MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CNIPA

- Area Organizzativa Omogenea CNIPADIR -

(Versione 2.1 del 16- 07-2007)

INDICE

1. PRINCIPI GENERALI

1.1. Premessa

Il decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000 concernente le "Regole tecniche per il protocollo informatico di cui al decreto del Presidente della Repubblica 20 ottobre 1998[1] n. 428" 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 degli artt. 50, comma 4 e 61 , comma 2, del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 20 dicembre 2000 ,già art.12 del citato DPR n.428 del 20 ottobre 1998).

Obiettivo del Manuale di gestione è descrivere sia il sistema di gestione documentale a partire dalla fase di protocollazione della corrispondenza in ingresso e in uscita e di quella interna, sia le funzionalità disponibili per gli addetti al servizio e per i 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'attività 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.
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 alla gestione dei flussi documentali ed archivistici in relazione ai procedimenti amministrativi del CNIPA, a partire dalla data di approvazione del presente manuale da parte del Collegio .
Il protocollo fa fede, anche con effetto giuridico, dell'effettivo ricevimento e della spedizione di un documento.

1.3. Definizioni e norme di riferimento

Ai fini del presente manuale si intende per:

[1] Il DPR 20 ottobre 1998, n 428, è stato abrogato con il DPR 20 dicembre 2000, n. 445.

- “amministrazione”, il Centro nazionale per l’informatica nella pubblica amministrazione - CNIPA;
- “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;
- “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;
- “Codice”, il decreto legislativo 7 marzo 2005 n. 82 – Codice dell’amministrazione digitale, aggiornato con le "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale" di cui al decreto legislativo 4 aprile 2006, n. 159.

Per le definizioni vedasi l’elenco riportato nell’allegato 1.
Di seguito si riportano gli acronimi utilizzati più frequentemente:

- **AOO** - Area Organizzativa Omogenea;
- **ASP** - *Application Service Provider* è la modalità di fruizione delle funzionalità di un programma applicativo da parte di un utente senza disporre del programma medesimo;
- **MdG** - Manuale di Gestione del protocollo informatico, 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;
- **RTI** - Raggruppamento Temporaneo di Imprese - il gruppo delle società aggiudicatarie della gara per fornire il servizio di protocollo informatico erogato in modalità ASP;
- **SdP** - Servizio di Protocollo informatico erogato in modalità ASP alle amministrazioni/AOO aderenti al servizio medesimo;
- **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 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 servizio di protocollo informatico; ovvero il soggetto, destinatario del documento, così come risulta dalla segnatura di protocollo nei campi opzionali.

Per le norme ed i regolamenti di riferimento vedasi l’elenco riportato nell’allegato 2.

1.4. Aree Organizzative Omogenee

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 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 e la gestione dei flussi documentali.
All’interno dell’amministrazione il sistema archivistico è unico.
Nel medesimo allegato 3, per l’AOO “Direzione” sono riportati, la denominazione, il codice identificativo della AOO, l’insieme degli UOR che la compongono con la loro articolazione in UU. Detto allegato è suscettibile di modifica in caso di inserimento di nuove AOO, UOP, UOR, UU o di riorganizzazione delle medesime.

All'interno della AOO in parola il sistema di protocollazione è totalmente centralizzato, nel senso che tutta la corrispondenza, in ingresso e in uscita, è gestita da una sola UOP.

1.5. Servizio per la gestione informatica del protocollo

Nella AOO "Direzione" è istituito il servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi. Al suddetto servizio è preposto il responsabile del servizio di protocollo informatico, della gestione dei flussi documentali e degli archivi (di seguito RSP).
Egli è funzionalmente indicato nel responsabile della "Sezione protocollo e archiviazione", strutture di staff al Direttore Generale, nominato con ordine di servizio numero 51/99 del 30 dicembre 99.
Il modello di atto di nomina del responsabile del servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi dell'AOO è riportato nell'allegato 4.

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

- predisporre lo schema del manuale di gestione del protocollo informatico con la descrizione dei criteri e delle modalità di revisione del medesimo;
- provvedere alla pubblicazione del manuale (eventualmente anche sul sito Internet dell'amministrazione);
- proporre i tempi, le modalità e le misure organizzative e tecniche finalizzate alla eliminazione di eventuali protocolli di area, i protocolli multipli, dei protocolli di telefax e, più in generale, dei protocolli diversi dal protocollo informatico;
- abilitare gli utenti dell'AOO all'utilizzo del SdP e definire per ciascuno di essi il tipo di funzioni più appropriate tra quelle disponibili;
- garantire il rispetto delle disposizioni normative durante le operazioni di registrazione e di segnatura di protocollo;
- garantire la corretta conservazione della copia del registro giornaliero di protocollo quotidianamente ricevuta dal SdP;
- sollecitare al RTI il ripristino del servizio in caso di indisponibilità del medesimo;
- garantire il buon funzionamento degli strumenti interni all'AOO e il rispetto delle procedure concernenti le attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso dall'esterno e le attività di gestione degli archivi;
- autorizzare le eventuali operazioni di annullamento della registrazione di protocollo;
- vigilare sull'osservanza delle disposizioni delle norme vigenti da parte del personale autorizzato e degli incaricati;
- curare l'apertura, l'uso e la chiusura del registro di protocollazione di emergenza con gli strumenti e le funzionalità disponibili nel SdP.

1.6. 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, , viene riversato almeno al termine della giornata lavorativa, nel rispetto della normativa vigente, sia su carta che su supporti informatici non riscrivibili all'interno del centro servizi del RTI e su carta nella AOO.

1.7. Firma digitale

Per l'espletamento delle attività istituzionali l'amministrazione fornisce la firma digitale o elettronica qualificata ai soggetti da essa delegati a rappresentarla.
Nell'allegato 5 viene riportato l'elenco delle persone titolari di firma digitale.

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 competenza ha ottemperato al dettato del decreto legislativo 30 giugno 2003, n.196 con atti formali aventi rilevanza interna ed esterna .
In relazione agli adempimenti interni specifici, gli addetti abilitati ad accedere al sistema di protocollo informatico e a trattare i dati di protocollo veri e propri, sono incaricati dal titolare dei dati e, se nominato, dal responsabile, previa adeguata informazione conferiscono il consenso all'amministrazione affinché questa possa comunicare i loro dati personali all'erogatore del SdP per consentire agli stessi l'accesso individuale al sistema di protocollazione e la definizione delle relative autorizzazioni.
Per quanto concerne gli adempimenti esterni, l'amministrazione:

- nomina, con atto formale il cui modello è riportato nell'allegato 6, tutte le società del raggruppamento temporaneo di imprese erogatrici del servizio di protocollo informatico e gestione documentale in modalità ASP. Tale adempimento è stato attuato contestualmente all'invio dell'"ordinativo di lavoro o piano di carico" al RTI stesso, insieme al quale è espressamente riportata la nomina in argomento;
- indica nell'atto di nomina richiamato nel punto precedente tutti i dati personali raccolti e trattati dal titolare:
  - ✓ necessari all'esecuzione del contratto-quadro per l'erogazione dei servizi GEDOC, nonché tutti i dati personali contenuti negli ordinativi di fornitura emessi dalle amministrazioni contraenti e necessari all'esecuzione di questi ultimi;
  - ✓ contenuti nei documenti elettronici oggetto dei servizi GEDOC;
  - ✓ ivi compresi quelli identificativi degli utenti dell'amministrazione acquisiti dalla stessa nell'ambito dell'esecuzione del contratto di adesione al servizio, necessari alla fruizione dei sopraccitati servizi.
- Attua idonee misure organizzative per garantire che i documenti trasmessi ad altre pubbliche amministrazioni riportino le sole informazioni relative a stati, fatti e qualità personali previste da leggi e/o da regolamenti e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite.

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. Tale casella costituisce l'indirizzo virtuale della AOO e di tutti gli uffici (UOR) che ad essa fanno riferimento.
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 munisce tutti i propri dipendenti compresi quelli per i quali non sia prevista la dotazione di un personal computer di una casella di posta elettronica convenzionale.

1.10. Sistema di classificazione dei documenti

Con l'inizio della attività operativa del protocollo informatico viene adottato un unico titolario

di classificazione per l'archivio centrale unico (logico) dell'amministrazione.
Si tratta di un sistema logico astratto che organizza i documenti secondo una struttura ad albero definita sulla base dell'organizzazione funzionale dell'AOO, consentendo di organizzare in maniera omogenea e coerente i documenti che si riferiscono ai medesimi affari o ai medesimi procedimenti amministrativi.
La definizione del sistema di classificazione è stata effettuata prima dell'avvio del sistema di protocollo informatico.
Al fine di agevolare e normalizzare, da un lato la classificazione archivistica e dall'altro l'assegnazione per competenza, sul SdP è stato predisposto un elenco degli Uffici Utente e dei dipendenti unitamente a quello di classificazione. L'elenco è una guida rapida di riferimento, in ordine alfabetico che, sulla base del titolario, permette l'immediata individuazione della classificazione e delle competenze.

1.11. Formazione

Nell'ambito dei piani formativi richiesti a tutte le amministrazioni dalla direttiva 13 dicembre 2001del Ministro della funzione pubblica sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni, l'amministrazione stabilisce percorsi formativi specifici e generali che coinvolgono tutte le figure professionali.

1.12. Accreditamento dell'AOO all'IPA

L'AOO, come accennato si è dotata di una casella di posta elettronica istituzionale certificata attraverso cui trasmette e riceve documenti informatici soggetti alla registrazione di protocollo, affidata alla responsabilità della UOP incaricata; quest'ultima procede alla lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta. L'amministrazione, nell'ambito degli adempimenti previsti, si è accreditata presso l'indice delle pubbliche amministrazioni (IPA), tenuto e reso pubblico dal medesimo fornendo le informazioni che individuano l'amministrazione e l'articolazione delle sue AOO.
Il codice identificativo dell'amministrazione associato a ciascuna delle proprie AOO, (CNIPADIR e CNIPAGAB) 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.

2. ELIMINAZIONE DEI REGISTRI DI PROTOCOLLO DIVERSI DAL REGISTRO UFFICIALE DI 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 dal presente manuale, tutti i documenti inviati e ricevuti dalla AOO sono registrati all'interno del registro ufficiale di protocollo informatico. Pertanto, tutti gli eventuali registri di protocollo, interni agli UOR e/o agli UU, diversi dal registro ufficiale di protocollo informatico, sono aboliti ed eliminati con l'entrata in vigore del manuale stesso.

Fanno eccezione:

- il registro di protocollo delle circolari interne;
- il registro di protocollo degli ordini di servizio;
- eventuali registri per la protocollazione di corrispondenza riservata in uso esclusivo al direttore generale, e al Presidente.

Il RSP esegue comunque, periodicamente, dei controlli a campione sugli UOR/UU per verificare la corretta esecuzione del piano e l'utilizzo regolare dell'unico registro ufficiale di protocollo, verificando, attraverso controlli ed ispezioni mirate, la validità dei criteri di classificazione utilizzati.

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

3.2. Generalità

Considerata la particolare modalità di fruizione del servizio di gestione del protocollo, gran parte delle funzioni/responsabilità di sicurezza sono demandate all'erogatore del SdP. All'AOO, in quanto fruitrice del servizio, è demandata la componente "locale" della sicurezza, poiché attraverso la propria organizzazione, nonché le sue misure e le politiche di sicurezza, essa contribuisce a stabilire adeguati livelli di sicurezza proporzionati al "valore" dei dati/documenti trattati.
Il piano di sicurezza:

- si articola, di conseguenza, in due componenti: una di competenza del RTI, una di competenza della AOO;
- si basa sui risultati dell'analisi dei rischi a cui sono esposti i dati e i documenti trattati, rispettivamente, nei locali dove risiedono le apparecchiature utilizzate dal SdP e nei locali della AOO;
- si fonda sulle direttive strategiche di sicurezza stabilite, rispettivamente, dal committente nei confronti del RTI e dal RSP nei confronti dell'AOO;
- definisce:
  - ✓ le politiche generali e particolari di sicurezza da adottare all'interno, rispettivamente, del Centro servizi e della AOO;
  - ✓ le modalità di accesso al SdP;
  - ✓ gli aspetti operativi della sicurezza, con particolare riferimento alle misure minime di sicurezza, *di cui al Disciplinare tecnico richiamato nell'allegato B) del D.lgs. 196/2003 - Codice in materia di protezione dei dati personali*;
  - ✓ i piani specifici di formazione degli addetti;
  - ✓ le modalità esecutive del monitoraggio periodico dell'efficacia e dell'efficienza delle misure di sicurezza.

Il piano in argomento è soggetto a revisione formale con cadenza almeno biennale. Esso può essere modificato a seguito di eventi gravi. I dati personali registrati nel *log* del sistema operativo, del sistema di controllo degli accessi e delle operazioni svolte con il SdP, saranno conservati dal RTI secondo le vigenti norme e saranno consultati solo in caso di necessità.

3.3. Formazione dei documenti – Aspetti attinenti alla sicurezza

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

- l'identificabilità del soggetto che ha formato il documento e l'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 redatti 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 della 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 13 gennaio 2004 ("Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici").

3.4. Gestione dei documenti informatici

Il sistema operativo delle risorse elaborative destinate ad erogare il servizio di protocollo informatico in modalità ASP è conforme alle specifiche previste dalla normativa vigente.
Il sistema operativo del *server* che ospita i *file* utilizzati come deposito dei documenti è configurato in maniera da consentire:

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

Il sistema di gestione informatica dei documenti:

- garantisce la disponibilità, la riservatezza e l'integrità dei documenti e del registro di protocollo;
- assicura la corretta e puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
- 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.

Per la gestione dei documenti informatici all'interno dell'AOO, il RPS fa riferimento alle norme stabilite dal responsabile del sistema informativo del CNIPA.

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 dal RTI per l'erogazione del SdP.
Nella conduzione del centro servizi destinato ad erogare il SdP, le qualifiche funzionali individuate sono le seguenti:

- responsabile del centro;
- responsabile della sicurezza;
- responsabile della tutela dei dati personali;
- responsabile dei sistemi e delle reti;
- *internal auditor*;
- responsabile del *call center;*
- operatore di sicurezza;
- operatore (sistemi e TLC);

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

- *sicurezza informatica* si occupa principalmente della definizione dei piani di sicurezza e della progettazione dei sistemi di sicurezza;
- *operativa sicurezza* ha il compito di realizzare, gestire e mantenere in efficienza le misure di sicurezza così da soddisfare le linee strategiche di indirizzo definite dalla funzione *sicurezza informatica*;
- *revisione* ha il compito di controllare le misure di sicurezza adottate, verificandone l'efficacia e la coerenza con le politiche di sicurezza.

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

- responsabile della sicurezza;
- responsabile centro servizi;
- operatori della sicurezza.

La componente organizzativa della sicurezza afferente l'AOO è articolata e gestita secondo quanto stabilito dall'Area "Funzionamento" Ufficio sistema informativo del CNIPA.

