CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione
via Isonzo, 21/b - 00198 Roma
tel. 06 85264.1
www.cnipa.gov.it

21 i Quaderni Manuale di gestione del protocollo informatico, dei documenti e dell'archivio delle pubbliche amministrazioni – *Modello di riferimento* numero 21 - febbraio 2006

CNIPA
Centro Nazionale per l'Informatica
nella Pubblica Amministrazione

21
febbraio 2006

i Quaderni

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

Modello di riferimento

21

febbraio 2006

i Quaderni

i Quaderni n. 21 febbraio 2006
Supplemento al n. 9/2006
del periodico "InnovAzione"

Registrato al Tribunale di Roma
n. 523/2003
del 15 dicembre 2003

Direttore responsabile
Franco Tallarita
(tallarita@cnipa.it)

Responsabile redazionale
Gabriele Bocchetta
(bocchetta@cnipa.it)

Quaderno a cura
di Guglielmo Longobardi
(longobardi@cnipa.it)

Redazione
Centro Nazionale
per l'Informatica nella
Pubblica Amministrazione
Via Isonzo, 21b
00198 Roma
Tel. 06 85264.1

I Quaderni
del Cnipa sono pubblicati
all'indirizzo:
www.cnipa.gov.it

Stampa
Stabilimenti Tipografici
Carlo Colombo S.p.A. - Roma

i Quaderni

sommario

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DELLE PUBBLICHE AMMINISTRAZIONI

MODELLO DI RIFERIMENTO

Presentazione

Il Modello di riferimento del manuale di gestione è stato redatto su iniziativa del Centro di competenza sul protocollo informatico e la trasparenza amministrativa[1] e ha lo scopo di fornire indicazioni per la stesura del manuale di gestione del protocollo informatico, dei documenti e dell'archivio che le pubbliche amministrazioni sono chiamate a predisporre ai sensi dell'art. 3, comma c) del decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2000 concernente le "Regole tecniche" per il protocollo informatico con le modalità riportate nel successivo art. 5.

La documentazione si compone di tre parti:

- il "Modello di riferimento di Manuale di gestione", che ogni singola amministrazione "personalizza" in base alle proprie caratteristiche, alla tipologia e alle specifiche esigenze;
- alcuni "Allegati" in cui inserire aspetti di dettaglio e variabili nel tempo, che rendono il Manuale di gestione flessibile in quanto permettono di effettuare modifiche e aggiornamenti non strutturali senza dover ripetere l'iter di approvazione formale dell'intero documento;
- una "Guida", che riporta regole e suggerimenti per la stesura del manuale.

Si ringrazia la Direzione generale degli archivi di Stato del Ministero per i beni e le attività culturali, e in particolare Maria Grazia Pastura, per la collaborazione fornita relativamente alla stesura del capitolo relativo al sistema di classificazione, fascicolazione e piano di conservazione e per aver messo a disposizione, attraverso il collegamento al proprio sito web, i modelli di titolari di classificazioni definiti per alcune tipologie di amministrazioni (Regioni, Comuni, Aziende sanitarie locali, ecc).

[1] Il Centro di competenza sul protocollo informatico e la trasparenza amministrativa è composto da Maria Pia Giovannini (Responsabile), Stefano Ercoli, Patrizia Gentili, Guglielmo Longobardi ed Emanuela Mariotti.

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.
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 DsPR 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;

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

- 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 *< inserire il nome dell'amministrazione per esteso >* a partire dal *< inserire data >*.
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, dell'effettivo ricevimento e spedizione di un documento.

1.3 DEFINIZIONI E NORME DI RIFERIMENTO

Ai fini del presente Manuale si intende:

- per "amministrazione", *< inserire il nome dell'amministrazione per esteso >*;
- 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.

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 16.2.

1.4 AREE ORGANIZZATIVE OMOGENEE E MODELLI ORGANIZZATIVI

o ***alternativa 1***

Per la gestione dei documenti, l'amministrazione ha adottato un modello organizzativo di tipo distribuito istituendo al suo interno le Aree Organizzative Omogenee (AOO) elencate nell'allegato 16.3.
All'interno di ciascuna AOO il sistema di protocollazione è unico.
In ogni AOO è istituito un servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi.
Nel medesimo allegato, per ogni AOO sono riportati: la denominazione, il codice identificativo della AOO, l'insieme degli UOR che la compongono con la loro articolazione in UU (***opzionale:*** e l'insieme delle Unità Organizzative di registrazione di Protocollo (UOP)).

- ***caso a***
  All'interno di ciascuna AOO il sistema di protocollazione è totalmente centralizzato, nel senso che tutta la corrispondenza in ingresso e in uscita è gestita da una sola UOP.
- ***caso b***
  All'interno di ciascuna AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, mentre è decentralizzato per la corrispondenza in uscita attraverso alcuni (o tutte le) UOR che svolgono anche i compiti di UOP.
- ***caso c***
  All'interno di ciascuna AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in ingresso e in uscita; in questo caso ogni UOR svolge anche i compiti di UOP.

o ***alternativa 2***

Per la gestione dei documenti, l'amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata < *inserire nome* > che è composta dall'insieme di tutti gli UOP/UOR/UU articolati come riportato nell'allegato 16.3.
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.

- ***caso a***
  All'interno della AOO il sistema di protocollazione è totalmente centralizzato nel senso che tutta la corrispondenza in ingresso e in uscita è gestita da una sola UOP.
- ***caso b***
  All'interno della AOO il sistema di protocollazione è centralizzato per la corrispondenza in entrata, mentre è decentralizzato, per la corrispondenza in uscita, attraverso alcune (o tutte le) UOR che svolgono anche i compiti di UOP.
- ***caso c***
  All'interno della AOO il sistema di protocollazione è totalmente distribuito per la corrispondenza in entrata e in uscita; pertanto ogni UOR svolge anche i compiti di UOP.

o ***(da inserire comunque…)***

L'allegato 16.3 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

In ogni 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).
Egli è funzionalmente individuato nel < *inserire nome del servizio* > alle dirette dipendenze della < *direzione, settore, area……. della AOO* > nominato con atto < *tipo… numero…. del … .*>.

Al servizio è preposto un dirigente ovvero 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.
L'atto che istituisce il servizio e individua il responsabile per ciascuna AOO è riportato nell'allegato 16.4, unitamente:

- alla denominazione del servizio;
- al nominativo del RSP;
- alla descrizione dei compiti assegnati al RSP;
- al nominativo del vicario del RSP nei casi di vacanza, assenza o impedimento di questi.

È compito del servizio:

- predisporre lo schema del Manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del Manuale (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 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 giornata lavorativa, va riversato, nel rispetto della normativa vigente, su supporti informatici non riscrivibili.

- ***caso a***
  Tali supporti rimovibili sono conservati da persona diversa da colui che ha realizzato il riversamento e dal RSP.
- ***caso b***
  Tali supporti rimovibili sono conservati dalla stessa persona che ha realizzato il riversamento, diversa dal RSP.

o ***(da inserire comunque ...)***
Per questo motivo l'amministrazione ha nominato un responsabile della conservazione delle copie di riserva. L'atto formale di nomina viene riportato nell'allegato 16.5.
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.
Nell'allegato 16.6 viene riportato l'elenco delle persone titolari di firma digitale e delle deleghe ricevute per la sottoscrizione di documenti digitali dell'amministrazione.

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 3.
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). 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

o ***alternativa 1***
Con l'inizio della attività operativa del protocollo unico viene adottato un unico titolario di classificazione per l'archivio centrale unico (logico) dell'amministrazione valido per tutte le AOO in cui è articolata l'amministrazione.

o ***alternativa 2***
Con l'inizio della attività operativa del protocollo unico viene adottato anche un unico titolario di classificazione all'interno di ciascuna AOO dell'amministrazione.

o ***alternativa 3***
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.

o ***(da inserire comunque ….)***
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 orga-

nizzare 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 capitolo 9.

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.

Tali iniziative formative, destinate a specialisti, funzionari e dirigenti sono riportate nell'allegato 16.7.

1.12 ACCREDITAMENTO DELL'AMMINISTRAZIONE/AOO ALL'IPA

L'amministrazione/AOO si dota 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 dal CNIPA 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 16.3.
Il codice identificativo della amministrazione associato a ciascuna delle proprie 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 comunica al CNIPA le procedure integrative che intende adottare ai sensi dell'art. 7 della citata deliberazione.

2. Eliminazione dei protocolli diversi dal protocollo informatico

Il presente capitolo riporta la pianificazione, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione dei protocolli diversi dal protocollo informatico.

2.1 Piano di attuazione

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 piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di settore, di reparto e multipli. A tal fine sono state svolte le seguenti attività:

- censimento preliminare dei diversi protocolli esistenti;
- analisi dei livelli di automazione;
- definizione degli interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico;
- valutazione dei tempi di sostituzione;
- stima dei costi derivanti.

Le informazioni raccolte ed il piano di azione che ne è derivato, riportato nell'allegato 16.8, tengono conto della realtà organizzativa dell'AOO e della necessità di gestire la fase transitoria connessa con l'esaurimento delle pratiche in essere, protocollate e gestite anteriormente all'avvio del sistema di protocollo informatico e gestione documentale di cui al presente Manuale.
Il RSP esegue comunque, periodicamente, dei controlli a campione sulla corretta esecuzione del piano e sull'utilizzo regolare di un unico registro di protocollo, verificando, attraverso controlli ed ispezioni mirate nelle varie UOP/UOR/UU, la validità dei criteri di classificazione utilizzati.

o ***opzione in caso di carenze infrastrutturali***
In via temporanea e transitoria, nelle more del completamento della informatizzazione del servizio per la tenuta del protocollo informatico e dell'archivio, ed in particolare finché non sarà allestita e resa operativa la rete informatica interna dell'amministrazione, possono essere mantenuti in esercizio registri particolari di protocollo per l'acquisizione e la spedizione di documenti aventi carattere di eccezionalità e di estrema urgenza.

3. 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.

3.1 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.

3.2 Generalità

Il RSP ha predisposto il piano di sicurezza (o lo ha fatto predisporre sotto la sua guida e responsabilità) 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 RSP ha 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) e di un profilo di autorizzazione;
- cambio delle password con frequenza almeno < ……*mestrale* > 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 < *riportare il servizio* > 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;
- gestione delle situazioni di emergenza informatica attraverso la costituzione di un gruppo di risorse interne qualificate (o ricorrendo a strutture esterne qualificate);
- 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 giornaliera, in modo non modificabile, delle copie del registro di protocollo, dei file di log di sistema, di rete e applicativo contenenti le informazioni sulle operazioni effettuate da ciascun utente durante l'arco della giornata, comprese le operazioni di backup e manutenzione del sistema.

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.

3.3 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, 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, 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.
Per 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.

3.4 GESTIONE DEI DOCUMENTI INFORMATICI

Il 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.

3.4.1 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…… < *riportare l'organizzazione del sistema informativo per la componente sicurezza* >.
Nella conduzione del sistema di sicurezza, dal punto di vista organizzativo, sono state individuate le seguenti funzioni specifiche:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>.

In relazione alla componente fisica della sicurezza sono stati definiti i seguenti ruoli:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>.

3.4.2 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:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>.

Le misure di sicurezza fisica hanno un'architettura multi livello:

- a livello di *sede dell'amministrazione/AOO* che ospita il sistema informatico: < *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>;

- a livello di *locale/i* che ospita/no le risorse elaborative e di trasmissione del sistema informatico: < *illustrare la realtà dell'amministrazione/AOO su questo aspetto* >.

3.4.3 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:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto* >.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura….

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto* >.

3.4.4 COMPONENTE INFRASTRUTTURALE DELLA SICUREZZA

Il sistema informatico utilizza i seguenti impianti:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto* >.

3.4.5 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 generati dal sistema operativo;
- dai log dei dispositivi di protezione periferica del sistema informatico (Intrusion Detection System (IDS), sensori di rete e firewall);
- dalle registrazioni del PdP.

Le registrazioni di sicurezza sono soggette alle seguenti misure:

- < *illustrare la realtà dell'amministrazione/AOO su questo aspetto* >.

In questa sede viene espressamente richiamato quanto indicato nell'ultimo capoverso del paragrafo 3.2 del presente Manuale.

3.5 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, informazio-

ni 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, (o, in alternativa, del servizio disponibile all'interno dell'amministrazione/AOO) oltre alle funzioni di un server SMTP tradizionale, svolge anche le seguenti operazioni:

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

Lo scambio per via telematica di messaggi protocollati tra AOO 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.

- ***opzione***

Per garantire alla AOO ricevente la possibilità di verificare l'autenticità della provenienza, l'integrità del messaggio e la riservatezza del medesimo, viene utilizzata la tecnologia di firma digitale a disposizione delle amministrazioni coinvolte nello scambio dei messaggi.

3.5.1 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.

3.5.2 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.

- ***opzione per comunicazioni interne***

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".

3.6 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:
< …. almeno la consultazione, l'inserimento, la modifica, l'annullamento; illustrare comunque la realtà dell'amministrazione/AOO su questo aspetto>.
Le regole per la composizione delle password e per il blocco delle utenze … *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.
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.

< illustrare le modalità con cui il PdP dell'amministrazione/AOO realizza il controllo delle autorizzazioni all'acceso ai documenti da parte degli utenti (es. ACL) >.
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.

3.6.1 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 distinguo-

no in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i seguenti criteri operativi:

- *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.

3.6.2 Accesso al registro di protocollo per utenti interni alla AOO

L'autorizzazione all'accesso ai registri di protocollo è regolata tramite i seguenti strumenti:

- *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.

La visibilità completa sul registro di protocollo è consentita solo….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.
L'utente assegnatario dei documenti protocollati è invece abilitato ….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.
L'operatore che gestisce lo smistamento dei documenti può ….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.
Nel caso in cui sia effettuata la registrazione di un documento sul protocollo particolare, la visibilità completa sul documento stesso è possibile solo….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*.
Tutti gli altri utenti possono accedere solo ai dati di registrazione e ….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto>*).

3.6.3 Utenti esterni alla AOO - Altre AOO/Amministrazioni

L'accesso al sistema di gestione informatica dei documenti dell'amministrazione da parte di altre AOO avviene 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 accedono ai sistemi di gestione informatica dei documenti attraverso il SPC utilizzano 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.

3.6.4 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.

3.7 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

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

3.7.1 SERVIZIO ARCHIVISTICO

Il responsabile del sistema archivistico dell'AOO ha individuato nella *< sede o locali >* la sede dell'archivio dell'amministrazione *(Opzionale…già attiva per questa funzione)*
Il responsabile del servizio in argomento ha effettuato la scelta 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).
Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha predisposto e reso noto, un piano individuando i soggetti incaricati di ciascuna fase.
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).

3.7.2 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 *< descrivere quelli utilizzati dalla AOO >* 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.

3.7.3 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 sono differenziati in base al livello di sicurezza loro attribuito:
< *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>.
È compito dell'ufficio che si occupa del servizio di sicurezza del sistema informativo *(o altra struttura/persona capace di svolgere lo stesso compito)* 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.
Il 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.

3.7.4 CONSERVAZIONE DELLE REGISTRAZIONI DI SICUREZZA

Un operatore addetto alla sicurezza dell'amministrazione/AOO, con periodicità < —— *?* —— >, provvede alla memorizzazione su supporto non riscrivibile dei seguenti file di sicurezza:
< *illustrare la realtà dell'amministrazione/AOO su questo aspetto*>.

I supporti così realizzati sono conservati in < *illustrare la realtà dell'amministrazione/AOO su questo aspetto*> per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.

3.7.5 RIUTILIZZO E DISMISSIONE DEI SUPPORTI RIMOVIBILI

Non è previsto il riutilizzo dei supporti rimovibili. Al termine del previsto periodo di conservazione i supporti sono distrutti secondo una specifica procedura operativa.

o ***(alternativa)***
È previsto il riutilizzo dei supporti rimovibili. 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.

3.8 POLITICHE DI SICUREZZA ADOTTATE DALLA AOO

Le politiche di sicurezza, riportate nell'allegato 16.9 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/o del responsabile del sistema informativo e/o del responsabile della tutela dei dati personali* > procedere al perfezionamento, alla divulgazione e al riesame e alla verifica delle politiche di sicurezza.
Il 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.

4. 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.

4.1 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.

4.2 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.

4.3 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.
Il 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.

4.4 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.

4.5 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".

4.6 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.

4.7 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 firme *(e le sigle se si tratta di documento analogico)* necessarie alla redazione e perfezione giuridica del documento in partenza devono essere apposte prima della sua protocollazione.
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.

4.8 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 dal CNIPA.
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 archivia-

zione al fine di garantirne l'immodificabilità (vedi art. 3 comma 3 del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).
Nell'allegato 16.10 viene riportato l'elenco del documenti prodotti dalla AOO soggetti, o meno, alla sottoscrizione digitale, distinti anche per tipologia di sottoscrizione.

4.9 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.

4.10 FIRMA DIGITALE

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.9 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).

4.11 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[2];
- verifica della validità del certificato. Questa attività è realizzata ….. *< illustrare la realtà dell'amministrazione/AOO su questo aspetto >;*
- verifica della firma (o delle firme multiple) con *< illustrare la realtà dell'amministrazione/AOO su questo aspetto;*

[2] 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 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 CNIPA con periodicità < — ? — >;
- trasformazione del documento in uno dei formati standard previsto dalla normativa vigente in materia (PDF 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; *(… opzionale)*
- 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.

4.12 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 (cfr. par. 3.5 Trasmissione e interscambio dei documenti informatici).
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.
Il 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.

5. 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.

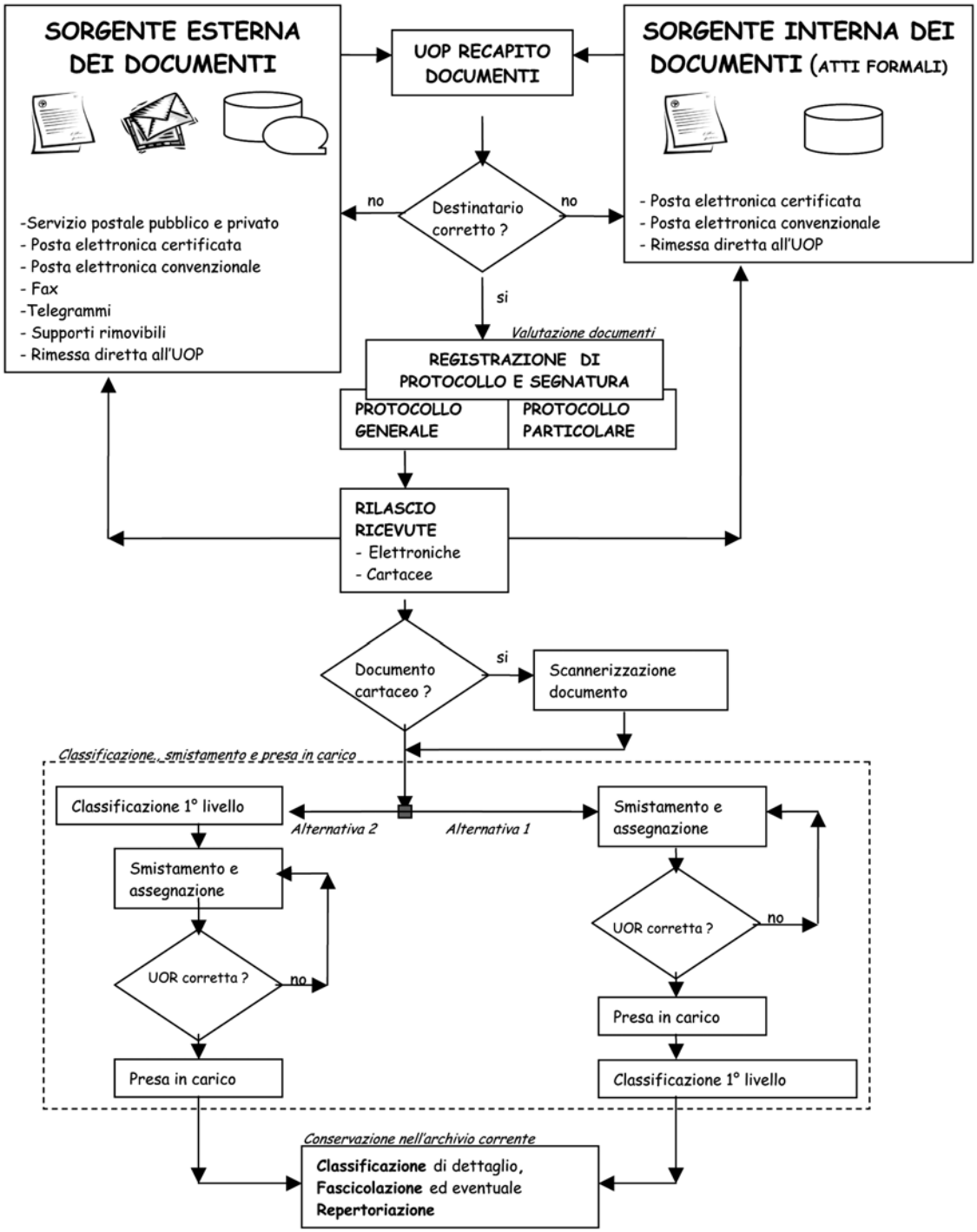
5.1 Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flussi 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*.

I flussi gestiti all'interno del sistema archivistico dell'amministrazione/AOO dalla sezione di deposito e storica dell'archivio sono sviluppati, per omogeneità e completezza di trattazione, nel successivo capitolo 9.
Come previsto dalla normativa vigente i flussi di seguito descritti sono il risultato del processo di censimento, di descrizione e di reingegnerizzazione dei processi dell'AOO, quale fase propedeutica ad un efficace ed efficiente impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO medesima.
I flussi relativi alla gestione dei documenti all'interno dell'AOO sono descritti graficamente nel paragrafo seguente prendendo in esame quelli che possono avere rilevanza giuridico-probatoria.
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 16.11.
I flussi documentali riportati nelle pagine seguenti hanno carattere puramente esemplificativo. Questi devono essere sostituiti da quelli reali dell'AOO. I flussi possono essere descritti anche senza l'ausilio degli schemi.

5.2 FLUSSO DEI DOCUMENTI RICEVUTI DALLA AOO



5.2.1 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.

I documenti che transitano attraverso il servizio postale sono ritirati quotidianamente secondo le regole stabilite dal RSP riportate nell'allegato 16.12.

5.2.2 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.
Il documento è di tipo informatico secondo i formati standard illustrati nel precedente capitolo.
I mezzi di recapito della corrispondenza considerati sono la posta elettronica convenzionale o certificata.
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.
In questo caso il mezzo di recapito del documento può essere il servizio di posta interna o il telefax.

5.2.3 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 solo alla/e 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.

5.2.4 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 alla casella di posta istituzionale e inviando un messaggio, per conoscenza, al mittente con l'indicazione della casella di posta corretta. I controlli effettuati sul messaggio sono quelli sopra richiamati.

5.2.5 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.

5.2.6 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 con le modalità descritte nel successivo capitolo 10.
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.

5.2.7 DOCUMENTI CARTACEI RICEVUTI A MEZZO POSTA CONVENZIONALE E TUTELA DEI DATI PERSONALI

Qualora una AOO sia organizzata per ricevere documenti su carta attraverso qualsiasi UOR aperta al pubblico, oltre, ovviamente alle UOP istituzionali, 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 xxxxxxx 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.

5.2.8 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".

5.2.9 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:

- busta indirizzata ad altra AOO della stessa amministrazione:
  a) si invia alla AOO corretta;
  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 alla AOO destinataria apponendo sulla busta la dicitura "Pervenuta ed aperta per errore";

- busta indirizzata ad altra amministrazione:
  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".

5.2.10 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 10.

5.2.11 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.

5.2.12 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.

o ***alternativa 1***

- apporre sulla copia così realizzata il timbro dell'amministrazione con la data e l'ora d'arrivo e la sigla dell'operatore.

o ***alternativa 2***

- apporre sulla copia così realizzata, con una procedura informatica, il timbro dell'AOO con la data e l'ora d'arrivo e la sigla dell'operatore.

o ***alternativa 3***

- apporre su un modulo specifico, con una procedura informatica, la data e l'ora d'arrivo e la sigla dell'operatore.

5.2.13 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.

5.2.14 CONSERVAZIONE DELLE RAPPRESENTAZIONI DIGITALI DI DOCUMENTI CARTACEI

I documenti ricevuti su supporto cartaceo, dopo le operazioni di registrazione e segnatura, sono acquisiti in formato immagine attraverso un processo di scansione.
Il processo di scansione avviene in diverse fasi:

- acquisizione delle immagini in modo tale che ad ogni documento, anche se composto da più pagine, corrisponda un unico file;
- verifica della leggibilità e della qualità delle immagini acquisite;
- collegamento 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.
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:

o ***alternativa 1 –*** distrutti (si ricorda che la distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche).

o ***alternativa 2*** – 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. (*opzionale* - Il documento cartaceo originale viene inviato al primo destinatario).
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 xx 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,
  - < *integrare l'elenco* >.

Le UOP/UU abilitate all'operazione di scansione dei documenti sono riportate nell'allegato 16.3.

5.2.15 CLASSIFICAZIONE, ASSEGNAZIONE E PRESA IN CARICO DEI DOCUMENTI

o ***alternativa 1***

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.

o ***alternativa 2***

Gli addetti alla UOP provvedono ad inviare il documento all'ufficio smistamento che identifica l'UOR di destinazione. Quest'ultimo:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore rinvia il documento all'ufficio smistamento di origine;
- in caso di verifica positiva, esegue l'operazione di presa in carico smistandola al proprio interno ad UU o direttamente al RPA;
- esegue la prima classificazione (o classificazione di primo livello) del documento sulla base del titolario di classificazione in essere presso l'amministrazione.

5.2.16 CONSERVAZIONE DEI DOCUMENTI NELL'ARCHIVIO CORRENTE

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

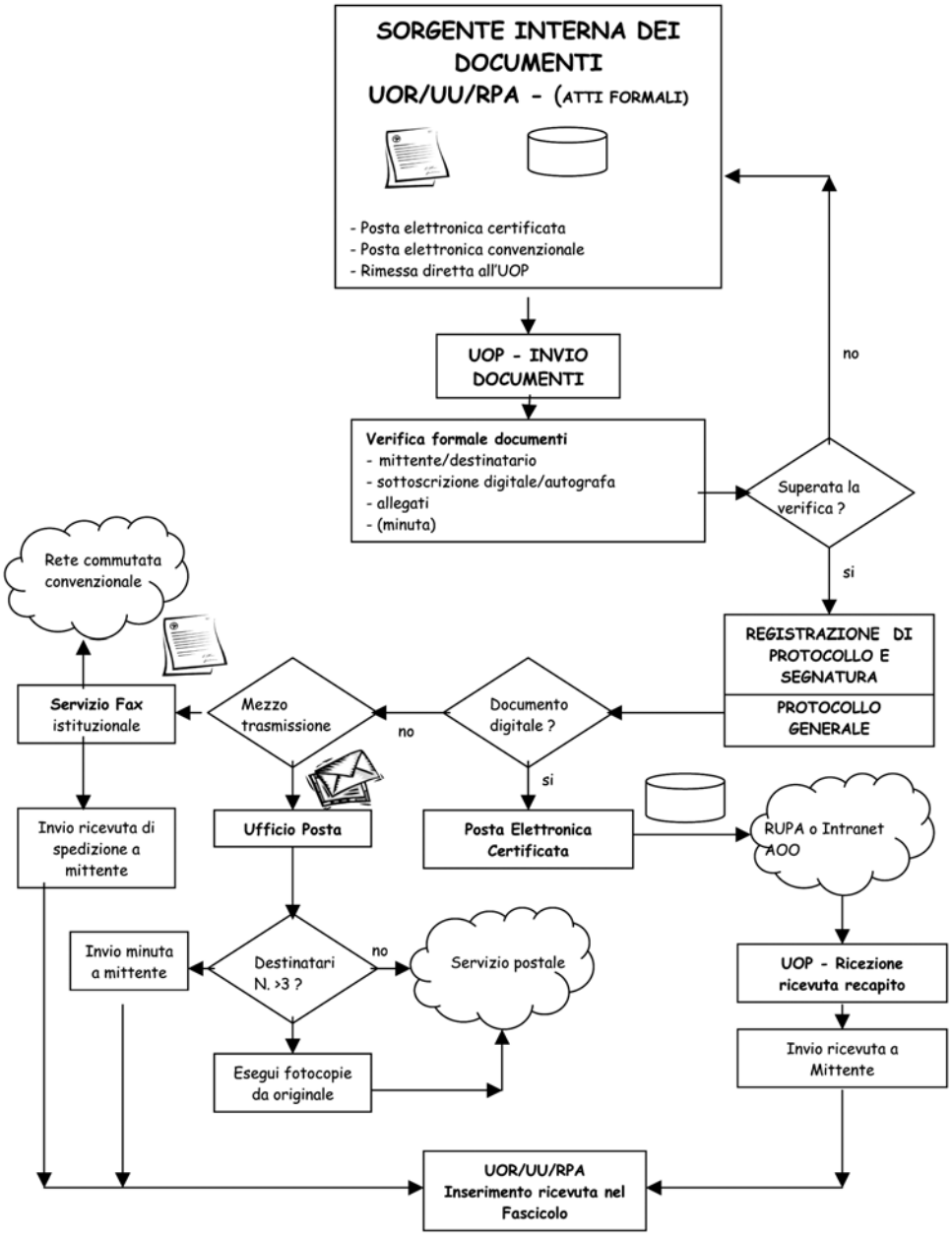
1. classificazione di livello superiore sulla base del titolario di classificazione adottato dall'AOO;
2. fascicolazione del documento secondo le procedure previste dall'AOO;

3. inserimento del fascicolo nel repertorio dei fascicoli nel caso di apertura di un nuovo fascicolo.

