ad un ruolo (o anche a tutti i ruoli esistenti) viene associata la regola 29 che prevede che a qualsiasi documento inserito con quel ruolo venga attribuito un livello di sicurezza;
- L'utente ogni qual volta lo ritenga necessario può attribuire ad un singolo documento protocollato un livello di sicurezza a sua discrezione utilizzando un'apposita funzionalità presente nelle maschere di inserimento e gestione documentale;
- È possibile parametrizzare un iter che preveda per un particolare tipo di documento, ad esempio PRIS posta riservata,l'attribuzione di un determinato livello di sicurezza in maniera automatica.

Consultazione documenti

Un documento con livello di riservatezza è normalmente visibile solo dal ruolo che lo ha creato e dalle UO destinatarie.

E' comunque possibile individuare dei ruoli (ad esempio il direttore generale) che visualizzino sempre i documenti tramite la funzione di "Visibilità Documenti".

Funzioni di configurazione

Regole

Il sistema **PdP** è estremamente parametrizzabile, infatti è possibile applicare delle regole all'interno del sistema che modificano il comportamento dello stesso in modo da soddisfare le esigenze degli utenti. Le regole possono essere abilitate per tutti gli utenti del sistema oppure solo per alcuni, in modo da differenziare il comportamento del sistema in base anche alle necessità delle singole UO.

Vengono elencati alcuni esempi di regole applicabili:

Descrizione	VALORI AMMESSI	Esempio

Il ruolo puo' inserire solo protocolli del tipo specificato A=Arrivo P=Partenza I=Interno	P/A/I	Se impostato a P gli utenti con questo ruolo possono solo inserire documenti ti tipologia Partenza
Il ruolo non puo' modificare documenti inseriti da altri utenti (i propri per n minuti). Se la regola non è presente e si ha l'abilitazione è sempre possibile la modifica	da 0 a 999 minuti	Se impostato a 10 , posso modificare i miei documenti entro 10 minuti, quelli di altri utenti N ON posso modificarli mai.
Il ruolo è abilitato alla protocollazione per i tipi documento specificati	uno o più codici della tabella DOC_TIPDOC separati da virgole	Se impostato a LET,FAX ,posso inserire solo documenti di tipo FAX e LET
Default in inserimento nuovo protocollo: CLASSIFICA,TIPO,ORIGINE,OGGETTO,MITT.INT.,CARICO,DATA DOC(S/N)	CLASSIFICA,TIPO.,ORIGINE,OGGETTO,MITT.INT.,CARICO,DATA DOC(S/N)	Se impostata e' possibile indicare i dati che si vuole che vengano proposti in inserimento di un nuovo protocollo
Dopo la Protocollazione deve essere attivata la form/pagina.	Il numero corrispondente a una form o pagina 802 = Dati Utente	Dopo la pressione del tasto aggiorna in fase di protocollazione si puo' far si che la procedura apra automaticamente una pagina (es. quella del timbro o della stampa della ricevuta)
Controllo su numero e data di protocollo del mittente (S=regola abilitata)	S=regola abilitata, altrim. regola non abilitata	Se impostata ad S, in fase di salvataggio se sono stati compilati i dati del mittente riguardanti il suo numero e la data del protocollo , vengono controllati che tale documento non sia già stato protocollato
Il ruolo non può modificare le anagrafiche inserite da altri utenti (Le proprie per n minuti). Se la regola non è presente e si ha l'abilitazione è sempre possibile la modifica	da 0 a 999	Se impostato a 10 , posso modificare le anagrafiche inserire da me entro 10 minuti, quelle inserite da altri mai.
Il ruolo non può modificare le pratiche inserite da altri utenti (Le proprie per n minuti). Se la regola non è presente e si ha l'abilitazione è sempre possibile la modifica	da 0 a 999	Se impostato a 10 , posso modificare i fascicoli inseriti da me entro 10 minuti, quelli inseriti da altri mai.
Il ruolo inserisce protocolli con il livello di sicurezza assegnato. Se la regola non è presente non viene assegnato nessun livello di sicurezza.	un valore corrispondente a un livello di sicurezza NULL per annullarlo	Se impostato ai documenti inseriti da questo ruolo viene applicato un livello di sicurezza che agisce sulle chiave implicite.
Abilitazione del ruolo all'annullamento dei protocolli (se la regola non è presente nessuno e' abilitato)	S/N	E' possibile abilitare la funzione di annullamento dei protocolli solo a ruoli specifici.
Il ruolo inserisce pratiche con il livello di sicurezza assegnato. Se la regola non è presente non viene assegnato nessun livello di sicurezza.	un valore corrispondente a un livello di sicurezza, NULL per annullarlo	Se impostato ai documenti inseriti da questo ruolo viene applicato un livello di sicurezza che agisce sulle chiave implicite.
Abilitazione alla cancellazione della pratica con apposito bottone .	S/N	Se impostato ad S, solo tale ruolo e' abilitato alla cancellazione del fascicolo.