3.4.2. Componente fisica della sicurezza

Il controllo degli accessi fisici alle risorse della sede del centro servizi è regolato secondo i seguenti principi:

- l'accesso è consentito soltanto al personale autorizzato per motivi di servizio;
- i meccanismi di controllo dell'accesso sono più selettivi all'aumentare del livello di protezione del locale;
- i visitatori occasionali, i dipendenti di aziende esterne e gli ospiti devono esplicare la procedura di registrazione. Essi non possono entrare e trattenersi nelle aree protette se non accompagnati da personale dell'erogatore del servizio (RTI) autorizzato a quel livello di protezione;
- ogni persona che accede alle risorse della sede in locali protetti è identificata in modo certo con sistemi di autenticazione forte;

- gli accessi alla sede sono registrati e conservati ai fini della imputabilità delle azioni conseguenti ad accessi non autorizzati;
- il personale della sede ha l'obbligo di utilizzare il *badge* sia in ingresso che in uscita dalla sede stessa.

Le misure di sicurezza fisica hanno un'architettura multilivello così articolata:

- a livello di *edificio*, attengono alla sicurezza perimetrale e sono atte a controllare l'accesso alla sede in cui sono ospitate risorse umane e strumentali;
- a livello di *centro di servizio*, sono destinate a controllare l'accesso ai locali del centro;
- a livello di *locale*, sono finalizzate a controllare l'accesso ai locali interni alla sede.

Il controllo degli accessi fisici alle risorse della sede dell'amministrazione/AOO è regolato secondo i principi stabiliti dall'Area "Funzionamento" Sezione Logistica e sicurezza del CNIPA.

3.4.3. Componente logica della sicurezza

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

- l'attivazione dei seguenti servizi di sicurezza che prevengono l'effetto "dannoso" delle minacce sulle vulnerabilità del sistema informatico:
  - ✓ identificazione, autenticazione ed autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP;
  - ✓ riservatezza dei dati;
  - ✓ integrità dei dati;
  - ✓ integrità del flusso dei messaggi;
  - ✓ non ripudio dell'origine (da parte del mittente);
  - ✓ non ripudio della ricezione (da parte del destinatario);
  - ✓ *audit* di sicurezza;
- la ridondanza dei sistemi di esercizio.

In base alle esigenze rilevate dall'analisi delle minacce e delle vulnerabilità, è stata implementata una infrastruttura tecnologica di sicurezza con una architettura "a strati multipli di sicurezza" conforme alle *best practices* correnti.
L'architettura realizza una soluzione centralizzata per l'identificazione, l'autenticazione e l'autorizzazione degli addetti delle AOO e degli operatori dell'erogatore del SdP, con le seguenti caratteristiche:

- unico *login server* per la gestione dei diritti di accesso ai servizi applicativi;
- unico sistema di *repository* delle credenziali di accesso degli utenti;
- unico database delle anagrafiche contenente tutti i profili di utenza.

La componente della sicurezza logica dell'AOO viene descritta nelle politiche di sicurezza dall'Area "Funzionamento" Ufficio sistema informativo del CNIPA.

3.4.4. Componente infrastrutturale della sicurezza

Presso il centro servizi dell'erogatore sono disponibili i seguenti impianti:

- antincendio;
- rilevazione dell'allagamento;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

Essendo il centro servizi lontano da insediamenti industriali e posto all'interno di un edificio adibito ad uffici, le sue condizioni ambientali per quanto riguarda polvere, temperatura, umidità,

vibrazioni meccaniche, interferenze elettriche e radiazioni elettromagnetiche e livelli di inquinamento chimico e biologico, sono tali da non richiedere misure specifiche di prevenzione oltre quelle già adottate per le sedi di uffici di civile impiego.

Gli impianti e le considerazioni precedenti valgono anche per la componente infrastrutturale della sicurezza per il CNIPA. In particolare:

- antincendio;
- luci di emergenza;
- continuità elettrica;
- controllo degli accessi e dei varchi fisici.

3.4.5. Gestione delle registrazioni di protocollo e di sicurezza

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

Le registrazioni di sicurezza sono costituite:

- dai *log* 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 dell'applicativo SdP, modulo GEDOC.

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

- l'accesso alle registrazioni è limitato, esclusivamente, ai sistemisti o agli operatori di sicurezza addetti al servizio di protocollo, come previsto dalle norme sul trattamento dei dati personali;
- le registrazioni del modulo GEDOC sono elaborate tramite procedure automatiche da parte degli operatori di sicurezza;
- l'accesso dall'esterno da parte di persone non autorizzate non è consentito in base all'architettura stessa del servizio, essendo controllato dal sistema di autenticazione e di autorizzazione e dal *firewall*;
- i supporti con le registrazioni di sicurezza sono conservati all'interno di un armadio ignifugo in un locale con controllo biometrico per l'accesso;
- i *log* di sistema sono accessibili ai sistemisti in sola lettura al fine di impedirne la modifica;
- l'operazione di scrittura delle registrazioni del SdP, modulo GEDOC è effettuata direttamente dagli applicativi;
- le registrazioni sono soggette a copia giornaliera su disco e a salvataggio su supporto ottico rimovibile;
- il periodo di conservazione del supporto ottico è conforme alla normativa vigente in materia

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

3.5. Trasmissione e interscambio dei documenti informatici

Gli addetti delle AOO alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi, a qualsiasi titolo, informazioni anche

in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni che, per loro natura o per espressa indicazione del mittente, sono destinate ad essere rese pubbliche.
Come previsto dalla normativa vigente, i dati e i documenti trasmessi per via telematica sono di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.
Al fine di tutelare la riservatezza dei dati personali, i dati, i certificati ed i documenti trasmessi all'interno della AOO o ad altre AOO, 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'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 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.

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 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.

Gli uffici organizzativi di riferimento (UOR) dell'AOO si scambiano documenti informatici attraverso l'utilizzo delle caselle di posta elettronica 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 (*UserID*) e privata (*Password*) 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:

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

Le regole per la composizione delle *password* e il blocco delle utenze valgono sia per gli amministratori delle AOO che per gli utenti delle AOO.
Le relative politiche di composizione, aggiornamento e, in generale di sicurezza, sono configurate sui sistemi di accesso come obbligatorie tramite il sistema operativo.
Il SdP fruito dall'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 da modifiche non autorizzate.

Ad ogni documento, all'atto della registrazione nel sistema di protocollo informatico, viene associata una *Access Control List* (ACL) che consente di stabilire quali utenti, o gruppi di utenti, hanno accesso ad esso (sistema di autorizzazione o profilazione utenza).
Considerato che il SdP segue la logica dell'organizzazione, ciascun utente 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'AOO.
I documenti non vengono mai visualizzati dagli utenti privi di diritti di accesso, neanche a fronte di una ricerca generale nell'archivio o di una ricerca *full text*.

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'AOO. Tali livelli si distinguono in: abilitazione alla consultazione, abilitazione all'inserimento, abilitazione alla cancellazione e alla modifica delle informazioni.
La gestione delle utenze rispetta i seguenti principi operativi:

- gli utenti creati non sono mai cancellati ma, eventualmente, disabilitati (su richiesta esplicita dell'amministratore dell'AOO o per errori di inserimento)
- la credenziale privata degli utenti e dell'amministratore AOO non transita in chiaro sulla rete, né al momento della prima generazione, né, successivamente, al momento del *login*.

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:

- *liste di competenza*, gestite dall'amministratore di AOO, per la definizione degli utenti abilitati ad accedere a determinate voci del titolario;
- *ruoli degli utenti*, gestiti dall'amministratore di ente (amministrazione), per la

specificazione delle macro-funzioni alle quali vengono abilitati;
- protocollazione "*particolare o riservata*", gestita dall'amministratore di ente, relativa a documenti sottratti alla consultazione da parte di chi non sia espressamente abilitato.

La visibilità completa sul registro di protocollo è consentita soltanto all'utente con il profilo di utenza di "Responsabile del registro" e limitatamente al registro dell'AOO sul quale è stato abilitato ad operare.
L'utente assegnatario dei documenti protocollati è invece abilitato ad una vista parziale sul registro di protocollo. Tale vista è definita dalle voci di titolario associate alla lista di competenza in cui l'utente è presente (sia come singolo, sia come ufficio).
L'operatore che gestisce lo smistamento dei documenti può definire riservato un protocollo ed assegnarlo per competenza ad un utente assegnatario.
Nel caso in cui sia effettuata una protocollazione riservata la visibilità completa sul documento è possibile solo all'utente a cui il protocollo è stato assegnato per competenza e ai protocollatori che hanno il permesso applicativo di protocollazione riservata (permesso associato al ruolo).
Tutti gli altri utenti (seppure inclusi nella giusta lista di competenza) possono accedere solo ai dati di registrazione (ad esempio: progressivo di protocollo, data di protocollazione) mentre vedono mascherati i dati relativi al profilo del protocollo (ad esempio : classificazione).

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 agli art. 72 e ss del d.lgs 7 marzo 2005 n. 82.
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

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

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'intera amministrazione, che coincide con il RSP, ha individuato nei locali al piano terra e negli armadi ubicati nei corridoi della sede istituzionale dell'amministrazione medesima, la sede del relativo archivio dell'amministrazione.

Il responsabile del servizio in argomento ha effettuato la scelta alla luce dei vincoli logistici imposti dall'edificio e della valutazione dei fattori di rischio che incombono sui documenti.
Per contenere i danni conseguenti a situazioni di emergenza, il responsabile del servizio ha, in corso di perfezionamento, un piano specifico individuando, i soggetti incaricati di ciascuna fase.

Al riguardo, sono state regolamentate le modalità di consultazione, soprattutto interne, al fine di evitare accessi a personale non autorizzato.

Il responsabile dell'archivio è a conoscenza, in ogni momento, della collocazione del materiale archivistico, avendo, a tal fine, 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.

3.7.2. Servizio di conservazione sostitutiva

Il servizio in parola è attualmente in fase di definizione.

3.7.3. Conservazione dei documenti informatici e delle registrazioni di protocollo all'interno del centro servizi del RTI

I luoghi di conservazione previsti per la salvaguardia dei supporti contenenti le registrazioni di protocollo e le registrazioni di sicurezza così sono differenziati in base al livello di sicurezza loro attribuito:

- armadi che devono essere mantenuti chiusi a chiave;
- armadi protetti (ignifughi e stagni), dotati di serratura di sicurezza;
- casseforti poste in locali ad alto livello di protezione.

E' compito del servizio sicurezza del centro servizi l'espletamento delle seguenti procedure atte ad assicurare la corretta archiviazione, disponibilità e leggibilità dei supporti.

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.

E' stato implementato e viene mantenuto aggiornato un archivio dei prodotti software (nelle disponibili versioni) necessari alla lettura dei supporti in gestione e ad un successivo riutilizzo dei dati archiviati.
Presso il centro servizi 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 con il quale è stato generato e la versione della *release*;
- la configurazione hardware e software necessaria per il suo riuso;
- la periodicità dell'eventuale *refresh* dei supporti.

Il servizio sicurezza dell'erogatore 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 di sicurezza dell'erogatore, provvede con periodicità almeno mensile, alla memorizzazione su supporto ottico dei seguenti oggetti:

- i *file* contenenti i *log* originali;
- le firme dei *file*.

I supporti sono archiviati in un armadio ignifugo dell'area sicurezza del centro servizi e sono conservati per un periodo minimo di cinque anni ove specifiche disposizioni di legge non ne prevedano la conservazione per un più lungo periodo.
Le modalità di archiviazione sono regolamentate da procedure specifiche.

3.7.5. Riutilizzo e dismissione dei supporti rimovibili

All'interno del centro servizi non è previsto il riutilizzo dei supporti rimovibili. Al termine del periodo di conservazione prestabilito i supporti sono distrutti secondo una specifica procedura operativa.

3.8. Politiche di sicurezza adottate dalla AOO

Le politiche di sicurezza, riportate nell'allegato 8**,** stabiliscono, sia le misure preventive per la tutela e l'accesso al patrimonio informativo, sia le misure consuntive per la gestione degli incidenti informatici.
È compito del responsabile della sicurezza e del responsabile della tutela dei dati personali del RTI procedere al perfezionamento, alla divulgazione, al riesame e alla verifica delle politiche di sicurezza.
Il riesame delle politiche di sicurezza è conseguente al verificarsi di incidenti attinenti alla 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 al RTI, 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 così classificabile:

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

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

- informatico;
- analogico.

Secondo quanto previsto dall'art. 40 del decreto legislativo n. 82/2005 "1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71" e "2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità".
Pertanto, soprattutto nella fase transitoria di migrazione verso l'adozione integrale delle tecnologie digitali da parte dell'amministrazione, il documento amministrativo può essere disponibile anche nella forma analogica.

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*, 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 tramite una persona dallo stesso delegata alle UOP e/o agli UOR aperti al pubblico.

A fronte delle tipologie descritte ne esiste una terza denominata "Ibrida" composta da un documento analogico (lettera di accompagnamento) e da un documento digitale che comportano diversi metodi di acquisizione.

4.2. Documento inviato

I documenti informatici, compresi di eventuali allegati, sono inviati, di norma, per mezzo della sola posta elettronica certificata se la dimensione del documento e/o di eventuali allegati, non supera la dimensione massima prevista, dal sistema di posta utilizzato dall'AOO, che è di 30 *Megabytes* , e con un limite di 50 destinatari.
In caso contrario, il documento informatico viene copiato, su supporto digitale rimovibile non modificabile e trasmesso al destinatario con altri mezzi di trasporto.

4.3. Documento interno formale

I documenti interni sono formati con tecnologie informatiche e, solo nella fase transitoria, lo scambio tra UOR/UU della AOO di documenti informatici di rilevanza amministrativa giuridico-probatoria, dopo averli trasformati in analogici, avviene per mezzo della posta interna cartacea.

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.

Per le richieste di parere prodotte già oggi interamente in formato digitale firmato la trasmissione avviene attraverso il SdP utilizzando la casella di posta elettronica certificata istituziolanle.

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.
Di conseguenza, per la formazione, la gestione e la sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascun UOR o UU della AOO adotta, nei limiti della propria autonomia organizzativa, le regole sopra illustrate ad eccezione della obbligatorietà dell'operazione di sottoscrizione e di protocollazione.

4.5. Il documento analogico - cartaceo

Per documento analogico si intende un documento amministrativo formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video) su supporto non digitale. Di seguito si farà 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 in possesso di tutti i requisiti di garanzia e d'informazione del mittente e del destinatario, stampato su carta intestata e munito di firma autografa.
Un documento analogico può essere convertito in documento informatico tramite opportune procedure di conservazione sostitutiva, descritte nel seguito del manuale.

4.6. Formazione dei documenti – Aspetti operativi

I documenti dell'amministrazione sono prodotti con sistemi informatici come previsto dalla vigente normativa.
Ogni documento formato per essere inoltrato formalmente all'esterno o all'interno:

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

Le firme *(e le sigle se si tratta di documento analogico)* necessarie alla redazione e perfezione sotto il profilo giuridico del documento in partenza devono essere apposte prima della sua protocollazione.
Le regole per la determinazione dei contenuti e della struttura dei documenti informatici sono definite dai responsabile 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 civico, CAP, città, provincia);
- il numero di telefono della UOR;
- il numero di fax della UOP;
- il codice fiscale dell'amministrazione.