5.2.17 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.

5.3 FLUSSO DEI DOCUMENTI INVIATI DALLA AOO



5.3.1 SORGENTE INTERNA DEI DOCUMENTI

Nel grafico di cui al paragrafo 5.3 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 o altra AOO della stessa 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 o altra AOO della stessa 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.
I mezzi di recapito della corrispondenza considerati sono quelli stessi richiamati nell'articolo 35 - Posta Elettronica Certificata.
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.

5.3.2 VERIFICA FORMALE DEI DOCUMENTI

o ***alternativa 1 – sistema centralizzato***
Tutti i documenti originali da spedire, siano essi in formato digitale o analogico, sono inoltrati alla/e UOP istituzionali:

- documenti informatici – nella casella di posta interna dedicata alla funzione di "appoggio" per i documenti digitali da trasmettere;
- documenti analogici – in busta aperta per le operazioni successive di protocollazione e segnatura. Sono consegnati in questa forma anche i documenti contenenti i dati personali sensibili o giudiziari in quanto il personale dell'UOP, che riceve la corrispondenza, è autorizzato al trattamento dei dati personali.

L'UOP provvede ad eseguire le verifiche di conformità della documentazione ricevuta (per essere trasmessa) allo standard formale richiamato nel capitolo precedente, cioè verifica che siano indicati correttamente il mittente e il destinatario, verifica che il documento sia sottoscritto in modalità digitale o autografa, la presenza di allegati se dichiarati.
Se il documento è completo, esso è registrato nel protocollo generale o particolare e ad esso viene apposta la segnatura in base alla tipologia di documentazione da inviare; in caso contrario è rispedito al mittente UOR/UU/RPA con le osservazioni del caso.

- ***alternativa 2 - sistema decentralizzato***

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.
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.

5.3.3 REGISTRAZIONE DI PROTOCOLLO E SEGNATURA

- ***alternativa 1 - sistema centralizzato***

Le operazioni di registrazione e di apposizione della segnatura del documento in partenza sono effettuate presso la UOP istituzionale. Il documento registrato presso il protocollo riservato riservato è contrassegnato anteponendo al numero della segnatura una sigla (ad es. "RIS")
In nessun caso gli operatori di protocollo sono autorizzati a riservare numeri di protocollo per documenti non ancora resi disponibili.
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.

- ***alternativa 2 - sistema decentralizzato***

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").

5.3.4 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.

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.

5.3.5 Trasmissione di documenti cartacei a mezzo posta

- ***alternativa 1 – sistema centralizzato***

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo anche all'affrancatura e all'eventuale pesatura, alla ricezione e alla verifica delle distinte di raccomandate compilate dagli uffici *(**opzionalmente** - I documenti da spedire su supporto cartaceo, nell'ambito della UOP, sono trasmessi all'ufficio addetto allo smistamento della posta centrale, se previsto, abilitato alla spedizione "fisica" della corrispondenza).*
L'UOP conserva, temporaneamente, la minuta da restituire al mittente.

- ***alternativa 2 – sistema decentralizzato***

La UOR provvede direttamente alla trasmissione "fisica" del documento in partenza e alla spedizione del documento, di norma il giorno lavorativo in cui è stato protocollato.
*(**opzionalmente** - I documenti da spedire su supporto cartaceo, nell'ambito della AOO, sono trasmessi all'ufficio addetto allo smistamento della posta centrale, se previsto, abilitato alla spedizione "fisica" della corrispondenza).*

5.3.6 Affrancatura dei documenti in partenza

L'UOP *(o in alternativa l'ufficio addetto allo smistamento della posta)* provvede alle operazioni necessarie per l'invio della corrispondenza in partenza (ad es.: pesatura e affrancatura delle lettere ordinarie, affrancatura delle lettere fuori formato, pesatura, timbratura ed affrancatura posta prioritaria, ricezione e verifica delle distinte di raccomandate compilate ed etichettate dagli uffici, pesatura, affrancatura e registrazioni delle raccomandate estere ecc.).
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP *(o in alternativa all'ufficio posta)* secondo le regole richiamate nell'allegato 16.12.

5.3.7 Conteggi spedizione corrispondenza

L'UOP *(o in alternativa l'ufficio posta)* effettua i conteggi relativi alle spese giornaliere e mensili sostenute per le operazioni di invio della corrispondenza.

5.3.8 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.

5.3.9 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.

- ***alternativa 1 - sistema centralizzato***

Le ricevute della avvenuta trasmissione sono trattenute, temporaneamente, dalla UOP che ha effettuato la trasmissione.

- ***alternativa 2 - sistema decentralizzato***

Le ricevute della avvenuta trasmissione sono trattenute dagli UOR/UU/RPA che hanno effettuato la trasmissione.

5.3.10 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.

- ***alternativa 1 - sistema centralizzato***

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.

- ***alternativa 2 - sistema decentralizzato***

Gli UOR che effettuano la spedizione di documenti informatici o cartacei direttamente curano anche l'archiviazione delle ricevute di ritorno.

6. Regole di smistamento ed assegnazione dei documenti ricevuti

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

6.1 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:
< illustrare la realtà dell'amministrazione/AOO su questo aspetto >.

Esempio di descrizione del flusso (smistamento, assegnazione e presa in carico) dei documenti registrati

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, documento.
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.
Una volta che al mittente iniziale (UOP) giunge notizia di presa in carico della corrispondenza, è cura di questo inviare, con le tecnologie adatte, il documento oggetto di lavorazione compilato nella parte di segnatura (o timbro di segnatura) al UOR/UU/RPA di competenza.
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 rconducibili 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 16.3 sono riportati gli UOR destinatari dello smistamento e autorizzati all'assegnazione dei documenti ricevuti dall'AOO e protocollati dagli UOP.

Nello stesso allegato, per ciascuna delle strutture in elenco, sono indicati:

- *l'indirizzo elettronico;*
- *le principali tipologie di documenti trattati che determinano i criteri di assegnazione della corrispondenza.*

o ***alternativa 1 - unità di smistamento distribuite***
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.

o ***alternativa 2 - unità di smistamento centralizzata***
Tutta la corrispondenza protocollata nell'arco della giornata viene inviata in visione al <direttore generale o segretario generale o RSP…… > affinché possa valutarla e controllare le assegnazioni suggerite, apportando eventuali modifiche o correzioni.
La corrispondenza ritorna alla/e UOP mittente/i per le eventuali correzioni e/o integrazioni e per l'assegnazione del documento precedentemente protocollato e segnato.

6.2 CORRISPONDENZA DI PARTICOLARE RILEVANZA

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, è preventivamente inviato in visione a *< direttore generale o segretario generale o RSP……>* che provvede ad individuare l'UOR competente a trattare il documento fornendo eventuali indicazioni per l'espletamento della pratica.

6.3 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.

6.4 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 successivemnbte trasmesso al RPA oppure essere conservato dalla UOP.
L'UOR competente ha notizia dell'arrivo del documento ad essa 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 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.

o ***opzione 1***
I documenti cartacei gestiti dalla UOP sono di norma smistati entro le xxx ore dal momento in cui sono pervenuti, salvo che vi siano, entro detto lasso di tempo, uno o più giorni non lavorativi, nel qual caso l'operazione di smistamento viene assicurata entro le 24 ore dall'inizio del primo giorno lavorativo successivo.

o ***opzione 2***
Il ritiro giornaliero della corrispondenza cartacea in arrivo da parte degli UOR/UU/RPA avviene presso le UOP ricevente/i.

6.5 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.

7. 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 (si veda il par. 1.4 del presente MdG), nell'allegato 16.3 è riportato, per ciascuna AOO, 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 di ciascuna AOO (o della AOO se unica), 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.

7.1 Servizio archivistico

- ***alternativa 1***

  L'amministrazione ha istituito il servizio archivistico e documentale denominato < *inserire il nome* > nell'ambito delle diverse AOO in cui è operante il servizio di protocollo e gestione documentale. Il sistema archivistico è unico e trasversale su tutte le AOO.
  Il servizio archivistico è competente a gestire l'intera documentazione archivistica, ovunque trattata, distribuita o conservata, ai fini della sua corretta classificazione, conservazione e ordinamento. Alla guida del servizio archivistico è preposto < *specificare il ruolo e il nominativo* >. Il responsabile del servizio archivistico si coordina con i diversi RSP a capo delle AOO.

- ***alternativa 2***

  - ***caso 2 a***

    Il servizio archivistico è funzionalmente integrato nel suddetto servizio per la tenuta del protocollo informatico, ma strutturalmente e gerarchicamente distinto.
    Alla guida del servizio archivistico è preposto < *specificare il ruolo e il nominativo* >.
    Il responsabile del servizio archivistico si coordina con il RSP a capo delle AOO.
  - ***caso 2 b***

    Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto servizio per la tenuta del protocollo informatico. Alla guida del servizio archivistico è preposto < *specificare il ruolo e ripetere il nome RSP o altro soggetto* >.

o ***alternativa 3***

L'amministrazione ha istituito il servizio archivistico denominato < *inserire il nome* > nell'ambito dell'unica AOO in cui è organizzato il servizio di protocollo e gestione documentale.

- ***caso 3a***
  Il servizio archivistico è funzionalmente integrato nel suddetto servizio per la tenuta del protocollo informatico ma strutturalmente e gerarchicamente distinto.
  Alla guida del servizio archivistico è preposto < *specificare il ruolo e il nominativo* >.
  Il responsabile del servizio archivistico si coordina con il RSP a capo delle AOO.
- ***caso 3b***
  Il servizio archivistico è funzionalmente e strutturalmente integrato nel suddetto servizio per la tenuta del protocollo informatico. Alla guida del servizio archivistico è preposto < *specificare il ruolo e ripetere il nome RSP o altro soggetto* >.

o ***(comunque ….)***

Nei casi di vacanza, assenza o impedimento del responsabile del servizio archivistico, questo sarà sostituito da - < *specificare ruolo e nome* >.
L'atto che istituisce il servizio e nomina il relativo responsabile è riportato nell'allegato 16.14.

7.2 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.

Al responsabile del servizio di conservazione sostitutiva sono attribuiti i compiti e le responsabilità specificatamente descritte nell'allegato 16.15.
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.

o ***opzionale***

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 (per l'AOO < *inserire nome* >) 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.

7.2.1 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.

7.2.2 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.

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

8.1 Documenti esclusi

Sono esclusi dalla registrazione di protocollo, le tipologie di documenti riportati nell'allegato 16.16.
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.

8.2 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 16.17.
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.

9. Sistema di classificazione, fascicolazione e piano di conservazione

9.1 Protezione e conservazione degli archivi pubblici

9.1.1 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.
Un esempio di piano di conservazione è riportato nell'allegato 16.18.
Il titolario e il piano di conservazione sono predisposti, verificati e/o confermati antecedentemente all'avvio delle attività di protocollazione informatica e di archiviazione, considerato che si tratta degli strumenti che consentono la corretta formazione, gestione e archiviazione della documentazione dell'amministrazione.
Spetta ai vertici dell'amministrazione medesima adottare il titolario e il piano di conservazione con atti formali.

9.1.2 Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti degli enti pubblici non territoriali 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 organi-

ci 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 direzione generale per gli archivi.
Relativamente agli enti pubblici non statali l'autorizzazione per l'eventuale rimozione e/o trasferimento dell'archivio, è demandata, per delega della direzione generale degli archivi, alle sovrintendenze archivistiche.
Lo scarto dei documenti degli archivi delle amministrazioni/AOO statali è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza corrispondente alla provincia o delle commissioni di scarto istituite presso ogni ufficio con competenza subprovinciale. Per gli enti pubblici non statali la competenza è delegata alla soprintendenza archivistica competente per territorio.
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.

9.2 TITOLARIO O PIANO DI CLASSIFICAZIONE

9.2.1 TITOLARIO

Il piano di classificazione è lo schema logico utilizzato per organizzare i documenti d'archivio in base alle funzioni e alle materie di competenza dell'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 16.19.
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.
Il titolario è elaborato da un gruppo di lavoro appositamente costituito all'interno dell'amministrazione/AOO e approvato dai competenti organi dell'amministrazione archivistica statale.

9.2.2 Classificazione dei documenti

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

9.3 Fascicoli e dossier

9.3.1 Fascicolazione dei documenti

Tutti i documenti registrati nel sistema informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
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.

9.3.2 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'amministrazione/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 16.20.

9.3.3 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 9.3.2, primo capoverso, il quale è tenuto anche all'aggiornamento del repertorio dei fascicoli.

9.3.4 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.

9.3.5 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.

9.3.6 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.

9.3.7 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).*

9.3.8 Repertorio dei dossier

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

9.4 Serie archivistiche e repertori

9.4.1 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[3].

[3] 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).

9.4.2 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.
Il repertorio è costantemente aggiornato.
All'interno dell'amministrazione sono istituiti i repertori generali indicati nell'allegato 16.21.

9.4.3 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 (che può coincidere con il RSP) 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.

9.4.4 VERIFICA DELLA CONSISTENZA DEL MATERIALE RIVERSATO NELL'ARCHIVIO DI DEPOSITO

L'ufficio ricevente esegue il controllo del materiale riversato.
Il 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.

9.5 SCARTO, SELEZIONE E RIORDINO DEI DOCUMENTI

9.5.1 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, *se già esiste*, o la predisposizione di un massimario di selezione e scarto e un piano di conservazione di atti dell'archivio.

o ***alternativa 1***

Se il massimario per l'amministrazione è stato già definito a livello locale, territoriale o nazionale, il vertice dell'amministrazione formalizza l'impiego di detto massimario all'interno dell'amministrazione medesima.

o ***alternativa 2***

In caso di predisposizione ex novo, il massimario viene proposto dal RSP (***opzionale*** - coadiuvato dal responsabile dell'archivio generale), alla direzione generale degli archivi del Ministero per i beni e le attività culturali e viene autorizzato con atto formale dall'organo competente dell'amministrazione.

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.

I documenti e gli atti sottoposti a procedura di scarto sono devoluti gratuitamente secondo quanto stabilito dal decreto del Presidente della Repubblica del' 8 gennaio 2001, n. 47 art. 8[4]. In particolare l'amministrazione/AOO intende procedere come di seguito descritto.

< *inserire la descrizione della procedura di cessione e distruzione dei documenti*>.

9.5.2 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.

9.5.3 VERSAMENTO DEI DOCUMENTI NELL'ARCHIVIO STORICO

o ***alternativa 1 – amministrazioni statali***

Gli organi giudiziari e amministrativi dello Stato versano all'Archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre quarant'anni, unitamente agli strumenti che ne garantiscono la consultazione.

Nessun versamento può essere ricevuto se non sono state effettuate le operazioni di scarto. Le spese per il versamento sono a carico delle amministrazioni versanti.

[4] Fino al 2001 la materia era regolata dal RDL 10 agosto 1928 n. 2034 art.16, e successive modifiche, che prevedeva la cessione obbligatoria gratuita alla CRI. Tale disposizione fu abrogata dal 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). L'art. 8 del DPR 47/2001 stabilisce che le modalità di cessione degli atti vengono stabilite da ciascuna amministrazione; esso dunque non configura un obbligo di cessione alla CRI, conferendo anzi all'amministrazione procedente facoltà di scelta tra la stessa Croce Rossa e le organizzazioni di volontariato. Nel maggio 2001, con decreto del Ministro del tesoro (DM 21 maggio 2001) è stata rinnovata alla CRI la concessione per il ritiro del materiale destinato allo scarto, prevista dalla vecchia disposizione del 1928, nel frattempo abrogata. Tale concessione, nel nuovo quadro normativo, deve considerarsi come conferita *in via non esclusiva*.

o ***alternativa 2 – altre amministrazioni***

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.

o ***(…. comunque…..)***

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

9.6 CONSULTAZIONE E MOVIMENTAZIONE DELL'ARCHIVIO CORRENTE, DI DEPOSITO E STORICO

9.6.1 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.

9.6.2 CONSULTAZIONE AI FINI GIURIDICO-AMMINISTRATIVI[5]

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 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.

[5] Il riferimento è alla legge 241/90 e successive modifiche.

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'àmbito 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:
   a) 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;
   b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria;
   c) 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;
   d) 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;
   e) 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".

9.6.3 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.

9.6.4 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 16.13.
Le richieste di accesso ai documenti della sezione storica dell'archivio possono essere inoltrate anche alla soprintendenza per i beni archivistici territorialmente competente, con apposito modulo da questa predisposto.
Le domande vengono evase durante gli orari di apertura al pubblico dell'URP e dell'archivio con la massima tempestività e comunque non oltre < xx > giorni dalla presentazione.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.
In tale caso il responsabile del servizio archivistico provvede a consentire l'accesso conformemente a criteri di salvaguardia dei dati dalla distruzione, dalla perdita accidentale, dall'alterazione o dalla divulgazione non autorizzata.
In caso di richieste di consultazione di materiale cartaceo che comportano l'attivazione di ricerche complesse, il termine di evasione della richiesta, di norma, si raddoppia.
L'ingresso all'archivio di deposito e storico è consentito solo agli addetti del servizio archivistico.
La consultazione dei documenti è possibile esclusivamente in un locale appositamente predisposto (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.
Le disposizioni dei commi precedenti si applicano anche alla consultazione di archivi storici presso le pubbliche amministrazioni che non si siano ancora dotate di apposito servizio per l'apertura alla pubblica consultazione degli archivi.

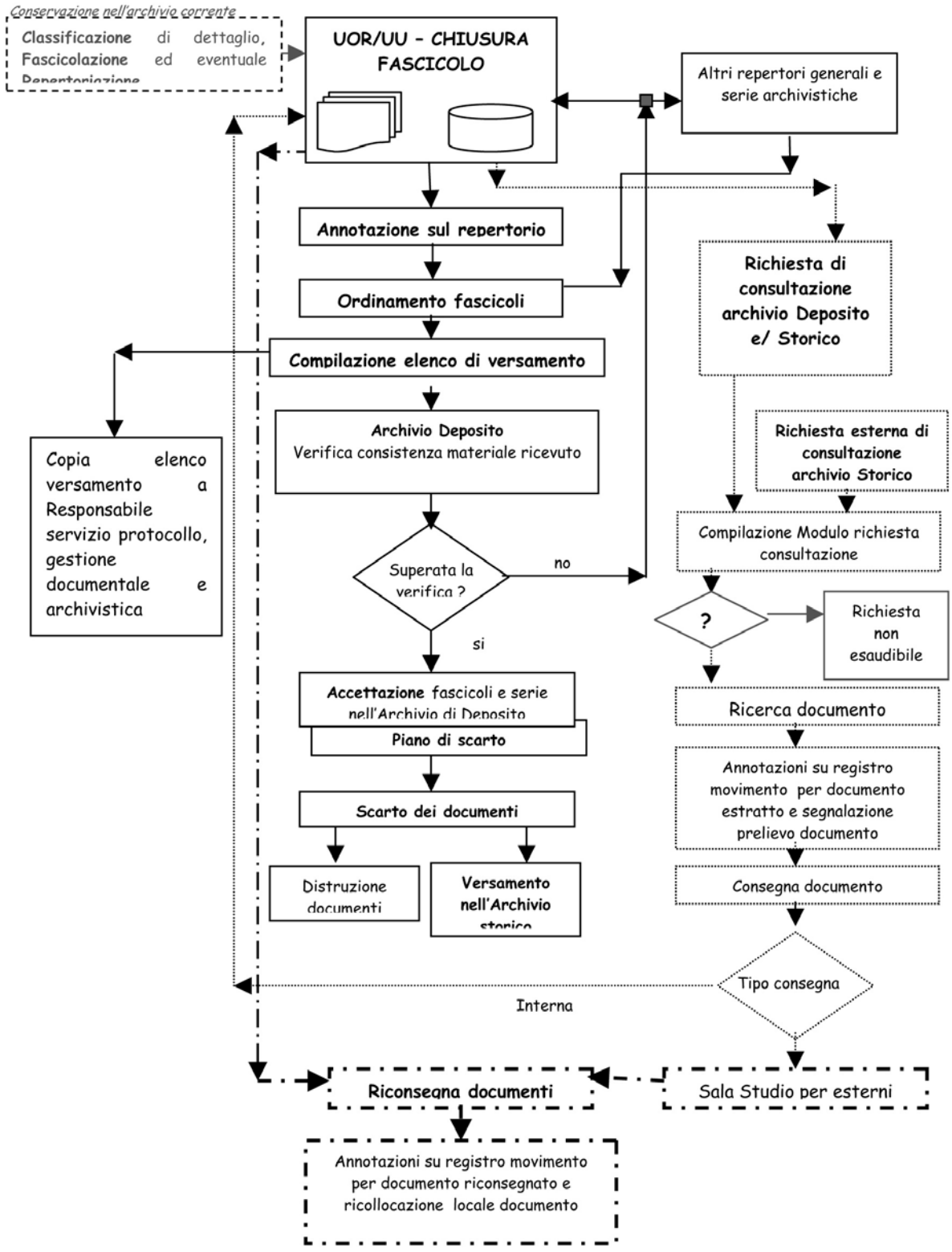
9.6.5 CONSULTAZIONE DA PARTE DI PERSONALE INTERNO ALL'AMMINISTRAZIONE

Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito o storica[6].
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.

9.6.6 SCHEMATIZZAZIONE DEL FLUSSO DEI DOCUMENTI ALL'INTERNO DEL SISTEMA ARCHIVISTICO

Nella pagina seguente viene riportata una rappresentazione grafica sintetica del complesso delle attività, delle norme e delle responsabilità illustrate nel presente capitolo che, nella loro totalità, costituiscono funzione strategica dell'amministrazione/AOO.

6 Concettualmente l'archivio storico e di deposito sono due entità separate, e soggette a un regime parzialmente differente. Tuttavia l'obbligo della costituzione di una sezione separata per l'archivio storico, già previsto per gli enti pubblici dal DPR 1409/1963, è stato soppresso dal TU e poi dal Codice dei beni culturali, in ragione del fatto che la maggior parte degli enti pubblici (gli enti pubblici territoriali) godono di autonomia statutaria, specie con riferimento ai servizi (gli altri quasi non esistono più, o si tratta di organismi in via di privatizzazione). L'organizzazione degli archivi e dei relativi servizi al pubblico è dunque demandata ai singoli Enti. Essa non deve confliggere con gli obblighi sanciti da leggi statali in materia di tutela, conservazione e valorizzazione.


Conservazione nell'archivio corrente
Classificazione di dettaglio, Fascicolazione ed eventuale
UOR/UU - CHIUSURA FASCICOLO
Altri repertori generali e serie archivistiche
Annotazione sul repertorio
Ordinamento fascicoli
Compilazione elenco di versamento
Richiesta di consultazione archivio Deposito e/ Storico
Copia elenco versamento a Responsabile servizio protocollo, gestione documentale e archivistica
Archivio Deposito
Verifica consistenza materiale ricevuto
Richiesta esterna di consultazione archivio Storico
Compilazione Modulo richiesta consultazione
Superata la verifica ?
no
si
?
Richiesta non esaudibile
Accettazione fascicoli e serie nell'Archivio di Deposito
Piano di scarto
Ricerca documento
Annotazioni su registro movimento per documento estratto e segnalazione prelievo documento
Scarto dei documenti
Distruzione documenti
Versamento nell'Archivio storico
Consegna documento
Tipo consegna
Interna
Riconsegna documenti
Sala Studio per esterni
Annotazioni su registro movimento per documento riconsegnato e ricollocazione locale documento

10. 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.

10.1 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.

10.2 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 CED ? del sistema informativo (?)* >.
È a carico < *del CED? o Settore/Direzione o….*> conservare in modalità sicura la copia del registro giornaliero di protocollo.

10.3 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.

10.3.1 DOCUMENTI INFORMATICI

I documenti informatici sono ricevuti e trasmessi in modo formale sulla/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.
Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

10.3.2 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 esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

10.4 Elementi facoltativi delle registrazioni di protocollo

Il 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 registra 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;

- termine di conclusione del procedimento amministrativo o di lavorazione del documento;
- indicazione del livello di sicurezza se diverso da quello standard applicato dal sistema di protocollazione;
- stato e tempi parziali delle procedure del procedimento amministrativo;
- 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.

10.4.1 ELEMENTI FACOLTATIVI DI INTERESSE DEL PDP

Ulteriori informazioni sul .....*< illustrare la realtà dell'amministrazione/AOO su questo aspetto >*.

10.5 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.

10.5.1 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'Extensible Markup Language* (XML) e compatibile con il *Document Type Definition* (DTD) reso disponibile dagli .....*<inserire nomi delle amministrazioni competenti >*
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.

10.5.2 DOCUMENTI CARTACEI

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione su di esso di un "segno" grafico 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 16.22.
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.

10.6 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.

10.7 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.

10.8 CASI PARTICOLARI DI REGISTRAZIONI DI PROTOCOLLO (DA CONTESTUALIZZARE[7])

10.8.1 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 16.17.

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 registrarli, farli registrare nel protocollo generale;
- se ritiene che non contengano dati rilevanti dal punto di vista amministrativo, il documento viene registrato nel protocollo particolare.

10.8.2 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.

10.8.3 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 con la dicitura "Questa registrazione di protocollo viene riportata sui documenti degli altri destinatari - Vedi elenco allegato alla minuta/copia presso l'UOR/UU/RPA".
Tale elenco, in formato cartaceo, viene allegato alla minuta dell'originale.

[7] I casi particolari elencati nel paragrafo 11.8 sono ripresi dall'esperienza delle amministrazioni centrali e locali che hanno pubblicato il Manuale di Gestione. In questo documento vengono elencati alcuni casi particolari ma non sono da ritenersi né esaustivi né tanto meno vincolanti nella compilazione del Manuale di Gestione.

10.8.4 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.

10.8.5 DOCUMENTI CARTACEI RICEVUTI A MEZZO TELEFAX

Il 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.

10.8.6 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.

10.8.7 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.

10.8.8 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, protocollate su un registro diverso da quello generale e inviate quotidianamente all'UOR competente.

10.8.9 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.

10.8.10 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.

10.8.11 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.

10.8.12 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.

10.8.13 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.

10.8.14 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".

10.8.15 COPIE PER CONOSCENZA

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 10.8.3. 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.

10.8.16 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 < *inserire valore o* 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.

10.8.17 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.
Il responsabile dell'immissione dei dati provvede alla registrazione di protocollo indicando contestualmente l'anno, il mese e il giorno, nel quale le informazioni temporaneamente riservate saranno accessibili nelle forme ordinarie.

10.8.18 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.

10.8.19 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.

10.9 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.

10.10 REGISTRAZIONI DI PROTOCOLLO

10.10.1 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.
- < *inserire eventuali altri accorgimenti* >.

10.10.2 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 o l'addetto incaricato di eseguire l'operazione di riversamento dei file in parola su due supporti rimovibili non riscrivibili è stato individuato nel < *specificare* >.
L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del file del registro di protocollo[8].
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.

[8] Le copie giornaliere generali di backup dell'intero sistema informativo dell'amministrazione/AOO esulano dai meccanismi di sicurezza qui richiamati.

(opzionale) Al termine delle operazioni giornaliere o, comunque entro il giorno successivo sono effettuate le seguenti operazioni di garanzia:

- < *inserire eventuali altri accorgimenti dell'AOO*>.

10.10.3 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[9] 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 della AOO, mentre la seconda copia è custodita presso < *specificare* >.
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.
Procedendo alle operazioni di riversamento con la periodicità prevista dalla deliberazione CNIPA n. 11/2004.