Configurazione scrivania

La scrivania virtuale di **PdP** è un cruscotto a disposizione degli utenti che consente di visualizzare tutti i documenti e le attività in corso di svolgimento a carico dell'utente. E' possibile, mediante funzioni di configurazione parametrizzarla in vari modi:

- È possibile parametrizzare il numero di colonne, i dati delle colonne che si vogliono rappresentare.

- È possibile visualizzare in modo differente le righe della scrivania in modo da poter distinguere visivamente e a colpo d'occhio situazioni differenti

E' possibile assegnare ad un iter di un documento una nota ed una priorità attraverso il tasto "Note" presente negli strumenti di scrivania. Le note e la priorità vengono utilizzate per comunicare ad un destinatario del documento una eventuale criticità nell'invio del documento stesso:
La presenza di note e/o priorità viene segnalata con una icona direttamente nella scrivania.
Sulla scrivania è possibile visualizzare una icona "lampadina" a fianco di un documento, posizionandosi con il mouse sulla icona della lampadina viene visualizzata una indicazione relativa alle attività da effettuare sul documento in questione. Le impostazioni delle attività su ogni documento possono essere impostate in fase di disegno dell'Iter documentale relativo alla tipologia di documento selezionato.

Gestioni dati utente

PdP mette a disposizione e gestisce una serie completa di campi nei quali l'Ente può memorizzare i dati in fase di protocollazione e gestione documentale. Tuttavia potrebbe esserci la necessità per l'Ente di inserire dati aggiuntivi non previsti .
In questo caso è possibile per l'Ente creare dei nuovi campi, ad uso specifico dell'Ente stesso scegliendo la tipologia di campo (numerico, alfanumerico, data, etc. e la label che apparirà a video.
I campi in questione vengono gestiti dinamicamente da **PdP** e compaiono sia nelle maschere di gestione documentale e di protocollo, sia nelle maschere delle ricerche.

Tipologia documenti

La Tabella della tipologia documenti contiene l'elenco dei tipi di procedimento dei documenti (ad esempio richiesta di ferie, comunicazione etc.) necessari per assegnare a ciascuno di essi l'iter prestabilito tramite il quale il documento deve muoversi all'interno dell'Ente.
Tale tabella contiene i seguenti dati:

- **Codice**: codice breve del tipo documento
- **Descrizione:** descrizione del tipo documento
- **Iter:** codice dell'iter da associare al tipo documento
- **Liv.Sic.:** Livello di sicurezza assegnato al tipo documento
- **Scarto**:Indica se la tipologia di documento può essere compresa nello scarto di archivio di un fascicolo
- **Data fine** data fine validità tipologia di documento, opzionale.