Il documento deve inoltre recare almeno le seguenti informazioni:

- il luogo di redazione[2];
- la data (giorno, mese, anno)[2];
- il numero di protocollo[2];
- il numero degli allegati, se presenti;
- l'oggetto;
- 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 digitale,
- sigla autografa dell'istruttore e sottoscrizione autografa del responsabile del procedimento amministrativo (RPA) e/o del responsabile del provvedimento finale, se trattasi di documento cartaceo

4.7. Sottoscrizione di documenti informatici

La sottoscrizione dei documenti informatici, quando prescritta, è ottenuta con un processo di firma digitale conforme alle disposizioni dettate dalla normativa vigente.
L'amministrazione, articolata nelle AOO richiamate nell'allegato 3, si configura come autorità di certificazione, accreditata, iscritta nell'elenco pubblico dei certificatori accreditati tenuto dal CNIPA.
I documenti informatici prodotti dall'AOO, indipendentemente dal software utilizzato per la loro redazione, prima della sottoscrizione con firma digitale, sono convertiti in uno dei formati standard previsti dalla normativa vigente in materia di archiviazione al fine di garantirne l'immodificabilità (vedi art. 3, comma 3, del decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004).

[2] Questo valore è riportato all'interno dell'etichetta di segnatura del protocollo.

4.8. 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.

4.9. Firma digitale

Lo strumento che soddisfa i primi tre requisiti di cui al precedente paragrafo 4.8 è la firma digitale utilizzata per inviare e ricevere documenti per l'AOO per sottoscrivere documenti, compresa la copia giornaliera del registro di protocollo e di riversamento, o qualsiasi altro *fil*e digitale con valenza giuridico-probatoria.
I messaggi ricevuti, sottoscritti con firma digitale, sono sottoposti a verifica di validità.
Tale processo si realizza con modalità conformi a quanto prescritto dalla normativa vigente in materia (si vedano le norme pubblicate sul sito www.cnipa.gov.it)

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

Nel SdP 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;
- verifica della validità del certificato; questa attività è realizzata verificando *on-line* le *Certificate Revocation List* (CRL) con una periodicità predefinibile parametricamente nel modulo GEDOC. Una giacenza in memoria temporanea (*cache)* di un'ora è considerata accettabile;
- verifica della firma (o delle firme multiple) con funzioni Java standard; in particolare, viene calcolata l'impronta del documento e verificata con quella contenuta nella busta "logica";
- verifica dell'utilizzo, nell'apposizione della firma, di un certificato 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 presso il CNIPA con periodicità settimanale;
- 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 SdP (modulo GEDOC) sia del documento originale firmato, sia del documento in chiaro;
- archiviazione delle componenti verificate e dei dati dei firmatari rilevati dal certificato in una tabella del database del SdP per accelerare successive attività di verifica di altri documenti ricevuti.

E' in corso l'aggiornamento dell'SdP allo standard di firma in formato PDF.

4.11. 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;io 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 (IPA), 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, e le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione.
L'UOP non effettua fotocopie della corrispondenza trattata, sia in ingresso che in uscita.

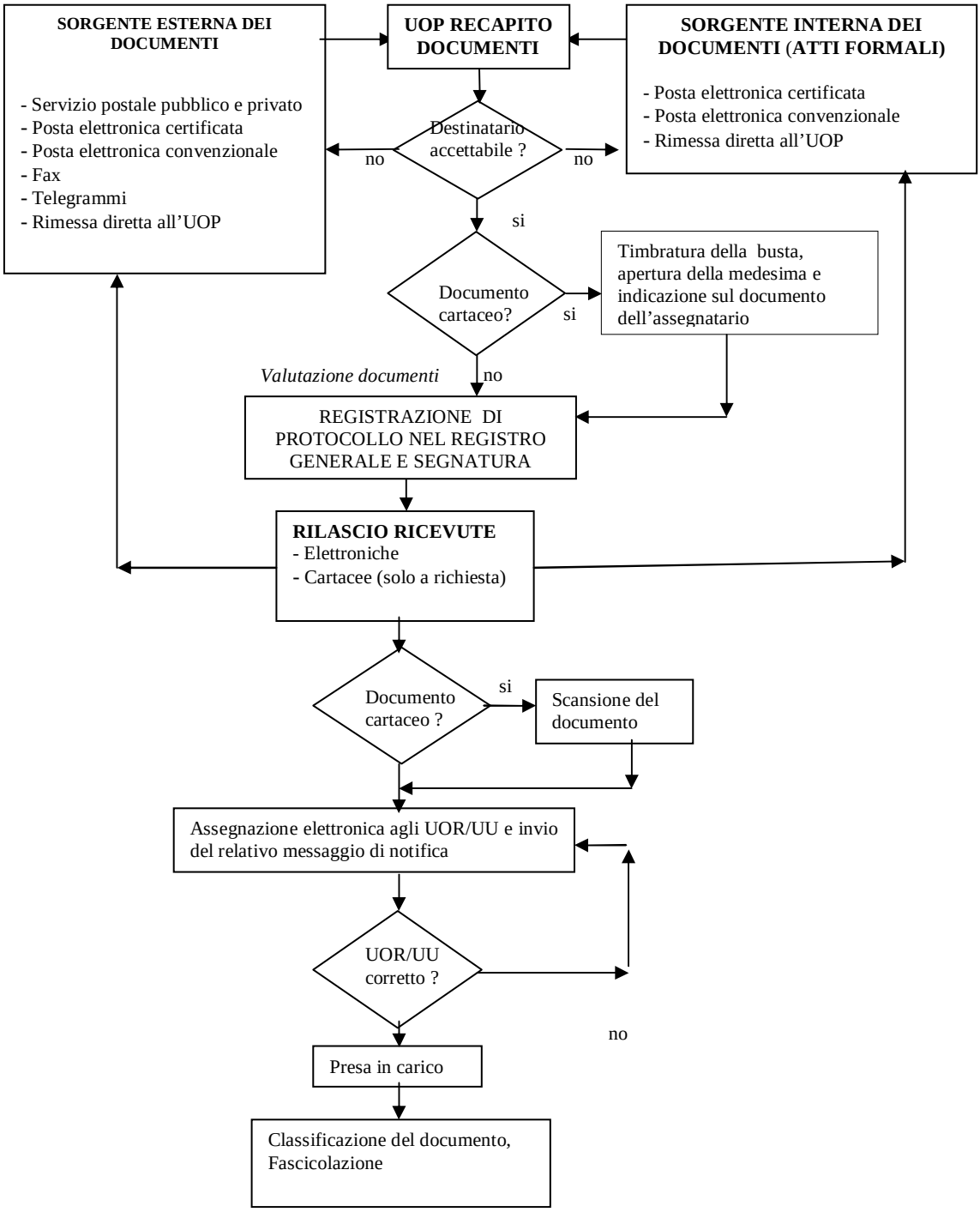
5.1. Generalità

Per descrivere i flussi di lavorazione dei documenti all'interno della AOO si fa riferimento ai diagrammi di flusso riportati nelle pagine seguenti.
Tali flussi sono stati predisposti prendendo in esame i documenti che possono avere rilevanza giuridico probatoria. 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 10.
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 è ricevuto e trasmesso per posta elettronica interna e non interessa il sistema di protocollo.

5.2. Flusso dei documenti in ingresso alla AOO



5.2.1. Provenienza esterna dei documenti

I documenti trasmessi da soggetti esterni all'AOO sono, oltre quelli richiamati nel capitolo precedente, i telefax, i telegrammi ed eventuali supporti digitali rimovibili allegati a documenti cartacei. Questi documenti sono recapitati alla UOP designata.
Gli apparati fax sono dislocati nelle singola aree operative, i fax pervenuti vengono inviati alla UOP per la protocollazione.

I documenti che transitano attraverso il servizio postale (pubblico o privato), indirizzati a tutta l'amministrazione, sono consegnati quotidianamente alla UOP in parola, che si fa carico di selezionare e smistare la corrispondenza destinata all'altra AOO GAB e quella nominativa.
Le modalità di gestione della corrispondenza in ingresso, stabilite dal RSP, sono riportate nell'allegato 9.

5.2.2. Provenienza di documenti interni formali

Per sorgente interna dei documenti si intende qualunque UOR/UU che invia formalmente la propria corrispondenza alla UOP della AOO per essere, a sua volta, trasmessa, nelle forme opportune, ad altro UOR o UU della stessa AOO.
Il documento è, di norma, di tipo analogico secondo i formati standard illustrati nel precedente capitolo. In questo caso, il mezzo di recapito della corrispondenza considerato è la posta interna.

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 UOP dell'AOO.
Quando i documenti informatici pervengono alla UOP, la stessa unità, previa verifica della validità della firma apposta e della leggibilità del documento, procede alla registrazione di protocollo ed alla assegnazione agli UOR/UU di competenza.
Nel caso in cui venga recapitato per errore un documento indirizzato ad altro destinatario lo stesso è restituito al mittente con le modalità che saranno successivamente illustrate.
L'operazione di ricezione dei documenti informatici avviene con le modalità previste dalle regole tecniche vigenti, recanti standard del formato dei documenti, modalità di trasmissione, definizioni dei tipi di informazioni minime ed accessorie 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 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 quello di una missiva non sottoscritta e comunque valutabile dal responsabile del procedimento amministrativo (RPA).
Il personale della UOP controlla quotidianamente i messaggi pervenuti nella casella di posta 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 stesso viene inoltrato alla casella di posta istituzionale. 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.
Nei casi in cui cun un documento cartaceo sono trasmessi gli allegati su supporto rimovibile, considerata l'assenza di standard tecnologici e formali in materia di registrazione di *file* digitali, la AOO si riserva la facoltà di acquisire e trattare tutti quei documenti informatici così ricevuti che riesce a decodificare e interpretare con le tecnologie a sua disposizione.
Superata questa fase il documento viene inserito nel flusso di lavorazione e sottoposto a tutti i controlli e adempimenti del caso.
L'acquisizione degli allegati digitali nel sistema SdP può avvenire solo se la grandezza totale di ogni allegato non supera il limite di 1 Megabyte.
Gli allegati che superano tale dimensione dovranno essere riversati su un apposito disco virtuale condiviso e visibile dagli utenti assegnatari.

5.2.6. Ricezione di documenti cartacei a mezzo posta convenzionale

I documenti pervenuti a mezzo posta sono consegnati alla UOP.
Le buste, o contenitori, sono inizialmente esaminati per una preliminare verifica dell'indirizzo e del destinatario apposti sugli stessi.
La corrispondenza relativa a bandi di gara non viene aperta, ma, dopo essere stata esaminata dal personale dell'Ufficio "Amministrazione gare e contratti", che appone sulla busta la data e l'ora di arrivo della busta medesima, viene registrata al protocollo con la segnatura applicata sull'esterno del plico e successivamente riconsegnata chiusa all'Ufficio competente.
La corrispondenza personale non viene aperta, né protocollata, ma viene 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, per ciò che concerne la registrazione di protocollo, è trattata come un documento cartaceo con le modalità descritte nel successivo capitolo 11.

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 ingresso viene timbrata all'arrivo alla UOP sull'involucro, viene, di norma, aperta il giorno lavorativo in cui è pervenuta, e contestualmente assegnata con indicazione manuale del destinatario sul documento medesimo e protocollata. La busta viene allegata al documento per la parte recante i timbri postali.

5.2.7. Errata ricezione di documenti digitali

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

5.2.8. Errata ricezione di documenti cartacei

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

5.2.9. Attività di protocollazione dei documenti

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

5.2.10. Rilascio di ricevute attestanti la ricezione di documenti informatici

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

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.

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

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

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

5.2.12. Conservazione dei documenti informatici

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

5.2.13. 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 che avviene secondo le fasi di seguito indicate:

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

- collegamento 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 sui sistemi del centro servizi, 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 deliberazione CNIPA 19 febbraio 2004, n. 11 vengono trattati diversamente in base alla loro tipologia.

Gli originali dei documenti cartacei ricevuti, di norma non vengono inviati alle UOR ma rimangono e vengono archiviati in ordine sequenziale di protocollo dalla UOP.
A questa regola fanno eccezione i documenti seguenti:

- richieste di parere (inviati all ufficio Pareri);
- corrispondenza riguardante il personale dipendente (inviata all'area Organizzazione e risorse umane)
- originale delle lettere-contratto firmate per accettazione (Ufficio "Amministrazione gare e contratti")
- originale delle fatture e documentazione contabile da esibire per eventuali controlli (Ufficio "Bilancio")

In ogni caso non vengono riprodotti in formato immagine i documenti che contengono dati sensibili secondo la normativa vigente (d.lgs. 196/2003)

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

Gli addetti alla UOP provvedono ad inviare il documento all'UOR che identifica l'UU di destinazione; l'UOR:

- esegue una verifica di congruità in base alle proprie competenze;
- in caso di errore restituisce il documento alla UOP mittente;
- in caso di verifica positiva, esegue l'operazione di presa in carico riassegnandola al proprio interno ad un 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'AOO, solo in assenza del meccanismo di assegnazione e classificazione automatica predisposto nel SdP..

5.2.15. Conservazione dei documenti nell'archivio corrente

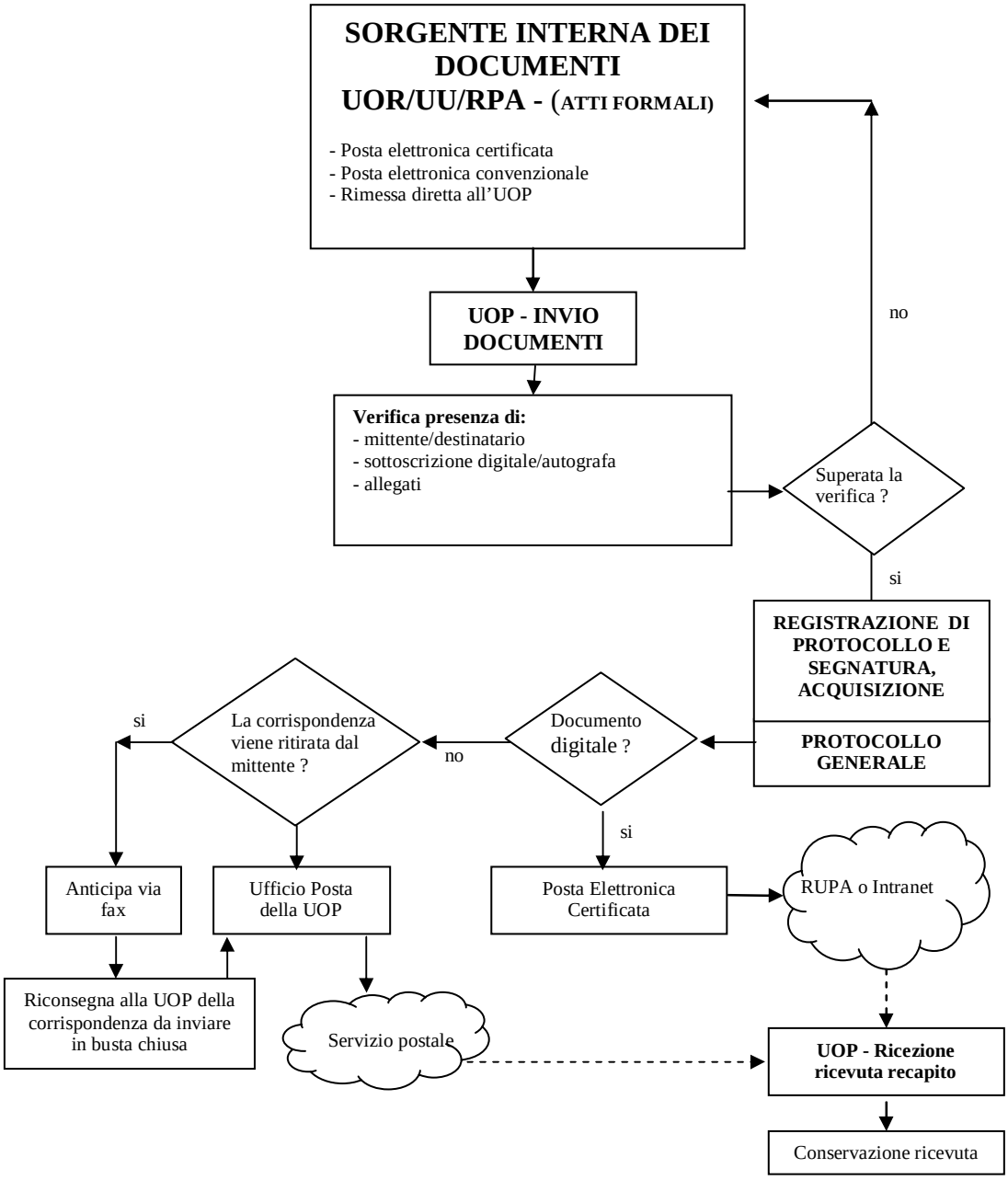
Durante l'ultima fase del flusso di lavorazione della corrispondenza in ingresso vengono svolte le seguenti attività:

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

5.2.16. Conservazione dei documenti e dei fascicoli nella fase corrente

All'interno di ciascun Ufficio Utente (UU) di ciascun UOR della AOO sono stati individuati gli addetti alla organizzazione e alla tenuta dei fascicoli "attivi" (e chiusi in attesa di riversamento nell'archivio di deposito) e alla conservazione dei documenti al loro interno.