[9] Il responsabile della conservazione e l'addetto incaricato della produzione delle copie su supporti rimovibili non riscrivibili possono coincidere.

11. 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.

11.1 Descrizione funzionale ed operativa

Di seguito viene fornita una elencazione sintetica delle principali funzioni del PdP.
Nell'allegato 16.23 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.

12. 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.

12.1 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 (xxxxx) profili d'accesso, sulla base delle rispettive competenze.

- *< illustrare la realtà dell'amministrazione/AOO su questo aspetto >*.

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 16.24 e sono costantemente aggiornate a cura del RSP.

12.2 Abilitazioni interne ad accedere ai servizi di protocollo

Gli utenti abilitati accedono al PdP ….. *<illustrare le modalità di accesso >*.

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 < …?... > crittografata e accessibile soltanto da un processo di sistema.
< *illustrare la realtà tecnico operativa dell'amministrazione/AOO su questo aspetto* >.
Tutte le utenze dell'AOO sono configurate con un *time-out* che provvede a disconnettere automaticamente l'applicazione dopo < XX > minuti di inattività.
Le sessioni multiple con la stessa *user ID* sono proibite e impedite dal PdP.

12.3 PROFILI DI ACCESSO

< *illustrare la realtà tecnico operativa dell'amministrazione/AOO su questo aspetto, quale, ad esempio, quella di seguito schematizzata* >.

12.3.1 UTENTE AMMINISTRATORE DI PDP

12.3.2 OPERATORE DI PROTOCOLLO

12.3.3 UTENTE ORDINARIO

12.4 MODALITÀ DI CREAZIONE E GESTIONE DELLE UTENZE E DEI RELATIVI PROFILI DI ACCESSO

Al fine di procedere alla creazione delle utenze <*illustrare la realtà tecnico operativa dell'amministrazione/AOO su questo aspetto, quale, ad esempio, quella di seguito schematizzata* >.
In caso di smarrimento della password, <*illustrare la realtà tecnico operativa dell'amministrazione/AOO su questo aspetto, quale, ad esempio, quella di seguito schematizzata* >.

12.5 RIPRISTINO DELLE CREDENZIALI PRIVATE D'ACCESSO

12.6 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 è 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 sono fornite tutte le informazioni necessarie per accedere a detti documenti amministrativi.

12.7 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, avviene secondo le modalità di interconnessione previste dalle norme e dai criteri tecnici emanati per la realizzazione della RUPA.
In questi casi, le pubbliche amministrazioni accedono ai sistemi di gestione informatica dei documenti utilizzando al momento la RUPA 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.

12.8 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.

13. 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.

13.1 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

13.2 Modalità di apertura del registro di emergenza

Il 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 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 16.3.

Servizio di gestione informatica del protocollo, dei documenti e degli archivi
Scheda di apertura/chiusura del registro di emergenza

< Identificativo dell'amministrazione >
< Identificativo dell'AOO >
< Identificativo della UOP abilitata >

Causa dell'interruzione: . . . . . .

Data: gg / mm / aaaa di inizio/ fine interruzione
(*depennare la voce incongruente con l'evento annotato)*
Ora dell'evento hh /mm
Annotazioni: . . . . . .

Numero protocollo xxxxxxx iniziale/finale
(*depennare la voce incongruente con l'evento annotato)*
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.

13.3 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, 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

13.4 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.
(opzionale...) *Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza (postazione di lavoro stand alone) a quello del protocollo generale e di evitare la duplicazione di attività di inserimento, le informazioni relative ai documenti protocollati in emergenza su una o più postazioni di lavoro dedicate della AOO, sono inserite nel sistema informatico di protocollo generale, utilizzando un'apposita funzione di recupero dei dati).*
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.

14. Gestione dei 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*).

14.1 Matrice delle correlazioni

I procedimenti amministrativi sono descritti nel "Catalogo dei procedimenti amministrativi", di cui il RSP cura 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 14.2.
La definizione del singolo procedimento amministrativo rappresenta il modello astratto di riferimento per lo svolgimento dell'attività amministrativa.
Il risultato concreto di questa attività sono 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 è effettuata sulla base delle competenze assegnate a ciascuna figura interna agli UOR/UU.

14.2 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, costituisce 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.

14.3 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.

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

15.1 Modalità di approvazione e aggiornamento del Manuale

L'amministrazione 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.

(***opzionale*** - *Per l'esecuzione di tali modifiche il RPS può avvalersi del comitato tecnico di gestione del protocollo informatico, gestione documentale ed archivistica, se costituito);*

15.2 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.

15.3 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.

15.4 Operatività del presente Manuale

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

Allegati

16. Allegati

16.1 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 raccolta ordinata degli atti spediti, inviati o comunque formati dell'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 o dalla Area Organizzativa Omogenea sono collegati tra loro da un rapporto di interdipendenza, determinato

	dal procedimento o dall'affare al quale si riferiscono. 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;
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;
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;
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 accer-

	tamento 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 DEI SERVIZI	Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica 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'alle-

	gato 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 1 lett. f) del DPR 28 dicembre 2000, n. 445*);
CERTIFICATORE	Il 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	Il 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 amministra-

	zione 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 D'IDENTITÀ ELETTRONICO	Il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età (*art. 1 comma 1 lett. e) 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.). I fascicoli costituiscono il tipo di unità archivistica più diffusa degli archivi contemporanei e sono costituiti, in base alle esigenze di servizio, secondo criteri che sono stabiliti per ciascuna voce del piano di classificazione al momento della sua elaborazione o del suo aggiornamento;
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 geo 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 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*);
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*);

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*);
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.

16.2 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).

16.3 AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO

16.3.1 MODELLO ORGANIZZATIVO DELL'AMMINISTRAZIONE

Denominazione dell'Amministrazione	
Codice identificativo assegnato all'Amministrazione	
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	
Elenco delle AREE ORGANIZZATIVE OMOGENEE – AOO	< denominazione AOO 1 >
	< denominazione AOO 2 >
	< denominazione AOO 3 >
	< denominazione AOO xx >

16.3.2 CARATTERIZZAZIONE DI CIASCUNA AREA ORGANIZZATIVA OMOGENEA

Denominazione dell'Area Organizzativa Omogenea		
Codice identificativo assegnato alla AOO		
Nominativo del Responsabile del Servizio di Protocollo informatico, gestione documentale e archivistica		
Casella di posta elettronica istituzionale dell'AOO (1)		
Indirizzo completo della sede principale della AOO a cui indirizzare l'eventuale corrispondenza convenzionale		
Data di istituzione della AOO		
Data di soppressione della AOO	Nulla	
Articolazione della AOO in Unità Organizzative di registrazione di Protocollo - UOP	Descrizione **(2)**	Tipo protocollazione: <Ingresso/Uscita> < Ingresso > < Uscita >
Articolazione della AOO in Uffici Organizzativi di Riferimento -UOR	**Descrizione (2)**	

(1) ***Opzione ed esempio:*** i messaggi di posta elettronica da inviare nella casella di posta istituzionale dovranno essere conformi alle seguenti regole tecniche:

- *Tipo messaggio*: messaggio di posta elettronica sottoscritto con firma digitale certificata conforme alle disposizioni correnti
- *Testo del messaggio*: caratteri ammessi: Times New Roman, Arial, Courier New, Verdana, Comic Sans MS
- *Dimensione dei caratteri del testo*: minimo 8, massimo 14
- *Allegati*: formato con caratteri tutti identici, anche nei titoli e nei paragrafi senza ulteriori informazioni di formattazione con estensione .txt o .pdf

(2) Compilare tante righe per quante sono le entità in cui è articolata l'Amministrazione

16.3.3 ARTICOLAZIONE DI CIASCUNA UNITÀ ORGANIZZATIVA DI REGISTRAZIONE DI PROTOCOLLO IN UFFICI UTENTE

Compilare la tabella seguente in caso di frammentazione delle UOP in UU

< Area Organizzativa Omogenea >	
< Unità Organizzativa di Protocollo >	< Nominativo del Responsabile dell'UOP >
Denominazione dell'Ufficio Utente (1)	< Inserire descrizione >
Nominativo del Responsabile dell'UU	< Nominativo del Responsabile dell'UU >
Ubicazione	< Indirizzo completo dell'UU >
Numero di telefono	
Numero di telefax	
UOP abilitata allo smistamento	(SI/NO)
UOP abilitata a eseguire la scannerizzazione dei documenti cartacei	(SI/NO)
UOP abilitata all'impiego del Registro di emergenza	(SI/NO)

(1) Compilare tante tabelle per quante sono le UOP e gli Uffici Utente di ciascuna UOP

16.3.4 ARTICOLAZIONE DI CIASCUN UFFICIO ORGANIZZATIVO DI RIFERIMENTO IN UFFICI UTENTE

< Area Organizzativa Omogenea >	
< Ufficio Organizzativo di Riferimento >	< Nominativo del Responsabile dell'UOR >
Ubicazione dell'UOR	< Indirizzo completo dell'UOR >
Denominazione dell'Ufficio Utente (1)	< Inserire descrizione >
Nominativo del Responsabile dell'UU	< Nominativo del Responsabile dell'UU >
Numero di telefono	
Numero di telefax	
UOR abilitato allo smistamento	(SI/NO)
Primo livello di classificazione: Titolo	

(1) Compilare tante tabelle per quante sono le UOP e gli Uffici Utente di ciascuna UOP

16.4 ATTO DI NOMINA DEL RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

Esempio di nomina

Determinazione n. xx del gg/mm/aaaa

Registro generale n.

Oggetto: **Nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e del suo Vicario.**

L'anno xxxx, il giorno xx del mese di < …….. >, nell'amministrazione di < *Inserire denominazione completa* > sita in < *inserire indirizzo e CAP* >

<< IL DIRIGENTE >>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi e delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

VISTO in particolare l'articolo 61, comma 2, il quale tra l'altro, stabilisce che presso il servizio gratuito del protocollo informatico, è preposto un dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali e di professionalità tecnico archivistica;

VISTO il Decreto ministeriale 14 ottobre 2003 "Approvazione delle linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi", nel quale sono indicati gli adempimenti delle amministrazioni relativamente al protocollo informatico ed alla gestione dei procedimenti amministrativi con tecnologie informatiche;

RITENUTO di individuare nel/nella signor/signora < *inserire nome e titolo amministrativo* >, in servizio presso l'Ufficio Utente < *inserire nome* >, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- 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 anche su Internet;
- 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 il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con il:
  - Responsabile dei sistemi informativi automatizzati,

  - Referente della pianificazione delle attività,
  - Responsabile della sicurezza dei dati personali, se nominato, o direttamente con il Titolare dei trattamenti dei dati di cui al d. lgs. 196/03,
  - Responsabile del servizio archivistico,
  - Responsabile della conservazione sostitutiva;

- attribuire il livello di autorizzazione di ciascun addetto all'accesso alle funzioni delle procedure applicative di gestione del protocollo informatico e gestione documentale distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento, alla modifica e alla cancellazione delle informazioni;
- 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 adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;
- curare, anche attraverso altri responsabili, le funzionalità del sistema di gestione informatica del protocollo e della gestione documentale 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 e del registro di emergenza in luoghi sicuri differenti;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso esterno o da altre Amministrazioni e le attività di gestione degli archivi, quali, trasferimento dei documenti all'archivio di deposito, disposizioni per la conservazione degli archivi e Archivi storici;
- autorizzare le operazioni di annullamento della registratura di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme correnti da parte del personale autorizzato e degli incaricati.

<< DETERMINA >>

1. di nominare il/la signore/a < *inserire nome e titolo amministrativo* >, quale Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi ai sensi dell'articolo 61 comma 2 del DPR n. 445/2000 con i compiti specificati nelle premesse.
2. di nominare vicario del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, per i casi di vacanza, assenza o impedimento del Responsabile, viene nominato il/la signor/signora <*nominativo e titolo amministrativo*> dell'Ufficio Utente <specificare>

16.5 ATTO DI NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE DELLE COPIE DI RISERVA DEL REGISTRO DI PROTOCOLLO INFORMATICO

Esempio di nomina

Determinazione n. xx del gg/mm/aaaa

Registro generale n.

Oggetto: **Nomina del Responsabile delle copie di riserva del registro di protocollo informatico.**

L'anno xxxx, il giorno xx del mese di < …….. >, nell'amministrazione di <*Inserire denominazione completa* > sita in < *inserire indirizzo e CAP* >

<< IL DIRIGENTE >>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che, al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, deve essere riversato su supporti informatici non riscrivibili e deve essere conservato da soggetto diverso dal responsabile del servizio appositamente nominato da ciascuna amministrazione ai sensi dell'art. 7, comma 7 del DPCM 31 0ttobre 2000;

VISTA la determinazione numero xx del gg/mm/aaa relativa alla nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;

CONSIDERATA l'esigenza di conservare in luogo sicuro le copie del registro di protocollo che quotidianamente vengono generate dal sistema informativo di protocollo;

RITENUTO di individuare nel/nella signor/signora < *inserire nome e titolo amministrativo*>, in servizio presso l'Ufficio Utente < *inserire nome* >, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o digitali) da conservare, dei quale tiene evidenza;
- organizzare, conseguentemente, il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
- archiviare e rendere disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
  - descrizione del contenuto dell'insieme dei documenti;

  - estremi identificativi del responsabile della conservazione;
  - estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
  - indicazione delle copie di sicurezza;
- mantenere e rendere accessibile un archivio del software dei sistemi operativi e dei programmi in gestione nelle eventuali diverse versioni per la leggibilità dei documenti conservati;
- verificare la corretta funzionalità del sistema e dei programmi in gestione;
- adottare, su indicazione del Responsabile del servizio di gestione del protocollo informatico, le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
- richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- definire e documentare le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale sui supporti informativi di propria pertinenza;
- verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

<< DETERMINA >>

3. di nominare il/la signore/a *<inserire nome e titolo amministrativo>*, quale Responsabile della conservazione delle copie di riserva del registro di protocollo informatico con i compiti specificati nelle premesse, ai sensi dell'art. 7, comma 5 del DPCM 31 ottobre 2000.

16.6 ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

NOMINATIVO	TITOLO/RUOLO NELL'AOO	ESTREMI E DESCRIZIONE DELLA DELEGA RICEVUTA

16.7 PIANO FORMATIVO PER IL PERSONALE DELL'AMMINISTRAZIONE PER L'ANNO 200X

Esempio di pianificazione della formazione

- ***Alternativa 1***
  Amministrazione < *Inserire nome* >

  Tenute presenti le disponibilità di bilancio, in relazione anche al combinato disposto dell'art. 2 del CCNL 31 marzo 1999 e dell'art. 4 del CCNL 1 aprile 1999, nella impossibilità di organizzare autonomi corsi, è favorita l'adesione a corsi di formazione gratuiti organizzati, per il personale dei servizi informatici e per quello impegnato nelle attività di registrazione del protocollo, dalle amministrazioni centrali o territoriali.

- ***Alternativa 1***
  Amministrazione < *Inserire nome* >
  Area Organizzativa Omogenea < *Inserire nome* >

PER IL PERSONALE DELL'AREA ORGANIZZATIVA OMOGENEA RICHIAMATA I PIANI FORMATIVI PREVISTI SONO QUELLI STESSI DEFINITI CON NOTA DEL GG/MM/AAAA, PROTOCOLLO XXXXXXX, AVENTE AD OGGETTO: ……..., PER IL MINISTRO DELLA FUNZIONE PUBBLICA SULLA FORMAZIONE E LA VALORIZZAZIONE DEL PERSONALE DELLE PUBBLICHE AMMINISTRAZIONI, QUI DI SEGUITO RICHIAMATI:

16.8 PIANO DI ELIMINAZIONE DEI PROTOCOLLI DIVERSI DAL PROTOCOLLO INFORMATICO

Il seguente elenco di registri di protocollo diversi dal registro di protocollo informatico è il risultato di un censimento preliminare dei diversi registri di protocollo in uso presso l'amministrazione.

I seguenti elenchi sono riportati a titolo esemplificativo

16.8.1 ELENCO DEI PROTOCOLLI INTERNI ELIMINATI IN AMBITO COMUNALE

- Registro di protocollo interno presso l'Ufficio di Polizia municipale;
- Registro di protocollo interno presso l'Ufficio Patrimonio.

16.8.2 ELENCO DEI PROTOCOLLI INTERNI ELIMINATI IN AMBITO PROVINCIALE

- Area Risorse e Organizzazione
- Servizio Risorse finanziarie
- Servizio UOA Economato
- Servizio Sviluppo organizzativo
- Area Ricerca e Sviluppo – Progetti speciali
  – Servizio Turismo Attività culturali

– Servizio Innovazione Supp. Marketing e Comunicazione

- Area Programmazione territoriale – Infrastrutture – Ambiente

– Servizio territoriale - Urbanistica – Trasporti

– Servizio Ambiente

– Supporto alla Pianificazione e alla Progettazione

- Area Attività economiche – Politiche formative e del lavoro
- Servizio Attività produttive – Mercato del Lavoro – Scuola – Formazione (utilizza lo stesso protocollo interno dell'Area)

– Servizio Agricoltura

– Rete agrometeorologica

- Segreteria del Consiglio
- Ufficio Affari istituzionali – Legale – Contratti
- Gabinetto di Presidenza
- Supporto Politiche socio-sanitarie
- Servizio Polizia provinciale – Vigilanza – Caccia e Pesca – Protezione civile
- Direttore generale
- Segretario generale
- Presidente
- Presidente del Consiglio provinciale
- Assessore [...]
- Centri per l'Impiego
- Ufficio Collocamento obbligatorio

16.9 POLITICHE DI SICUREZZA

16.9.1 POLITICHE ACCETTABILI DI USO DEL SISTEMA INFORMATIVO

16.9.1.1 Premessa

1. 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.
2. 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.

3. 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.

16.9.1.2 Scopo

1. Lo scopo di queste politiche è sottolineare l'uso accettabile del sistema informatico dell'Amministrazione.
2. Le regole sono illustrate per proteggere gli impiegati e l'Amministrazione.
3. 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.

16.9.1.3 Ambito di applicazione

1. Queste politiche si applicano a tutti gli impiegati dell'Amministrazione, al personale esterno (consulenti, personale a tempo determinato, ...) e agli impiegati della/e ditta/e < *inserire nome* > , includendo tutto il personale affiliato con terze parti.
2. Queste politiche si applicano a tutti gli apparati che sono di proprietà dell'Amministrazione o "affittate" da questa.

16.9.1.4 Politiche – Uso generale e proprietà

1. 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.
2. 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.
3. Le singole aree o settori o Divisioni o Direzioni, sono responsabili della creazione di linee guida per l'uso personale di Internet/Intranet/Extranet. In caso di assenza di tali politiche gli impiegati dovrebbero essere guidati dalle politiche generali dell'Amministrazione e in caso di incertezza, dovrebbero consultare il loro Dirigente.
4. 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.
5. 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.

16.9.1.5 Politiche - Sicurezza e proprietà dell'informazione

1. 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.

2. 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 quattro mesi, ad eccezione di coloro che trattano dati personali sensibili o giudiziari per i quali il periodo si riduce a tre mesi.
3. 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.
4. Uso delle tecniche e della modalità di cifratura dei file coerentemente a quanto descritto in materia di confidenzialità dall'Amministrazione.
5. Poiché le informazioni archiviate nei PC portatili sono particolarmente vulnerabili su essi dovrebbero essere esercitate particolari attenzioni.
6. Eventuali attività di scambio di opinioni del personale dell'Amministrazione all'interno di "new 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.
7. 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.
8. 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.
9. 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.

16.9.2 POLITICHE - ANTIVIRUS

16.9.2.1 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.

16.9.2.2 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.

16.9.2.3 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.

16.9.2.4 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 RSP stabilisce le protezioni software da adottare sulla base dell'evoluzione delle tecnologie disponibili sul mercato.

16.9.2.5 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.

16.9.3 POLITICHE - USO NON ACCETTABILE

1. 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).

2. In nessun caso o circostanza il personale è autorizzato a compiere attività illegali utilizzando le risorse di proprietà dell'Amministrazione.
3. 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.

16.9.3.1 Attività di rete e di sistema

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. 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.
2. 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.
3. È rigorosamente proibita l'esportazione di software, informazioni tecniche, tecnologia o software di cifratura, in violazione delle leggi nazionali ed internazionali.
4. Introduzione di programmi maliziosi nella rete o nei sistemi dell'Amministrazione.
5. 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.
6. 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.
7. Effettuare offerte fraudolente di prodotti, articoli o servizi originati da sistemi dell'Amministrazione con l'aggravante dell'uso di credenziali fornite dall'Amministrazione stessa.
8. Effettuare affermazioni di garanzie, implicite o esplicite, a favore di terzi ad eccezione di quelle stabilite nell'ambito dei compiti assegnati.
9. 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:
   a. accessi illeciti ai dati per i quali non si è ricevuta regolare autorizzazione,
   b. attività di "sniffing";
   c. disturbo della trasmissione;
   d. spoofing dei pacchetti;
   e. negazione del servizio;
   f. le modifiche delle mappe di instradamento dei pacchetti per scopi illeciti;

g. attività di scansione delle porte o del sistema di sicurezza è espressamente proibito salvo deroghe specifiche.

10. Eseguire qualsiasi forma di monitor di rete per intercettare i dati in transito.
11. Aggirare il sistema di autenticazione o di sicurezza della rete, dei server e delle applicazioni.
12. Interferire o negare l'accesso ai servizi di ogni altro utente abilitato.
13. 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.
14. Fornire informazioni o liste di impiegati a terze parti esterne all'Amministrazione.

16.9.3.2 Attività di messaggistica e comunicazione

Le attività seguenti sono rigorosamente proibite senza nessuna eccezione.

1. 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).
2. Ogni forma di molestia via e-mail o telefonica o con altri mezzi, linguaggio, durata, frequenza o dimensione del messaggio.
3. Uso non autorizzato delle informazioni della testata delle e-mail,
4. Sollecitare messaggi di risposta a ciascun messaggio inviato con l'intento di disturbare o collezionare copie.
5. Uso di messaggi non sollecitati originati dalla Intranet per altri soggetti terzi per pubblicizzare servizi erogati dall'Amministrazione e fruibili via Intranet stessa.
6. Invio di messaggi non legati alla missione dell'Amministrazione ad un grande numero di destinatari utenti di news group (news group spam).

16.9.4 LINEE TELEFONICHE COMMUTATE (ANALOGICHE E DIGITALI)

16.9.4.1 Scopo

1. Di seguito vengono illustrate le linee guida per un uso corretto delle linee telefoniche commutate (analogiche convenzionali) e digitali (ISDN, ADSL).
2. Queste politiche coprono due diversi usi distinti: linee dedicate esclusivamente ai telefax e linee di collegamento alle risorse elaborative dell'Amministrazione.

16.9.4.2 Ambito di applicazione

1. 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.

16.9.4.3 Politiche – Scenari di impatto sull'Amministrazione

1. Esistono due importanti scenari che caratterizzano un cattivo uso delle linee di comunicazione che tentiamo di tutelare attraverso queste politiche.
2. 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.
3. 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.

16.9.4.4 Politiche – Telefax

1. 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;
2. Le postazioni di lavoro che sono capaci di inviare e ricevere fax non devono essere utilizzate per svolgere questa funzione.
3. 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.

16.9.4.5 Politiche – Collegamento di PC alle linee telefoniche analogiche

1. La politica generale è quella di non approvare i collegamenti diretti dei PC alle linee telefoniche commutate.
2. 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.

16.9.4.6 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.

16.9.5 POLITICHE PER L'INOLTRO AUTOMATICO DI MESSAGGI DI POSTA ELETTRONICA

16.9.5.1 Scopo

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

16.9.5.2 Ambito di applicazione

1. 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.

16.9.5.3 Politiche

1. 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.
2. 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.

16.9.6 POLITICHE PER LE CONNESSIONI IN INGRESSO SU RETE COMMUTATA

16.9.6.1 Scopo

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

16.9.6.2 Ambito di applicazione

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

16.9.6.3 Politiche

1. 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 sfida/risposta (challenger/response).
2. 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.

3. 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.
4. 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.

16.9.7 POLITICHE PER L'USO DELLA POSTA ISTITUZIONALE DELL'AMMINISTRAZIONE

16.9.7.1 Scopo

1. 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.

16.9.7.2 Ambito di applicazione

1. 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.

16.9.7.3 Politiche – Usi proibiti

1. 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.

16.9.7.4 Politiche – Uso personale

- ***Alternativa 1***
  1. 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.
  2. Il personale dell'Amministrazione, nel rispetto dei principi della privacy, non avrà controlli sui dati archiviati a titolo personale, ricevuti o trasmessi.
  3. 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.

- ***Alternativa 2***

4. Non è ammesso l'uso della posta istituzionale per usi personali e, in ogni caso, non si deve dare seguito a catene di lettere o messaggi scherzosi, di disturbo o di altro genere.

16.9.8 POLITICHE PER LE COMUNICAZIONI WIRELESS

16.9.8.1 Scopo

1. Queste politiche proibiscono l'accesso alla rete dell'Amministrazione via rete wireless insicura.
2. 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.

16.9.8.2 Ambito di applicazione

1. 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.
2. Dispositivi wireless e/o reti senza connettività alla Intranet dell'Amministrazione, sono esclusi da queste politiche.

16.9.8.3 Politiche – Registrazione delle schede di accesso

1. Tutti i "punti di accesso" o le "stazioni base" collegati alla Intranet devono essere registrati e approvati dal responsabile della sicurezza.
2. 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.

16.9.8.4 Politiche – Approvazione delle tecnologie

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

16.10. SOTTOSCRIZIONE DEI DOCUMENTI FORMATI DALL'AOO

16.10.1 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

16.10.2 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

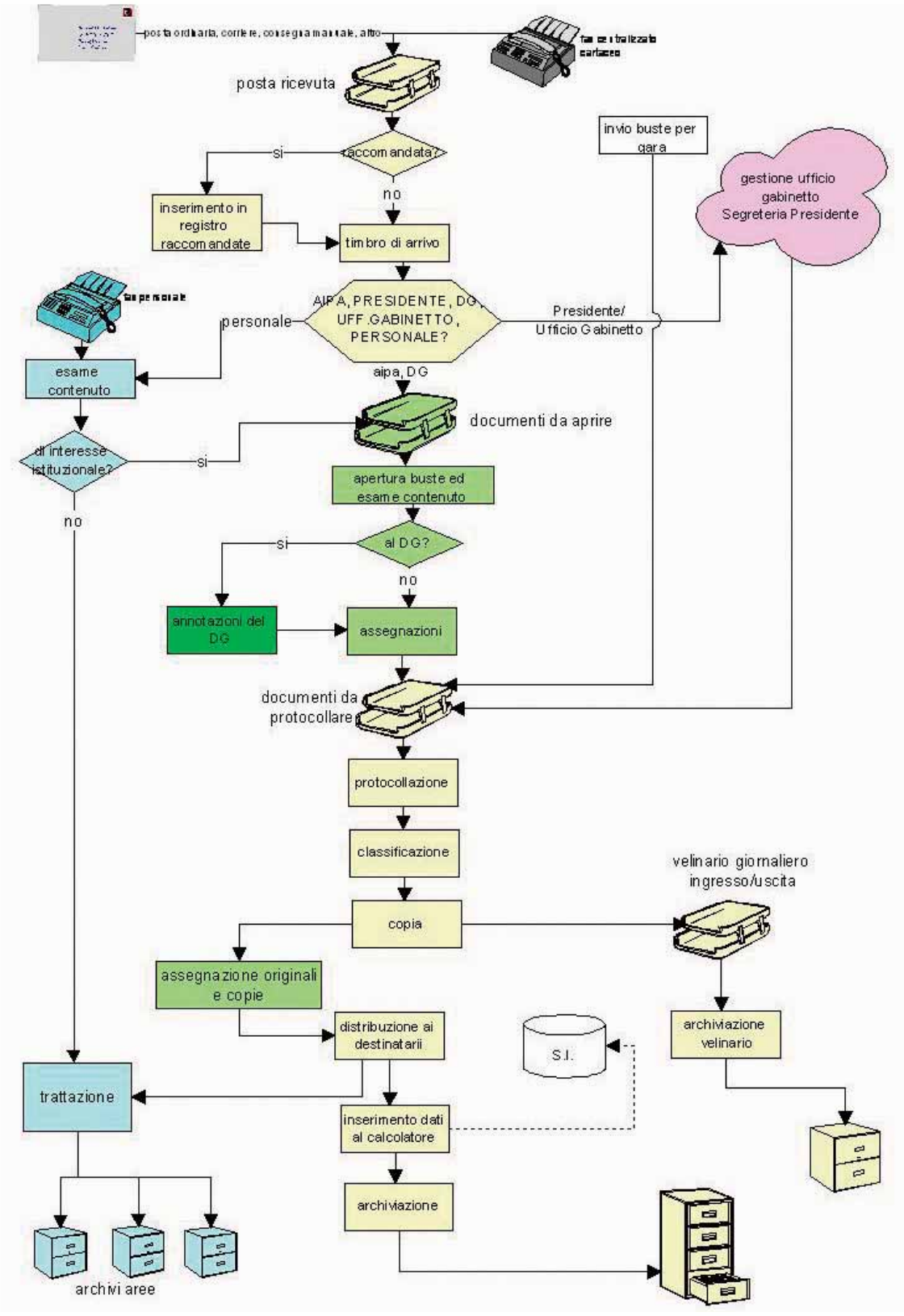
- Verifiche condizioni sociali utenti
- Rilascio nulla osta obiettori
- Aggiornamento carichi di lavoro
- Comunicazioni per ordinativi incassi
- Richieste rimborsi
- Comunicazioni per pagamenti aree PEEP
- Comunicazioni pagamenti per attività estrattive
- Predisposizione schema contratti di locazione
- 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 C.I.
- 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.