Accesso al sistema

Autenticazione utenti

PdP mette a disposizione quattro possibili soluzioni per l'autenticazione utente

1. Autenticazione standard

La prima, quella standard, utilizza esclusivamente il database di **PdP**. Gli utenti vengono definiti all'interno del DB e l'autenticazione è completamente indipendente dal sistema informatico esterno ad **PdP**

2. Autenticazione tramite Active Directory

Si prevede la possibilità di interrogare un dominio Active Directory. Vengono riconosciuti dal sistema i soli utenti in grado di effettuare con successo LOGIN sul client che interroga il sistema. Un apposito metodo di **PdP** si occupa di simulare una LOGIN utilizzando nome utente e password fornite dall'utente. In caso di esito positivo il sistema provvederà poi a validare l'utente con le informazioni presenti nel db di **PdP**, mentre in caso negativo verrebbe negato l'accesso all'applicativo.
In questo caso inoltre tutti gli utenti di rete sono potenziali utenti di **PdP**. Il sistema provvede automaticamente ad inserire l'utente nella banca dati di **PdP** al primo accesso al sistema, attribuendogli il RUOLO DEFAULT (scrivania DUMMY). Sarà poi onere dell'amministratore di **PdP** caricarlo in struttura col ruolo più corretto.

3. Autenticazione tramite LDAP (pagina ASP)

Una terza possibilità consente di interrogare un qualunque server LDAP (sia esso Active Directory oppure OpenLDAP) per verificare la presenza di un utente, le sue credenziali di accesso e la sua appartenenza o meno ad un gruppo che individua i potenziali utenti accreditati ad usare **PdP**.
In questo caso il server LDAP può non essere il domain controller del sistema su cui risiede **PdP**.
Nel caso in cui il server LDAP non permetta l'anonymous binding, per la ricerca/validazione degli utenti, vengono utilizzate le credenziali dell'utente dell'applicativo **PdP**.

4. Autenticazione tramite LDAP (script PHP)

Così come la precedente, anche l'ultima possibile configurazione permette la facoltà di interrogare un qualunque server LDAP tramite cui validare i dati forniti durante l'accesso all'applicativo.
Questa modalità necessità dell'installazione dell'interprete PHP (versione 4.x oppure 5.x), e quindi di un apposito script per l'autenticazione utente.

Assieme allo script per l'autenticazione e' presente anche un file di configurazione, in cui specificare i dati per la connessione al server LDAP.

Integrazione LDAP
Si veda quanto descritto nel paragrafo precedente
Documenti informatici
La Gestione Documentale (identificata nel sistema dalla sigla D.M.: Document Management) consente di associare a ciascun documento, già memorizzato nel database attraverso dati strutturati (come il tipo, l'oggetto, la data, ecc.), uno o più allegati, quali testi, immagini, note o qualsiasi tipo di documento in formato elettronico, attraverso l'uso di applicativi di utilizzo comune (Word, Excel, Notepad, ...) oppure già presenti sul computer locale o in rete.
Per ogni allegato, oltre all'oggetto stesso, vengono memorizzate alcune informazioni che consentono di individuare la tipologia dell'allegato, la presenza della firma digitale e dell'impronta, le modalità di archiviazione.
Inoltre, per ogni allegato sono gestiti data e autore di inserimento e dell'ultimo aggiornamento e può essere mantenuta traccia di versioni successive.
La Gestione Documentale consente di gestire diverse modalità di archiviazione:
- RDBMS prescelto per l'attivazione dell'applicazione;
- file system;
- Integrazione con una piattaforma di EDMS (es.: Hummingbird, Documentum, ecc.).