5.3. Flusso dei documenti in uscita 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 uscita" 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 nel paragrafo 4.11 – Uso della 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 all'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

Tutti i documenti originali da spedire, siano essi in formato digitale o analogico, sono inoltrati alla UOP istituzionale:

- nella casella di posta elettronica interna dedicata alla funzione di "appoggio" per i documenti digitali da trasmettere nel caso di documenti informatici;
- in busta aperta per le operazioni di protocollazione e segnatura nel caso di documenti analogici *tranne i documenti contenenti dati personali sensibili o giudiziari.*

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

5.3.3. Registrazione di protocollo e segnatura

Le operazioni di registrazione e di apposizione della segnatura del documento in uscita sono effettuate presso la UOP istituzionale. 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, come, ad esempio, nel caso di spedizioni per raccomandata con ricevuta di ritorno, posta celere, corriere, è a cura della UOP.

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 propri di certificatore accreditato iscritto nell'elenco pubblico tenuto dal CNIPA.
Per la spedizione dei documenti informatici, l'AOO si avvale del servizio di "posta elettronica certificata",conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, offerto da un soggetto esterno in grado di assicurare la sicurezza del canale di comunicazione, di dare certezza sulla data di spedizione e di consegna dei documenti attraverso una procedura di rilascio delle ricevute di ritorno elettroniche.
Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono 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

La UOP provvede direttamente a tutte le operazioni di spedizione della corrispondenza provvedendo:

- alla consegna all'ufficio postale di tutta la corrispondenza ;
- alla predisposizione delle ricevute di invio e di ritorno per le raccomandate, unitamente alla distinta delle medesime da rilasciare all'ufficio postale.

5.3.6. Affrancatura dei documenti in partenza

Tutte le attività di affrancatura della corrispondenza inviata per posta vengono svolte dal servizio postale (Poste S.p.a.).
Al fine di consentire il regolare svolgimento di tali operazioni, la corrispondenza in partenza deve essere consegnata alla UOP secondo le regole richiamate nell'allegato 9.

5.3.7. Documenti in partenza per posta convenzionale con più destinatari

Qualora i destinatari siano più di uno vengono inviate solo le copie dell'unico originale prodotto dall' UOR/UU .

5.3.8. Trasmissione di documenti cartacei a mezzo telefax

Questo tipo di trasmissione viene, di norma, eseguita previa protocollazione direttamente dagli UOR/UU che producono il documento.Sul documento trasmesso via fax può essere apposta la dicitura: "La trasmissione via fax del presente documento non prevede l'invio del documento originale". Solo su richiesta del destinatario verrà trasmesso anche l'originale.

Le ricevute della avvenuta trasmissione sono trattenute dagli UOR/UU che hanno inviato il fax.

5.3.9. Inserimento delle ricevute di trasmissione nel fascicolo

La minuta del documento cartaceo spedito, ovvero le ricevute dei messaggi telefax o delle raccomandate, ovvero le ricevute digitali del sistema di posta certificata utilizzata per lo scambio dei documenti digitali, sono conservate all'interno del relativo fascicolo.

Gli UOR/UU curano anche l'archiviazione delle ricevute di ritorno delle raccomandate. Queste ultime, sulle quali, precauzionalmente, è stato trascritto sia il numero di protocollo attribuito al documento a cui esse si riferiscono, sia l'UOR/UU mittente, sono inizialmente raccolte dalla UOP e successivamente consegnate alle UOR/UU medesime previo rilascio di ricevuta di consegna.

6. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI RICEVUTI

Il presente capitolo contiene le regole di assegnazione dei documenti in ingresso adottate dalla UOP.

6.1. Regole disponibili con il SdP

L'assegnazione dei documenti protocollati e segnati avviene sfruttando le funzionalità di seguito descritte.
Il SdP, per abbreviare il processo di assegnazione del materiale documentario oggetto di lavorazione, utilizza l'organigramma dell'AOO.

All'assegnazione segue la presa in carico del documento da parte del RPA, che provvede a inoltrarlo, se del caso, all'addetto istruttore della pratica. In questa sede viene eseguita la classificazione del documento secondo le voci del titolario.

6.2. Attività di assegnazione

Di seguito viene descritta con maggiore dettaglio l'operazione di assegnazione dei documenti ricevuti illustrata nel flusso di lavorazione del precedente paragrafo 5.2

L'attività di assegnazione consiste nell'operazione di inviare direttamente dalla UOP il documento protocollato e segnato all'UOR competente e la contestuale trasmissione del materiale documentario oggetto di trattazione.
Con l'assegnazione si provvede ad attribuire la responsabilità del procedimento amministrativo ad un soggetto fisico che si identifica nel RPA designato.
Preso atto dell'assegnazione, il RPA verifica la competenza e, se esatta, provvede alla presa in carico del documento che gli è stato assegnato.
Una volta che al mittente iniziale (UOP) giunge notizia della presa in carico della corrispondenza, questo provvede ad inviare, con le tecnologie adeguate, il documento in questione compilato nella parte 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 incaricata della gestione del procedimento a cui il documento si riferisce e prende in carico il documento. I termini per la definizione del procedimento amministrativo che prende avvio dal documento decorrono comunque dalla data di protocollazione.

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

6.3. Corrispondenza di particolare rilevanza

Quando un documento pervenuto appare di particolare rilevanza, indipendentemente dal supporto utilizzato, viene inviato in busta chiusa direttamente al Presidente o al Direttore;

6.4. 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 interni al centro servizio.
L'UOR competente ha notizia dell'assegnazione di detti documenti tramite un messaggio di posta elettronica di notifica di assegnazione.
Il responsabile dell'UOR è in grado di visualizzare i documenti, attraverso le funzionalità del SdP e, in base alle abilitazioni possedute, 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 ed assegnare il documento in questione.

La "presa in carico" dei documenti informatici viene registrata dal SdP 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" e/o "per conoscenza" lo ricevono esclusivamente in formato digitale.

6.5. Assegnazione dei documenti ricevuti in formato cartaceo

Al termine delle operazioni di registrazione, segnatura dei documenti ricevuti dall'AOO in formato cartaceo, i documenti medesimi sono assegnati al RPA di competenza per via informatica attraverso la rete interna dell'amministrazione. L'originale cartaceo riceve il seguente trattamento:

- viene acquisito in formato immagine con l'ausilio di *scanner*.;
- può essere successivamente trasmesso/ritirato al/dal RPA, oppure essere conservato dalla UOP.

I documenti cartacei gestiti dalla UOP sono di norma assegnati entro il giorno successivo a quello di ricezione, salvo che vi figurino, 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.

L'UOR competente ha notizia dell'arrivo del documento ad esso indirizzato tramite un messaggio di posta elettronica. Attraverso le funzioni del SdP e in base alle abilitazioni previste il responsabile dell'UOR 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 nelle UOR di competenza coincide con la data di assegnazione degli stessi.

6.6. Modifica delle assegnazioni

Nel caso di assegnazione errata, l'UOR/UU che riceve il documento comunica l'errore alla UOP, 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. REGOLE DI ASSEGNAZIONE DEI DOCUMENTI INVIATI

Il presente capitolo riporta le regole di gestione dei documenti in uscita adottate dalla UOP.

L'UOP dopo aver protocollato in uscita il documento lo assegna all'ufficio proponente.
Tale assegnazione è generata automaticamente dal SdP ed è la conferma dell'avvenuta protocollazione del documento..

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

Il presente capitolo individua l'unità organizzativa responsabile 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, nell'allegato 3 è riportata l'articolazione della AOO in UOR e UU.
Relativamente alla organizzazione e alla tenuta dei documenti della AOO in cui è articolata l'amministrazione, all'interno della AOO in parola, è stato istituito il servizio archivistico.
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.

8.1. Servizio archivistico

L'amministrazione ha istituito il servizio archivistico e documentale denominato "Sezione protocollo e archiviazione", che si occupa di gestire anche la componente archivistica dell'altra AOO-GAB. Di conseguenza, il sistema archivistico è unico e trasversale ad ambedue le AOO.
Il servizio archivistico è competente a gestire l'intera documentazione archivistica, ovunque trattata, distribuita o conservata, ai fini della sua corretta collocazione, classificazione, e conservazione. Al servizio archivistico è preposto lo stesso RSP.

9. ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO E DOCUMENTI SOGGETTI A REGISTRAZIONE PARTICOLARE

9.1. Documenti esclusi

Sono, 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 come riportato nell'allegato 11.

9.2. 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 11.
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.

10. SISTEMA DI CLASSIFICAZIONE, FASCICOLAZIONE E PIANO DI CONSERVAZIONE

10.1. Protezione e conservazione degli archivi pubblici

10.1.1. Caratteristiche generali

Il presente capitolo contiene 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 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.
Il titolario e il piano di conservazione sono adottati dall'amministrazione con atti formali.

10.1.2. Misure di protezione e conservazione degli archivi pubblici

Gli archivi e i singoli documenti dello Stato, delle regioni e degli enti pubblici 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, e deve essere conservato nella sua organicità. L'eventuale trasferimento ad altre persone giuridiche di complessi organici di documentazione è subordinato all'autorizzazione della direzione generale per gli archivi.
L'archivio di deposito e l'archivio storico non possono essere rimossi dal luogo di conservazione senza l'autorizzazione della suddetta direzione generale per gli archivi.
Lo scarto dei documenti dell'archivio in parola è subordinato all'autorizzazione della direzione generale per gli archivi, su proposta delle commissioni di sorveglianza istituite presso ciascun ufficio con competenza a livello provinciale o delle commissioni di scarto istituite presso ogni ufficio con competenza "subprovinciale".
Per l'archiviazione e la custodia nella sezione di deposito, o storica, dei documenti contenenti dati personali, si applicano le disposizioni di legge sulla tutela della riservatezza dei dati personali, sia che si tratti di supporti informatici che di supporti convenzionali.

10.2. Titolario o piano di classificazione

10.2.1. 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.

Il titolo individua per lo più funzioni primarie e di organizzazione dell'ente (macrofunzioni); le successive partizioni, classi e sottoclassi, corrispondono a specifiche competenze che rientrano concettualmente nella macrofunzione descritta dal titolo, articolandosi gerarchicamente tra loro in una struttura ad albero rovesciato, secondo lo schema riportato nell'allegato 12.
Titoli, classi, sottoclassi etc. sono nel numero prestabilito dal titolario di classificazione e non sono modificabili né nel numero né nell'oggetto, se non per provvedimento esplicito del vertice 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.
L'aggiornamento del titolario compete esclusivamente al vertice dell'amministrazione, su proposta del RSP. La revisione, anche parziale, del titolario viene proposta dal RSP quando 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.
Il sistema di protocollazione garantisce la storicizzazione delle variazioni di titolario e la possibilità di ricostruire le diverse voci nel tempo, mantenendo stabili i legami dei fascicoli e dei documenti con la struttura del titolario vigente al momento della produzione degli stessi.
Per ogni specifica voce viene riportata la data di inserimento e la data di variazione.
Di norma le variazioni vengono introdotte a partire dal 1 gennaio dell'anno successivo a quello di approvazione del nuovo titolario e hanno durata almeno per l'intero anno.
Rimane possibile, se il sistema lo consente, di registrare documenti in fascicoli già aperti fino alla conclusione e alla chiusura degli stessi.
Il titolario è stato elaborato da un gruppo di lavoro appositamente costituito all'interno dell'AOO ed è stato approvato dai competenti organi dell'amministrazione archivistica statale.

10.2.2. 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), il numero del fascicolo ed eventualmente del sottofascicolo.
Le operazioni di classificazione vengono svolte interamente dagli UOR/UU destinatari/istruttori di atti.

10.3. Fascicoli e *dossier*

10.3.1. Fascicolazione dei documenti

Tutti i documenti registrati nel sistema di protocollo informatico e/o classificati, indipendentemente dal supporto sul quale sono formati, sono riuniti in fascicoli.
Ogni documento, dopo la 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.

10.3.2. Apertura del fascicolo

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

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

10.3.3. Chiusura del fascicolo

Il fascicolo viene chiuso al termine del procedimento amministrativo o con l'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 precedente, primo capoverso, il quale è tenuto pertanto all'aggiornamento del repertorio dei fascicoli.

10.3.4. Processo di assegnazione dei fascicoli

Quando un nuovo documento viene recapitato all'AOO, 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'UU cui è assegnata la pratica;
- 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 RPA;
  - ✓ invia il documento con il relativo fascicolo, al dipendente, che dovrà istruire la pratica per competenza.

10.3.5. Modifica dell'assegnazione dei fascicoli

Quando si verifica un errore nell'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.

10.3.6. 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.
Il repertorio dei fascicoli è costantemente aggiornato.

10.3.7. 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 l'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).

10.3.8. 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.