16.10.3 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

16.11 DESCRIZIONE DEI FLUSSI DEI DOCUMENTI INFORMALI ALL'INTERNO DELL'AOO

Esempio di descrizione dei flussi



16.12 REGOLE DI RACCOLTA E CONSEGNA DELLA CORRISPONDENZA CONVENZIONALE AL SERVIZIO POSTALE NAZIONALE

1. La corrispondenza viene quotidianamente raccolta dal servizio postale pubblico dal personale dell'Ufficio Posta della UOP dell'Amministrazione/AOO alle ore xx. di ogni giorno;
2. La corrispondenza da inviare, lettere ordinarie e raccomandate o assicurate, o… viene consegnata in busta chiusa al servizio postale pubblico alle ore xx. (o in alternativa, in occasione della raccolta della corrispondenza) di ogni giorno;
3. 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 xx,xx di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta.

16.13 MODULO DI CONSULTAZIONE DELLA SEZIONE DI DEPOSITO E STORICA DELL'ARCHIVIO

All'Amministrazione < *inserire nome* >
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: .....
.....

< *Città sede dell'Amministrazione* >, lì .....
L'OPERATORE RICEVENTE: .....
IL RESPONSABILE DELL'ARCHIVIO: .....

16.14 NOMINA DEL RESPONSABILE DEL SERVIZIO ARCHIVISTICO

Esempio di nomina

Determinazione n. xx del gg/mm/aaaa

Registro generale n.

Oggetto: **Nomina del Responsabile del Servizio archivistico**

L'anno xxxx, il giorno xx del mese di < …….. >, nell'amministrazione di < *Inserire denominazione completa* > sita in < *inserire indirizzo e CAP* >

<< IL DIRIGENTE...>>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che il sistema di gestione informatica dei documenti deve garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato, art. 52, comma 1 lettera f) del testo unico;
CONSIDERATO inoltre la materia trattata richiede conoscenze e competenze specifiche;
VISTA la determinazione numero xx del gg/mm/aaaa relativa alla nomina del Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi;

RITENUTO di individuare nel/nella signor/signora < *inserire nome e titolo amministrativo* >, in servizio presso l'Ufficio Utente < *inserire nome* >, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- collaborare con il Responsabile del servizio per la tenuta del protocollo e la gestione documentale per:
  - predisporre lo schema del Manuale di gestione,
  - stabilire i criteri minimi di sicurezza informatica del sistema,
  - organizzare il sistema di gestione dei flussi documentali e la classificazione dei documenti, lo smistamento e l'assegnazione dei documenti alle UOR (sulla scorta dell'organigramma dell'Amministrazione), la costituzione e la repertoriazione

dei fascicoli, l'individuazione dei responsabili della conservazione dei documenti e dei fascicoli nella fase corrente,

- stabilire i livelli di accesso ai documenti archivistici e regolamentare le forme di consultazione interna ed esterna dell'archivio, nel rispetto della normativa sulla tutela della riservatezza dei dati personali, con particolare riferimento all'allegato "A.2 Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" del d. lgs. 196/03;

- organizzare la fase di versamento dei documenti dagli uffici all'Archivio generale, insieme con gli strumenti di corredo, e predisporre l'elenco dei fascicoli e delle serie ricevute;
- curare e garantire la conservazione dell'archivio nella fase di deposito;
- predisporre il piano di conservazione dei documenti, prescritto dal DPR 445/2000, art. 68;
- predisporre il massimario di scarto;
- effettuare la selezione periodica dei documenti e procedere allo scarto o al trasferimento nella separata sezione d'archivio del materiale destinato alla conservazione permanente.

<< DETERMINA >>

4. di nominare il/la signore/a < *inserire nome e titolo amministrativo* >, quale Responsabile del Servizio archivistico con i compiti specificati nelle premesse.

16.15 NOMINA DEL RESPONSABILE DELLA CONSERVAZIONE SOSTITUTIVA

Esempio di nomina

Determinazione n. xx del gg/mm/aaaa

Registro generale n.

Oggetto: **Nomina del Responsabile del Servizio di conservazione sostitutiva**

L'anno xxxx, il giorno xx del mese di < …….. >, nell'amministrazione di < *Inserire denominazione completa* > sita in < *inserire indirizzo e CAP* >

<< IL DIRIGENTE...>>

PREMESSO che il decreto del Presidente della Repubblica 28 dicembre 2000 n. 445 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa" pone l'obiettivo della razionalizzazione della gestione di flussi documentali coordinata con la gestione di procedimenti amministrativi da parte delle pubbliche amministrazioni, al fine di migliorare i servizi e potenziare supporti conoscitivi delle stesse secondo i criteri di economicità, efficacia e trasparenza dell'azione amministrativa;

CONSIDERATO che il sistema di gestione informatica dei documenti deve garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalla normativa corrente, ovvero altri formati non proprietari;

VISTO l'art. 62 comma 1 del DPR n. 445/2000 concernente le procedure di salvataggio e conservazione delle informazioni del sistema di gestione elettronica dei documenti;

VISTA la determinazione numero xx del gg/mm/aaaa relativa alla nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;

CONSIDERATO che Il Responsabile sopra richiamato intende delegare le attività operative di conservazione sostitutiva dei documenti digitali dell'Amministrazione/AOO a soggetto diverso da se medesimo;

RITENUTO di individuare nel/nella signor/signora < *inserire nome e titolo amministrativo* >, in carico presso l'Ufficio Utente < *inserire nome* >, la figura professionale più idonea ad espletare i compiti di seguito indicati:

- rendere le informazioni trasferite sempre consultabili;
- provvedere alla conservazione degli strumenti hardware e software atti a garantire la consultabilità dei documenti conservati;
- eseguire, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici rimovibili.

<< DETERMINA >>

di nominare il/la signore/a < *inserire nome e titolo amministrativo* >, quale Responsabile del Servizio di conservazione sostitutiva con i compiti assegnati nelle premesse.
Il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, mantiene la responsabilità della corretta esecuzione delle operazioni.

16.16 ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

16.16.1 ELENCO VALIDO PER QUALSIASI AMMINISTRAZIONE

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 accompagnati da lettera di trasmissione
- Certificati e affini
- Documentazione già soggetta, direttamente o indirettamente, a registrazione particolare (es. fatture, vaglia, assegni)

16.16.2 ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE IN AMBITO COMUNALE

- 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 di avvenuta notifica

16.16.3 ELENCO DEI DOCUMENTI ESCLUSI DALLA PROTOCOLLAZIONE IN AMBITO UNIVERSITARIO

- Atti preparatori interni
- Certificazioni non meccanizzate
- Certificati di servizio personale docente di ruolo e non di ruolo
- Certificati di servizio personale tecnico amministrativo (a tempo determinato o indeterminato, CEL)
- Certificati situazioni retributive e contributive personale strutturato e non strutturato
- Certificazioni studenti
- Estratti conto bancario
- Report (o registro) delle presenze
- Visite fiscali (si protocollano solo quelle "sfavorevoli" al dipendente, ad es. per assenza)
- Trasferimento sede legale – comunicazione
- Cambio banca – comunicazioni
- Lettere di accompagnamento di fatture
- Progetti formativi e di orientamento – stage
- Richiesta conferma conseguimento titolo di studio
- Restituzioni dei buoni mensa da parte dei ristoratori o ditte convenzionate
- 730 corrispondenza e modelli (come sopra)
- Avvisi di pagamento – comunicazioni di bonifici bancari
- Avviso di vacanza presso altri atenei (bando in Internet)
- Bandi di altri atenei di selezione per assegni per la collaborazione ad attività di ricerca
- Convocazioni dei CCL e dei CDF

16.17 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

Per i procedimenti amministrativi o gli affari per i quali si renda necessaria la riservatezza delle informazioni o il differimento dei termini di accesso, è previsto 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.

16.17.1 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE PER TUTTE LE AMMINISTRAZIONI

- 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.

16.17.2 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE IN AMBITO SANITARIO

- Espianto d'organo (registro tenuto presso la Direzione medica di presidio);
- Denunce di:
  - morsicatura;
  - malattie infettive;
  - morte traumatica;
- Denunce di nascita (registro tenuto presso il Centro di nascita Dipartimento materno infantile);
- Domande di concorso, stati di servizio e di frequenza, denunce infortuni (vengono protocollati dall'Ambito Risorse umane);
- Collegio sindacale (registro tenuto presso la Segreteria dell'Ambito Bilancio);
- Contratti;
- Buoni d'ordine;
- Deliberazioni del Direttore generale;
- Verbali di gara o contratti redatti in forma pubblica;
- Disposizioni dei Direttori di UU.OO. amministrative.

16.17.3 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE IN AMBITO PROVINCIALE

- Deliberazioni di Giunta e Consiglio;
- Determinazioni organizzative;
- Decreti;
- Ordinanze;
- Contratti;
- Richieste e rilascio autorizzazioni e permessi per transiti eccezionali;
- Verbali di infrazione alle Leggi di caccia, pesca, codice della strada redatti da Agenti di Polizia provinciale;
- Rilascio licenze per autotrasporto di merci in conto proprio;
- Registro tenuta Albo provinciale degli autotrasportatori di cose per conto di terzi;
- Buoni d'ordine;
- Documenti che rientrano nel Sistema Informativo Lavoro utilizzato a livello nazionale.

16.17.4 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE IN AMBITO COMUNALE

- **UOR - Affari generali ed istituzionali**
  - Atti rogati o autenticati dal segretario comunale (registrazione informatica e cartacea);
  - Contratti e convenzioni (registrazione informatica e cartacea);
  - Verbali delle adunanze del Consiglio comunale (registrazione informatica);
  - Verbali delle adunanze della Giunta comunale (registrazione informatica);
  - Verbali degli organi collegiali del Comune (registrazione informatica);
  - Autorizzazioni commerciali (registrazione cartacea);
  - Autorizzazioni artigiane (registrazione cartacea);
  - Autorizzazioni turistiche (registrazione cartacea);
  - Autorizzazioni di pubblica sicurezza (registrazione cartacea);
  - Autorizzazioni di polizia mortuaria (registrazione informatica);
  - Autorizzazioni igienico-sanitaria e veterinaria (registrazione cartacea);
  - Licenze di pesca (registrazione cartacea);
  - Certificati di iscrizione all'anagrafe canina;
  - Atti di stato civile (registrazione informatica);
  - Pubblicazioni di matrimonio (registrazione informatica);
  - Carte d'identità (registrazione informatica);
  - Certificati anagrafici;
  - Tessere elettorali (registrazione informatica);
  - Rapporti incidenti (registrazione informatica);
  - Verbali oggetti smarriti;
  - Verbali CdS (registrazione informatica);
  - Richieste permessi transito ZTL.
- **UOR - Affari generali ed istituzionali**
  - Fatture attive (registrazione informatica);
  - Liquidazioni (registrazione informatica);
  - Mandati di pagamento (registrazione informatica);
  - Reversali (registrazione informatica);
  - Dichiarazioni ICI (registrazione informatica).
- **UOR – Polizia municipale**
  - Registro verbali di violazione regolamenti e leggi varie;
  - Fatture emesse registri IVA;
  - Autorizzazioni sanitarie registro autorizzazioni sanitarie;
  - Autorizzazioni commerciali registro autorizzazioni commerciali;
  - Autorizzazioni di pubblico esercizio registro autorizzazioni di pubblico;

- I verbali di violazione del Codice della strada ed i verbali di violazioni amministrative.

- **UOR - Affari culturali, educativi e sociali**
  - Dichiarazioni per la certificazione ISEE – Riccometro (registrazione cartacea)

- **Altri documenti**
  - Deliberazioni di Consiglio comunale registro delle deliberazioni del consiglio comunale;
  - Deliberazioni di Giunta comunale registro delle deliberazioni della giunta comunale;
  - Determinazioni dei responsabili dei servizi registro delle determinazioni;
  - Decreti protocollati al protocollo generale;
  - Ordinanze registro delle ordinanze;
  - Contratti in forma pubblica;
  - 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.

16.18 PIANO DI CONSERVAZIONE

16.18.1 PIANO DI CONSERVAZIONE APPLICATO IN AMBITO COMUNALE

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

16.18.1.1 Documentazione da conservare senza limiti di tempo

- Atti delle Commissioni elettorali mandamentali concernenti la presentazione delle candidature;
- Atti e documenti del contenzioso legale;

- Atti relativi ai lavori pubblici, eseguiti e non eseguiti, limitatamente a originali dei progetti e dei loro allegati, perizie di spesa, libri delle misure;
- Bilanci e consuntivi originali (o nell'unica copia esistente);
- Contratti;
- Corrispondenza generale del servizio esattoria e tesoreria;
- Corrispondenza, salvo quanto indicato nella seconda parte;
- Deliberazioni destinate a formare la raccolta ufficiale del Consiglio e della Giunta;
- Documentazione generale per la richiesta di mutui, anche estinti;
- Elenchi dei poveri;
- Fascicoli degli amministratori e dei membri delle commissioni;
- Fascicoli del personale in servizio e in quiescenza, di ruolo e non di ruolo;
- Inventari dei beni mobili e immobili del Comune;
- Inventari, schedari, rubriche e repertori dell'archivio, libretti o schede di trasmissione di carte tra i vari uffici, anche non più in uso;
- Libri contabili obbligatori in base alle leggi fiscali;
- Libri infortuni o documentazione equivalente;
- Libri mastri, libri giornale, verbali di chiusura dell'esercizio finanziario;
- Liste di leva e dei renitenti;
- Ordinanze e circolari del Comune;
- Originali dei verbali delle Commissioni di concorso;
- Piani commerciali, licenze e autorizzazioni amministrative all'esercizio del commercio fisso;
- Piani regolatori generali e particolareggiati; piani delle lottizzazioni; regolamenti edilizi; licenze, concessioni e autorizzazioni edilizie;
- Posizioni previdenziali, stipendiali, tributarie dei dipendenti quando non integralmente conservate nei fascicoli personali;
- Programmi pluriennali di attuazione e piani di suddivisione in lotti delle aree suscettibili di attività estrattiva;
- Protocolli della corrispondenza;
- Qualunque atto o documento per il quale una legge speciale imponga la conservazione illimitata;
- Registri dei verbali e protocolli delle Commissioni comunali;
- Registro della popolazione comprensivo dei fogli di famiglia eliminati, registri e specchi riassuntivi del movimento della popolazione;
- Regolamenti e capitolati d'oneri;
- Rilevazioni di carattere statistico non pubblicate;
- Ruoli delle imposte comunali;
- Ruoli matricolari;
- Ruoli riassuntivi del personale e Libri matricola;

- Tariffe delle imposte di consumo e delle altre tasse riscosse a tariffa;
- Verbali delle aste;
- Verbali delle Commissioni elettorali;
- Verbali di sezione per l'elezione dei consigli comunali e dei consigli circoscrizionali.

16.18.1.2 Documentazione eliminabile dopo cinque anni

- Annotazioni marginali eseguite agli atti di stato civile provenienti da altri comuni e altre assicurazioni di trascrizione relative agli stessi;
- Atti relativi a concorsi a borse di studio e premi (conservando la seguente documentazione: originale degli atti della Commissione o dei comitati, gli eventuali rendiconti speciali, una copia degli stampati e dei manifesti, il registro delle opere esposte in occasione di mostre artistiche e simili);
- Atti relativi alla costituzione e all'arredamento dei seggi (conservando il prospetto delle sezioni e della loro ubicazione);
- Atti relativi alla regolamentazione della propaganda (conservando la documentazione riassuntiva;
- Atti relativi all'orario degli ambulatori;
- Atti relativi all'organizzazione di censimenti;
- Atti rimessi da altri Enti per l'affissione all'albo;
- Atti rimessi da altri Enti per notifiche;
- Autorizzazioni all'uso di impianti culturali e sportivi (conservando eventuali atti riassuntivi);
- Avvisi di convocazione delle Commissioni;
- Bollettari di prelevamento oggetti dall'Economato;
- Bollettari di ricevute dell'esattoria;
- Brogliacci di viaggio degli automezzi comunali;
- Carteggi per la richiesta di atti notori e di certificati diversi con eventuale copia degli stessi;
- Carteggio interlocutorio per la concessione in uso di locali e oggetti di proprietà comunale;
- Carteggio relativo alla contabilità per registri di stato civile (conservando le fatture per dieci anni);
- Certificazioni per richieste ai fini della fruizione di assegni di studio;
- Circolari per l'orario degli uffici e per il funzionamento degli uffici;
- Comunicazioni relative a variazioni anagrafiche;
- Consiglio regionale e provinciale - Carteggio con gli uffici militari per aggiornamento di ruoli;
- Consiglio regionale e provinciale - Carteggio tra comuni per l'aggiornamento dei ruoli matricolari;
- Consiglio regionale e provinciale - Matrici di richieste di congedi anticipati;

- Consiglio regionale e provinciale - Verbali dell'Ufficio centrale circoscrizionale relativi al completamento delle operazioni elettorali;
- Consiglio regionale e provinciale - Verbali sezionali privi di allegati (comunque non prima della decisione di eventuali ricorsi);
- Conto dell'Economato (conservando eventuali prospetti generali);
- Copia di deliberazioni per liquidazione indennità alla Commissione elettorale mandamentale e ad altre commissioni non comunali;
- Copia di delibere per pagamento di gettoni di presenza ai partecipanti alle commissioni;
- Copia di lettere di trasmissione di denunce di malattie infettive;
- Copie degli elenchi dei buoni libro concessi e documentazione di supporto (conservando l'elenco dei percipienti ed eventuali relazioni o rendiconti speciali; eventuali fatture dovranno essere conservate per dieci anni);
- Copie degli inviti agli utenti convocati per la verifica biennale dei pesi e delle misure o per altri adempimenti;
- Copie delle comunicazioni delle sezioni relative ai dati parziali sul numero dei votanti (conservando eventualmente la copia dei fonogrammi trasmessi per l'insieme delle sezioni);
- Copie di attestati di servizio;
- Copie di atti giudiziari notificati dal Comune;
- Copie di atti notori;
- Copie di deliberazioni per contributi assistenziali diversi (conservando le richieste o le proposte);
- Copie di deliberazioni per contributi ad enti e associazioni diverse (conservando le richieste);
- Copie di delibere di liquidazione di contributi per concerti, attività culturali, biblioteca comunale, biblioteche scolastiche (conservando la corrispondenza o la richiesta, una copia dei programmi e dei manifesti e gli elenchi dei libri forniti);
- Copie di delibere di liquidazioni dei compensi al personale straordinario per corsi serali e carteggio transitorio sui corsi (conservando gli atti di interesse per il personale che ha prestato servizio e relazioni finali, programmi di spesa, altri documenti riassuntivi);
- Copie di istruzioni a stampa (conservandone una per ciascuna elezione);
- Copie e minute dei progetti, sia realizzati che non realizzati;
- Corrispondenza interlocutoria per commemorazioni e solennità civili (conservando carteggi generali per l'organizzazione delle manifestazioni, una copia degli inviti, degli stampati e dei manifesti, gli atti dei comitati, eventuali rendiconti particolari ed eventuali fatture per dieci anni);
- Corrispondenza per la richiesta di licenze di pubblica sicurezza o rilasciate da altri uffici;
- Corrispondenza per la richiesta e la trasmissione di certificati di esito di leva;

- Corrispondenza relativa alla formazione delle schede personali, alle aggiunte o alle cancellazioni dalle liste;
- Delegazioni alla celebrazione di matrimonio in altri comuni;
- Documenti di carico e scarico dei bollettari delle imposte;
- Domande di allacciamento all'acquedotto e richieste di concessione di illuminazione, ove le stesse non facciano fede di contratto (in tal caso saranno eliminabili cinque anni dopo l'esaurimento del contratto);
- Domande di commercianti per deroghe all'orario dei negozi;
- Domande di occupazione temporanea di spazi ed aree pubbliche per fiere, mostre, comizi, feste (conservando quelle relative a concessioni permanenti [p.es. passi carrabili] per quarant'anni ed eventuali registri indefinitamente);
- Domande di partecipazione alla Befana e ad altre elargizioni;
- Domande per la concessione dei libretti di lavoro e libretti restituiti al Comune;
- Domande per la richiesta di certificati, carteggi per la loro trasmissione;
- Domande per pubbliche affissioni (conservando le pratiche che hanno dato luogo a contenzioso);
- Elenchi dei turni di servizio della Polizia municipale (conservando i regolamenti);
- Elezioni dei deputati alla costituente - Verbali degli uffici centrali di circoscrizione concernenti il completamento delle operazioni di votazione;
- Elezioni dei deputati alla costituente - Verbali sezionali con allegati;
- Elezioni della Camera e del Senato - Carteggio relativo alla designazione dei rappresentanti di lista presso gli uffici di sezione, dal 1976;
- Elezioni della Camera e del Senato - Verbali degli uffici centrali di circoscrizione per il completamento delle operazioni;
- Elezioni della Camera e del Senato - Verbali sezionali, privi di allegati;
- Estratti dei verbali dell'Ufficio centrale circoscrizionale relativi al riesame di voti contestati;
- Fascicoli e schede personali dei giudici popolari;
- Fascicoli e schede personali di cittadini cancellati dalle liste per morte o emigrazione;
- Lettere di rifiuto di partecipazione alle aste, offerte di ditte non prescelte;
- Lettere di trasmissione di carte d'identità;
- Lettere di trasmissione di passaporti; autorizzazioni alla richiesta degli stessi;
- Libretti dei veicoli;
- Liste dei giudici popolari;
- Liste sezionali se esistono le liste generali;
- Matrici dei certificati elettorali in bianco e non consegnati;
- Matrici delle proposte di annotazioni marginali inviate alle Procure;
- Matrici di bollettari per acquisto materiali di consumo per l'ufficio tecnico;
- Matrici di buoni di acquisto generi di refezione e comunque di consumo;

- Matrici o copie di comunicazioni anagrafiche ad altri uffici comunali;
- Moduli per l'accertamento al diritto del trasporto gratuito degli alunni (conservando eventuali relazioni riassuntive);
- Note di frequenza, ricevute di pagamento di rette e domande di esonero per scuole materne (conservando gli elenchi dei beneficiati; eventuali fatture dovranno essere conservate per dieci anni);
- Parlamento europeo - Carteggi relativi alle designazioni dei rappresentanti di lista presso gli uffici di sezione (conservando eventualmente la documentazione contenente dati più generali);
- Parlamento europeo - Estratti del verbale dell'Ufficio elettorale provinciale per il riesame delle schede di voti contestati (non prima della decisione c.s.);
- Parlamento europeo - Verbali dell'Ufficio elettorale provinciale per il riesame delle schede di voti contestati (non prima della decisione c.s.);
- Parlamento europeo - Verbali dell'Ufficio provinciale relativi al completamento di operazioni;
- Parlamento europeo - Verbali sezionali privi di allegati (non prima della decisione di eventuali ricorsi previsti dagli artt. 42 e 43 della L. 24 gennaio 1979, n. 18);
- Prospetti dei lavori eseguiti dai cantonieri;
- Prospetti di carattere pubblicitario, richiesti e non richiesti, preventivi di massima non utilizzati;
- Referendum abrogativi - Carteggio relativo alla designazione dei rappresentanti dei partiti e dei gruppi politici e dei comitati promotori presso le sezioni (conservando eventualmente la documentazione contenente dati generali);
- Referendum abrogativi - Estratti del verbale dell'Ufficio provinciale per il referendum relativo al riesame dei voti contestati e provvisoriamente non assegnati, per ogni sezione;
- Referendum abrogativi - Verbali di completamento dello spoglio delle schede eseguito da parte dell'Ufficio provinciale per il Referendum;
- Referendum abrogativi - Verbali sezionali privi di allegati;
- Referendum istituzionale - Verbali degli uffici centrali circoscrizionali concernenti il completamento delle operazioni di votazione.
- Referendum istituzionale - Verbali sezionali con allegati;
- Registri e bollettari di spese postali;
- Registro di carico e scarico dei bollettari;
- Richiesta di invio di notizie varie relative ai militari (esclusi i periodi bellici);
- Rubriche interne per il calcolo dei congedi e delle aspettative;
- Scadenzari dell'Ufficio elettorale per la compilazione delle liste;
- Schede personali dei giovani compresi nella leva di altri comuni o deceduti prima della stessa;
- Schede personali dei militari da includere nella lista di leva;

- Solleciti di pagamento fatture pervenuti al Comune;
- Stampati e circolari per campagne nazionali di lotta contro le malattie;
- Tabelle provvisorie delle preferenze non costituenti verbale;
- Telegrammi della Prefettura per l'esposizione della bandiera nazionale conservando le ordinanze e gli avvisi del sindaco;
- Verbali di consegna di materiale elettorale; verbali di controllo dei verbali sezionali per l'accertamento che non vi siano fogli in bianco;
- Visite fiscali dei dipendenti comunali e diverse.

16.18.1.3 Documentazione eliminabile dopo sette anni

- Fogli di lavoro straordinario (conservando eventuali prospetti riassuntivi);
- Fogli di presenza dei dipendenti;
- Modelli 740 (copia per il Comune); i sette anni decorrono dall'anno cui si applica la dichiarazione.