Il repository corrente è impostato al momento dell'installazione (insieme agli altri parametri definibili dall'utente) e può essere modificato dall'amministratore del sistema in base alle necessità dell'utente.
I dati gestiti da DM sono:
- Id. Documento: Contiene l'identificativo del documento a cui è associato l'allegato
- Id: Il progressivo viene assegnato automaticamente dal sistema e rappresenta l'identificativo dell'allegato
- Estensione: consiste nella parte finale del nome del file preceduta dal punto che consente di associare il tipo di programma in base alle impostazioni del computer (es.: doc per i file Word, xls per i file Excel, ecc.)
- Sottoestensione: è un dato opzionale usato per trattamenti particolari in PdP (es.: file generati da merge oppure estensione originaria di documenti con firma digitale)
- Versione: il sistema consente di gestire più versioni dello stesso allegato, per mantenere la profondità storica di successive revisioni. Al momento dell'inserimento la versione è assegnata uguale a zero
- Id.Base: contiene l'identificativo dell'allegato originario: per l'utente finale, l'allegato è sempre individuabile da Identificativo originario/versione (esempio: 123/0, 456/3, ecc.). Nel caso della versione zero, Id e Id.Base coincidono
- Repository: contiene l'indicatore della modalità di archiviazione dell'allegato
- Ruolo di inserimento: contiene il ruolo assunto dall'utente al momento dell'inserimento. Questo dato viene utilizzato per controllare le abilitazioni alla modifica dell'allegato
- Percorso: viene valorizzato solo per allegati su file system (Repository = F) e indica il percorso della cartella di memorizzazione su disco composta dalla cartella di riferimento più la sottocartella delle migliaia
- Nome file: viene valorizzato solo per allegati su file system (Repository = F) e indica il nome del file composto dal progressivo di sistema e dall'estensione
- Principale: indicatore di allegato principale: consente di distinguere tra più allegati quello principale dagli allegati veri e propri. Il sistema imposta automaticamente il primo allegato di un documento come principale, ma l'utente può modificarne il valore.
- Commento: contiene eventuali informazioni aggiuntive sull'allegato; a volte viene impostato automaticamente dal sistema
- Impronta: contiene il valore dell'impronta dell'allegato per controllarne l'integrità e la non modificabilità
- Firma: contiene l'indicatore di firma digitale (S/vuoto) e viene impostato dal sistema nel caso di un documento a cui è stata applicata la firma digitale
- Check-Out: contiene l'indicatore di "check-out"; consente di segnalare che l'allegato è stato riservato da un utente in modifica
- Id.Parere: contiene l'identificativo dell'allegato di cui l'allegato stesso rappresenta un parere
- Archiviazione: contiene i dati di archiviazione: in caso di archiviazione dell'allegato su supporti esterni, sono riportato i dati necessari all'individuazione del supporto di archiviazione
- Inserimento: Contiene la data e l'utente del primo inserimento
- Ultimo aggiornamento: contiene la data e l'utente dell'ultimo aggiornamento

Formati documenti informatici
Con la gestione Dm per gli allegati inseriti vengono classificati nelle seguenti classi:
"MERGE", "PARERE", "GRAFFETTA", "SEGNATURA", "CONFERMA", "ECCEZIONE", "SCAN" e sono attribuite automaticamente dal sistema rispettivamente: in fase di composizione atto, in fase di generazione di un parere,

in fase di acquisizione da file system, in fase di acquisizione da interoperabilità, acquisizione da scanner (singola o massiva).
I formati di files supportati da **PdP** sono tutti quelli compatibili con windows. E' comunque necessario, per visualizzare e gestire i files, avere installato sui singoli client le applicazioni che li gestiscono.
Nel caso in cui un file venga firmato la sua estensione diventa "p7m" mentre l'estensione originale del documento non firmato viene concatenata nella sottoestensione.
Esempi

1) Nell'ipotesi in cui ad esempio si firmasse un merge la coppia estensione-sottoestensione sarebbe "p7m-merge.doc"
2) Nell'ipotesi in cui un documento word venga acquisito da file system la coppia estensione-sottoestensione sarebbe "doc-graffetta" dove "doc" è il valore del campo estensione e "graffetta" quello del campo sottoestensione. Se poi questo venisse firmato si otterrebbe "p7m-graffetta.doc"
3) Nell'ipotesi di generazione di pdf di un documento word la coppia estensione-sottoestensione sarebbe "pdf-doc" dove "pdf" è il valore del campo estensione e "doc" quello del campo sottoestensione
4) Se il word fosse acquisito dal file system e poi trasformato in pdf si avrebbe "pdf-graffetta.doc"