10.4. Consultazione e movimentazione dell'archivio corrente, di deposito e storico

10.4.1. Principi generali

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

10.4.2. Consultazione ai fini giuridico-amministrativi

Il diritto di accesso ai documenti è disciplinato dall'art. 24 della legge 7 agosto 1990, n. 241 come sostituito dall'art. 16 della legge 11 febbraio 2005, n.15, che qui di seguito si riporta:
"Esclusione dal diritto di accesso.
1. Il diritto di accesso è escluso:
a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo;
b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano;

c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione;
d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psicoattitudinale relativi a terzi.
2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.
3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.
4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.
5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.
6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi:
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 “

10.4.3. Consultazione da parte di personale esterno all’amministrazione

La domanda di accesso ai documenti viene presentata/inviata alla UOP, che provvede a smistarla al servizio archivistico.
Presso la UOP, a cui fa capo il servizio archivistico, sono disponibili appositi moduli, come quelli riportati nell’allegato 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.
Con la medesima procedura viene formulata richiesta di accesso alle informazioni raccolte, elaborate ed archiviate in formato digitale.
In tal 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.
L'ingresso all'archivio di deposito, e storico, è consentito solo agli addetti del servizio archivistico.
La consultazione dei documenti è possibile esclusivamente sotto la diretta sorveglianza del personale addetto.
Il rilascio di copie dei documenti dell'archivio, quando richiesto, avviene previo rimborso delle spese di riproduzione, secondo le procedure e le tariffe stabilite dall'amministrazione.
In caso di pratiche momentaneamente irreperibili, in cattivo stato di conservazione, in restauro o rilegatura, oppure escluse dal diritto di accesso conformemente alla normativa vigente, il responsabile rilascia apposita dichiarazione.

10.4.4. Consultazione da parte di personale interno all'amministrazione

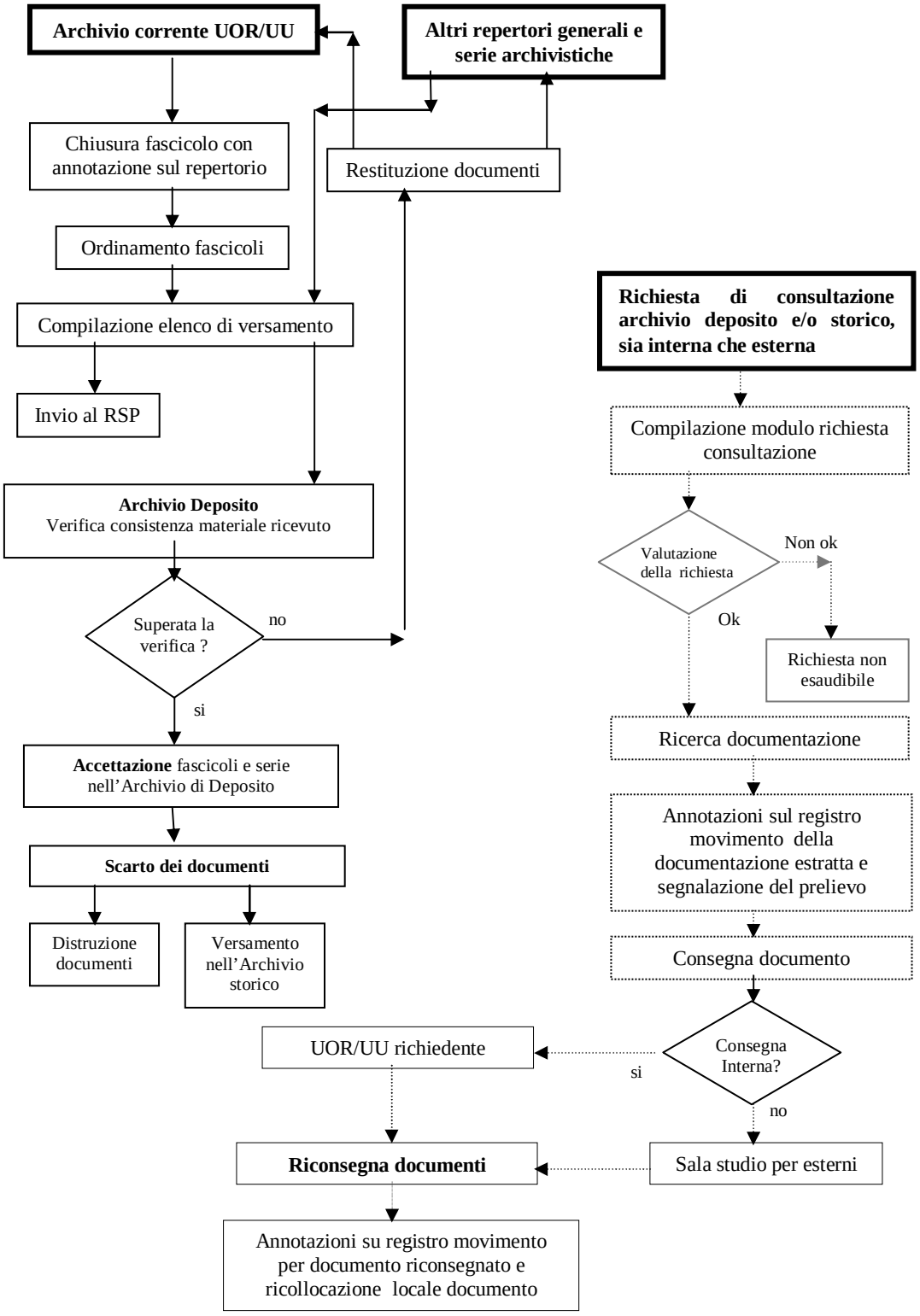
Gli UOR, per motivi di consultazione, possono richiedere in ogni momento al servizio archivistico i fascicoli conservati nella sezione archivistica di deposito, o storica, compilando appositi moduli, come quello riportato nell'allegato 13.
L'affidamento temporaneo di un fascicolo già versato all'archivio 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, come quello riportato nell'allegato 13, 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 conservata 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 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, degli stessi rispettandone la sedimentazione archivistica e il vincolo.

Nel caso di accesso ad archivi informatici, le formalità da assolvere sono stabilite da adeguate politiche e procedure di accesso alle informazioni stabilite dall'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.

10.4.5. 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 una funzione strategica dell'amministrazione.


Archivio corrente UOR/UU
Altri repertori generali e serie archivistiche
Chiusura fascicolo con annotazione sul repertorio
Restituzione documenti
Ordinamento fascicoli
Compilazione elenco di versamento
Invio al RSP
Archivio Deposito
Verifica consistenza materiale ricevuto
Superata la verifica ?
no
si
Accettazione fascicoli e serie nell'Archivio di Deposito
Scarto dei documenti
Distruzione documenti
Versamento nell'Archivio storico
Richiesta di consultazione archivio deposito e/o storico, sia interna che esterna
Compilazione modulo richiesta consultazione
Valutazione della richiesta
Non ok
Ok
Richiesta non esaudibile
Ricerca documentazione
Annotazioni sul registro movimento della documentazione estratta e segnalazione del prelievo
Consegna documento
Consegna Interna?
si
no
UOR/UU richiedente
Riconsegna documenti
Sala studio per esterni
Annotazioni su registro movimento per documento riconsegnato e ricollocazione locale documento

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

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

11.1. Unicità del protocollo informatico

Nell'ambito della AOO il registro generale di protocollo è unico al pari della numerazione progressiva delle registrazioni di protocollo.
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.
Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici.

11.2. 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 diverso, ai sensi dell'art.7. comma 5, del DPCM 31 ottobre 2000, (*responsabile della conservazione delle copie*) dal RSP ed appositamente nominato dall'AOO.
Tale operazione viene espletata all'interno del centro servizi.

11.3. Registrazione di protocollo

Di seguito vengono illustrate le regole "comuni" di registrazione del protocollo, valide per tutti i tipi di documenti trattati dall'AOO (ricevuti, trasmessi ed interni formali, digitali o informatici e analogici).
Su ogni documento ricevuto, o spedito, dall'AOO è effettuata una registrazione di protocollo con il sistema di gestione del protocollo informatico, consistente nella memorizzazione dei dati obbligatori.
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;
- il destinatario del documento;
- l'oggetto del documento;

Le variazioni su "oggetto", "mittente" e "destinatario" vengono mantenute con un criterio di storicizzazione dall'SdP, evidenziando data, ora e utente che ha effettuato la modifica.
Le registrazioni di protocollo, in armonia con la normativa vigente, prevedono elementi accessori, rilevanti sul piano amministrativo, organizzativo e gestionale, sempre che le rispettive informazioni siano disponibili.
Tali dati facoltativi sono descritti nei paragrafi seguenti.

11.3.1. Documenti informatici

I documenti informatici sono ricevuti, e trasmessi, in modo formale sulla/dalla casella di posta elettronica certificata istituzionale dell'AOO.
La registrazione di protocollo di un documento informatico sottoscritto con firma digitale è eseguita dopo che l'operatore 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, che si può riferire sia al corpo del messaggio che ad uno dei *file* ad esso allegati che può assumere la veste di documento principale.
Tali documenti sono memorizzati nel sistema, in modo non modificabile, al termine delle operazioni di registrazione e segnatura di protocollo.
Le UOP ricevono i documenti informatici interni di tipo formale da protocollare all'indirizzo di posta elettronica interno preposto a questa funzione.

11.3.2. Documenti analogici (cartacei e supporti rimovibili)

I documenti analogici sono ricevuti e trasmessi con i mezzi tradizionali della corrispondenza.
La registrazione di protocollo di un documento cartaceo ricevuto, così come illustrato nel seguito, viene sempre eseguita in quanto l'AOO ha la funzione di registrare l'avvenuta ricezione.
Nel caso di corrispondenza in uscita o interna formale, l'UOP esegue la registrazione di protocollo dopo che il documento ha superato tutti i controlli formali sopra richiamati.

11.4. Elementi facoltativi delle registrazioni di protocollo

Al fine di migliorare l'efficacia e l'efficienza dell'azione amministrativa, il RSP, con proprio provvedimento, può modificare e integrare gli elementi facoltativi del protocollo richiamati nella circolare AIPA 7 maggio 2001 n. 28.
La registrazione degli elementi facoltativi del protocollo, può essere modificata, integrata e cancellata in base alle effettive esigenze della UOP o degli UOR.
In caso di necessità, i dati facoltativi sono modificabili senza necessità di annullare la registrazione di protocollo, fermo restando che il sistema informatico di protocollo registra tali modifiche.

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

- Il numero di protocollo e la data o solo data se presente;
- ulteriori informazioni sul mittente/destinatario, soprattutto se persona giuridica;
- l'indirizzo completo del mittente/destinatario (via, numero civico, CAP, città, provincia, stato civile, sesso);
- il numero di matricola (se dipendente interno dell'amministrazione);
- il codice fiscale;
- il numero della partita IVA;
- il recapito telefonico;
- il recapito telefax;
- gli indirizzi di posta elettronica;
- la chiave pubblica della firma digitale;
- il consenso all'uso della *e_mail* in termini di *privacy*.

11.5. 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.

11.5.1. Documenti informatici

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

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

E' facoltativo riportare le seguenti informazioni:

- denominazione dell'amministrazione;
- indice di classificazione;
- 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, ufficio destinatario;
- individuazione 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.

11.5.2. Documenti cartacei

La segnatura di protocollo di un documento cartaceo avviene attraverso l'apposizione di una etichetta sulla 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.

L'etichetta autoadesiva ha il formato e il contenuto riportato nell'allegato 14.
L'operazione di segnatura dei documenti in partenza viene integralmente eseguita dalla UOP, ovvero viene effettuata dall'UOR/UU/RPA competente che redige il documento se è abilitata, come UOP, alla protocollazione dei documenti in uscita.
L'operazione di acquisizione dell'immagine dei documenti cartacei viene effettuata solo dopo che l'operazione di segnatura è stata eseguita, in modo da "acquisire" con l'operazione di scansione, come immagine, anche il "segno" sul documento.
Se è prevista l'acquisizione del documento cartaceo in formato immagine, il "segno" della segnatura di protocollo viene apposto sulla prima pagina dell'originale; in caso contrario il "segno" viene apposto sul retro della prima pagina dell'originale.

11.6. Annullamento delle registrazioni di protocollo

La necessità di modificare - anche un solo campo tra quelli obbligatori della registrazione di protocollo, registrate in forma non modificabile - per correggere errori verificatisi in sede di immissione manuale di dati o attraverso l'interoperabilità dei sistemi di protocollo mittente e destinatario, comporta l'obbligo di annullare l'intera registrazione di protocollo.
Le informazioni relative alla registrazione di protocollo annullata rimangono memorizzate nel registro informatico del protocollo per essere sottoposte alle elaborazioni previste dalla procedura, ivi comprese le visualizzazioni e le stampe, nonché la data, l'ora e l'autore dell'annullamento e gli estremi dell'autorizzazione all'annullamento del protocollo rilasciata dal 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.

Analoga procedura di annullamento va eseguita quando, stante le funzioni primarie di certificazione riconosciute dalle norme alla UOP, emerge che ad uno stesso documento in ingresso, ricevuto con mezzi di trasmissione diversi quali, ad esempio, fax, originale cartaceo, e_mail siano stati attribuiti più numeri di protocollo.

11.7. Livello di riservatezza

IL SdP applica automaticamente il livello di riservatezza "base" a tutti i documenti protocollati.
Il trattamento di documenti che richiedono/prevedono livelli maggiori di sicurezza esula dal presente manuale.
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 invece che hanno un livello di riservatezza superiore lo mantengono.

11.8. Casi particolari di registrazioni di protocollo

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

11.8.1. Circolari e disposizioni generali

Gli ordini di servizio, di norma, non vengono protocollati.
Le circolari ricevute vengono protocollate nel registro ufficiale di protocollo.
Le disposizioni generali e tutte le altre comunicazioni interne, di norma, si registrano con un solo numero di protocollo nel registro di protocollo interno.

11.8.2. Documenti cartacei in uscita 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.

11.8.3. 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.

11.8.4. Documenti cartacei ricevuti a mezzo *telefax*

Il documento ricevuto a mezzo telefax è un documento analogico a tutti gli effetti.
All'interno della AOO i documenti possono essere inviati e ricevuti direttamente dagli UOR/UU; per i fax ricevuti questi ultimi hanno il compito di consegnarli alla UOP per le operazioni di protocollazione.
Il documento da chiunque trasmesso ad una 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.

Il documento in uscita 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 del fax.

La copertina, del telefax ed il rapporto di trasmissione vengono anch'essi inseriti nel fascicolo per documentare tempi e modi dell'avvenuta spedizione.

11.8.5. Protocollazione di un numero consistente di documenti cartacei

Quando si presenti la necessità di protocollare un numero consistente di documenti, sia in ingresso (ad es. scadenza di gare o di 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.

11.8.6. 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, gli stessi saranno accantonati e protocollati successivamente. In questo caso al mittente, o al suo delegato, viene rilasciata ugualmente ricevuta senza gli estremi del protocollo.

11.8.7. Fatture, assegni e altri valori di debito o credito

Le fatture, gli assegni o altri valori di debito o credito sono protocollate sul registro ufficiale di protocollo e inviate quotidianamente, in originale, alla UOR competente.

11.8.8. Protocollazione di documenti inerenti gare di appalto confezionate 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 viene aperta dalla UOP, ma viene timbrata dalla medesima che provvede ad inoltrarla alla UOR/UU competente; quest'ultima provvede a sottoscrivere il plico, a riportare sul medesimo la data, l'ora di arrivo ed a riconsegnarla alla UOP per la protocollazione del plico in parola.
Il plico così protocollato viene riconsegnato all'UOR/UU che provvede alla custodia, con mezzi idonei, sino all'espletamento della gara.
Dopo l'apertura delle buste, l'UOR che gestisce la gara riporta gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.
Per motivi organizzativi tutti gli UOR sono tenuti ad informare con congruo anticipo il RSP dell'AOO in merito alle scadenze di concorsi, gare, bandi di ogni genere.