16.18.1.4 Documentazione eliminabile dopo dieci anni

- Atti dei concorsi: copie dei verbali della Commissione giudicatrice;
- Atti di liquidazioni di lavoro straordinario per elezioni;
- Atti relativi a liquidazione di spese "a calcolo";
- Atti relativi a liquidazione di spese di rappresentanza;
- Atti relativi al riparto dei diritti di segreteria e stato civile, sanitari e tecnici;
- Atti relativi all'acquisto di autoveicoli e alla loro manutenzione, con dépliant pubblicitari (conservando proposte di spesa, verbali d'asta, contratti);
- Atti relativi all'alienazione di mobili fuori uso e di oggetti vari;
- Atti relativi alle contravvenzioni sanitarie (conservando i registri, se esistenti);
- Autorizzazioni al trasporto di salme fuori del comune;
- Avvisi di pagamento per compartecipazione di imposte erariali a favore del comune;
- Bollettari di riscossione delle imposte di consumo e delle sue contravvenzioni (conservando i registri e i prospetti delle contravvenzioni);
- Bollettari per la riscossione delle contravvenzioni;
- Bollettari per la riscossione dell'imposta sulla pubblicità, pubbliche affissioni e occupazione di suolo pubblico;
- Carteggi di liquidazione delle missioni ai dipendenti e agli amministratori, con relative tabelle di missione e documentazione allegata, salvo, se esistenti, prospetti generali;
- Carteggi di ordinaria e straordinaria manutenzione delle scuole (conservando proposte di spesa, contratti, verbali d'asta e progetti originali);
- Carteggi per acquisto di vestiario per specifiche categorie di dipendenti (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per acquisto di attrezzature varie, di mobili e di materiale di cancelleria e pulizia per uffici (conservando proposte di spesa, verbali d'asta e contratti);

- Carteggi per acquisto di macchine d'ufficio e di materiale per la loro manutenzione e per la cancelleria (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per la fornitura di combustibile per riscaldamento (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per l'acquisto di carburante per gli automezzi (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi per l'acquisto di materiali per l'Ufficio tecnico e il magazzino comunale (conservando proposte di spesa, verbali d'asta, contratti);
- Carteggi per l'organizzazione della leva, locali e arredamento, materiali, cancelleria (conservando i contratti relativi a forniture);
- Carteggi per pulizia di locali (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi relativi a ordinaria e straordinaria manutenzione di sedi di uffici giudiziari o carceri, (conservando proposte di spesa, progetti originali, verbali d'asta e contratti);
- Carteggi relativi a sottoscrizione di abbonamenti a giornali e riviste e ad acquisto di pubblicazioni amministrative;
- Carteggi relativi all'acquisto di materiali di consumo (conservando proposte di spesa, verbali d'asta e contratti);
- Carteggi relativi all'acquisto di materiali per illuminazione pubblica, segnaletica stradale, manutenzione di giardini, piazze, vie, argini dei fiumi, fognature;
- Carteggio interlocutorio e copia di atti per mutui estinti ed accettazioni di eredità;
- Carteggio interlocutorio relativo alle associazioni di comuni;
- Carteggio vario transitorio con le farmacie comunali;
- Cartelle personali dei contribuenti cessati (conservando i ruoli);
- Cartellini delle carte d'identità scadute e carte scadute e restituite al Comune (caso per caso, i carteggi ad esso relativi);
- Copie dei mandati e delle reversali e dei loro allegati;
- Copie dei preventivi e dei consuntivi (conservando il progetto del bilancio);
- Copie di atti per lavori ai cimiteri (conservando l'originale del progetto, i verbali d'asta, i contratti, il conto finale dei lavori e tutti i documenti originali);
- Copie di avvisi per esumazione di salme nei cimiteri (conservando per almeno 40 anni il registro delle lettere spedite e degli avvisi consegnati);
- Corrispondenza relativa al personale del Consiglio e delle Commissioni e alla liquidazione dei loro compensi;
- Denunce mediche di malattie contagiose a carattere non epidemico se trasmesse ad altri uffici;
- Domande di ammissione a colonie;
- Domande di concessione di sussidi straordinari;
- Domande di iscrizione all'elenco dei poveri (conservando l'elenco);

- Domande di partecipazione (conservando per 40 anni i diplomi originali di studio e/o i documenti militari); copie di manifesti inviate ad altri enti e restituite; elaborati scritti e pratici; copie di avvisi diversi; copie di delibere;
- Domande e certificazioni di ditte per essere incluse nell'Albo degli appaltatori comunali;
- Fatture liquidate;
- Inviti alle sedute del Consiglio e della Giunta (conservando gli ordini del giorno con elenco dei destinatari, i fascicoli delle interpellanze ed eventuali progetti e relazioni); mancanza di questi, le loro copie;
- Matrici dei permessi di seppellimento;
- Matrici delle imposte;
- Ordini di sequestro di medicinali in commercio eseguiti su direttive superiori;
- Registri delle riscossioni dei diritti di segreteria e stato civile (conservando eventuali prospetti riassuntivi annuali);
- Richieste di informazioni da parte di ospedali ed enti assistenziali;
- Schedari delle imposte;
- Stati di avanzamento di lavori pubblici;
- Verbali delle contravvenzioni di polizia (conservando i registri);
- Verbali di interramento di animali inadatti all'alimentazione;
- Verbali sezionali dei referendum abrogativi;
- Verifiche di cassa dell'imposta di consumo e registro di carico e scarico dei suoi bollettari;

16.18.1.5 Documentazione eliminabile dopo quarant'anni

- Diplomi originali di studio o militari conservati nella documentazione relativa ai concorsi, eventualmente eliminabili prima dei quarant'anni previa emanazione di un'ordinanza con intimazione al ritiro;
- Domande relative a concessioni permanenti;
- Registri degli atti notificati per altri uffici;
- Registro delle lettere spedite agli eredi per esumazione di salme nei cimiteri;
- Matricole delle imposte;

16.18.1.6 Documentazione eliminabile dopo cinquant'anni

- Mandati di pagamento e riscossione (comprese le eventuali fatture e le cosiddette "pezze d'appoggio", ma conservando l'eventuale carteggio originale come relazioni, perizie, ecc. che talvolta è rimasto allegato al mandato).

16.18.2 PRONTUARIO DI SELEZIONE PER GLI ARCHIVI DELLE AZIENDE SANITARIE LOCALI E DELLE AZIENDE OSPEDALIERE

http://www.archivi.beniculturali.it/divisione_III/prontuarioscarto2005.htm

16.19 TITOLARIO DI CLASSIFICAZIONE

Di seguito vengono riportati alcuni **esempi di titolari** destinati a pubbliche amministrazioni.
L'illustrazione non vuole essere completa o esaustiva, ma vuole essere solo una guida alle amministrazioni che devono perfezionare il loro titolario di classificazione da riportare nel proprio Manuale.
Allo scopo di rendere disponibili le versioni sempre aggiornate e/o pubblicate dalla Direzione generale degli Archivi di Stato, anziché riportare di seguito i citati titolari, viene fornito il *link* al sito ufficiale della predetta Direzione dove sono pubblicate:

http://www.archivi.beniculturali.it/divisione_III/comuni/interventi.html

Altri titolari:

- Titolario delle camere di Commercio definito dal Comitato tecnico scientifico per gli archivi delle Camere di commercio - Sottocommissione per la revisione del titolario d'archivio:
  http://www.camerecultura.it/index.pdf

16.20 MODELLO DI "CAMICIA" DEL FASCICOLO

< All'interno del presente allegato ogni Amministrazione/AOO, riporta il proprio modello di Fascicolo >

16.21 REPERTORI GENERALI

Esempio di repertori generali presenti nelle Amministrazioni comunali

REPERTORI DI DOCUMENTI IN DOPPIO ESEMPLARE

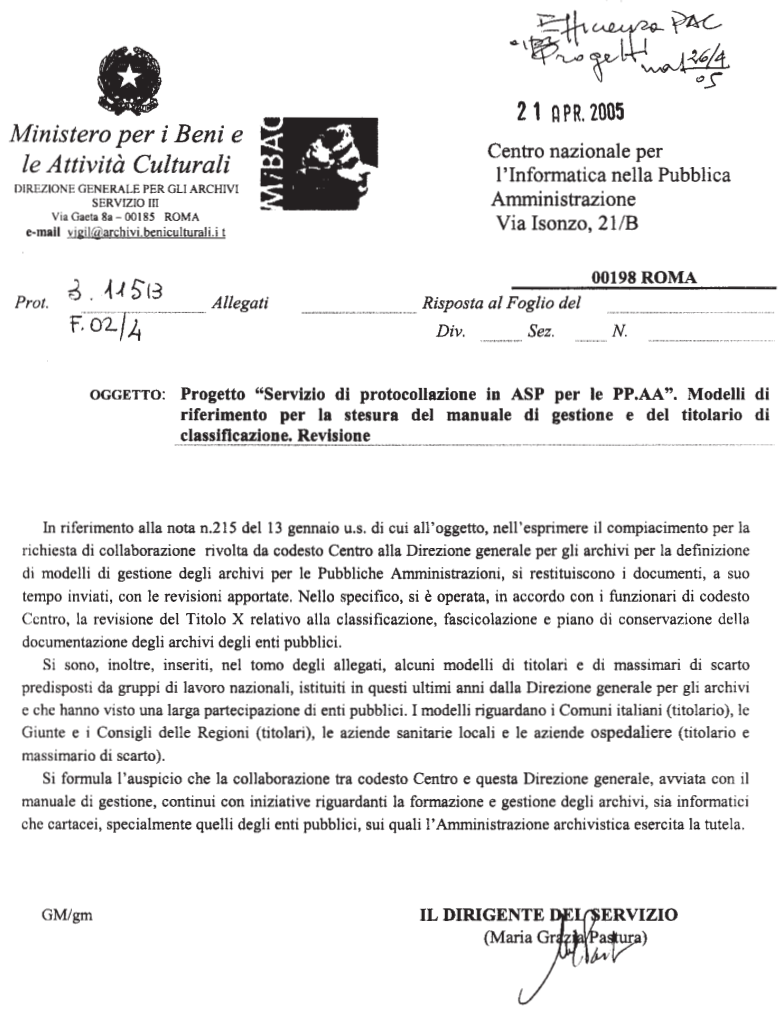
- Ordinanze emanate dal Sindaco;
- Decreti del Sindaco;
- Ordinanze emanate dai dirigenti (un unico repertorio);
- Determinazioni dei dirigenti;
- Deliberazioni del Consiglio comunale;
- Deliberazioni della Giunta comunale;
- Atti rogati dal segretario comunale (contratti e atti unilaterali in forma 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).

16.22 TIMBRO DI ARRIVO PER LA CORRISPONDENZA CARTACEA IN INGRESSO – ELEMENTI DELLA SEGNATURA



Ministero per i Beni e le Attività Culturali
DIREZIONE GENERALE PER GLI ARCHIVI
SERVIZIO III
Via Gaeta 8a – 00185 ROMA
e-mail vigil@archivi.beniculturali.i t

21 APR. 2005

Centro nazionale per
l'Informatica nella Pubblica
Amministrazione
Via Isonzo, 21/B

00198 ROMA

Prot. 3.11513 F.02/4 *Allegati* *Risposta al Foglio del* *Div.* *Sez.* *N.*

OGGETTO: **Progetto "Servizio di protocollazione in ASP per le PP.AA". Modelli di riferimento per la stesura del manuale di gestione e del titolario di classificazione. Revisione**

In riferimento alla nota n.215 del 13 gennaio u.s. di cui all'oggetto, nell'esprimere il compiacimento per la richiesta di collaborazione rivolta da codesto Centro alla Direzione generale per gli archivi per la definizione di modelli di gestione degli archivi per le Pubbliche Amministrazioni, si restituiscono i documenti, a suo tempo inviati, con le revisioni apportate. Nello specifico, si è operata, in accordo con i funzionari di codesto Centro, la revisione del Titolo X relativo alla classificazione, fascicolazione e piano di conservazione della documentazione degli archivi degli enti pubblici.

Si sono, inoltre, inseriti, nel tomo degli allegati, alcuni modelli di titolari e di massimari di scarto predisposti da gruppi di lavoro nazionali, istituiti in questi ultimi anni dalla Direzione generale per gli archivi e che hanno visto una larga partecipazione di enti pubblici. I modelli riguardano i Comuni italiani (titolario), le Giunte e i Consigli delle Regioni (titolari), le aziende sanitarie locali e le aziende ospedaliere (titolario e massimario di scarto).

Si formula l'auspicio che la collaborazione tra codesto Centro e questa Direzione generale, avviata con il manuale di gestione, continui con iniziative riguardanti la formazione e gestione degli archivi, sia informatici che cartacei, specialmente quelli degli enti pubblici, sui quali l'Amministrazione archivistica esercita la tutela.

GM/gm

IL DIRIGENTE DEL SERVIZIO
(Maria Grazia Pastura)

Centro nazionale per l'informatica
Entrata - AOO CNIPA
Prot. n. 0003572 Roma, 27/04/2005

16.23 DESCRIZIONE FUNZIONALE ED OPERATIVA DEL PRODOTTO DI PROTOCOLLO (PDP) INFORMATICO IN USO PRESSO L'AREA ORGANIZZATIVA OMOGENEA

< Riportare integralmente la descrizione dettagliata ed operativa del Prodotto di Protocollo informatico adottato dall'Amministrazione/AOO >

16.23.1 FUNZIONALITÀ DI ACCESSO AL PDP

16.23.2 FUNZIONALITÀ DI AMMINISTRAZIONE DEL PDP

16.23.3 FUNZIONALITÀ DI REGISTRAZIONE DEL PROTOCOLLO

16.23.4 FUNZIONALITÀ DI ACCESSO AI DATI DEL REGISTRO DI PROTOCOLLO

16.23.5 GESTIONE FASCICOLI

16.23.6 ...ALTRE FUNZIONALITÀ DEL PDP

16.24 ABILITAZIONI ALL'UTILIZZO DELLE FUNZIONALITÀ DEL PRODOTTO DI PROTOCOLLO (PDP) E DEI DOCUMENTI

Per ogni gruppo di utenti del sistema di protocollazione e gestione informatica dei documenti con il PdP, di seguito vengono illustrati i possibili permessi applicativi attraverso cui definire le abilitazioni allo svolgimento delle operazioni di gestione del protocollo e dei documenti.

16.24.1 MAPPA DEI RUOLI

Nell'ambito delle funzionalità del PdP in argomento, è possibile definire i seguenti **ruoli** per i soggetti che interagiscono con il sistema:
< elencare i diversi ruoli previsti dal PdP e descriverne i privilegi, ovvero le autorizzazioni assegnate al ruolo >

16.24.2 PERMESSI E FUNZIONI APPLICATIVE

< Nome dell'Amministrazione completo >
< Nome dell'Area Organizzativa Omogenea completo >
< Nome della UOP o UOR completo >
Ruolo amministrativo. *< Dirigente/Capo Servizio/Istruttore pratiche/Impiegato>*
Ruolo funzionale: *< Inserire uno dei possibili ruoli dell'utente del PdP>*
< All'interno del presente allegato ogni Amministrazione/AOO, riporta il proprio modello "timbro di segnatura" o "etichetta di segnatura" da apporre sui documenti ricevuti ed inviati>

FUNZIONI / RUOLI	FUNZIONALITÀ	ABILITAZIONE

Legenda abilitazioni:
C = Consultazione
I = Inserimento *e anche modifica e consultazione*
M = Modifica *e anche consultazione*
A = Annullamento *e anche inserimento, modifica e consultazione*

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

1. Guida alla stesura del Manuale di gestione: attività preliminari

1.1 Premessa

Obiettivo della Guida è favorire:

- la descrizione del sistema di gestione del protocollo, della documentazione amministrativa e del sistema archivistico in conformità a quanto previsto dalla normativa vigente;
- l'avvio e/o l'accelerazione concreta del processo di ammodernamento funzionale della Pubblica Amministrazione (PA) in termini *tattici* di digitalizzazione della PA e *strategici* di realizzazione della società dell'informazione.

Lo **scopo** è invece quello di contribuire concretamente, con esempi e alternative, alla redazione rapida e completa del Manuale di gestione del protocollo informatico, dei documenti e dell'archivio (MdG) quale espressione sia interna che esterna delle regole e delle procedure operative individuate dall'Amministrazione, ovvero dalle Aree Organizzative Omogenee (AOO), per gestire in modo efficace ed efficiente il servizio di protocollo informatico, semplificare ed accelerare l'azione amministrativa e realizzare la trasparenza dell'amministrazione.
La Guida è rivolta specificatamente alle PP.AA. che hanno implementato, o intendono implementare, il servizio di protocollo informatico, di gestione documentale e di archivistica *in house* sul proprio sistema informatico e che devono ancora realizzare il MdG in argomento o intendono perfezionarlo.
In ottemperanza a quanto stabilito dalle direttive e dalle norme di seguito richiamate, le regole e le procedure riportate sul MdG dovranno essere definite a conclusione delle attività preliminari di rilevazione, di analisi e di ridisegno dei processi produttivi interni all'Amministrazione connesse con la gestione dei documenti, la migrazione dei documenti dal supporto cartaceo al supporto informatico, l'introduzione di un sistema di classificazione e di un piano di conservazione, nonché la definizione delle linee strategiche di gestione del sistema archivistico e delle procedure ad esso collegate. Il complesso di queste attività mette ancora una volta in evidenza quanto sia:

- riduttivo, continuare a intendere il servizio di protocollo come un generatore di numeri sequenziali da attribuire ai documenti pervenuti e/o usciti dall'Amministrazione;
- limitativo interpretare il servizio di protocollo informatico, di gestione documentale e di archivistica come una trasposizione dal supporto cartaceo a quello informatico;

- opportuna, in termini di efficienza, la visione integrata e moderna della gestione documentale, nell'arco del suo ciclo di vita, all'interno del sistema archivistico in cui la registrazione del protocollo è la fase iniziale di tale processo.

Nell'ambito dei compiti e delle responsabilità dell'amministrazione inerenti al servizio di protocollazione, di gestione dei documenti e dell'archivio, il rispetto delle norme, la fruibilità del servizio, l'adozione delle misure di sicurezza e di tutela dei dati personali è totale e diretta.
Nella Guida vengono esaminati gli adempimenti delle amministrazioni, le funzionalità minime, la gestione documentale e la gestione dei flussi lavorativi, nel rispetto della struttura degli argomenti in capitoli così come stabilito dall'art. 5 del DPR n. 445/2000.
L'impostazione espositiva della guida, è quella di fornire un documento accessibile a tutti i destinatari finali nel quale i riferimenti normativi sono stati sostituiti quasi ovunque con la trasposizione diretta delle norme.
Il **Manuale di gestione del protocollo informatico, dei documenti e dell'archivio** si compone di tre parti:

- la **Guida** vera e propria, che riporta le regole ed i suggerimenti per la stesura del MdG;
- il **modello di riferimento per la compilazione del MdG** contenente la struttura di un Manuale con alcune soluzioni organizzative alternative tratte da alcuni esempi di manuali di gestione;
- gli **allegati** al MdG dei quali si consiglia la predisposizione allo scopo di evitare l'iter di approvazione formale del Manuale di gestione a seguito di variazioni minime.

La Guida, in particolare, è articolata in due parti:

- la prima, riporta le considerazioni di ordine generale e le attività preliminari necessarie all'avvio del servizio di protocollo informatico e gestione documentale da parte delle amministrazioni e delle Aree Organizzative Omogenee;
- la seconda, riporta le indicazioni utili alla predisposizione di ciascun capitolo e paragrafo del MdG.

Nell'*allegato 16.1 al MdG* vengono raccolte le sigle e le descrizioni dei termini più ricorrenti nella Guida e nel Manuale; nell'*allegato 16.2 del MdG* viene riportata la normativa di riferimento.
Per quanto la presente Guida sia inerente alla gestione informatica o digitale del protocollo e dei documenti, come rilevata dalla realtà operativa e dai manuali di altre PA, questa prima edizione, tratta anche gli aspetti operativi relativi all'impiego del protocollo informatico in un contesto in cui la documentazione digitale "convive" con quella cartacea. Non si tratta di un disguido o di una disattenzione alle norme, ma di una necessità dettata:

- dalla necessità di gestire la situazione transitoria di molte amministrazioni che hanno pianificato e avviato la gestione elettronica dei documenti e che ancora operano integralmente con documenti cartacei;
- dalla assenza, presso alcune amministrazioni, di tecnologie sicure di identificazione e autenticazione degli interlocutori esterni alle amministrazioni stesse, quali cittadini ed imprese, e di trasmissione/ricezione di atti.

Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **MdG -** Manuale di Gestione del protocollo informatico, dei documenti e dell'archivio;
- **RPA** Responsabile Procedimento Amministrativo - il personale che ha la responsabilità dell'esecuzione degli adempimenti amministrativi e/o degli affari;
- **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 competenza, di funzione amministrativa assegnata, 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.

1.2 AMBITO DI APPLICAZIONE DELLA GUIDA

(cfr. paragrafo 1.2 del MdG) La presente Guida è focalizzata sull'elemento minimo autoconsistente, previsto dalle norme, in termini di sistema archivistico e di gestione documentale delle Aree Organizzative Omogenee – AOO. Tale impostazione deriva dalle seguenti motivazioni:

- l'eterogeneità delle PA alle quali è rivolta la presente Guida;
- i diversi modelli organizzativi delle amministrazioni;
- l'intenzione di fornire un contributo alla definizione del MdG alle amministrazioni che hanno optato per un servizio di protocollo informatico, di gestione documentale e di archivistica realizzato *in house.*

Tale approccio consente infatti di soddisfare le esigenze, sia delle piccole amministrazioni costituite da una sola AOO, sia di quelle più grandi con più AOO, considerato che ciascuna di queste deve, appunto, predisporre il MdG ed operare con il proprio registro di protocollo.
Ciò significa, ad esempio, che le pubbliche amministrazioni centrali, organizzate su più AOO, disporranno di più registri di protocollo e potranno fare riferimento sia ad un proprio archivio (logico) che ad un unico archivio centrale (logico dell'Amministrazione), peraltro già presente in diverse realtà.
La distinzione tra archivio logico e fisico, *nel senso di contenitore*, è importante perché anche se una amministrazione decide di raccogliere fisicamente in uno stesso ambiente,

chiamato archivio centrale, gli archivi logici di diverse AOO, saremo sempre di fronte ad archivi distinti, caratterizzati da diversi titolari di classificazione.
Nel caso in cui, invece, una amministrazione decidesse di avere un unico archivio logico, (anche fisicamente frammentato in sedi diverse) dovrà stabilire delle regole comuni di gestione della documentazione valide per tutte le proprie AOO in termini di titolario di classificazione, del piano di conservazione e di gestione della sezione corrente, di deposito e storica dell'archivio e delle modalità di accesso, di consultazione e di studio della documentazione.

1.3 LIMITI DI APPLICABILITÀ DELLA GUIDA

Per quanto il CNIPA, con la presente Guida, abbia tentato di generalizzare le soluzioni organizzative, tecniche e funzionali connesse con l'introduzione del sistema di protocollazione informatica e di gestione documentale, ovvero abbia tentato di esemplificare casi "riusabili", la presente Guida deve essere interpretata come tale e non come succedaneo del MdG.
Infatti le amministrazioni si differenziano, non solo per "missione", dimensione, storia, organizzazione e tecnologia, ma anche per la politica di sviluppo nel settore in termini, sia di tempi di reazione e velocità di adeguamento, che di approccio:

- minimale, caratterizzato da una gradualità di realizzazione
- integrato, caratterizzato da una visione iniziale completa, che pone al centro del sistema documentale il "servizio di protocollazione" quale collante e nodo operativo dell'Amministrazione/AOO.

Nel primo caso il protocollo informatico si pone come il punto di avvio del processo di trasformazione dell'Amministrazione da una gestione cartacea dei documenti ad una gestione sempre più elettronica dei documenti.
Nel secondo caso, siamo in presenza di un unico sistema di "governo elettronico" dell'Amministrazione.
In tutti i casi, il livello minimale deve essere finalizzato a creare non solo un sistema di protocollo in linea con la normativa, ma anche un sistema elettronico di gestione documentale, con la conseguente eliminazione dei documenti cartacei una volta trasformati in digitale.
Come si evincerà dai paragrafi seguenti il Manuale deve essere redatto:

- a conclusione dell'analisi dei processi afferenti all'intero ciclo di vita dei documenti, della loro razionalizzazione e reingegnerizzazione;
- sulla base:
  - delle funzionalità del PdP,
  - dei risultati raggiunti dall'analisi dei rischi,
  - delle politiche di sicurezza adottate,
  - del piano di sicurezza predisposto

e diventa consistente descrivendo le soluzioni tecnico-organizzative e procedurali individuate.
In questa fase di analisi dei processi, occorre inoltre distinguere il *sistema informativo* per la gestione del protocollo informatico e gestione documentale da quello *informatico* per la stessa finalità. Quest'ultimo deve infatti essere considerato il mezzo e non il fine per gestire l'insieme integrato di dati, di funzioni, di tecnologie (accesso, riversamento e conservazione), di procedure, di procedimenti e di documenti.

1.4 APPROCCIO METODOLOGICO ADOTTATO PER LA STESURA DELLA GUIDA

La presente Guida è stata predisposta:

- coerentemente a tutta la normativa vigente in materia di gestione elettronica dei documenti, di misure di sicurezza adottate e di protezione dei dati personali;
- sulla base delle professionalità presenti nel CNIPA;
- sulla base delle esperienze maturate nel settore, sia dal CNIPA stesso che da diverse PP.AA. che hanno avviato il servizio di protocollazione e gestione informatica della documentazione sia con soluzioni *in house* che in modalità ASP con altri fornitori di servizi;
- per consentire un riuso delle esperienze raccolte dal CNIPA in qualità di Centro di competenza nella materia oggetto della Guida;
- per diffondere i risultati di gruppi di lavoro, coordinati dalla direzione generale archivi di Stato del Ministero per i beni e le attività culturali, appositamente costituiti per lo studio di queste tematiche anche con riferimento alla messa a punto dei titolari di classificazione e dei massimari di selezione e scarto;
- nello spirito di fornire indicazioni sull'esatta applicazione delle normativa di riferimento alle amministrazioni destinatarie.

Il Manuale di gestione, predisposto da ciascuna AOO, deve pertanto:

- descrivere le modalità operative di protocollazione, di gestione, di conservazione e di accesso ai documenti amministrativi, affinché ogni operatore possa trovare nel Manuale le istruzioni necessarie per svolgere correttamente, per qualsiasi tipo di documento, le operazioni di registrazione (o non registrazione), di fascicolazione e di archiviazione;
- definire compiti e responsabilità del personale dell'Amministrazione all'interno delle AOO;
- fornire le istruzioni per il corretto e sicuro funzionamento e per l'accesso al servizio;
- essere reso pubblico secondo le modalità previste dai singoli ordinamenti.

Considerato che il MdG deve essere approvato dagli organi di vertice dell'Amministrazione e che tale Manuale, per sua natura, è soggetto a revisioni periodiche o straordinarie, si suggerisce di predisporre un Manuale "parametrico" e quindi flessibile e snello con allegati specifici in modo da disporre sempre di un Manuale aggiornato senza richiedere la formale approvazione dei vertici.

Gli allegati al MdG suggeriti, ma non obbligatori, sono i seguenti:

1. Definizioni;
2. Norme e regole di riferimento;
3. Aree Organizzative Omogenee e modello organizzativo;
4. Atto di nomina del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi;
5. Atto di nomina del responsabile della conservazione delle copie di riserva del registro di protocollo informatico;
6. Elenco delle persone titolari di firma digitale;
7. Piani formativi per il personale dell'Amministrazione per l'anno 200x;
8. Piano di eliminazione dei protocolli diversi dal protocollo informatico;
9. Politiche di sicurezza;
10. Sottoscrizione dei documenti formati dall'AOO;
11. Descrizione dei flussi documentali all'interno della AOO;
12. Regole di raccolta e consegna della corrispondenza convenzionale al servizio postale nazionale;
13. Modulo di consultazione della sezione di deposito e storica dell'archivio;
14. Nomina formale del responsabile del servizio archivistico;
15. Nomina del responsabile della conservazione sostitutiva;
16. Elenco dei documenti esclusi dalla protocollazione;
17. Elenco dei documenti soggetti a registrazione particolare;
18. Piano di conservazione;
19. Titolario di classificazione;
20. Modello di "camicia" del fascicolo;
21. Repertori generali;
22. Timbro di arrivo della corrispondenza cartacea in ingresso – elementi della segnatura;
23. Descrizione funzionale ed operativa del PdP utilizzato per la gestione del protocollo e della documentazione;
24. Abilitazioni all'utilizzo delle funzionalità del sistema di gestione informatica del protocollo e dei documenti.

1.5 OSSERVAZIONI SUI MANUALI PREDISPOSTI DA ALCUNE AMMINISTRAZIONI

L'esame dei MdG pervenuti al Centro di competenza del protocollo informatico del CNIPA unitamente a quelli direttamente rilevati su Internet, predisposti dagli enti locali, pubbliche amministrazioni centrali, camere di commercio, strutture sanitarie e università, ha evidenziato, salvo rare eccezioni:

- l'assenza generalizzata di richiami ad attività di analisi e riorganizzazione dei processi produttivi, di analisi del rischio, di definizione delle politiche di sicurezza e di predisposizione del piano di sicurezza;

- una diversa organizzazione dei manuali e un diverso approfondimento delle soluzioni adottate per assolvere al dettato della normativa[1];
- scarsa attenzione alle modalità di accesso alle informazioni detenute dalle amministrazioni da parte di cittadini e imprese;
- l'assenza di riferimenti espliciti alle finalità, alle responsabilità e alle modalità di adozione delle norme sulla tutela dei dati personali.

In relazione alla eliminazione dei protocolli diversi da quello informatico generale, è opportuno sottolineare che non è aderente alla norma la soluzione adottata dalla quasi totalità delle amministrazioni e pubblicata sui relativi MdG, che prevede l'eliminazione "drastica" dei protocolli esistenti senza nessuna altra informazione in ordine ai tempi o alle modalità di migrazione e di adozione del protocollo informatico.
Dalle rilevazioni effettuate sullo stato di attuazione della normativa sul protocollo informatico, è emerso che numerose amministrazioni hanno definito le proprie AOO senza procedere preliminarmente ad una analisi dei processi, alla loro semplificazione e alla conseguente riorganizzazione dell'Amministrazione stessa.
Tali attività devono essere ritenute propedeutiche all'introduzione di sistemi informatici per la gestione del protocollo informatico.

1.6 ATTIVITÀ PRELIMINARI

(cfr. capitolo I del MdG) Sono riportate di seguito le iniziative di tipo organizzativo che devono essere adottate dalle amministrazioni in via preliminare per introdurre l'automazione della gestione elettronica dei documenti.