Immodificabilità dei documenti
Gli allegati ai documenti sono modificabili solo dagli utenti che lo hanno inserito, e un'icona sulla finestra indica questo stato.
I documenti firmati digitalmente non sono più modificabili, a meno che non si tolga la firma.
I documenti improntati non sono più modificabili.
Integrazione con le altre funzioni
E' anche possibile eseguire la conversione in formato PDF dell'allegato al documento selezionato come nuova versione (solo per i testi con estensione DOC,TXT e RTF).
Visualizzazione e stampa dei documenti
In **PdP** è possibile visualizzare gli allegati dei documenti tramite i software che ne gestiscono la tipologia. Ad esempio un allegato pdf è visualizzabile e stampabile sono se sul client e' installato Acrobat Reader.
È inoltre possibile effettuare la stampa degli allegati sia sottoforma di copia conforme, se gli allegati risultano firmati digitalmente, o come copia semplice.
Funzioni di integrazione con altri sistemi

Integrazione con firma digitale
PdP integra i dispositivi di Firma Digitale di tutte le Certification Authority nel pieno rispetto dei principi di autenticazione, integrità, riservatezza e non ripudiabilità.
Integrazione con Office Automation
PdP supporta i sistemi di produttività individuale quali Microsoft Office e Open Office.
Integrazione con acquisizione immagini
PdP e' integrato con software che consentono di effettuare la scansione massiva tramite il riconoscimento dei codici a barre contenuti nella segnatura di protocollo. L'integrazione consente l'abbinamento automatico del documento informatico con la registrazione di protocollo presente nel sistema **PdP**.
Integrazione con posta elettronica
PdP mette a disposizione la possibilità di integrare nella procedura caselle di posta elettronica sia certificata che tradizionale. Tale integrazione permette di ricevere e inviare mail direttamente da interfaccia senza dover utilizzare altre procedure.
L'account in **PdP** viene associato all'utente della procedura. Più possono avere la medesima casella di posta associata.

Allegato 14 - Abilitazioni all'utilizzo delle funzionalità del prodotto di protocollo (PdP) e dei documenti

In questo allegato, per ciascuna unità di personale assegnata ad un Ufficio utente dell'Area Organizzativa Omogenea, si devono specificare le abilitazioni all'utilizzo delle funzionalità del sistema. La tabella seguente definisce per ciascun utente dei servizi le abilitazioni alle funzioni della gestione del protocollo e documentale.
Le colonne hanno il seguente significato.

a) registrazione di protocollo dei documenti in arrivo (A);
b) registrazione di protocollo dei documenti in partenza (P);
c) classificazione dei documenti (C);
d) presa in carico e assegnazione interna dei documenti ricevuti (PC);
e) fascicolazione dei documenti (F);
f) protocollazione dei documenti nel registro di emergenza (PE);
g) versamento dei fascicoli chiusi nell'archivio di deposito (VAD);
h) consultazione della banca dati documentale (CBD).