11.8.9. Protocollazione delle domande di iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata confezionate su supporti cartacei

La corrispondenza, dal cui involucro si evince che si tratta di una domanda di iscrizione nell'elenco pubblico dei gestori di posta elettronica, non viene aperta dalla UOP, ma protocollata con l'applicazione dell'etichetta autoadesiva di segnatura sulla confezione. Successivamente viene inoltrata alla UOR/UU competente. Questi ultima, dopo l'apertura della busta, ha l'obbligo di riportare gli estremi di protocollo indicati sulla confezione esterna su tutti i documenti in essa contenuti.

11.8.10. 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 ingresso che per quelli in uscita.

11.8.11. 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.

11.8.12. Protocollazione dei messaggi di posta elettronica convenzionale

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

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

11.8.13. Protocollazione di documenti digitali pervenuti erroneamente

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

11.8.14. Ricezione di documenti cartacei pervenuti erroneamente

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

11.8.15. Copie per "conoscenza"

Nel caso di copie per conoscenza si deve utilizzare la procedura descritta nel paragrafo 11.8.2. In particolare, chi effettua la registrazione e lo smistamento dell'originale e delle copie, registra sul registro di protocollo a chi sono state inviate le copie "per conoscenza".

11.8.16. Differimento delle registrazioni

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

Qualora nei tempi sopra indicati non possa essere effettuata la registrazione di protocollo 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 rinvio 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.

11.8.17. Corrispondenza personale o riservata

La corrispondenza personale non viene aperta, ma viene consegnata al destinatario, il quale, dopo averne preso visione, se reputa che i documenti ricevuti devono essere comunque protocollati perché riguardano problematiche istituzionali, provvede a trasmetterli alla UOP per la protocollazione.

11.8.18. 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 gli 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 relativo fascicolo.

11.9. Gestione delle registrazioni di protocollo con il SdP

Le registrazioni di protocollo informatico, l'operazione di "segnatura" e la registrazione delle informazioni annullate o modificate nell'ambito di ogni sessione di attività di registrazione sono effettuate attraverso il SdP.
Il sistema di sicurezza del centro servizi garantisce la protezione di tali informazioni sulla base delle relativa architettura tecnologica, sui controlli d'accesso e i livelli di autorizzazione realizzati.

11.10. Registrazioni di protocollo

11.10.1. Attribuzione del protocollo

Al fine di assicurare l'immodificabilità dei dati e dei documenti soggetti a protocollo, il SdP appone al documento protocollato un riferimento temporale, come previsto dalla normativa vigente.
Il SdP assicura l'esattezza del riferimento temporale con l'acquisizione periodica del tempo ufficiale di rete.
Come previsto dalla vigente normativa in materia di protezione dei dati personali le AOO aderenti al SdP sono informate della necessità di non inserire informazioni "sensibili" e "giudiziarie" nel campo "oggetto" del registro di protocollo.

11.10.2. Registro informatico di protocollo

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

- estrazione delle registrazioni del giorno corrente 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 SdP.

L'uso combinato dei meccanismi permette di conferire validità e integrità ai contenuti del *file* del registro di protocollo.

E' inoltre disponibile per le UOP del SdP una funzione applicativa di "Stampa registro di protocollo" per il salvataggio su supporto cartaceo dei dati di registro.
Al termine delle operazioni giornaliere o comunque entro il successivo giorno lavorativo, all'interno del centro servizi dell'erogatore del SdP sono effettuate le seguenti operazioni di garanzia:

- *export* delle tabelle contenenti i dati dei registri di protocollo delle AOO e loro acquisizione dai sistemi di esercizio sulla stazione di gestione dell'area sicurezza;
- cifratura dei *file* per i quali è prevista questa operazione;
- apposizione della firma digitale sui file da archiviare;
- riversamento dei *file* in parola su due supporti rimovibili non riscrivibili.

11.10.3. Tenuta delle copie del registro di protocollo

Presso il centro servizi un operatore di sicurezza, provvede con periodicità giornaliera, alla memorizzazione su supporto ottico, in duplice copia, dei seguenti oggetti:

- i *file* cifrati delle tabelle dei registri di protocollo delle AOO;
- le firme dei *file* dei registri di protocollo delle AOO eseguite dall'operatore di sicurezza.

Le copie dei supporti sono conservate dal responsabile della sicurezza negli armadi ignifughi dell'area sicurezza del centro servizi per tutta la durata del contratto di servizio e, comunque, nel rispetto delle norme vigenti.
Le modalità di archiviazione sono regolamentate dal responsabile dell'RSP..

Presso l'AOO dell'amministrazione contraente, che quotidianamente riceve, via *e-mail* dal SdP, copia del registro giornaliero di protocollo in formato PDF, il responsabile della conservazione della copia del registro di protocollo, un delegato, può, sia stampare il *file* ricevuto, sia riversarlo su supporto ottico non riscrivile.

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

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

12.1. Descrizione funzionale ed operativa

La descrizione completa delle funzionalità dell'applicativo di protocollo è disponibile e consultabile insieme ai manuali operativi via internet sul sito *www.protocolloasp.gov.it.* nella sezione documenti/manuali.

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 SdP.

13.1. Il registro di emergenza

Qualora non fosse possibile fruire del SdP 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 il registro di emergenza non venga utilizzato, il RSP annota sullo stesso il mancato uso.
Le registrazioni di protocollo effettuate sul registro di emergenza sono identiche a quelle eseguite sul 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 sono associati 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.
Il SdP realizza il registro di emergenza con un applicativo specifico, scaricabile dal sito "protocolloasp.gov.it", da installare sulle postazioni di lavoro delle AOO in modalità *stand alone*, fuori linea.

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 *realtime*, le operazioni di protocollo siano svolte sul registro di emergenza 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 riportato di seguito.
L'elenco delle UOP abilitate alla registrazione dei documenti sui registri di emergenza è riportato nell'allegato 3.
Le modalità operative di impiego dell'applicativo del registro di emergenza sopra richiamato sono dettagliatamente riportate nel documento "Modalità organizzative per la fruizione del registro di emergenza per gli utenti del servizio di protocollo in modalità ASP".

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

CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione -
Area Organizzativa Omogenea DIREZIONE
Unità Organizzativa di registrazione di Protocollo

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 della tenuta del protocollo autorizza l'uso del registro di emergenza per periodi successivi di durata non superiore ad 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 gli stessi previsti dal protocollo generale.
Durante il periodo di interruzione del SdP, il responsabile della gestione del centro servizio (o persona da lui delegata) informa costantemente il "call center" del RTI sui tempi di ripristino del servizio in parola affinché possa fornire le informazioni aggiornate alle AOO che ne fanno richiesta.

13.4. Modalità di chiusura e di recupero del registro di emergenza

E' compito del RSP verificare la chiusura del registro di emergenza.
E' compito del RSP, o di un suo delegato, riportare dal registro di emergenza al registro di protocollo generale del SdP le protocollazioni relative ai documenti protocollati in emergenza attraverso le postazioni di lavoro abilitate, entro cinque giorni dal ripristino delle funzionalità del SdP.
Al fine di ridurre la probabilità di commettere errori in fase di trascrizione dei dati riportati dal registro di emergenza 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.
Le modalità operative di recupero dei dati acquisiti in emergenza con l'applicativo in parola, sono dettagliatamente riportate nell'omonimo documento "Modalità organizzative per la fruizione del registro di emergenza per gli utenti del servizio di protocollo in modalità ASP".
Una volta ripristinata la piena funzionalità del SdP, il RSP provvede alla chiusura del registro di emergenza, annotando, sullo stesso il numero delle registrazioni effettuate e la data e l'ora di chiusura.
Per semplificare la procedura di chiusura del registro di emergenza il RSP inutilizza il modulo utilizzato nella fase di apertura del registro di emergenza.

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

14.1. Modalità di approvazione e aggiornamento del manuale

L'amministrazione adotta il presente "Manuale di gestione" su proposta del responsabile del servizio di protocollo informatico.

Il presente manuale potrà essere aggiornato a seguito di:

- normativa sopravvenuta;
- introduzione di nuove pratiche tendenti a migliorare l'azione amministrativi in termini di efficacia, efficienza e trasparenza;
- inadeguatezza delle procedure rilevate nello svolgimento delle attività correnti;
- modifiche apportate negli allegati dal RSP.

14.2. Regolamenti abrogati

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

14.3. Pubblicità del presente Manuale

Il presente manuale, a norma dell'art. 22 della legge 7 agosto 1900, n. 241, è disponibile alla consultazione del pubblico che ne può prendere visione in qualsiasi momento.
Inoltre copia del presente manuale è:

- fornita a tutto il personale dell'AOO e se possibile, viene resa disponibile mediante la rete intranet;
- inviata all'organo di revisione;
- pubblicato sul sito internet dell'amministrazione.

14.4. Operatività del presente manuale

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

ALLEGATI
AL
MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI DOCUMENTI E DELL'ARCHIVIO DEL CNIPA

- Area Organizzativa Omogenea CNIPADIR –

(Versione 2.0 del 18-06-2007)

INDICE DEGLI ALLEGATI

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 (Si veda l'art. 1, comma 1,lettera 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 (Si veda l'art. 1, comma 1, lettera o) del dPR n.445/2000;
AMMINISTRAZIONI PUBBLICHE	Le amministrazioni 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 le scuole di ogni ordine e grado e le istituzioni educative, le aziende ed le 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, comma1 lettera z) del d.lgs.7 marzo 2005, n.82)
ARCHIVIO	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 dall'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'archivio è unico, anche se, convenzionalmente, per motivi organizzativi, tecnici, funzionali e di responsabilità, viene suddiviso in tre sezioni: corrente, di deposito e storica;
ARCHIVIO CORRENTE	Il complesso dei documenti relativi ad affari e a procedimenti amministrativi in corso di istruttoria e di trattazione o comunque per i quali esista un interesse attuale;
ARCHIVIO DI DEPOSITO	Il 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 per i quali esista un interesse sporadico;

ARCHIVIO STORICO	L'insieme 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 (Si veda l'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 (Si veda l'art.2, lettera n) del dPCM 31 ottobre 2000);
ASSEGNAZIONE	L'operazione d'individuazione dell'Ufficio Utente (UU) competente per la trattazione del procedimento amministrativo o dell'affare, cui i documenti si riferiscono;
AUTENTICAZIONE DI SOTTOSCRIZIONE	L'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive (l'art 1., comma 1, lettera 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 lettera 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 letterao) 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, lettera. p) 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 lettera d 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. 1comma 1, lettera 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 D.P.C.M. 31 ottobre 2000, articolo 15, comma 3).(Si veda l'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 (Si veda l'art. 1, comma 1 lettera e) del d.lgs..7 marzo 2005, n.82)
CERTIFICATO QUALIFICATO	Il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art. 1 comma 1 lettera 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 lettera 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 lettera 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, lettera 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 lettera 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 lettera 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 lettera 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, lettera d) 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 lettera 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 lettera b) del d.lgs. 30 giugno 2003 n.196);
DATO PUBBLICO	Il dato conoscibile da chiunque (art. ,1comma 1, lettera n) del d.lgs..7 marzo 2005, n.82);
DATO A CONOSCIBLITÀ LIMITATA	Il dato la cui conoscibilità riservata per legge o regolamento a specifici soggetti o categorie di soggetti (art. ,1comma 1, lettera 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 dal art.1 comma 1 lettera h) del dPR 28 dicembre 2000, n. 445;
DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE	Il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato (Si veda l'art.1 comma 1 lettera 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 lettera m 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, lettera a) della 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 (Si veda art.,1 comma 1, lettera 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 (ad esempio: documenti cartacei), come le immagini su film (ad esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (ad esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia (art 1, comma 1, lettera b). della 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. della deliberazione CNIPA del 19 febbraio 2004, n.11);
DOCUMENTO ARCHIVIATO	Documento informatico, anche sottoscritto, sottoposto al processo di archiviazione elettronica (Si veda art 1,.comma 1, lettera h) della 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.,1comma 1, lettera c) del dPR 28 dicembre 2000, n. 445);
DOCUMENTO D'IDENTITÀ	La carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del titolare .(art.1,comma 1, lettera 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, lettera.e) del dPR 28 dicembre 2000, n.445);
DOCUMENTO INFORMATICO	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, comma 1, lettera t) del d.lgs..7 marzo 2005, n.82);
DOSSIER	Aggregazione di più fascicoli che può essere costituito 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, lettera 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, lettera 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 delle 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 da insiemi 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 diffuso 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, lettera 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, letteraq) 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, lettera 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 lettera c 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, lettera 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 (Si veda art.4 comma 1 lettera 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 m 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 genaio 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	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, lettera n) del dPR 28 dicembre 2000, n. 445);
MARCA TEMPORALE	Evidenza informatica che consente la validazione temporale (art.1, comma 1, lettera m) del dPCM 13 gennaio 2004);
MASSIMARIO DI SELEZIONE E SCARTO DEI DOCUMENTI/PIANO DI CONSERVAZIONE	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'art. 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 così come modificato dall'articolo 6 del d.lgs.. 23 gennaio 2002, n. 10 (art 1, comma 1, lettera f) della 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'art. 31 del d.lgs 30 giugno 2003 n.196. (Si veda art.4 comma 3 lettera 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 di altri dati in forma elettronica (art.4, comma 3, lettera 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, lettera v) del d.lgs..7 marzo 2005, n.82);
PIANO DI CONSERVAZIONE DEGLI ARCHIVI	Vedi massimario 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, lettera 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 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 (Si veda art 1 lettera q. della 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, lettera g) del d.lgs. 30 giugno 2003 n.196);
RESPONSABILE DEL	Il responsabile del servizio per la tenuta del protocollo informatico,

SERVIZIO DI PROTOCOLLO	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)	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, lettera g) del dPCM 13 gennaio 2004) o ad un messaggio di posta elettronica certificata (Si veda art.1, comma 1, lettera 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, lettera n) . della 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, lettera 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, lettera 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, lettera 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, lettera 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 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, lettera 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, lettera 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, lettera 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.