1.6.1 DEFINIRE L'AMBITO DI APPLICAZIONE DEL MANUALE DI GESTIONE

(cfr. paragrafo 1.2 del MdG) Nel Manuale dovrà espressamente essere definito l'ambito di applicazione del medesimo.

1.6.2 RICHIAMARE LE DEFINIZIONI E LE NORME

(cfr. paragrafo 1.3 del MdG) Sul Manuale dovranno essere raccolti in un glossario i termini utilizzati con i relativi acronimi e le corrispondenti definizioni. E' inoltre opportuno che il Manuale contenga un elenco della normativa di riferimento.

1.6.3 INDIVIDUARE E PUBBLICARE SULL'INDICE PA LE AREE ORGANIZZATIVE OMOGENEE

(cfr. paragrafo 1.4 del MdG) Come già anticipato, prima di procedere alla individuazione delle AOO è opportuno effettuare l'analisi dei processi per la loro semplificazione, articolandola per fasi così come descritto nelle "linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi" di cui al decreto del Ministro per l'innovazione e le tecnologie 14 ottobre 2003, considerando che:

- una AOO è definita come un insieme di UOR che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali;
- gli UOR raggruppano più UU caratterizzati dalle stesse competenze;

[1] Anche per questo motivo la presente Guida ha adottato integralmente l'indice dei capitoli definito dall'art. 5 comma 2 del DPCM 31/10/2000.

- un UOR associato ad una AOO è un utente dei servizi messi a disposizione da questa attraverso le UOP.

Tale attività di riorganizzazione dell'Amministrazione è fondamentale, perché consente di limitare/ottimizzare le funzioni ed il numero delle UOP e degli UOR in modo da:

- ridurre il numero e la frammentazione dei registri di protocollo;
- ottimizzare i procedimenti, i processi e l'accesso ai medesimi;
- definire le metriche della prestazione complessiva di processo;
- dare consistenza all'intero sistema di archiviazione.

Nella fase di analisi organizzativa qui richiamata, oltre agli aspetti operativi connessi con l'introduzione del protocollo informatico e della gestione documentale, gli elementi principali da tenere in considerazione per favorire il successo dell'iniziativa, sono:

- la formazione del personale, peraltro obbligatoria ai sensi della direttiva del Ministro della funzione pubblica del 13 dicembre 2001;
- il dimensionamento degli organici tenendo presente la diversa organizzazione derivante dall'introduzione di un protocollo informatico,
- la definizione dei profili professionali;
- l'assegnazione di incarichi di coordinamento;
- l'individuazione di referenti e capi progetto a seconda delle dimensioni dell'amministrazione e quindi della tipologia di progetto previsto.

Al termine di tale processo, l'AOO sarà caratterizzata dalle UOP, UOR, UU, sulla base di una attenta valutazione delle variabili sopra enunciate. Di tale definizione dovrà essere data notizia nel MdG.
A titolo informativo, la lettura dei manuali richiamati nella bibliografia allegata alla presente Guida evidenzia che:

- le amministrazioni comunali, le aziende sanitarie locali, le aziende ospedaliere, le amministrazioni provinciali, le scuole e le camere di commercio, tendono ad identificarsi in un'unica AOO anche con più UOP in uscita;
- le università tendono ad organizzarsi in più AOO:
  - una di ateneo che accomuna il rettorato e le varie direzioni funzionali (amministrazione, segreterie studenti, …);
  - una per ciascuna entità (dipartimento, istituto, …) dotata di autonomia finanziaria.
- Le amministrazioni centrali dello Stato, ai sensi dell'art. 50, comma 5 del DPR n. 445/2000 "provvedono alla gestione informatica dei documenti presso gli uffici di registrazione di protocollo già esistenti alla data di entrata in vigore del testo unico presso le direzioni generali e le grandi ripartizioni che a queste corrispondono, i dipartimenti, gli uffici centrali di bilancio, le segreterie di gabinetto" e di conseguenza sono organizzate su più AOO".

Vale la pena di ricordare che all'interno di una AOO il sistema archivistico e l'annesso servizio di protocollazione, è unico, indipendentemente dalla dimensione e dell'organizzazione della AOO medesima. Per questi motivi saranno unici:

- il MdG;
- il regolamento che descrive le operazioni e le procedure archivistiche, i relativi strumenti ed i responsabili. Al riguardo, per il carattere scientifico del regolamento stesso, si suggerisce di predisporlo all'interno del servizio archivio generale dell'Amministrazione, seguendo le direttive condivise a livello nazionale.

Nell'ipotesi di una amministrazione organizzata in più AOO può sorgere la necessità di gestire un solo archivio, caratterizzato da un solo titolario di classificazione come illustrato nel precedente paragrafo 2.

1.6.4 INDIVIDUARE E PUBBLICARE SULL'INDICE PA LE UNITÀ ORGANIZZATIVE RESPONSABILI DI PROTOCOLLAZIONE

Sulla base delle risultanze precedenti, all'interno di ciascuna AOO (o dell'unica AOO), ogni amministrazione deve definire le UOP che utilizzano il sistema protocollazione e di gestione dei documenti e dei flussi documentali sia in ingresso che in uscita, sia quelli interni formali come sarà specificato nel seguito. La modalità di individuazione e di istituzione delle Unità Organizzative responsabili delle attività di registrazione del Protocollo (UOP) viene riportata nel paragrafo 2.5 della presente Guida.

1.6.5 ISTITUIRE IL SERVIZIO PER LA GESTIONE INFORMATICA DEL PROTOCOLLO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI

(cfr. paragrafo 1.4 del MdG) Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle proprie AOO. Il servizio è posto alle dirette dipendenze della stessa AOO.
Al servizio deve essere preposto un soggetto in possesso di idonei titoli e requisiti professionali o di professionalità tecnico-archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente.
È compito del servizio:

a) attribuire il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
b) garantire che le operazioni di registrazione e di segnatura di protocollo si svolgano nel rispetto della vigente normativa;
c) garantire la corretta produzione e conservazione del registro giornaliero di protocollo;
d) tenere cura che le funzionalità del sistema, in caso di guasti o anomalie, siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;

e) conservare le copie del registro di protocollo informatico quotidianamente prodotte, in luoghi sicuri differenti da quelli di produzione;

f) garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso e le attività di gestione degli archivi;

g) autorizzare le operazioni di annullamento del protocollo;

h) vigilare sull'osservanza delle disposizioni normative e regolamentari correnti e del MdG.

Per quanto concerne l'aspetto archivistico dell'intero processo di gestione dei flussi documentali, sulla base dell'analisi svolte sull'argomento si rileva che:

- è conveniente integrare nella stessa UOP anche le funzioni di gestione dell'archivio se si tratta di una (o quella) che svolge un ruolo principale nella ricezione della corrispondenza nel caso di più UOP (esempio, l'ufficio di protocollo generale);
- è opportuno che il servizio archivistico, integrato o meno nelle funzioni della UOP, sia ricondotto alla direzione, o area, o settore affari generali per aumentarne la capacità impositiva nei confronti delle diverse AOO, o dell'intera AOO, evitando di legarlo ai destini delle altre direzioni, o aree, o settori giudicati troppo settoriali;
- è assolutamente da evitare la frammentazione del servizio archivistico, in quanto ciò potrebbe influire negativamente sulla capacità organizzativa dell'intera struttura.

1.6.6 INDIVIDUARE LE FIGURE RESPONSABILI DEI SERVIZI INTERNI ALLA AOO

All'interno delle AOO vengono svolte una serie di attività che possono essere organizzate e assegnate a specifici servizi.
Ciascuna amministrazione può assegnare i compiti relativi a ciascun servizio a uno o a più soggetti fermo restando che la responsabilità del servizio per gestione informatica dei documenti, dei flussi documentali e degli archivi è sempre e comunque del RSP.
In ogni caso è opportuno rendere pubbliche le nomine dei soggetti che opereranno sotto la guida e la responsabilità del RSP inserendole negli allegati del MdG.
Tale scelta permette una separazione tra persone incaricate e ruoli all'interno del MdG.

1.6.6.1 Responsabile del servizio per la Tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi

(cfr. paragrafo 1.5 del MdG) Al responsabile della tenuta del protocollo, della gestione dei flussi documentali e degli archivi (RSP) devono essere assegnati i seguenti compiti:

- 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 anche per via telematica;
- 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 il piano per la sicurezza informatica relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici d'intesa con:
  - il responsabile dei sistemi informativi automatizzati;
  - il referente della pianificazione delle attività;
  - il responsabile della sicurezza dei dati personali, se nominato, o direttamente con il titolare dei trattamenti dei dati di cui al d.lgs. n. 196/03;
  - il responsabile del servizio archivistico;
  - il responsabile della conservazione sostitutiva;
- attribuire il livello di autorizzazione (ruolo) di ciascun addetto all'accesso alle funzionalità offerte dal PdP provvedendo a distinguere competenze e ruoli in base alle abilitazioni alla consultazione, all'inserimento, alla modifica e alla cancellazione delle informazioni;
- garantire il rispetto della normativa vigente durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta produzione e la conservazione del registro giornaliero di protocollo;
- garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti dalla AOO adottando i formati standard, ovvero altri formati che sono comunque descritti nel MdG;
- curare le funzionalità del sistema affinché, in caso di guasti o anomalie, siano ripristinate nel più breve tempo possibile e, comunque entro le ventiquattro ore dal blocco delle attività;
- conservare le copie di salvataggio delle informazioni del sistema e del registro di emergenza in luoghi sicuri differenti da quello che custodisce il registro giornaliero di protocollo;
- garantire il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi, quali, il trasferimento dei documenti all'archivio di deposito, la conservazione degli archivi correnti e degli archivi storici;
- autorizzare le operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza della normativa vigente in materia da parte del personale.

Questa figura deve necessariamente essere individuata e indicata su un allegato del MdG. Per i casi di vacanza, assenza o impedimento del Responsabile, deve essere nominato un vicario.

1.6.6.2 Responsabile della conservazione delle copie di riserva del Registro di Protocollo

(cfr. paragrafo 1.6 del MdG) Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della

giornata lavorativa, deve essere riversato su supporti informatici non riscrivibili e deve essere conservato da persona diversa dal RSP.
Per questo motivo l'Amministrazione deve provvedere a nominare un soggetto incaricato di tale compito che può, ad esempio, all'occorrenza, coincidere con il responsabile della conservazione sostitutiva. Le procedure di riversamento e custodia delle copie dovranno essere illustrate nel piano di sicurezza del MdG.

1.6.7 FORNITURA DEGLI STRUMENTI PER LA FIRMA DIGITALE AI RAPPRESENTANTI DELL'AMMINISTRAZIONE

(cfr. paragrafo 1.7 del MdG) L'Amministrazione deve fornire ai dirigenti e/o ai funzionari chiamati, a diverso titolo, a rappresentare l'Amministrazione verso l'esterno, e al responsabile della conservazione sostitutiva dei documenti informatici, una firma digitale e le risorse strumentali per l'apposizione della firma digitale.

1.6.8 TUTELA DEI DATI PERSONALI

(cfr. paragrafo 1.8 del MdG) L'amministrazione titolare dei dati di protocollo e dei dati personali contenuti nella documentazione amministrativa di propria pertinenza, è chiamata ad assolvere integralmente il dettato del d. lgs. n. 196/2003 adottando opportune iniziative sia all'interno che nei rapporti con le altre Amministrazioni/AOO.
In relazione ai dati trattati all'interno dell'Amministrazione, è necessario redigere una specifica lettera d'incarico da recapitare agli addetti alla protocollazione in quanto autorizzati a trattare i dati di protocollo veri e propri ed i documenti associati.
Per quanto concerne i dati dell'Amministrazione trattati, a diverso titolo, all'esterno da soggetti pubblici e/o privati, l'Amministrazione deve individuare le persone responsabili appartenenti ai soggetti pubblici e/o privati che trattano i dati personali di sua pertinenza.
Non sono trattati in questa Guida, in quanto strettamente correlati alla specifica realtà tecnico-organizzativa di ciascuna Amministrazione, gli adempimenti relativi:

- ai certificati ed ai documenti trasmessi ad altre pubbliche amministrazioni, che prevedono la trasmissione delle sole informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite;
- alla definizione delle apposite autorizzazioni, *in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente*, rilasciate dall'Amministrazione certificante all'Amministrazione procedente per consentire a quest'ultima l'accesso diretto agli archivi della certificante, *ai sensi dell'art. 42 del DPR n. 445/2000.*

Le regole adottate e le modalità operative definite dall'Amministrazione a tutela dei dati personali, dovranno comunque essere rese note nel piano di sicurezza del MdG, come previsto dalla normativa in materia, indipendentemente dall'attivazione del protocollo informatico.

1.6.9 ATTIVAZIONE DELLE CASELLE DI POSTA ELETTRONICA

(cfr. paragrafo 1.9 del MdG) In attuazione di quanto previsto dalla normativa in materia di impiego della posta elettronica nelle pubbliche amministrazioni è necessario che le singole amministrazioni provvedano a:

- dotarsi di una casella di posta elettronica certificata istituzionale pubblicata sull'Indice delle Pubbliche Amministrazioni (IPA). Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento. A tal proposito, si suggerisce di attivare una casella di posta elettronica destinata soltanto alla raccolta della documentazione che successivamente deve essere trasmessa all'esterno;
- dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e a attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza, 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.

I titolari della caselle di posta elettronica dovranno procedere, almeno una volta al giorno, alla lettura della corrispondenza ivi pervenuta, adottando i metodi di conservazione della corrispondenza più opportuni in relazione alle varie tipologie di messaggi ed ai tempi di conservazione previsti.

1.6.10 PREDISPOSIZIONE DEL SISTEMA DI CLASSIFICAZIONE

(cfr. paragrafo 1.10 del MdG) La classificazione dei documenti, destinata a realizzare una corretta organizzazione dei documenti nell'archivio a partire dalla fase corrente, è obbligatoria per legge ed è attuata attraverso il piano di classificazione (**titolario**), cioè "un sistema precostituito di partizioni astratte gerarchicamente ordinate, individuato sulla base dell'analisi delle funzioni dell'ente, al quale deve ricondursi la molteplicità dei documenti prodotti".
Il titolario, illustrato nel capitolo 9 del Modello di MdG, deve essere predisposto, verificato e/o confermato antecedentemente all'avvio delle attività di protocollazione informatica in quanto è lo strumento che consente la gestione e la sistemazione della documentazione dell'amministrazione. Spetta a ciascuna amministrazione adottare il proprio titolario con un atto formale.
Il Manuale di gestione dovrà inoltre indicare, oltre al piano di classificazione:

- le modalità di aggiornamento del titolario;
- i tempi, i criteri e le regole di selezione e di conservazione dei documenti;
- l'uso di supporti sostitutivi.

1.6.11 ATTIVITÀ DI FORMAZIONE CORRELATA AL SISTEMA DI PROTOCOLLO INFORMATICO

(cfr. paragrafo 1.11 del MdG) Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva del Ministro della funzione pubblica del 13 dicembre 2001 sulla

formazione e la valorizzazione del personale delle pubbliche amministrazioni, una particolare attenzione deve essere rivolta allo sviluppo e alla diffusione delle competenze nel campo dell'innovazione tecnologica.
Il processo di digitalizzazione della Pubblica Amministrazione presuppone, infatti, la presenza di figure professionali dotate di competenza specialistica.
L'attività formativa non dovrà, pertanto, limitarsi alla sola alfabetizzazione informatica ma dovrà prevedere anche la formazione degli specialisti, dei funzionari e dei dirigenti sui seguenti temi:

- gestione del cambiamento organizzativo;
- analisi e reingegnerizzazione delle procedure amministrative;
- protezione dei dati personali;
- sicurezza informatica.

Le Amministrazioni dovranno, inoltre, adottare opportune iniziative rivolte alla formazione del personale per incentivare l'uso della posta elettronica.
Per quanto riguarda il personale dirigente l'Amministrazione dovrà realizzare i relativi percorsi formativi tenendo conto delle attività programmate.

1.6.12 COMUNICAZIONI AL CNIPA

Le Amministrazioni devono comunicare al CNIPA, per ogni AOO istituita, il nominativo del Responsabile del Servizio per la tenuta del Protocollo informatico, della gestione dei flussi documentali e degli archivi e la casella ufficiale di posta elettronica per l'iscrizione delle AOO nell'Indice della Pubbliche amministrazioni (IPA).

1.6.12.1 Accreditamento dell'amministrazione presso l'Indice delle Pubbliche Amministrazioni

Ciascuna Amministrazione che intenda trasmettere/ricevere documenti informatici soggetti alla registrazione di protocollo deve accreditarsi presso l'Indice delle Amministrazioni Pubbliche e delle aree organizzative omogenee fornendo almeno le seguenti informazioni identificative dell'Amministrazione stessa:

- denominazione della Amministrazione;
- codice identificativo proposto per la Amministrazione;
- indirizzo della sede principale della Amministrazione;
- elenco delle proprie AOO.

Quest'ultimo elenco comprende a sua volta, per ciascuna Area Organizzativa Omogenea:

- la denominazione;
- il codice identificativo;
- la casella di posta elettronica;
- il nominativo del Responsabile del Servizio per la tenuta del Protocollo informatico, per la gestione dei flussi documentali e degli archivi;
- la data di istituzione;

– l'eventuale data di soppressione;
– l'elenco degli UOR e degli UU dell'AOO.

Il codice associato a ciascuna Area Organizzativa Omogenea è generato ed attribuito autonomamente dalla relativa Amministrazione.
L'Indice delle Pubbliche Amministrazioni, pubblicato su Internet, è accessibile da parte di tutti i soggetti pubblici o privati secondo modalità LDAP definito nella specifica pubblica RFC 1777.
Ciascuna Amministrazione deve comunicare tempestivamente all'IPA l'eventuale modifica del codice identificativo e la data da cui decorre la modifica stessa in modo da garantire l'affidabilità dell'indirizzo di posta elettronica; con la stessa tempestività ciascuna Amministrazione comunica la soppressione ovvero la istituzione di una AOO nella forma dovuta.
L'obbligo di accreditamento ricorre per tutte le Pubbliche Amministrazioni di cui all'art.1, comma 2 del decreto n.29 del 3 febbraio 1993.

1.6.12.2 Adozione di procedure integrative al processo di conservazione sostitutiva
(cfr. paragrafo 1.13 del MdG) Come previsto dalla deliberazione CNIPA n. 11 del 19 febbraio 2004, i soggetti pubblici o privati che intendano avvalersi del processo di conservazione sostitutiva dei documenti possono adottare accorgimenti e procedure integrative, nel rispetto di quanto previsto dalla deliberazione medesima, comunicando preventivamente al CNIPA quali accorgimenti e procedure intendano adottare.

2. Guida alla stesura dei capitoli del Manuale di gestione

2.1 Eliminazione dei protocolli diversi dal protocollo informatico

(cfr. capitolo 2 del MdG) Il presente paragrafo fornisce indicazioni in merito alla **pianificazione, alle modalità e alle misure organizzative e tecniche finalizzate all'eliminazione dei protocolli diversi dal protocollo informatico.** Il piano di attuazione del protocollo informatico prevede l'eliminazione dei diversi protocolli di settore, di reparto e multipli. A tal fine è necessario svolgere le seguenti attività:

- censire preliminarmente i diversi protocolli esistenti;
- eseguire l'analisi dei livelli di automazione;
- definire gli interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico;
- stimare i tempi di sostituzione;
- stimare i costi derivanti.

Il risultato è un piano di azione che tiene conto della realtà organizzativa dell'Amministrazione, della capacità di gestire il transitorio, etc.
Il piano è particolarmente significativo per i registri di protocollo interno che dovranno confluire nel registro generale di protocollazione informatica.

2.2 Piano di sicurezza dei documenti informatici

(cfr. capitolo 3 del MdG) Il presente paragrafo riporta indicazioni in merito al perfezionamento del **piano di sicurezza dei documenti informatici relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti stessi.**

2.2.1 Generalità

Come già anticipato nelle premesse, il responsabile del servizio per la tenuta del protocollo informatico ha, tra l'altro, il compito di predisporre il piano di sicurezza in argomento che contempli almeno i seguenti aspetti:

- esecuzione dell'analisi dei rischi che incombono sui dati (personali e non) e/o sui documenti trattati;
- definizione delle politiche di sicurezza da adottare all'interno della AOO di cui è responsabile (*nel caso di più AOO appartenenti alla stessa Amministrazione le poli-*

tiche di sicurezza devono essere coerenti, al limite uguali, con quelle stabilite a livello di intera Amministrazione);

- pianificazione degli interventi da attuare in esito ai risultati ottenuti dalle attività precedenti in termini di misure di sicurezza da adottare 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 n. 196 del 30 giugno 2003 – Codice in materia di protezione dei dati personali*, in caso di trattamenti di dati personali;
- predisposizione, all'occorrenza, di piani specifici di formazione degli addetti;
- monitoraggio periodico del piano di sicurezza.

Il piano di sicurezza deve essere revisionato con cadenza almeno biennale. In caso di eventi straordinari si provvede a una revisione estemporanea.
Considerata la modalità di erogazione e fruizione del servizio di protocollo informatico (realizzazione *in house*), tutte le funzioni e le responsabilità della sicurezza sono a carico del RSP dell'AOO.
Di conseguenza il RSP deve eseguire (o far eseguire) l'analisi del rischio, predisporre (o far predisporre) le politiche di sicurezza da divulgare al personale dell'AOO di competenza e, all'occorrenza, predisporre (o far predisporre) il piano di sicurezza garantendo il soddisfacimento dei seguenti requisiti minimi di sicurezza del servizio di gestione del protocollo informatico basato sul PdP acquisito:

- riservatezza;
- integrità;
- disponibilità;
- non ripudio dei messaggi scambiati all'interno ed all'esterno della AOO.

Tali requisiti sono richiamati anche nell'allegato 2 "Base minima di sicurezza" della Direttiva MIT del 16 gennaio 2002 "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali".
Il presente piano deve quindi illustrare gli aspetti operativi della sicurezza conseguenti e connessi ai risultati ed alle iniziative avviate in materia.
In ogni caso le misure di sicurezza adottate, o in fase di avvio, non dovranno essere descritte dettagliatamente nel MdG in quanto la loro divulgazione non è opportuna sotto il profilo della sicurezza.
Per l'analisi del rischio si fa riferimento a quanto diffusamente riportato nei seguenti documenti:

- "i Quaderni AIPA", Capitolo 6 – (Analisi dei rischi) – supplemento al n. 9-10/1999 di informazioni – linee guida per la definizione di un piano di sicurezza;
- la "Guida operativa per redigere il documento programmatico sulla sicurezza" (Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, n. 196) pubblicato l'11 giugno 2004;
- le "proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione" pubblicate a marzo 2004

d'intesa dal Ministro per l'innovazione e le tecnologie e il Ministero delle telecomunicazioni.

Per le linee guida alla pubblicazione delle politiche di sicurezza si fa riferimento a quanto diffusamente riportato nei "i Quaderni AIPA", Capitolo 7 – politiche di sicurezza – del supplemento al n. 9-10/1999 di informazioni – linee guida per la definizione di un piano di sicurezza.
Nel MdG i paragrafi concernenti il piano di sicurezza possono essere raccolti in uno solo, all'interno del quale risultino illustrate le misure di sicurezza adottate (generali e particolari) e le politiche di sicurezza.

2.2.2 FORMAZIONE DEI DOCUMENTI - ASPETTI DI SICUREZZA

(cfr. paragrafo 3.3 del MdG) Nel relativo paragrafo devono essere riportate le indicazioni di sicurezza in merito alle misure, alle politiche ed alle regole di sicurezza adottate dalla AOO per la formazione dei documenti informatici *(nel successivo paragrafo 2.3 saranno trattati gli aspetti operativi).*
In conformità a quanto disposto dalle norme vigenti in materia, le risorse strumentali e le procedure utilizzate per la formazione dei documenti informatici delle pubbliche amministrazioni devono garantire:

- l'identificabilità del soggetto che ha formato il documento e l'Amministrazione di riferimento;
- la sottoscrizione, quando prescritta, dei documenti informatici tramite la 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'accessibilità ai documenti informatici tramite sistemi informativi automatizzati;
- la leggibilità dei documenti nel tempo;
- l'interscambiabilità dei documenti.

Le funzionalità del PdP e dell'ambiente elaborativo della AOO garantiscono il rispetto dei requisiti di riservatezza, di integrità, di disponibilità e non ripudio oltre a quelli sopra richiamati.
La produzione, la trasmissione, la gestione e la conservazione di documenti informatici presentano caratteristiche e problematiche proprie rispetto ai documenti analogici, in particolare per ciò che concerne gli aspetti relativi all'autenticità, all'affidabilità, alla stabilità.
La normativa in materia prevede che i formati dei documenti della Pubblica Amministrazione "devono possedere almeno i seguenti requisiti:

- non alterabilità del documento durante le fasi di accesso e conservazione;
- immutabilità nel tempo del contenuto e della sua struttura.

A tale fine i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto".

Per la formazione e la gestione di documenti informatici per i quali non è prevista la sottoscrizione, le Amministrazioni possono utilizzare sistemi elettronici di identificazione ed autenticazione nell'ambito della propria autonomia organizzativa e dei processi di razionalizzazione, ovvero possono decidere di uniformare le tecnologie di formazione dei documenti utilizzando quelle che garantiscono i requisiti minimi di cui sopra.
La formazione dei documenti cartacei esula dalla presente Guida.

2.2.3 GESTIONE DEI DOCUMENTI INFORMATICI

(cfr. paragrafo 3.4 del MdG) Il sistema di gestione informatica dei documenti della AOO deve:

- garantire la sicurezza del sistema;
- garantire la corretta e la puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dalla AOO e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
- consentire il reperimento delle informazioni riguardanti i documenti registrati;
- consentire, 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;
- garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.

In relazione a quanto sopra, di seguito vengono fornite indicazioni essenziali per soddisfare i requisiti minimi di riservatezza, di integrità e di disponibilità dei documenti.
Uno dei primi requisiti da soddisfare per garantire l'adeguato livello di riservatezza di un documento è quello di effettuarne la classificazione attraverso la valutazione della criticità o della attualità che l'informazione contenuta nel documento riveste per l'Amministrazione.
I livelli di classificazione della riservatezza che si suggerisce di adottare in fase di protocollazione dei documenti nel registro di protocollo generale (distinto dal registro di protocollo particolare) sono quelli definiti nel PdP in uso presso l'AOO che quantomeno corrispondono alle seguenti categorie:

- non classificati;
- riservati.

Un documento mantiene il livello di classificazione assegnato nella fase di creazione o acquisizione per l'intero ciclo di vita all'interno dell'AOO e non può più essere modificato dagli addetti se non con richieste di modifica indirizzata al RSP.
Garantire l'integrità di un documento significa adottare misure di sicurezza destinate a contrastare o a evidenziare eventuali modifiche (dolose o colpose) del documento

rispetto a quando è stato formato (ad esempio dal soggetto mittente) o acquisito dall'AOO.
Il MdG deve riportare le soluzioni adottate dalla AOO per garantire i requisiti di sicurezza sopra richiamati.

2.2.3.1 Componente organizzativa della sicurezza

(cfr. paragrafo 3.4.1 del MdG) La componente organizzativa della sicurezza, che consiste nella definizione di una struttura operativa dedicata alla gestione della sicurezza, concerne principalmente alle attività svolte nella parte del sistema informativo della AOO erogatore del servizio di protocollo. Tale componente dovrà essere riportata sul MdG.

2.2.3.2 Componente fisica della sicurezza

(cfr. paragrafo. 3.4.2 del MdG) La componente fisica della sicurezza, da riportare sul MdG, ha lo scopo di proteggere il sistema informativo dai rischi originati da:

- furti e atti vandalici;
- calamità naturali;
- l'accesso illecito ai locali dell'Amministrazione/AOO dove risiedono le postazioni di lavoro di accesso e fruizione delle funzionalità del PdP, e dove sono ubicate le componenti hardware e software del sistema informativo.

2.2.3.3 Componente logica della sicurezza

(cfr. paragrafo 3.4.3 del MdG) La componente logica della sicurezza è ciò che garantisce i requisiti di integrità, di riservatezza di disponibilità e non ripudio dei dati, delle informazioni e dei messaggi. Nel MdG, *nei limiti di quanto richiesto nel precedente paragrafo 8.1, settimo capoverso*, devono essere illustrate le modalità di implementazione dei requisiti di sicurezza sopra richiamati.

2.2.3.4 Componente infrastrutturale della sicurezza

(cfr. paragrafo 3.4.4 del MdG) Questa componente assicura la continuità elettrica dei sistemi e le condizioni climatiche adeguate al corretto funzionamento delle risorse strumentali e garantisce l'efficienza del sistema di rilevazione e di spegnimento degli incendi.