UO	Servizio	Descrizione	A	P	C	PC	F	PE	VAD	CBD
c_769-01	**SETTORE AFFARI ED ORGANI ISTITUZIONALI**					S				
	c_769-01-01	*Servizio Segreteria Generale, Contratti e Società partecipate*		S	S		S		S	S
	c_769-01-02	*Servizio Provveditorato ed Economato Comunale*		S	S		S		S	S
	c_769-01-03	*Servizio Mercato Ittico*		S	S		S		S	S
c_769-02	**SETTORE INNOVAZIONE E SERVIZI AI CITTADINI**									
	c_769-02-01	*Servizio Sportello Unico del Cittadino, Anagrafe, Stato Civile, Elettorale*		S	S		S		S	S
	c_769-02-02	*Servizio Sviluppo Organizzativo e Sistemi Informativi*		S	S		S		S	S
	c_769-02-03	*Servizio Rapporti con i cittadini, gestione documentale, comunicazione pubblica*	S	S	S		S	S	S	S
c_769-03	**SETTORE GESTIONE RISORSE**					S				
	c_769-03-01	*Servizio Gestione Risorse Umane, Pianificazione strategica, Controllo di gestione*		S	S		S		S	S
	c_769-03-02	*Servizio Bilancio, Contabilità e Riscossioni*		S	S		S		S	S
	c_769-03-03	*Servizio Sportello equità e Catasto*		S	S		S		S	S
	c_769-03-04	*Servizio Segreteria particolare del Sindaco*		S	S		S		S	S
c_769-04	**SETTORE SVILUPPO E QUALITA' DEL TERRITORIO E DELL'ECONOMIA LOCALE**					S				
	c_769-04-01	*Servizio Sportello Unico delle Imprese*	S	S	S		S		S	S
	c_769-04-02	*Servizio Amministrativo e del Demanio Marittimo*		S	S		S		S	S
	c_769-04-03	*Servizio Sportello dell'Edilizia*	S	S	S		S		S	S
	c_769-04-04	*Servizio Pianificazione, Programmazione urbanistica, Sviluppo Sostenibile e Sistema Informativo Territoriale*		S	S		S		S	S
	c_769-04-05	*Servizio Qualità Urbana*								
c_769-05	**SETTORE SERVIZI ALLA PERSONA**					S				
	c_769-05-01	*Servizio Disabilità e Disagio Mentale*		S	S		S		S	S
	c_769-05-02	*Servizi Minori e Terza Età, Inclusione Sociale e Politiche per la Casa*		S	S		S		S	S
c_769-06	**SETTORE PROGETTAZIONE E MANUTENZIONE OPERE PUBBLICHE**					S				
	c_769-06-01	*Servizio manutenzione del patrimonio, viabilità e immobili*		S	S		S		S	S
	c_769-06-02	*Servizio progettazione e realizzazione opere pubbliche*		S	S		S		S	S
	c_769-06-03	*Servizio Coordinamento Sicurezza* e Infrastrutture		S	S		S		S	S
	c_769-06-04	*Servizi Amministrativi e Programmazione OO.PP.*		S	S		S		S	S

	c_769-06-05	*Servizio Aree Verdi, Cimitero e Parchi Urbani*	S	S	S		S		S	S
	c_769-06-06	*Servizio Sostenibilità, accessibilità, aree protette e controllo opere pubbliche*		S	S		S		S	S
	c_769-06-07	*Servizio Sviluppo Europa, Sviluppo del Porto e Città del Territorio*		S	S		S		S	S
c_769-07	**SETTORE POLIZIA MUNICIPALE**					S				
	c_769-07-01	*Comando Polizia Municipale e Protezione Civile*	S	S	S		S		S	S
	c_769-07-02	*Servizio Segreteria, Viabilità e Infortunistica stradale*		S	S		S		S	S
	c_769-07-03	*Servizio Tutela urbanistica, ambientale e gestione del territorio*		S	S		S		S	S
	c_769-07-04	*Servizio Amministrativo, Trasporto Pubblico Locale e Traffico*		S	S		S		S	S
c_769-08	**SETTORE CULTURA, SPORT, TURISMO, SCUOLA, GIOVANI**					S				
	c_769-08-01	*Servizi per la cultura e il turismo, progetti e rapporti con le Università, Biblioteche e Musei*		S	S		S		S	S
	c_769-08-02	*Servizi per lo Sport e Politiche per i Giovani*		S	S		S		S	S
	c_769-08-03	*Servizio Diritto allo Studio, Trasporti scolastici e mense*		S	S		S		S	S
c_769-09	**SEGRETERIA GENERALE**					S				
c_769-10	**U.O.A. AFFARI LEGALI**					S				