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. D.P.R. 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. 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.
4. D.P.C.M. 28 ottobre 1999 - Gestione informatica dei flussi documentali nelle pubbliche amministrazioni. (G.U. 11 dicembre 1999, n. 290)
5. 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. (GU. 27 dicembre 1999, n. 302)
6. D.P.C.M 31 ottobre 2000 - Regole tecniche per il protocollo informatico; valido ai sensi dell'art. 78 del D.P.R. 28 dicembre 2000, n. 445. (G.U. n. 272 del 21 novembre 2000)
7. 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 D.P.R. 10 novembre 1997, n. 513. (G.U. 14 dicembre 2000, n. 291)
8. D.P.R. 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (G.U. 20 febbraio 2001, n. 42)
9. Circolare 16 febbraio 2001, n.27 – "Art. 17 del dPR 10 novembre 1997, n. 513 - Utilizzo della firma digitale nelle pubbliche amministrazioni".
10. Decreto legislativo 30 marzo 2001, n. 165 - "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche".
11. Circolare AIPA 7 maggio 2001, n. 28 - Articolo 18, comma 2, del dPCM 31 ottobre 2000 Recante regole tecniche per il protocollo informatico di cui al D.P.R. 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)
12. Circolare AIPA 21 giugno 2001, n. 31 (Art. 7, comma 6, del D.P.C.M. 31 ottobre 2000 recante "Regole tecniche per il protocollo informatico di cui al D.P.R. 20 ottobre 1998, n. 428" - requisiti minimi di sicurezza dei sistemi operativi disponibili.)
13. Direttiva del 13 dicembre 2001 del Ministro per la funzione pubblica - Formazione del personale. (G.U. del 31 gennaio 2002, n. 26)
14. Direttiva 16 gennaio 2002, del Dipartimento per l'innovazione e le tecnologie - Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali.
15. Decreto legislativo 23 gennaio 2002, n. 10 - Recepimento della direttiva 1999/93/CE sulla firma elettronica.
16. Direttiva 9 dicembre 2002 del Ministro per l'innovazione e le tecnologie-Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.
17. Direttiva del Ministro per l'innovazione e le tecnologie, 20 dicembre 2002 - Linee guida in materia di digitalizzazione dell'amministrazione.
18. Legge 27 dicembre 2002, n. 289 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato.
19. D.P.R. 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.
20. Decreto legislativo 30 giugno 2003, N. 196 - Codice in materia di protezione dei dati personali.
21. Decreto 14 ottobre 2003 del Ministro - 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)
22. Direttiva 27 novembre 2003 del Ministro per l'innovazione e le tecnologie - Impiego della posta elettronica nelle pubbliche amministrazioni. (G.U. 12 gennaio 2004, n. 8)
23. Direttiva 1999/93/CE del Parlamento europeo e del consiglio del 13 dicembre 2003.

24. Direttiva 18 dicembre 2003 - Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004. (G.U. 4 aprile 2004, n. 28)
25. D.P.C.M. 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)
26. 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.
27. 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).

3 AREE ORGANIZZATIVE OMOGENEE E MODELLO ORGANIZZATIVO

3.1 MODELLO ORGANIZZATIVO DELL'AMMINISTRAZIONE

Denominazione dell'Amministrazione	Centro nazionale per l'Informatica nella pubblica amministrazione
Codice Identificativo assegnato all'Amministrazione	**CNIPA**
Indirizzo completo della sede principale dell'Amministrazione a cui indirizzare l'eventuale corrispondenza convenzionale	Via Isonzo 21/b – 00198 Roma
Elenco delle AREE ORGANIZZATIVE OMOGENEE – AOO	**DIREZIONE**
	GABINETTO

3.2 CARATTERIZZAZIONE DELL' AREA ORGANIZZATIVA OMOGENEA

Denominazione dell'Area Organizzativa Omogenea	**DIREZIONE**	
Codice Identificativo assegnato alla AOO	**CNIPADIR**	
Nominativo del responsabile del servizio di protocollo informatico, gestione documentale e archivistica	**Antonio NATALE**	
Casella di posta elettronica istituzionale dell'AOO	**cnipadir@cert.cnipa.it**	
Indirizzo completo della sede principale della AOO a cui indirizzare cui indirizzare l'eventuale corrispondenza convenzionale	Via Isonzo 21/b – 00198 Roma	
Data di istituzione della AOO	**30/12/1999**	
Data di soppressione della AOO		
Articolazione della AOO in Unità Organizzative di registrazione di Protocollo - UOP	Unità Organizzativa di registrazione di Protocollo Generale	Tipo protocollazione: Ingresso/Uscita
Articolazione della AOO in Uffici Organizzativi di Riferimento -UOR	• Strutture di staff al direttore generale • Indirizzo, supporto e verifica P.A.C. • Innovazione per le regioni e gli enti locali • Infrastrutture nazionali condivise • Progetti, applicazioni e servizi • Regolazione e formazione • Governo e monitoraggio delle forniture ICT • Funzionamento • Organizzazione e risorse umane	

3.3 ARTICOLAZIONE DI CIASCUN UFFICIO ORGANIZZATIVO DI RIFERIMENTO IN UFFICI UTENTE

L'organigramma completo ed aggiornato è presente in Internet sul sito www.cnipa.gov.it.

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

L'ordine di servizio per la nomina del responsabile del servizio di protocollo è il 51/99 del 30/12/1999 da quale si evince che il responsabile del servizio di protocollo informatico è il Sig. Antonio NATALE

5 ELENCO DELLE PERSONE TITOLARI DI FIRMA DIGITALE

Nominativo	Titolo
Livio ZOFFOLI	Presidente CNIPA
Caterina CITTADINO	Direttore generale CNIPA

6 ATTO DI DESIGNAZIONE DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Con riferimento al trattamento dei dati personali, sensibili e giudiziari eventualmente trattati nell'erogazione del servizio di protocollo in modalità ASP, il CNIPA, nell'Adunanza del 9 marzo 2006, ha provveduto a designare responsabile di tale trattamento le società EDS-Electronic Data System Italia S.p.A, in qualità di impresa mandataria, e da A.T Kearney S.p.A., Elsag S.p.A., Elea S.p.A., Infocamere S.c.p.A., Delta Dator S.p.A. e Elsag STI S.p.A, costituenti il raggruppamento temporaneo di imprese aggiudicatario del relativo appalto

7 MODALITÀ DI EROGAZIONE DEL SERVIZO DI CONSERVAZIONE SOTITUTIVA

Le modalità sono in corso di definizione. Non appena saranno definite e approvate verranno riportate nel presente capitolo.

8 POLITICHE DI SICUREZZA

8.1 ESTRATTO DELLE POLITICHE DI SICUREZZA ADOTTATE DAL RTI NEL CENTRO SERVIZIO

8.1.1 Classificazione della sicurezza

I componenti, le informazioni e i dati gestiti presso il centro servizi sono stati suddivisi convenzionalmente secondo quattro livelli di sicurezza come di seguito indicato. La suddetta classificazione si applica alle informazioni più rilevanti in termini di "valore" assegnato dall'Amministrazione.

- *Pubblico.* Si riferisce a componenti o informazioni che non richiedono protezione specifica;
- *Interno.* E' richiesto per componenti o informazioni con divieto di divulgazione all'esterno dell'RTI oppure di proprietà o di consultazione di terze parti autorizzate. Sono classificati a questo livello:
  - ✓ i dati personali comuni, salvo particolari esigenze;
  - ✓ i registri di protocollo (del servizio REPRO) se non contenenti dati personali sensibili e giudiziari.
- *Confidenzial.;* E' assegnato ai componenti o informazioni rilevanti ai fini della sicurezza o per la conduzione del Centro Servizi oppure di proprietà o di consultazione di terze parti autorizzate con le quali è stabilito un formale accordo scritto. Sono considerati materiale confidenziale e classificati a questo livello:
  - ✓ i dati personali sensibili e giudiziari, salvo esigenze più restrittive;
  - ✓ i registri di protocollo (del servizio REPRO) contenenti dati personali sensibili e giudiziari;
  - ✓ documenti e supporti rimovibili contenenti dati appartenenti alle Amministrazioni (servizio GEDOC);
  - ✓ documenti critici ai fini della sicurezza (specifiche di progettazione, configurazione, di indirizzamento, ecc.);
  - ✓ log di sicurezza;
  - ✓ risultati dei test di penetrabilità e degli *audi*t;
  - ✓ *report* dei livelli di servizio;
  - ✓ gli archivi che la Società è impegnata a conservare per disposizioni di legge.
- *Altamente riservato.* E' richiesto per componenti o informazioni di particolare rilevanza la cui diffusione può arrecare un pericolo immediato dal punto di vista della sicurezza o un danno notevole per la conduzione del Centro. Le password e le eventuali chiavi di crittografia sono classificate a questo livello.

Il corretto livello di classificazione da attribuire a informazioni o componenti si basa sui concetti di danno potenziale (diretto, indiretto o consequenziale), cioè la tipologia e l'entità del danno che potrebbe derivare da eventuali diffusioni non autorizzate, perdite o usi indebiti di una determinata informazione e di appetibilità, ossia la percezione dell'interesse che l'informazione assume per i terzi, interni, o esterni, e che potrebbe portare ad un utilizzo per scopi illeciti o dannosi.

8.1.2 Utilizzo del servizio di protocollo

8.1.2.1 Configurazione della postazione di lavoro - Browser

Il *browser* previsto per l'utilizzo dei servizi di protocollo è Internet Explorer 6.0.
Può essere impostato con un livello di protezione "medio", impostabile tramite il menu "Strumenti" e "Opzioni Internet".

Nel caso in cui il certificato digitale del *web server* del centro servizi, necessario per la connessione SSL, non sia stato emesso da una *Certification Authority* accreditata, è necessario la sua acquisizione dal portale e importazione nel *repository* di IE.

8.1.2.2 Configurazione della postazione di lavoro - Antivirus

I posti di lavoro devono essere dotati di un prodotto antivirus installato a cura e spese dell'Amministrazione/AOO al fine di prevenire la diffusione di software malevolo (*virus* e *worms*) proteggendo sia la stazione di lavoro che le reti alle quali l'utente è collegato.
E' responsabilità dell'utente verificarne la presenza, l'attivazione del monitor *real-time* e l'aggiornamento delle *virus signatures*. È necessario configurare una modalità di aggiornamento automatica con periodicità giornaliera.

8.1.3 Gestione dell'utenza

8.1.3.1 Responsabilità

La responsabilità delle azioni compiute nella fruizione del servizio di protocollo in modalità ASP è dell'utente fruitore del servizio.
Gli utenti autorizzati ad accedere al servizio di protocollo dispongono di una propria credenziale personale, costituita da una parte pubblica ed una riservata.
Ogni nuovo utente autorizzato viene registrato secondo una specifica procedura con la quale vengono annotate le informazioni relative all'utente, alla sua credenziale pubblica, la qualifica e i diritti d'accesso.
La coppia di credenziali non deve mai essere ceduta a terzi. La responsabilità delle operazioni compiute tramite una utenza è sempre del legittimo titolare, anche se compiute in sua assenza.

8.1.3.2 Postazioni di lavoro degli utenti del Servizio

Per la corretta fruizione del servizio di protocollo informatico e gestione documentale e al fine di tutelarne l'accesso è necessario che l'utente adotti almeno le seguenti buone norme di comportamento relative alla gestione del proprio posto di lavoro:

- la stazione di lavoro non deve essere lasciata incustodita, anche per brevi periodi, con la sessione attiva,
- prima di allontanarsi, anche momentaneamente, devono essere attivati i sistemi di protezione esistenti relativamente alla stazione di lavoro (ad esempio, blocco tramite Ctrl-Alt-Canc con *password* locale).

In generale deve essere adottata la politica della cosiddetta "scrivania pulita" che obbliga a non lasciare materiale riservato incustodito al di fuori dell'orario di lavoro e invita a riporre il materiale di lavoro (documenti, supporti) negli appositi armadi, secondo il livello di sicurezza, di disattivare la stazione di lavoro, di tenere chiusi i locali.

8.1.4 Comunicazioni con il gestore del servizio - *Call Center*

Le persone delle Amministrazioni autorizzate ad accedere ai servizi del *Call Center* sono gli utenti registrati al servizio, gli amministratori di AOO e i referenti del servizio presso le Amministrazioni.
Normalmente, per richieste di informazioni generiche sull'utilizzo del servizio o per la risoluzione di problemi inerenti l'impiego degli applicativi non è effettuata nessuna verifica dell'identità dell'utente che effettua la chiamata.
Nel caso in cui dovessero essere richieste informazioni di tipo riservato o sensibili dal punto di vista della sicurezza, l'operatore effettua un'operazione di *call-back* della telefonata per accertarsi dell'identità dell'interlocutore.

8.1.5 Segnalazione di malfunzionamenti o problemi di sicurezza

E' compito di tutto il personale utente vigilare sull'osservanza delle misure di sicurezza, di segnalare possibili problemi relativi alla sicurezza o all'erogazione del servizio, di porre in atto le misure ed i comportamenti previsti dalle norme al fine di raggiungere e mantenere il livello di sicurezza e di servizio prefissato, in rapporto alle proprie mansioni e capacità.
Le segnalazioni relative a carenze di sicurezza o a malfunzionamenti che possono generare problemi di sicurezza possono essere indirizzate sia al *Call Center,* sia direttamente alla gestione del centro servizi o al servizio di sicurezza.

9 REGOLE DI GESTIONE DELLA CORRISPONDENZA CONVENZIONALE IN INGRESSO E IN USCITA AL/DAL SERVIZIO POSTALE NAZIONALE

La corrispondenza in ingresso viene consegnata alla *Reception* del CNIPA, che provvede a consegnarla alla UOP.

La corrispondenza viene quotidianamente consegnata al/dal personale della UOP dell'AOO, al servizio postale pubblico.
La corrispondenza in uscita, raccolta e predisposta dalla UOP medesima, viene consegnata quotidianamente in busta chiusa al suddetto servizio postale.

Gli Uffici Utente devono far pervenire la posta in partenza all'UOP che esegue la spedizione, entro e non oltre le ore 11.00 di ogni giorno lavorativo. Eventuali situazioni di urgenza saranno valutate dal RSP, che potrà autorizzare, in via eccezionale, procedure diverse da quella standard descritta

10 ELENCO DEI DOCUMENTI ESCLUSI DALLA REGISTRAZIONE DI PROTOCOLLO

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

- gazzette ufficiali, Bollettini ufficiali della P.A;
- notiziari P.A;
- giornali, riviste, libri;
- materiali pubblicitari;
- note di ricezione di circolari ed di disposizioni;
- materiali statistici;
- atti preparatori interni;
- offerte/preventivi di terzi non richiesti;
- inviti a manifestazioni che non attivino procedimenti amministrativi;
- biglietti d'occasione (condoglianze, auguri, congratulazioni, ringraziamenti, ecc.);
- allegati, se non accompagnati da lettera di trasmissione;

11 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'AOO, un registro di protocollo riservato, non disponibile alla consultazione dei soggetti non espressamente abilitati. In questo ambito rientrano:

- 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, commi 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 e dall'art. 8 del dPR 27 giugno 1992 n. 352, nonché dalla legge n. 196/2003 (e successive modifiche ed integrazioni) e norme collegate.