2.2.3.5 Gestione delle registrazioni di protocollo e di sicurezza

(cfr. paragrafo 3.4.5 del MdG) Le registrazioni di sicurezza sono costituite dalle informazioni di diverso tipo (dati, transazioni, registrazioni, ecc.) presenti o transitate sulle componenti hardware e software del servizio di protocollo informatico che occorre conservare così come richiesto dalla normativa vigente allo scopo di:

- dirimere dispute legali che abbiano come oggetto di contesa le operazioni effettuate sul sistema stesso;
- analizzare dettagliatamente lo svolgersi di eventuali incidenti di sicurezza.

Le registrazioni di sicurezza considerate sono:

- i log di sistema, generati dal sistema operativo dei *server* su cui è installato il PdP;

- i log dei dispositivi di protezione periferica dell'infrastruttura di rete di accesso al sistema informativo;
- le registrazioni generate dal PdP della AOO.

Nel corrispondente paragrafo del MdG devono essere descritti i meccanismi per la scrittura "sicura" di tali registrazioni.

2.2.4 TRASMISSIONE E INTERSCAMBIO DEI DOCUMENTI INFORMATICI

Nel relativo paragrafo del MdG occorre indicare le misure di sicurezza adottate dalla AOO per realizzare trasmissioni sicure, in termini di:

- riservatezza della corrispondenza;
- titolarità del messaggio;
- aspetti della privacy;
- funzionalità del servizio di posta elettronica certificata.

2.2.4.1 All'esterno della AOO (interoperabilità dei sistemi di protocollo informatico)
(cfr. paragrafo 3.5.1 del MdG). 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 le attività ed i processi amministrativi conseguenti. Le misure di sicurezza che dovranno essere esplicitate nel MdG dovranno fare riferimento alle regole di interoperabilità vigenti, e di trasmissione dei documenti informatici, firmati digitalmente e inviati attraverso l'utilizzo della posta elettronica.

2.2.4.2 All'interno della AOO
(cfr. paragrafo. 3.5.2 del MdG) Per lo scambio dei messaggi all'interno della AOO con la posta elettronica non si richiede una particolare forma di protezione se l'accesso alla rete Intranet:

- è garantito da adeguate credenziali di autenticazione individuali costituite da una parte pubblica ed una riservata;
- è protetto da adeguate misure perimetrali di sicurezza associate a prodotti antivirus sempre aggiornati.

2.2.5 ACCESSO AI DOCUMENTI INFORMATICI

(cfr. paragrafo 3.6 del MdG) Per i documenti dell'archivio corrente nel MdG viene fatto riferimento alle funzionalità ed alle misure di sicurezza disponibili nel PdP per garantire l'accesso ai documenti informatici.
Nel MdG devono essere illustrate le misure di sicurezza adottate per garantire il diritto di accesso ai documenti amministrativi, secondo le modalità stabilite dall'articolo 22 della legge 7 agosto 1990, n. 241, recante "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi.
Per l'archivio di deposito e per l'archivio storico costituito sempre da documenti informatici, si deve fare esplicito riferimento, oltre che alla definizione delle modalità di accesso

e consultazione ed alle misure di sicurezza fisica e logica, alle ulteriori regole stabilite dalla AOO per individuare i documenti sottratti all'accesso, relativi a:

  - procedimenti tributari;
  - attività della Pubblica Amministrazione diretta all'emanazione di atti normativi, etc.
  - procedimenti selettivi contenenti informazioni di carattere psicoattitudinale
- al "codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" di cui all'allegato a2 del Codice in materia di protezione dei dati personali - decreto legislativo n. 196/2003[2].

2.2.6 CONSERVAZIONE DEI DOCUMENTI INFORMATICI

(cfr. paragrafo 3.7 del MdG)

2.2.6.1 Servizio archivistico

Il primo aspetto da considerare per garantire la "conservazione" del materiale documentario è la scelta della sede o dei locali da destinare allo scopo. Di tale attività si fa carico il responsabile del sistema archivistico che valuta i fattori di rischio che incombono sui documenti. Tali fattori di rischio possono essere suddivisi in tre grandi tipologie:

- ambientale, *in termini di possibili incendi, allagamenti, tempeste e bufere, variazioni di temperatura, umidità, illuminazione, ovvero dei livelli di inquinamento chimico, biologico, elettromagnetico, ecc.*;
- gestione degli accessi, delle movimentazioni e delle consultazioni;
- esistenza di piani di gestione delle situazioni di emergenza.

I requisiti ambientali della sede devono essere stabiliti da apposite regole tecniche, per le quali si deve inoltre:

- predisporre e testare periodicamente il piano di emergenza individuando gli incaricati di ciascuna fase;
- regolamentare minutamente le modalità di consultazione soprattutto interne, abolendo privilegi e accessi incontrollati;
- essere in ogni momento a conoscenza della collocazione del materiale archivistico attraverso elenchi di consistenza del materiale facente parte dell'archivio di deposito e un registro sul quale annotare i movimenti delle singole unità archivistiche.

Ciascuna AOO deve garantire la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti dalle norme correnti, ovvero altri formati standard che devono essere riportati sul MdG.
Il responsabile della conservazione sostitutiva dei documenti, in sintonia con il presente piano generale e con le linee guida tracciate dal RSP, definisce la procedura per la corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovi-

[2] Naturalmente sono esclusi dall'accesso i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801 e successive modificazioni, nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, da specifico regolamento governativo e dalle pubbliche amministrazioni.

bile non riscrivibile. Al riguardo, nella fase di definizione del piano di attuazione delle modalità operative, in termini di sicurezza, le AOO devono:

1. assicurare, per ogni aggiornamento del sistema, il pieno recupero e la riutilizzazione delle informazioni acquisite con le versioni precedenti;
2. garantire che le informazioni trasferite siano sempre consultabili. A tal fine, il responsabile per la tenuta del sistema di gestione informatica dei documenti dispone, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale:
   - la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici;
   - la distruzione dei supporti originali.

È inoltre consentito l'utilizzo di qualsiasi altro supporto di memorizzazione digitale, comunque idoneo a garantire la conformità dei documenti agli originali.

2.2.6.2 Conservazione in ambito PdP

Relativamente agli adempimenti e agli obblighi a carico delle AOO che operano con applicazioni realizzate in proprio le modalità di conservazione dei documenti informatici illustrate nel MdG devono riportare la descrizione completa delle misure di sicurezza adottate a livello di server, di postazioni di lavoro e di protezione fisica dei locali interessati dalla conservazione dei documenti informatici.

2.2.7 POLITICHE DI SICUREZZA ADOTTATE DALL'AOO

(cfr. paragrafo 3.8 del MdG) A seguito delle analisi svolte e descritte nei paragrafi precedenti nel MdG possono essere riportate le politiche di sicurezza che la AOO intende adottare per proteggere il proprio patrimonio documentale.
Le politiche devono contenere le misure preventive per la tutela del patrimonio informativo e l'accesso alle informazioni e sistemi di rilevazione degli incidenti verificatisi nel tempo allo scopo di prevenire eventuali malfunzionamenti futuri.
Per evitare l'inosservanza delle misure di sicurezza, si suggerisce di definire, prima della loro pubblicazione, le procedure da seguire in caso di riscontrata violazione delle politiche di sicurezza.

2.3 MODALITÀ DI UTILIZZO DI STRUMENTI INFORMATICI PER LO SCAMBIO DI DOCUMENTI

(cfr. capitolo 4 del MdG) Il presente paragrafo riporta le modalità di utilizzo degli strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'Area Organizzativa Omogenea.
Per quanto concerne la descrizione dell'utilizzo degli strumenti informatici che vengono utilizzati per realizzare lo scambio sicuro dei documenti informatici devono essere presenti almeno: la posta elettronica, le tecnologie che realizzano gli standard formali del sistema di protocollazione (XML, SMTP, MIME) e la firma digitale.

In relazione all'uso di altre tecnologie quali gli scanner, i supporti di memorizzazione rimovibili (CD ROM, DVD, pen drive, floppy disk, etc.), le reti Intranet, i sistemi di workflow, ecc., la relativa descrizione delle modalità di utilizzo sarà effettuata dalle AOO che ne fanno uso.
Prima di entrare nel merito alle modalità di utilizzo degli strumenti informatici per realizzare lo scambio dei documenti occorre caratterizzare l'oggetto di scambio: il documento amministrativo che, in termini funzionali può essere così classificato:

- ricevuto;
- inviato;
- interno formale (*a valenza giuridico-probatoria*);
- interno informale (*note ed appunti di ausilio all'esecuzione dell'affare senza nessuna valenza giuridico-probatoria*).

Ciascuna di queste tipologie, coerentemente al dettato delle norme vigenti, dovrà essere solo di tipo informatico. Solo nella fase transitoria di migrazione verso una amministrazione che opera integralmente in digitale, il documento amministrativo può essere disponibile anche nella forma analogica (di solito carta). Si rammenta che, *ai sensi dell'art. 53, comma 5 del DPR n. 445/2000* sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'Amministrazione e tutti i documenti informatici.
Lo scambio dei documenti informatici può essere effettuato con diversi mezzi e modalità. In ogni caso:

- "Nelle operazioni riguardanti le attività di produzione, di immissione, di conservazione, di riproduzione e di trasmissione di dati, di documenti e di atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate sia il soggetto che ha effettuato l'operazione".
- All'interno dei messaggi protocollati, prodotti ed inviati da una AOO mittente, devono essere previste le seguenti componenti:
  - un documento informatico primario;
  - un numero qualsiasi di documenti informatici allegati;
  - una segnatura informatica.
- Il documento primario che deve essere scambiato tra AOO deve essere sottoscritto con firma digitale.
- L'AOO deve indicare nel MdG le tipologie di documenti informatici - diversi da quelli primari destinati ad altra amministrazione - per i quali:
  - è prevista la sottoscrizione con firma digitale;
  - non è prevista la sottoscrizione;
  - sono ammesse le firme digitali difformi da quanto previsto dalla normativa corrente per i documenti a rilevanza interna.

- L'elenco delle tipologie di documenti che devono essere obbligatoriamente sottoscritti per consentirne la protocollazione in uscita e il personale che ha delega di firma per l'amministrazione devono essere indicati nel MdG e devono essere resi disponibili dalle AOO alle UOP.
- Ciascuna AOO ricevente stabilisce se e come utilizzare le informazioni facoltative contenute nella segnatura di protocollo per automatizzare i processi di assegnazione e trattamento dei documenti. Le possibili scelte della AOO sulle modalità di trattamento delle informazioni facoltative dovranno, comunque, essere riportate nel MdG.

Scopo degli strumenti informatici per lo scambio dei messaggi e degli *standard* di composizione dei messaggi è garantire:

- l'integrità del messaggio;
- la riservatezza del messaggio;
- il non ripudio dei messaggi;
- l'automazione dei processi di protocollazione e di 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 dell'avvenuta ricezione;
- l'interoperabilità dei sistemi informativi pubblici.

In aggiunta alle modalità di scambio dei documenti informatici previste dalla normativa in materia, le amministrazioni possono utilizzare altre modalità di trasmissione degli stessi documenti purché descritte nel MdG.

2.4 DESCRIZIONE DEL FLUSSO DI LAVORAZIONE DEI DOCUMENTI

(cfr. capitolo 5 del MdG) Il relativo paragrafo riporta la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o scambiati internamente, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.
Descrivere i flussi di lavorazione significa formalizzare le fasi dei processi di gestione dei documenti acquisiti (*ricevuti o formati in seno alla AOO*), trasmessi e scambiati internamente, integrati nei flussi di lavoro dell'AOO (movimentazione, lavorazione e conservazione nell'archivio corrente). La descrizione dei flussi di seguito illustrata è relativa a tali processi, all'interno dei quali devono essere descritti in dettaglio nel MdG gli aspetti operativi connessi con l'impiego delle tecnologie digitali e con metodi tradizionali (carta).
Prima di effettuare la descrizione del flusso di lavorazione è necessario descrivere il sistema documentario nazionale, ed effettuare una analisi dei processi volta al miglioramento degli stessi attraverso l'operazione definita di reingegnerizzazione.
Tali attività sono propedeutiche al corretto impiego del sistema di protocollazione informatica e gestione documentale all'interno della AOO.

In un sistema di gestione e tenuta dei documenti devono essere tenuti presenti oltre che il documento e il suo contenuto anche i collegamenti che esso ha con altri documenti dell'archivio e in particolare con quelli che riguardano un medesimo affare.
Per grandi linee il flusso documentale è caratterizzato dalla fase di acquisizione o formazione del documento, dalla classificazione, dalla lavorazione, dall'invio e dalla conservazione.
L'intero processo sinteticamente rappresentato, si colloca a livello di sistema documentario quale "concetto" più ampio di quello archivistico dato che si riferisce, non solo all'insieme dei documenti prodotti o acquisiti dalla AOO nell'esercizio delle sue funzioni, ma anche dall'insieme delle regole, delle procedure e delle risorse per la loro formazione, organizzazione, reperimento, utilizzo e conservazione.
Il sistema di gestione dei flussi documentali deve quindi:

- fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
- consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
- fornire informazioni statistiche sull'attività dell'ufficio;
- consentire lo scambio di informazioni con altri sistemi di gestione dei flussi documentali di altre AOO al fine di determinare lo stato e l'iter dei procedimenti complessi.

Sul MdG i processi sopra richiamati possono essere riportati sia come diagramma di flusso, sia in modo descrittivo.
Il riuso della descrizione dei flussi di lavorazione e della sequenza delle operazioni riportata nei Modelli del MdG, eseguita a titolo esemplificativo, si ritiene non obbligatoria e comunque non vincolante in quanto tale descrizione deve rappresentare il flusso dei documenti della specifica AOO.
Poiché il Manuale è relativo a tutto il sistema di gestione dei documenti, è necessario descrivere anche i flussi di lavorazione dei documenti non soggetti a registrazione di protocollo generale. Essendo tale descrizione specifica di ogni AOO, ciascuna di queste provvede autonomamente alla descrizione del proprio flusso dei documenti interni.
Nelle pagine seguenti viene riportata, a titolo esemplificativo, la descrizione dei flussi di lavorazione dei documenti ricevuti e inviati. La lavorazione dei documenti all'interno del sistema archivistico viene riportata, nel capitolo 9 del Modello di MdG intitolato "Sistema di classificazione, fascicolazione e piano di conservazione".
La AOO deve adottare gli schemi che meglio rappresentano la propria realtà e deve descriverli ad un livello di dettaglio paragonabile a quello riportato nel Modello di Manuale.

Diagramma di flusso dei documenti ricevuti alla AOO

(ivi compresi quelli a circolazione interna)

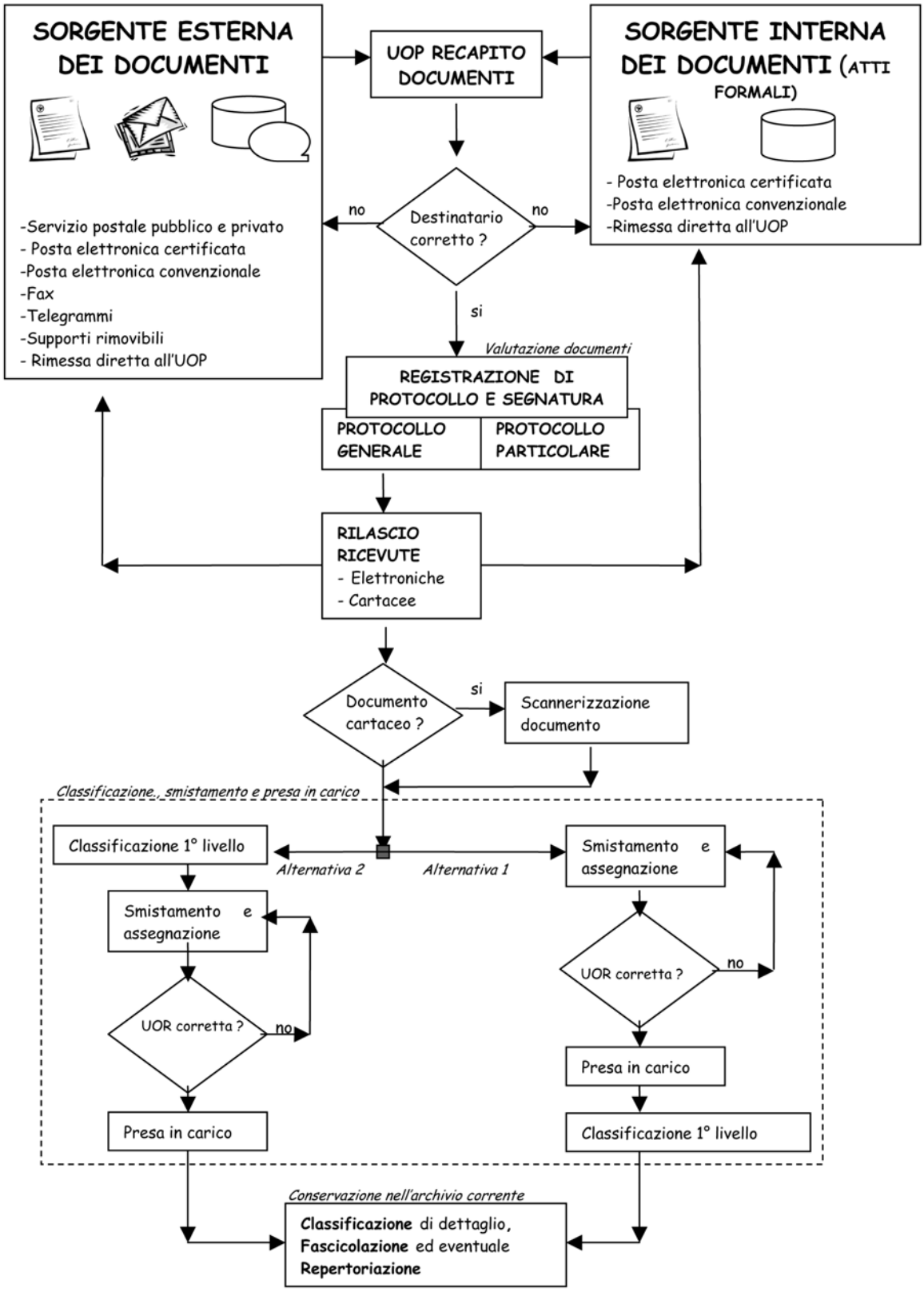
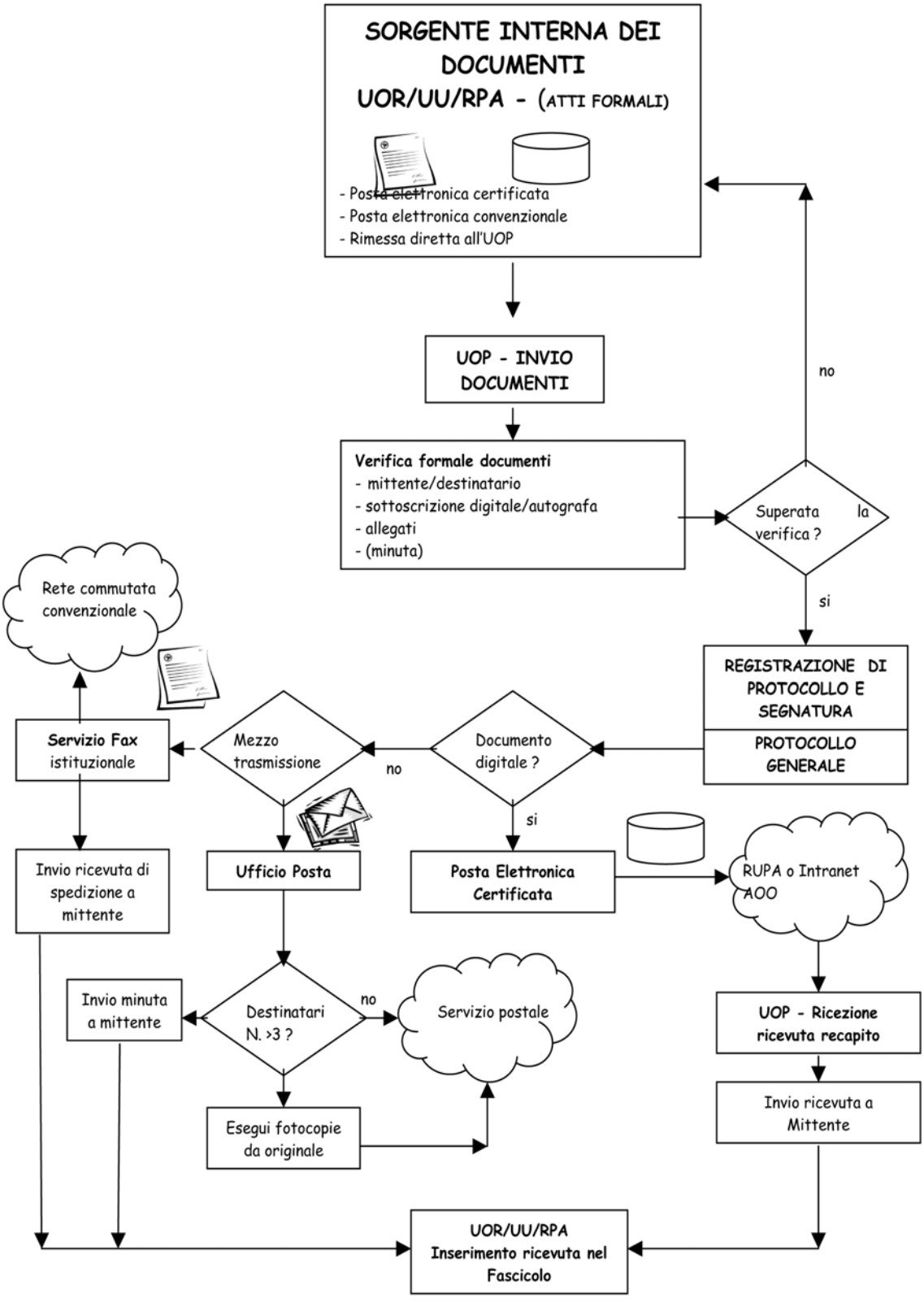


Diagramma di flusso dei documenti inviati dalla AOO
(ivi compresi quelli a circolazione interna)



2.5 REGOLE DI SMISTAMENTO ED ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

(cfr. capitolo 6 del MdG) Il relativo paragrafo riporta le regole di smistamento e di assegnazione dei documenti ricevuti con l'individuazione dei criteri per l'ulteriore eventuale inoltro verso AOO della stessa Amministrazione e/o verso altre Amministrazioni/AOO.
Ciascuna Amministrazione stabilisce autonomamente le modalità di inoltro e di assegnazione dei documenti al singolo UOR e UU e le descrive nel Manuale di gestione.
Tali modalità devono essere dettagliate e complete soprattutto se l'AOO opera direttamente su documenti informatici che consentono di eseguire automaticamente l'assegnazione e la presa in carico.
All'interno di una AOO l'assegnazione può essere effettuata direttamente da parte delle UOP o, in alternativa, possono essere previste strutture intermedie di smistamento.
Gli operatori di protocollo che utilizzano le funzioni del PdP devono essere invitati a non riportare, per quanto possibile, dati personali nel campo "oggetto" della maschera di registrazione del protocollo e devono essere formalmente "incaricati" del trattamento dei dati personali. E' opportuno che anche il personale che opera nelle strutture di smistamento sia espressamente "incaricato" dal titolare o dal responsabile (se nominato) de trattamento dei dati personali considerato che, attraverso le informazioni contenute nel campo "oggetto" si possono trattare i dati personali comuni, sensibili e giudiziari.

2.6 UO RESPONSABILI DELLE ATTIVITÀ DI REGISTRAZIONE DI PROTOCOLLO, ORGANIZZAZIONE E TENUTA DOCUMENTI

(cfr. capitolo 7 del MdG) Il relativo paragrafo riporta le Unità Organizzative responsabili delle attività di registrazione di Protocollo, di organizzazione e tenuta dei documenti all'interno della AOO.
In base al modello organizzativo adottato dall'amministrazione, nel MdG devono essere descritti, nell'allegato corrispondente, gli aspetti organizzativi della AOO in termini di funzioni che devono svolgere:

- le UOP;
- gli UOR e gli UU;
- i RPA anche in relazione alle modalità di tenuta dell'archivio corrente;
- gli addetti all'archivio.

In relazione alla organizzazione e alla tenuta dei documenti dell'Amministrazione all'interno di ciascuna AOO, deve essere formalmente istituito il servizio archivistico e il servizio per la conservazione sostitutiva e devono essere definite le strutture dedicate alla conservazione dei documenti siano essi informatici che cartacei.
I servizi qui richiamati e le strutture di conservazione dei documenti devono essere individuati e formalizzati prima dell'attivazione del servizio di gestione informatica del protocollo, dei documenti e degli archivi.

2.6.1 INDIVIDUARE E PUBBLICARE LE UOP - UNITÀ ORGANIZZATIVE RESPONSABILI DI PROTOCOLLAZIONE

Per quanto concerne la definizione e la organizzazione delle UOP l'Amministrazione opta per la soluzione più adatta alle proprie caratteristiche, dimensioni, dispiegamento sul territorio ed organizzazione.
In particolare può essere adottata una delle due seguenti soluzioni:

- sistema totalmente centralizzato, caratterizzato da un'unica UOP per la ricezione e la trasmissione della corrispondenza;
- sistema totalmente distribuito, caratterizzato da più sedi/uffici di registratura (UOP) per la ricezione e la trasmissione della corrispondenza necessariamente supportato da una adeguata infrastruttura telematica ed applicativa che garantisca l'univocità del protocollo.

È ovviamente possibile optare per soluzioni intermedie *(ad esempio, unica UOP di ricevimento posta e più UOP di spedizione)* che, in alcuni casi, meglio si adattano alle esigenze dell'Amministrazione, ovvero alla sua evoluzione.
A seguito di tale attività è possibile redigere lo schema relativo all'organigramma dell'AOO. È opportuno che tale organigramma sia riportato in allegato al MdG e reso pubblico per favorire il corretto invio delle istanze e l'accesso degli interessati alle UOR/UU responsabili dei procedimenti.

2.6.2 RESPONSABILE DEL SERVIZIO ARCHIVISTICO

Nell'ambito del servizio per la gestione informatica dei documenti, dei flussi documentali e degli archivi, può essere prevista la figura di responsabile del servizio archivistico a cui il Responsabile del Servizio di Protocollo (RSP) può delegare i seguenti compiti:

- collaborare con il Responsabile del Servizio per la tenuta del Protocollo e la gestione documentale per:
  - predisporre lo schema del Manuale di gestione;
  - stabilire i criteri minimi di sicurezza informatica del sistema;
  - organizzare il sistema di gestione dei flussi documentali e la classificazione dei documenti, lo smistamento e l'assegnazione dei documenti alle UOR (sulla scorta dell'organigramma dell'Amministrazione), la costituzione e la repertoriazione dei fascicoli, l'individuazione dei responsabili della conservazione dei documenti e dei fascicoli nella fase corrente;
  - stabilire i livelli di accesso ai documenti archivistici e regolamentare le forme di consultazione interna ed esterna dell'archivio, nel rispetto della normativa sulla tutela della riservatezza dei dati personali, con particolare riferimento all'allegato "A.2 Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici" del d. lgs. 196/03;

- organizzare la fase di versamento dei documenti dagli uffici all'Archivio generale, insieme con gli strumenti di corredo, e predisporre l'elenco dei fascicoli e delle serie ricevute;
- curare e garantire la conservazione dell'archivio nella fase di deposito;
- predisporre il piano di conservazione dei documenti, prescritto dal DPR 445/2000, art. 68;
- predisporre il massimario di scarto;
- effettuare la selezione periodica dei documenti e procedere allo scarto o al trasferimento nella separata sezione d'archivio del materiale destinato alla conservazione permanente.

2.6.3 RESPONSABILE DELLA CONSERVAZIONE SOSTITUTIVA

Al responsabile della conservazione sostitutiva vengono attribuiti i compiti e le responsabilità definite dal RSP specificatamente indirizzati alla corretta esecuzione delle operazioni di salvataggio dei dati su supporto informatico rimovibile adottando le regole e procedure più idonee a garantire nel tempo la leggibilità dei medesimi.
In particolare:

- è consentito il trasferimento su supporto informatico rimovibile delle informazioni di protocollo relative ai fascicoli che fanno riferimento a procedimenti conclusi;
- le informazioni trasferite dovranno essere sempre consultabili. A tal fine, il RSP dispone, in relazione all'evoluzione delle conoscenze scientifiche e tecnologiche, con cadenza almeno quinquennale, la riproduzione delle informazioni del protocollo informatico su nuovi supporti informatici.