12 TITOLARIO DI CLASSIFICAZIONE

01.00.00.Indirizzo, programmazione e controllo
- 01.01.00.Norme e direttive generali
  - 01.01.01.Nazionali
  - 01.01.02.Comunitarie e internazionali
- 01.02.00.Pianificazione
  - 01.02.01.Disposizioni generali
  - 01.02.02.Piano strategico
  - 01.02.03.Elaborazione del piano triennale e del piano esecutivo; relazione annuale dell'attività
  - 01.02.04.Dati e programmi degli enti
- 01.03.00.Organi di indirizzo e controllo
  - 01.03.01.Nomina, revoca, dimissioni, composizione
  - 01.03.02.Regolamento e funzionamento
  - 01.03.03.Attività e supporto all'attività
- 01.04.00.Attività di supporto e indirizzo
  - 01.04.01.Consulenza e supporto
  - 01.04.02.Gruppi di lavoro e attività congiunte
- 01.05.00.Rapporti internazionali
  - 01.05.01.Rapporti nell'ambito della Comunità europea
  - 01.05.02.Rapporti con organismi internazionali

02.00.00.Regolamentazione
- 02.01.00.Protocolli di intesa e attività congiunte
  - 02.01.01.Gruppi di lavoro, nazionale, e internazionale
  - 02.01.02.Accordi e convenzioni
- 02.02.00.Regolamentazione tecnica
  - 02.02.01.Analisi e studi nei diversi settori di applicazione
  - 02.02.02.Proposta, istruttoria e emanazione
  - 02.02.03.Interpellanze e quesiti sulla regolamentazione emanata
- 02.03.00.Consulenza normativa
  - 02.03.01.Consulenza legislativa al Presidente del Consiglio dei Ministri.
  - 02.03.02.Osservatorio legislativo e giurisprudenziale e quadro normativo di riferimento
  - 02.03.03.Consulenza giuridica, interna ed istituzionale

03.00.00.Monitoraggio, sperimentazione e verifica
- 03.01.00.Pareri e osservazioni
  - 03.01.01.Richieste generiche
  - 03.01.02.Richieste di osservazioni (di tipo consulenziali)
  - 03.01.03.Richieste specifiche, istruttoria e parere
  - 03.01.04.Attività post-parere
- 03.02.00.Stato di informatizzazione
  - 03.02.01.Relazione sullo stato di informatizzazione della P.A. (CED e sistemi)
  - 03.02.02.Iniziative e programmi delle P.A. europee (studi e analisi)
  - 03.02.03.Regioni e Enti locali
- 03.03.00.Monitoraggio
  - 03.03.01.Qualificazione Monitori
  - 03.03.02.Valutazione dei contratti
  - 03.03.03.Monitoraggio dei contratti e convenzioni di grande rilievo e diversi
  - 03.03.04.Monitoraggio dei progetti diversi (Regioni e Enti locali)
- 03.04.00.Osservatorio e pianificazione della spesa pubblica
  - 03.04.01.Osservatorio spesa amministrazioni centrali
  - 03.04.02.Osservatorio spesa amministrazioni locali
  - 03.04.03.Contratti-quadro e capitolati per convenzioni
  - 03.04.04.Qualità e certificazione dei fornitori
- 03.05.00.Osservatorio del mercato e sperimentazione

03.05.01.Studi e indagini per istruttorie e pareri
03.05.02.Evoluzione tecnologica e sperimentazione
03.05.03.Richieste delle Amministrazioni sul mercato ICT
04.00.00.Progetti, formazione, applicazioni per l'efficienza delle pubbliche amministrazioni
04.01.00.Front office
04.01.01.Disposizioni generali, normativa, regolamenti
04.01.02.Servizi ai cittadini
04.01.03.Servizi alle imprese
04.01.04.Servizi dati territoriali
04.01.05.Gestione siti
04.01.06.Digitale terrestre
04.01.07.Verifiche, consulenze e monitoraggio
04.02.00.Back office
04.02.01.Disposizioni generali, normativa, regolamenti
04.02.02.Sistemi contabili
04.02.03.Sistemi di pagamento
04.02.04.Gestione procedimenti amministrativi, flussi documentali, work-flow
04.02.05.Gestione anagrafiche e banche dati
04.02.06.Verifiche, consulenze e monitoraggio
04.03.00.Interoperabilità, cooperazione interamministrativa
04.03.01.Disposizioni generali, normativa, regolamenti
04.03.02.Cooperazione applicativa e sistemi di interscambio
04.03.03.Flussi informativi, interoperabilità e condivisione di dati
04.03.04.Recupero di prodotti e riuso
04.03.05.Verifiche, consulenze e monitoraggio
04.04.00.Soluzioni informatiche per accessibilità, sicurezza, identificazione e autenticazione
04.04.01.Disposizioni generali, normativa, regolamenti
04.04.02.Accessibilità e uso dei siti e dei programmi, approvazione e attuazione
04.04.03.Sicurezza, integrità
04.04.04.Carte (CIE, CNS, ecc.)
04.04.05.Gestione dei certificatori
04.04.06.Verifiche, consulenze e monitoraggio
04.05.00.Formazione e valorizzazione professionale
04.05.01.Disposizioni generali, normativa, regolamenti
04.05.02.Linee guida e strumenti per la formazione
04.05.03.Iniziative diverse per promuovere la formazione
04.05.04.Seminari, corsi e convegni
04.06.00.Altre azioni progettuali della PA
04.06.01.Partecipazione a progetti delle amministrazioni
04.06.02.Commissioni e gruppi di lavoro per attività tecnico/scientifiche
04.06.03.Avviamento iniziative progettuali
04.06.04.Progetti comunitarie e internazionali
04.06.05.Verifiche, consulenze e monitoraggio
05.00.00.Infrastrutture per le PA
05.01.00.Connettività e interoperabilità
05.01.01.Disposizioni generali, normativa, regolamenti
05.01.02.Reti e interconnessioni (implementazione e rafforzamento) a livello nazionale
05.01.03.Reti internazionali (accordi, progetti)
05.02.00.Condivisione e cooperazione
05.02.01.Disposizioni generali, normativa, regolamenti
05.02.02.Sistemi generali di condivisione
05.02.03.Cooperazione degli applicativi
05.02.04.Nuove soluzioni (open source, ecc.)
05.03.00.Sicurezza e certificazione
05.03.01.Disposizioni generali, normativa, regolamenti
05.03.02.Attività di certificazione

05.03.03.Gestione dei certificatori
06.00.00.Promozione e attuazione progettuale di Regioni e Enti locali
06.01.00.Linee di azioni progettuali, linee guida
06.01.01.Individuazione, proposte
06.01.02.Elaborazione e disposizioni applicative
06.02.00.Accordi-quadro, convenzioni, cooperazione
06.02.01.Proposte, attività e incontri preparatori
06.02.02.Elaborazione, revisione e modifiche, sottoscrizione
06.03.00.Consulenza, assistenza tecnica e strutture periferiche di supporto
06.03.01.Divulgazione, assistenza e consulenza per i progetti
06.03.02.Comitati istituzionali, tavoli congiunti, iniziative di collaborazione
06.03.03.Convenzioni e accordi con organismi centrali e territoriali
06.03.04.Figure professionali (individuazione, reclutamento, ecc.)
06.03.05.Diffusione, riuso, condivisione di prodotti e risorse
06.03.06.Creazione e gestione di strutture (Crc, ecc.)
06.03.07.Iniziative diverse e attività
06.04.00.Gestione progetti
06.04.01.Progetti in applicazione delle linee guida
06.04.02.Progetti specifici
06.04.03.Valutazione (presentazione, analisi e valutazione)
06.04.04.Gestione fasi progettuali (attuazioni, verifiche, relazioni, pagamenti, ecc.)
07.00.00.Organizzazione e controllo interno, rappresentanza
07.01.00.Organizzazione interna
07.01.01.Disposizioni generali, normativa, regolamenti
07.01.02.Funzioni e competenze (assegnazione, definizioni, regolamenti)
07.01.03.Istituzioni di nuove strutture centrali (richieste, atto dispositivo)
07.01.04.Strutture periferiche
07.02.00.Controllo di gestione
07.02.01.Procedure, individuazioni attività
07.02.02.Verifiche, relazioni e pareri
07.03.00.Rappresentanza e rapporti esterni
07.03.01.Inviti e partecipazione (eventi in ambito istituzionale)
07.03.02.Patrocinio, sponsorizzazione e organizzazione eventi
07.03.03.Rapporti con la stampa e la televisione
07.03.04.Rapporti con organismi diversi (su temi generali non direttamente inerenti l'attività istituzionale)
08.00.00.Gestione dei sistemi informativi e della documentazione (sistemi informativi e documentazione del Cnipa)
08.01.00.Reti e infrastrutture
08.01.01.Impianto (rafforzamento e implementazione)
08.01.02.Funzionamento e manutenzione
08.02.00.Gestione dati
08.02.01.Raccolta ed elaborazione (compreso aperture di caselle di posta)
08.02.02.Diffusione e condivisione (sito intranet e internet, aree di lavoro, ecc.)
08.03.00.Sicurezza e accesso
08.03.01.Procedure e piano
08.03.02.Utenti e autorizzazioni (chiavi, ecc.)
08.04.00.Archivio e biblioteca
08.04.01.Procedure, regolamentazioni, disposizioni (manuale, ecc.)
08.04.02.Gestione e conservazione (strumenti e attività: registri, repertori, piani, cataloghi e inventari)
08.04.03.Accesso e consultazione
08.05.00.Pubblicazioni
08.05.01.Pubblicazioni periodiche (amministrative e tecniche)
08.05.02.Distribuzione e pubblicità (richieste, spedizioni, ecc.)
09.00.00.Affari legali
09.01.00.Contenzioso giudiziale e stragiudiziale

09.01.01.Ricorsi nell'ambito dell'attività di funzionamento (fornitori, ecc.)
09.01.02.Ricorsi nell'ambito istituzionale (utenti, amministrazioni, ecc.)
09.01.03.Ricorsi del personale dell'ente
09.02.00.Consulenza al Direttore Generale e alle aree operative
09.03.00.Arbitrato e ricorsi amministrativi
10.00.00.Gestione delle risorse umane
10.01.00.Reclutamento del personale
10.01.01.Disposizioni generali
10.01.02.Procedure di concorso e selezione
10.01.03.Domande di assunzione, assegnazione, distacco (dall'esterno)
10.02.00.Organico, trattamento giuridico, disposizioni
10.02.01.Disposizioni (circolari, ecc.)
10.02.02.Pianta organica, ruoli e inquadramento
10.03.00.Stato giuridico, assunzione e cessazione
10.03.01.Assunzione e cessazione; presa servizio, licenziamento, dimissioni, trasferimento, distacchi, comandi, tempo parziale, qualifica, avanzamenti, titoli, note di merito e provvedimento disciplinare (fascicolo individuale principale)
10.03.02.Trattamento di quiescenza (fascicolo individuale: richiesta di pensionamento e istruttoria)
10.03.03.Richieste e attestazioni di servizio (fascicoli annuali o pluriennali)
10.04.00.Trattamento economico
10.04.01.Disposizioni
10.04.02.Stipendio (comprese trattenute) e competenze accessorie
10.04.03.Incentivazioni, rimborsi, gettoni di presenza
10.04.04.Trattamento fine rapporto e servizio, riscatto
10.05.00.Adempimenti fiscali, contributivi, previdenziali, assistenziali e assicurativi
10.05.01.Disposizioni
10.05.02.Pagamenti e accertamenti
10.05.03.Attestazioni
10.06.00.Attività di servizio
10.06.01.Turni, lavoro straordinario, reperibilità, missioni, presenze e assenze (ferie, ecc.)
10.06.02.Permessi (non retribuiti), congedi e aspettative (fascicoli o sottofascicoli individuali comunque collegati a quelli principali)
10.06.03.Incarichi, assegnazioni, interventi (convegni, per relazioni, ecc.); attestazioni di servizio
10.06.04.Procedimenti disciplinari e provvedimenti comprese le segnalazioni (fascicoli individuali)
10.07.00.Personale non strutturato, consulenti e collaboratori
10.07.01.Albo dei consulenti (tenuta, aggiornamento, richieste diverse)
10.07.02.Componenti degli organi collegiali (fascicoli individuali)
10.07.03.Incarichi di consulenze, collaborazioni (fascicoli individuali)
10.07.04.Stage
10.08.00.Formazione e aggiornamento (per il personale interno)
10.08.01.Disposizioni
10.08.02.Partecipazione e organizzazione
10.08.03.Inviti, attestazioni e certificazioni
10.09.00.Servizi al personale
10.09.01.Attività ricreativa e culturale
10.09.02.Finanziamenti e prestiti
10.09.03.Contributi, premi e borse di studio
10.09.04.Agevolazioni e servizi affini
10.10.00.Tutela della salute e sorveglianza sanitaria
10.10.01.Disposizioni
10.10.02.Visite mediche periodiche, legali e collegiali (richiesta, verbale di visita, esonero)

10.10.03.Idoneità per ambiente di lavoro; segnalazioni e denunce, ispezioni, verifiche (relazioni, ecc.)
10.10.04.Infortuni e causa di servizio
10.10.05.Nomina del responsabile della sicurezza, medici competenti (nomina, incarichi)
10.11.00.Relazioni sindacali
10.11.01.Rappresentanti (elezioni, nomine)
10.11.02.Concessioni spazi
10.11.03.Attività (riunioni, ecc.)
11.00.00.Gestione delle risorse finanziarie
11.01.00.Entrate (contabilizzazione e incassi)
11.01.01.Ordinarie e straordinarie
11.01.02.Prestazioni per conto terzi e servizi
11.02.00.Uscite (contabilizzazione e liquidazione delle spese, compresi solleciti)
11.02.01.Uscite per attività istituzionali
11.02.02.Uscite per attività di funzionamento
11.02.03.Beni e servizi
11.02.04.Personale
11.03.00.Gestione del bilancio preventivo e consuntivo
11.03.01.*Budget*, relazione e contabilità analitica per centri di costo e per attività/progetti
11.03.02.Preconsuntivi, consuntivi economici mensili e progressivi (rendiconti, ecc.)
11.03.03.Assestamento e modifiche
11.03.04.Relazioni e verifiche di bilancio
11.04.00.Adempimenti fiscali e contributivi
11.04.01.Rendicontazione e verifiche
11.04.02.Rapporti con enti diversi
11.05.00.Servizi di cassa, economato e tesorerie
11.05.01.Contabilità e rendiconto
11.05.02.Rapporti con banche tesoriere
12.00.00.Immobili, beni e servizi ausiliari (comprese attività contrattuali per gli acquisti)
12.01.00.Inventario dei beni
12.01.01.Tenuta e aggiornamento
12.01.02.Responsabile
12.02.00.Acquisti, dismissioni e gestione beni
12.02.01.Gare e procedure di acquisto diverse (anche in rete)
12.02.02.Acquisti in economia (fascicolo di fornitura)
12.02.03.Fornitura (gestione e rapporto con il fornitore)
12.02.04.Manutenzione
12.03.00.Gestione degli immobili
12.03.01.Nuovi immobili e spazi (richieste e offerte, indagini di mercato, valutazione, ecc.)
12.03.02.Manutenzione (ordinaria e straordinaria), messa a norma impianti e strutture
12.03.03.Sistemazione logistica e allocazione
12.03.04.Amministrazione degli immobili (assicurazione, catasto, ecc.)
12.04.00.Servizi
12.04.01.Vigilanza, sicurezza interna, pulizia
12.04.02.Autoparco e noleggio di autovetture
12.04.03.Utenze diverse e servizi postali
12.04.04.Altri servizi (centro tecnico, ecc.)

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

Al CNIPA- Centro nazionale per l'informatica nella pubblica amministrazione
Servizio Archivistico
Via Isonzo 21/b
00198 Roma

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

Richiedente _____ : Interno ☐ Esterno ☐

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: _____
_____
_____

Roma lì _____ L'operatore ricevente: _____
Il Responsabile dell'Archivio: _____

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

Di seguito viene riportato il facsimile del timbro di segnatura utilizzato dal SdP dell'AOO **CNIPADIR**