2.7 ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

(cfr. capitolo 8 del MdG) Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dalla AOO e tutti i documenti informatici interni di rilevanza giuridico-probatoria.

Ne sono esclusi i documenti richiamati nell'articolo 53, comma 5, DPR n. 445/00.
Nel Manuale di gestione devono essere riportati espressamente questi documenti ed altri eventuali documenti che l'AOO non intende registrare nel protocollo generale.
Se il PdP lo consente, tali documenti possono essere registrati nel PdP attraverso specifiche funzionalità che operano su registri (personalizzabili dalla AOO) diversi da quello del protocollo informatico generale.

2.8 ELENCO DEI DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

(cfr. capitolo 8 del MdG) Il presente paragrafo "fornisce l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento".
Ogni AOO deve autonomamente riportare nell'allegato corrispondente del MdG l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento.

Qualora un documento informatico pervenga ad una UOP di una AOO per canali diversi dai sistemi di posta elettronica compatibili con il protocollo SMTP/MIME, è responsabilità dell'ufficio stabilire, se il documento sia soggetto alla registrazione di protocollo ovvero a registrazione particolare.
Tali modalità di trattamento dei documenti informatici devono essere formalizzate anticipatamente sul MdG unitamente alla corrispondenza cartacea ordinaria, ai messaggi telefax, alle raccomandate e alle assicurate.

2.9 IL SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

(cfr. capitolo 9 del MdG) Il corrispondente paragrafo riporta il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, anche con riferimento all'uso di supporti sostitutivi.
Le amministrazioni determinano autonomamente e in modo coordinato con le AOO (*peraltro autonome in termini di adozione del sistema di classificazione*), le modalità con cui i documenti sono fascicolati e correlati ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo.
Il sistema di classificazione, assieme al repertorio dei fascicoli, è lo strumento che permette di:

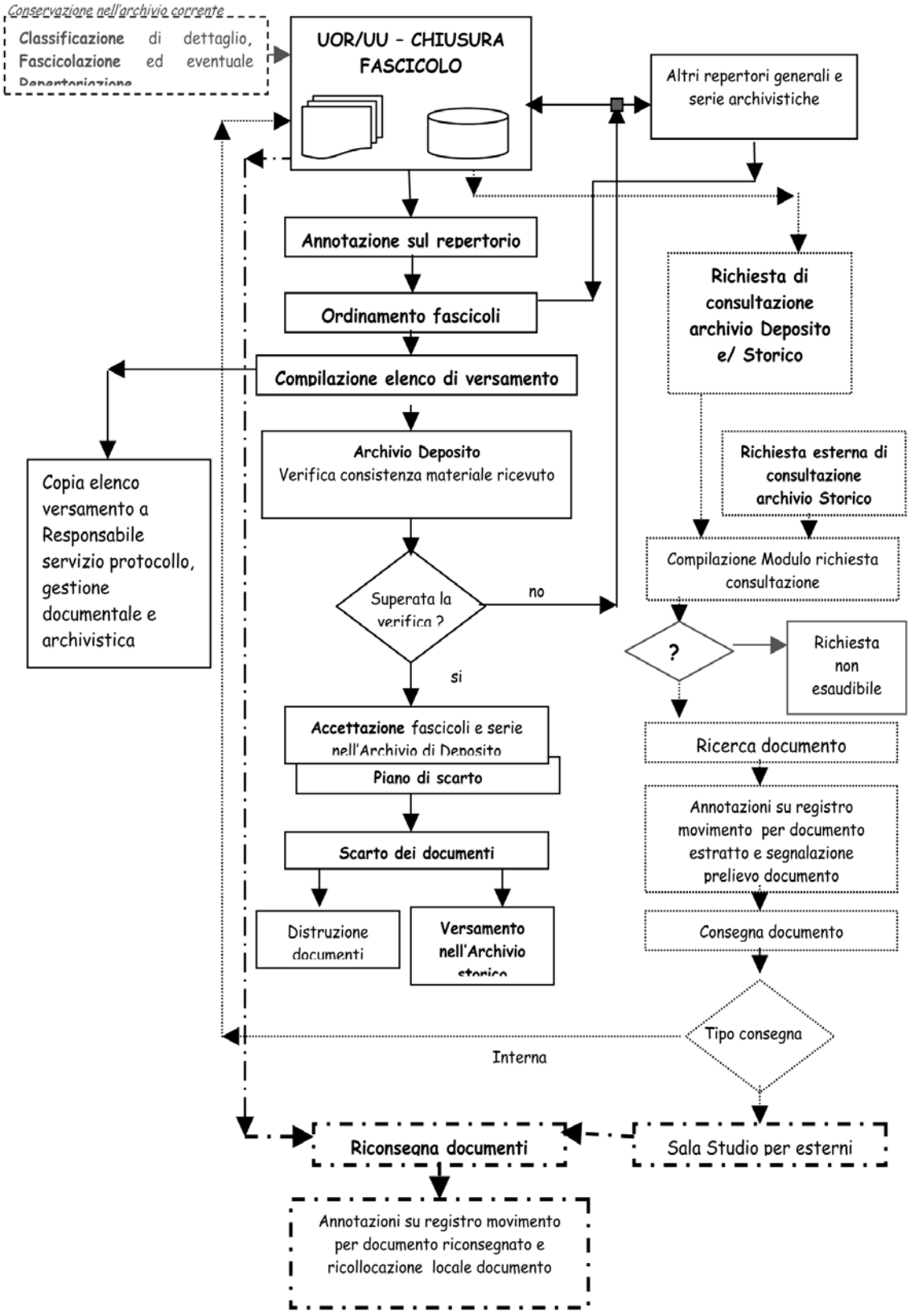
- organizzare tutti i documenti secondo un assetto logico, con riferimento alle funzioni (missione) e alle attività (competenze) svolte dall'amministrazione interessata;
- favorire la reperibilità del documento facendo riferimento sia all'argomento, ai contenuti e all'ufficio competente.

Un sistema di classificazione è caratterizzato dalla stabilità, legata alla missione e alle funzioni dell'Amministrazione/AOO.

Può risultare infine opportuno:

- riportare nel capitolo in argomento, il diagramma di flusso dei documenti all'interno del sistema archivistico che schematizza attività e momenti di vita dei fascicoli;
- predisporre un allegato specifico che, in modo ordinato e completo, stabilisca le "Regole generali per la costituzione, l'organizzazione e la fruizione" dell'archivio dell'Amministrazione/AOO. Il regolamento allegato a titolo esemplificativo è relativo ai comuni.

Diagramma di flusso dei documenti all'interno del sistema archivistico



2.10 MODALITÀ DI PRODUZIONE E DI CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO INFORMATICO

(cfr. capitolo 10 del MdG) Il relativo paragrafo riporta 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.
Indipendentemente dalla tecnologia utilizzata (digitale o analogica), ad ogni documento ricevuto e trasmesso dalla AOO, corrisponde una unica operazione di registrazione e segnatura di protocollo.
La registrazione di protocollo di ogni documento ricevuto o spedito dalla AOO deve essere effettuata mediante la memorizzazione delle seguenti informazioni minime:

- numero di protocollo del documento, generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo, assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, destinatario per i documenti spediti, registrati in forma non modificabile;
- oggetto del documento, registrato in forma non modificabile;
- l'impronta del documento informatico, se trasmesso o ricevuto per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Nel caso di documenti informatici la registrazione di protocollo può essere apposta sia al corpo del messaggio inviato/ricevuto sia ad uno o più dei file ad esso allegati.
I messaggi di posta elettronica ricevuti da una AOO che sono soggetti alla registrazione di protocollo, devono essere indirizzati, preferibilmente, alla casella di posta elettronica istituzionale dell'AOO destinataria del messaggio. L'eventuale indicazione del soggetto destinatario del documento, va riportata nella segnatura di protocollo secondo le modalità ed i formati previsti dalla regole tecniche in vigore.
In aggiunta alle modalità sopra espresse, le AOO possono utilizzare altre modalità di trasmissione di documenti informatici purché siano descritte nel Manuale di gestione.
Il sistema di protocollazione deve consentire la 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. L'assegnazione delle informazioni nelle operazioni di registrazione e segnatura di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati.
Il MdG deve inoltre riportare le indicazioni in merito alle misure di sicurezza adottate dall'Amministrazione/AOO per la raccolta e la conservazione delle copie delle registrazioni di protocollo generale quotidianamente generate dal PdP.

2.11 DESCRIZIONE DEL SISTEMA DI PROTOCOLLO INFORMATICO

(cfr. capitolo 11 del MdG) Il relativo paragrafo riporta la descrizione delle funzionalità del sistema di protocollo informatico con particolare riferimento alle modalità di utilizzo.

La descrizione dovrà essere effettuata indicando con chiarezza e completezza le modalità di utilizzo del sistema da parte di tutti coloro che sono abilitati ad operare nel sistema medesimo. Questa descrizione, all'occorrenza, può limitarsi a fornire una descrizione delle principali funzionalità rimandando i dettagli a specifici manuali.
Le AOO devono garantire almeno le "funzionalità minime" del sistema di protocollo informatico come previsto dalla normativa vigente. Le operazioni di registrazione, di segnatura di protocollo e quelle di classificazione sopra richiamate, costituiscono attività necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle amministrazioni.
Per garantire le funzionalità minime obbligatorie è necessario che il sistema di protocollo permetta di effettuare non solo le operazioni di registrazione e segnatura ma anche quelle di conservazione e di consultazione della documentazione al fine di rendere possibile l'accesso alla documentazione da parte degli addetti abilitati sia in modalità locale che in modalità remota.

2.12 RILASCIO DELLE ABILITAZIONI DI ACCESSO ALLE INFORMAZIONI DOCUMENTALI

(cfr. capitolo 12 del MdG) Il relativo paragrafo fornisce indicazioni in merito ai criteri e alle modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali.
Sono previsti tre tipi di accesso ai dati, ai documenti ed alle informazioni del sistema informatico di protocollo:

1. accesso al sistema da parte degli utenti appartenenti alla stessa AOO;
2. accesso al sistema da parte dei soggetti esterni alla AOO che esercitano il diritto di accesso ai documenti amministrativi;
3. accesso al sistema da parte di altre AOO.

Per tutti i tipi di accesso, anche in conformità alla normativa vigente di protezione dei dati personali, le AOO dovranno stabilire quali sono le abilitazioni necessarie e le diverse modalità di interrogazione, di selezione e di estrazione delle informazioni, a seconda del grado di riservatezza delle stesse e della tipologia di utenti, utilizzando a tal fine la firma digitale o certificati di autenticazione.
Sul Manuale, dovranno essere pubblicate:

A. le modalità per il rilascio delle abilitazioni all'interno e all'esterno dell'AOO;
B. le politiche di accesso e le autorizzazioni al trattamento dei documenti previste dall'AOO, sia nel caso di accesso diretto (da locale o remoto), sia nel caso di una struttura e/o ufficio che tiene rapporti con il pubblico.

(A) L'accesso al sistema da parte degli utenti appartenenti alla AOO, nonché la ricerca, la visualizzazione e la stampa di tutte le informazioni relative alla gestione dei documenti sono disciplinati dai criteri di abilitazione stabiliti dal RSP.
(B) Per l'esercizio del **diritto** di accesso dall'esterno ai documenti amministrativi, possono essere utilizzate tutte le informazioni del sistema di gestione informatica dei documen-

ti anche mediante l'impiego di procedure applicative operanti al di fuori del sistema e strumenti che consentono l'acquisizione diretta delle informazioni da parte dell'interessato. A tal fine le pubbliche amministrazioni determinano i criteri tecnici ed organizzativi per l'impiego, anche per via telematica, del sistema di gestione informatica dei documenti per il reperimento, la visualizzazione e la stampa delle informazioni e dei documenti.
Nel caso di accesso effettuato mediante strumenti che consentono l'acquisizione diretta delle informazioni e dei documenti da parte dell'interessato, le misure organizzative e le norme tecniche sopra richiamate indicano, altresì, le modalità di identificazione del soggetto anche mediante l'impiego di strumenti informatici per la firma digitale del documento informatico, come previsto dalla normativa in materia.
Nel caso di accesso effettuato da soggetti non appartenenti alla Pubblica Amministrazione possono essere utilizzate le funzioni di ricerca e di visualizzazione delle informazioni e dei documenti messe a disposizione - anche per via telematica - attraverso gli Uffici per le Relazioni con il Pubblico.

2.13 MODALITÀ DI UTILIZZO DEL REGISTRO DI EMERGENZA

(cfr. capitolo 13 del MdG) Il corrispondente paragrafo riporta le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente.
Il RSP autorizza lo svolgimento anche Manuale delle operazioni di registrazione di protocollo effettuate su uno o più registri di emergenza, ogni volta che per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema.
Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il RSP può autorizzare l'uso del registro di emergenza per periodi di tempo superiori e comunque per non più di una settimana. Sul registro di emergenza sono riportati gli estremi del provvedimento di autorizzazione.
Per ogni giornata di registrazione di emergenza deve essere riportato sul relativo registro il numero totale di operazioni registrate.
La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'AOO.
Le informazioni relative ai documenti protocollati in emergenza devono essere inserite nel sistema informatico del protocollo generale senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza deve essere attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza.
Le modalità operative con cui vengono adottate le norme sopra richiamate devono essere riportate nel MdG.

2.14 GESTIONE DEI PROCEDIMENTI

(cfr. capitolo 14 del MdG) Anche se non espressamente richiesto dalla normativa vigente in materia di protocollo informatico e gestione documentale, nel più ampio, integrato e

completo contesto dell'e-government, è importante raccogliere in modo ordinato i risultati del riesame dei procedimenti amministrativi caratterizzanti la AOO.

Al riguardo si suggerisce di costituire una banca dati dei procedimenti amministrativi, dei loro iter e dei responsabili (RPA), da aggiornare con la registrazione dell'avvio e degli stati di avanzamento dei procedimenti stessi.
Nei modelli di MdG viene riportato un esempio di definizione e impiego di dette banche dati.

2.15 APPROVAZIONE E AGGIORNAMENTO DEL MANUALE, NORME TRANSITORIE E FINALI

(cfr. capitolo 15 del MdG) All'interno del Manuale in argomento, è opportuno prevedere un apposito paragrafo che disciplina i criteri e le modalità di aggiornamento.

Bibliografia

[1] AIPA, GEDOC 2, *Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni,* settembre 2000.

[2] AIPA - GEDOC, *Studio di prefattibilità sul sistema di gestione dei flussi di documenti,* 24 febbraio 1997.

[3] CNIPA, *Proposta di schema per il manuale di gestione.*

[4] Scuola Superiore della Pubblica Amministrazione, *La metodologia per la definizione di piani di classificazione in ambiente digitale,* a cura di E. Aga Rossi e M. Guercio, Roma, 2005.

[5] M. Grandi, G. Longobardi, S. Pigliapoco, M.P. Giovannini, G. Butti, *Il protocollo informatico nella Pubblica Amministrazione*, a cura di D. Piazza, Maggioli Editore, marzo 2003.

[6] Università degli studi di Padova, Trieste e Bologna e Istituto Universitario di Architettura di Venezia, *Manuale di Gestione del protocollo informatico,* versione 1.1 del 10 luglio 2001.

[7] Regione Marche, Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni – FDRM, *Linee guida per la stesura del manuale di gestione per l'archivio dei Comuni.*

[8] P. Mariotti, *Le politiche di sicurezza delle informazioni*, Università degli Studi di Siena, Facoltà di Ingegneria, Dipartimento di Ingegneria delle Informazioni, Progetto Sicurnet.

[9] M. Guercio, *La gestione elettronica dei documenti e la tenuta degli archivi, Principi generali e requisiti archivistici – La gestione integrata dei documenti nella pubblica Amministrazione.*

[10] G. Penzo Doria, *La linea dell'arco – Criteri di redazione di titolari di classificazione.*

[11] Provincia Bologna, *Progetto DOCAREA, Modello di manuale di gestione dei documenti conforme al DPCM 31 ottobre 2000,* versione 0 rev. 3, luglio 2003.

[12] Provincia Bologna, *Progetto DOCAREA, Regolamento generale per gli archivi comunali,* versione 0 – rev. 1.

[13] Comune di Fabriano (Provincia di Ancona), *Manuale di gestione dei flussi documentali e del protocollo informatico,* versione 1.0 del 11-12-2003.

[14] Comune di Fabriano (Provincia di Ancona), *Allegati al Manuale di gestione dei flussi documentali e del protocollo informatico,* versione 1.0 del 11-12-2003.

[15] Comune di Mirabello Sannitico (Provincia di Campobasso), *Regolamento per la tenuta del protocollo e dell'archivio - manuale per la gestione del protocollo informatico,* 2004.

[16] G. PERONDI, *Manuale di gestione e conservazione dei documenti,* Progetto Archivio-Protocollo Camera di commercio di Lodi, versione 1.2 giugno 2003.

[17] Regione Marche, Dipartimento Affari Istituzionali e generali, Scuola di Formazione del Personale Regionale, *Tecniche per la elaborazione di un modello organizzativo e archivistico idoneo alla gestione informatica dei documenti e schema di riferimento per la elaborazione del manuale di gestione dei documenti.*

[18] Ministero della salute, *Manuale di gestione del protocollo informatico,* bozza 15 luglio 2003.

[19] Area Organizzativa Omogenea sede ACI, *Manuale di gestione del protocollo informatico,* versione a cura del Servizio Patrimonio e della Direzione Sistemi Informativi.

[20] Istituto Nazionale per il Commercio Estero, *Manuale di gestione elettronica dei documenti,* versione 1.3 del 30 ottobre 2003, bozza.

[21] Agenzia del Territorio, *Manuale di gestione del protocollo, dei flussi documentali ed archivi-Bozza per discussione versione light*, a cura dalla Direzione Centrale O.S.I. - Ufficio Organizzazione, edizione giugno 2003.

[22] Comune di Cariati (Provincia di Cosenza), *Regolamento per la tenuta del protocollo e dell'archivio manuale per la gestione del protocollo informatico.*

[23] Comune di Castiglione Casentino (Provincia di Cosenza), *Manuale di gestione del Protocollo informatico,* novembre 2003.

[24] Distretto scolastico 53, Istituto Tecnico Industriale Statale "Augusto Righi" di Taranto, *Manuale di gestione del protocollo informatico.*

[25] Amministrazione Provinciale di Piacenza, *Manuale di gestione dei documenti conforme al DPCM 31 ottobre 2000 – bozza,* Piacenza 25.02.2002.

[26] Comune di Giulianova Marche (Provincia di Macerata), *Disposizioni per la gestione del protocollo informatico.*

[27] *Manuale di Gestione del protocollo informatico della Comunità Montana del Catria e Nerone.*

[28] L. RICCIOTTI, *Protocollo Informatico e Gestione dei Flussi documentali - Manuale di gestione*, versione 1.0, Comune di Macerata.

[29] *Manuale di gestione del protocollo informatico della Camera di commercio industria artigianato e agricoltura di Torino*, versione 1.0 del 31 ottobre 2003.

[30] S. CAMPAGNA, *Manuale di Gestione del Protocollo Informatico dei Flussi documentali e degli Archivi,* Camera di Commercio Industria Artigianato e Agricoltura di Prato, versione 1.0 del 31-12-2003.

[31] Camera di Commercio Industria Artigianato e Agricoltura di Alessandria, *Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi,* versione 1.0 del 22-12-2003.

[32] Comune di Agevola (Provincia di Napoli), *Manuale di Gestione Protocollo Informatico.*

[33] Comune di Argenta (Provincia di Ferrara), Settore Segreteria Affari Generali Sviluppo Economico - U.O.C. Protocollo, *Manuale di gestione del protocollo.*

[34] Comune di Cavarzere (Provincia di Venezia), *Manuale di gestione dei documenti del Comune di Cavarzere.*

[35] Comune di Chiavari (Provincia di Genova), *Manuale di gestione del Protocollo, dei flussi documentali e degli archivi.*

[36] Comune di Colorno (Provincia di Parma), *Manuale di gestione del Protocollo e dei flussi documentali.*

[37] Comune di Breda di Piave (Provincia di Treviso), *Manuale di gestione del Protocollo informatico e del servizio archivistico comunale,* 30-12-2003.

[38] Comune di Foligno (Provincia di Ancona), *Manuale di gestione ed archiviazione dei documenti del Comune di Foligno.*

[39] R. GRAZIANI, *Manuale di gestione dei documenti,* Comune di Gallio (Provincia di Vicenza), 21-11-2003.

[40] Comune di Modena, *Regolamento generale del Servizio Archivio del Comune di Modena.*

[41] Comune di Momo (Provincia di Novara), *Manuale di gestione del Protocollo.*

[42] Comune di Montagnana (Provincia di Padova), *Manuale di gestione del Protocollo – Archivio.*

[43] Comune di Montecatini Terme (Provincia di Pistoia), *Regolamento per la tenuta del Protocollo Generale, l'organizzazione e la gestione dell'Archivio Storico, Corrente e di Deposito,* 28-03-02.

[44] Comune di Omegna (Provincia di Verbania), *Manuale di gestione del protocollo informatico,* 31-10-2000.

[45] Comune di Ostellato (Provincia di Ferrara), *Manuale di gestione dei documenti.*

[46] Comune di Ninnai (Provincia di Cagliari), *Regolamento per la gestione del protocollo informatico e dei flussi documentali,* 30-09-2002.

[47] Comune di Terricola (Provincia di Pisa), *Manuale di gestione del protocollo informatico e dei flussi documentali e degli archivi*, a cura del gruppo di lavoro Rete Archivistica Provinciale di Pisa, dicembre 2003.

[48] Comune di Imperia, Settore Informatica e Servizi Demografici, *Manuale di gestione del Protocollo informatico.*

[49] Comune di Perugia, *Manuale di gestione del Protocollo informatico.*

[50] Comune di Viareggio (Provincia di Lucca), Servizio Organizzazione del Personale e Servizi Informativi, *Regolamento per la gestione del protocollo informatico e dei flussi documentali del Comune di Viareggio.*

[51] Comune di Baceno (Provincia di Verbania), *Protocollo informatico – manuale di gestione.*

[52] Comune di Cumiana (Provincia di Torino), *Protocollo informatico – manuale di gestione e conservazione dei documenti*, 18-03-2004.

[53] Comune di Novate Milanese (Provincia di Milano), *Regolamento per la gestione del protocollo e dell'archivio,* 28-11-2000.

[54] Comunità Montana dell'Appennino Faentino (Provincia di Ravenna), *Manuale di gestione del protocollo, dei flussi documentale e degli archivi.*

[55] Comune di Civitanova Marche (Provincia di Macerata), *Disposizioni per la gestione del protocollo informatico.*

[56] Provincia di Macerata, *Manuale di gestione del flussi documentali e del protocollo informatico,* versione 1.0.

[57] Comune di Pisa, *Regolamento per la gestione, tenuta e tutela dei documenti amministrativi.*

[58] RUPAR Puglia, *Guida al protocollo informatico.*

[59] Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni, *Linee guida per la stesura del manuale di gestione per l'archivio dei Comuni.*

[60] *Linee guida per la conservazione e lo scarto della documentazione conservata presso le istituzioni scolastiche della provincia autonoma di Trento.*

[61] Provincia Caserta, *Manuale di gestione del Protocollo Informatico ASL CE/2 di Aversa.*

[62] Azienda Ospedaliera di Parma, *Manuale di gestione del protocollo informatico*, Parma.

[63] Azienda Ospedale Università San Martino di Genova**,** *Manuale di gestione del Protocollo Informatico,* Genova.

[64] Istituto Giannina Gaslini, Ospedale Pediatrico, *Manuale di gestione,* versione 1.0, Genova, 16-12-03.

[65] *Manuale di gestione del Protocollo informatico dell'Università degli Studi di Trieste,* Trieste.

[66] Università degli Studi del Sannio, *Manuale di gestione del protocollo informatico.*

[67] F. TROMBONE, *Informatizzazione del Protocollo e dei Flussi documentali*, Università degli Studi di Napoli, Napoli.

[68] Università degli Studi di Pavia, *Manuale di gestione del protocollo informatico*, Pavia, 23-07-2003.

[69] *Regolamento per la gestione, tenuta e tutela dei documenti amministrativi dal protocollo all'archivio storico per l'Amministrazione Centrale dell'Università Ca' Foscari di Venezia*, Venezia.

[70] UNIONCAMERE, Comitato tecnico scientifico per gli archivi delle Camere di Commercio, Sottocommissione per la revisione del titolario d'archivi, *Titolario di classificazione dei documenti d'archivio delle Camere di Commercio*, dicembre 2000.

[71] Gruppo di lavoro per la formulazione di proposte e modelli per la riorganizzazione dell'archivio dei Comuni, *Piano di classificazione (= Titolario) per gli archivi dei Comuni italiani.*

[72] Camera di Commercio Industria Artigianato e Agricoltura Prato, *Massimario di selezione - Manuale di gestione del protocollo informatico.*

[73] Soprintendenza Archivistica per la Toscana, *Massimario di scarto per i comuni – 2002.*

[74] S. GUIATI, *Massimario di selezione e conservazione della provincia di Pisa,* Pisa.

[75] Province dell'Emilia Romagna, *Bozza di modello di titolario per le province.*

[76] Provincia di Cosenza, *Titolario di classificazione degli atti.*

[77] Istituto Zooprofilattico Sperimentale della Lombardia e dell'Emilia Romagna, *Proposta di titolario di classificazione degli atti Progetto Archivio - Protocollo.*

[78] Gruppo di lavoro Direzione generale per gli Archivi del Ministero per i beni e le attività culturali e della ASL "Salerno 2", *Titolario di classificazione per gli archivi delle AA.SS.LL. e le AA.OO.*

[79] Università e Amministrazione centrale, *Titolario di classificazione per l'Amministrazione centrale.*

[80] "Regolamento del sistema archivistico di ateneo" in *Bollettino ufficiale UNI-FI,* anno II - N. 5 - Maggio 2003.

[81] Università degli Studi di Padova, *Titolario di classificazione per le strutture didattiche, di ricerca e di servizio previste dallo statuto.*

[82] Università degli studi di Trieste, *Titolario di classificazione per l'Amministrazione centrale 25-10-2000.*

[83] Progetto DOCAREA, *Modello di Titolario per le province*, versione 0, rev.1, dicembre 2003.

"I QUADERNI" CNIPA

ULTIMI NUMERI PUBBLICATI:

N. 20 **RAPPORTO 2005 - *COMMISSIONE INTERMINISTERIALE ICT DISABILI***
GENNAIO 2006

N. 19 **VOICE OVER IP NELLA PUBBLICA AMMINISTRAZIONE ITALIANA**
NOVEMBRE 2005

N. 18 **3RD WORKSHOP ON LEGISLATIVE XML**
NOVEMBRE 2005

N. 17 **LINEE GUIDA PER L'IMPIEGO DELLE TECNOLOGIE BIOMETRICHE NELLE PA**
INDICAZIONI OPERATIVE
SETTEMBRE 2005

N. 16 **DIGITALE TERRESTRE ED *E*-GOVERNMENT**
LUGLIO 2005

N. 15 **LA BIOMETRIA ENTRA NELL'*E*-GOVERNMENT**
MARZO 2005

N. 14 **VADEMECUM SULL'IMPIEGO DELLE NUOVE TECNOLOGIE A BANDA LARGA NELLE AREE PERIFERICHE**
MARZO 2005

N. 13 **LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT**
ESEMPI DI APPLICAZIONE
GENNAIO 2005

N. 12 **LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT**
APPALTO PUBBLICO DI FORNITURE ICT
GENNAIO 2005

N. 11 **LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT**
STRATEGIE DI ACQUISIZIONE DELLE FORNITURE ICT
GENNAIO 2005

N. 10 **LINEE GUIDA SULLA QUALITÀ DEI BENI E DEI SERVIZI ICT**
PRESENTAZIONE DELLE LINEE GUIDA
GENNAIO 2005

N. 9 **LINEE GUIDA PER L'IMPIEGO DELLE TECNOLOGIE BIOMETRICHE NELLE PUBBLICHE AMMINISTRAZIONI**
NOVEMBRE 2004

N. 8 **"TANTE LEGGI: COME ORIENTARSI?"**
NOVEMBRE 2004

N. 7 **L'*E*-LEARNING NELLE PUBBLICHE AMMINISTRAZIONI**
LE LINEE GUIDA
LA DIRETTIVA MINISTERIALE
OTTOBRE 2004

N. 6 **L'*E*-LEARNING NELLA FORMAZIONE CONTINUA DELLA PA**
SETTEMBRE 2004